UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LES IDENTIFIANTS DÉCENTRALISÉS AU SERVICE DE LA PROTECTION DE L'IDENTITÉ NUMÉRIQUE : LE CAS D'UNE BANQUE CANADIENNE

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

MAÎTRISE EN TECHNOLOGIES DE L'INFORMATION

PAR

LUIS ALBERTO PASTOR RODRIGUEZ

JANVIER 2026

REMERCIEMENTS

Tout d'abord, je souhaite exprimer ma profonde gratitude à mon directeur de recherche Régis Barondeau pour son soutien tout au long de ce mémoire. Dès notre première rencontre dans le cours d'introduction à la technologie blockchain, j'ai vu en vous un professeur passionné par la quête intellectuelle, une passion qui a fait écho en moi. Merci Régis de m'avoir pris sous votre aile malgré vos nombreuses responsabilités, merci de m'avoir soutenu même durant votre sabbatique et surtout merci de m'avoir transmis votre passion pour la technologie blockchain.

Je souhaite également remercier tout.e.s mes professeur.e.s de l'ESG UQAM. J'aimerais accorder trois mentions spéciales. La première est pour ma professeure Claudine Bonneau qui m'a initialement fait découvrir le monde de la recherche avec le projet synthèse au baccalauréat. La deuxième pour mon professeur Martin Cloutier qui a su piquer davantage mon intérêt pour la recherche avec les cours de méthodologie. Et la dernière au chargé de cours Sahbi Boukhit qui lors d'un cours a exprimé une phrase qui résonne encore à mes oreilles aujourd'hui : « Le futur des TI c'est la blockchain ». Tous ces professeurs ont contribué à mon succès et là où j'en suis, donc je vous en suis reconnaissant.

Merci également à la banque où j'ai pu entamer mes entretiens semi-dirigés. Merci à tous les participants d'avoir accepté de prendre part à mon projet de recherche. Sans vous, ma recherche n'aurait pas la même valeur.

Merci à mes parents de penser tous les jours à moi et de m'offrir votre amour inconditionnel. Merci de toujours croire en moi et en mes rêves. Merci aussi à tous mes amis, surtout durant les dernières semaines et mois avant la fin de mon mémoire. Vous m'avez tous toujours montré votre support et vos mots m'ont permis de continuer et de rester accroché jusqu'au bout.

Finalement, le plus énorme merci revient sans aucun doute à ma fiancée Claire. Ton amour et ton soutien quotidien m'ont donné l'énergie pour ne jamais baisser les bras. Merci de m'avoir accompagné durant cette épreuve sans toi je n'y serai jamais arrivé. Alors Claire celle-là, elle est pour toi.

DÉDICACE

Me enseiñaste a caminar con dignidad,
Sigues siendo el faro que orienta mi travesía,
O simplemente la luz que me guía en la niebla.

No hay logro que no lleve su huella,
Me debo a su ser, a su amor incansable.
Sigues tú también, compañera de mi alma,
Todavía a mi lado, creyendo en mis sueños cuando yo titubeaba.

A ustedes, mis padres queridos, por darme raíces y alas.
A ti, mi amor, por caminar conmigo en las buenas y en las malas.
Este trabajo es tan mío como suyo.
Como diría la mona : Amo.

TABLE DES MATIÈRES

LISTE DES FIGURES ix

LISTE TABLEAUX xiii

LISTRE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES xiv

RÉSUMÉ xvii

ABSTRACT xviii

INTRODUCTION 1

CHAPITRE 1 PROBLÉMATIQUE, QUESTIONS ET OBJECTIFS DE LA RECHERCHE 5

CHAPITRE 2 REVUE DE LA LITTÉRATURE 17

2.1 Systèmes bancaires traditionnels 19
2.1.1 Gestion des données des clients dans les SBT 19
2.1.2 Gestion de la relation client 20
2.1.3 Gestion de l'identité et des accès des clients (GIAC) dans les SBT 22
2.1.3.1 Définition de l'identité numérique 22
2.1.3.2 Modèle d'identité centralisé 23
2.1.3.3 Modèle d'identité fédéré 25
2.1.4 Mécanismes de sécurisation des échanges de données dans les SBT 27
2.1.5 Méthodes d'authentification des clients dans les SBT 28
2.1.6 Méthodes d'autorisation des clients dans les SBT 29
2.1.7 Solutions existantes de la GIAC dans les SBT 30
2.1.7.1 Active Directory (AD) 30
2.1.7.2 Azure Active Directory (Azure AD) 31
2.1.7.3 Okta 33

2.2 Technologie blockchain (TBC) 39
2.2.1 Fondements et principes de la technologie blockchain (TBC) 40
2.2.1.1 Historique de la blockchain 43
2.2.1.2 Structure d'un bloc et chaîne de blocs 46
2.2.1.3 Notions de décentralisation et d'immutabilité 48
2.2.2 La cryptographie et la sécurité 50
2.2.2.1 Fonctions de hachage 50
2.2.2.2 Arbre de Merkle 51
2.2.2.3 Preuves cryptographiques et Zero-Knowledge Proofs (ZKP) 52
2.2.3 Mécanismes de consensus et validation des transactions 53
2.2.3.1 Preuve de travail (PoW) 54
2.2.3.2 Proof of Stake (PoS) 55
2.2.4 Dimensions systémiques, opérationnelles et applicatives de la blockchain 56
2.2.4.1 Trilemmes 56
2.2.4.1.1 Trilemme des TI 56

2.2.4.1.2 Trilemme de la blockchain 57
2.2.4.2 Typologie de blockchains : publique, privée, avec et sans permissions 58
2.2.4.3 Définition et fonctionnement des contrats intelligents 60
2.2.4.4 Finance Décentralisée (DeFi) 63
2.2.4.5 Jetons non-fongibles (NFTs), Redevances et actifs numériques 65
2.3 Systèmes bancaires décentralisés (SBD) 69
2.3.1 Gestion de l'identité et des accès des clients (GIAC) dans les SBD 69
2.3.1.1 Modèle centré sur l'utilisateur 70
2.3.1.2 Modèle décentralisé 72
2.3.2 Identité décentralisée 74
2.3.2.1 Identité auto-souveraine (IAS) 76
2.3.2.2 Identifiants décentralisés (IDD) 81
2.3.2.3 Informations d'identification vérifiables (IIV) 84
2.3.3 Solutions existantes de la GIAC dans les SBD 86
2.3.3.1 Verified.Me 87
2.3.3.2 Hyperledger 89
2.3.3.3 Sovrin 92
2.3.3.4 Polygon ID / Privado ID 94
2.3.3.5 Key Event Receipt Infrastructure (KERI) 96
2.4 Conclusion de la revue de littérature 100
CHAPITRE 3 CADRE CONCEPTUEL 102
3.1 Les affordances de Gibson (1977) 102
3.2 La GIA selon Kuperberg 103
3.3 Cadre conceptuel selon l'adaptation du modèle de Kuperberg et des affordances de Gibson 105
CHAPITRE 4 MÉTHODOLOGIE 108
4.1 Étapes et démarche de la recherche 108
4.2 Cadre d'échantillonnage et recrutement des participants 110
4.3 Présentation du profil des participants 111
4.3.1 Employés et haute direction de la banque 112
4.3.2 Experts Blockchain 114
4.4 Instrument de collecte des données 114
4.4.1 Préparation des guides d'entretien 114
4.4.2 Entretiens semi-dirigés 116
4.5 Cadre d'analyse des résultats 117
4.5.1 NVivo 15 118
4.5.2 Grille d'analyse pour codage thématique itératif 120
4.6 Perspective éthique 123
CHAPITRE 5 ANALYSE DES RÉSULTATS 124
5.1 Présentation du contexte de l'étude de cas 124

5.1.1 Interaction avec le client 125
5.1.2 Présentation des perceptions générales des employés et de la haute direction 129
5.2 Analyse des lacunes du processus actuel de gestion l'identité numérique 131
5.2.1 Problèmes de gouvernance de données 132
5.2.1.1 Tokenisation et fraude 133
5.2.1.2 Fragmentation des systèmes et processus : SAP CRM, MDM et KYC 135
5.2.2 Sécurité 143
5.2.2.1 Simplicité et efficacité au prix de la sécurité 144
5.2.2.2 Enjeux d'authentification 147
5.2.2.3 Enjeux avec l'intelligence artificielle 149
5.2.3 Réticence au changement 150
5.2.3.1 Culture organisationnelle 151
5.2.3.2 Enjeux d'expérience client et employé 152
5.2.4 Synthèse de l'analyse des lacunes du processus actuel de gestion de l'identité 153
5.3 Analyse des défis et opportunités liés à l'intégration des IDDs 156
5.3.1 Défis des IDDs – Implémentation 157
5.3.1.1 Complexité d'intégration 158
5.3.1.2 Défis techniques d'une infrastructure d'IAS 160
5.3.1.3 Mise en œuvre et interopérabilité 164
5.3.2 Défis des IDDs – Humain 166
5.3.2.1 Last Mile 167
5.3.2.2 Résistance au changement 168
5.3.3 Opportunités des IDDs – Amélioration des processus 170
5.3.3.1 Diminution des risques 171
5.3.3.2 Simplification & Portefeuille numérique 174
5.3.3.3 Autres opportunités 176
5.3.4 Opportunités des IDDs – Humain 178
5.3.4.1 Fiabilité perçue 179
5.3.4.2 Autonomisation & Remise du pouvoir aux individus 181
5.3.5 Opportunités des IDDs – Solutions 183
5.3.5.1 Solution Key Event Receipt Infrastructure 184
5.3.5.2 Solution Hyperledger & Corda 188
5.3.6 Synthèse de l'analyse des opportunités et défis de l'intégration des IDDs 191
5.4 Analyse de la vision stratégique de la haute direction 194
5.4.1 Positionnement stratégique 195
5.4.1.1 Plan de transformation numérique et alignement stratégique 195
5.4.1.2 Précurseurs ou Retardataires 199
5.4.1.3 Business Case 201
5.4.2 Pilotage interne de l'adoption technologique 204
5.4.2.1 Adoption technologique 204
5.4.2.1.1 Prise de décision 205
5.4.2.1.2 Gestion du changement et Leadership 209
5.4.2.2 Implications organisationnelles 211
5.4.3 Environnement de gouvernance stratégique 213
5.4.3.1 Concurrence 213
5.4.3.2 Gouvernance 214

5.4.3.3 Réglementaire 215
5.4.3.4 Réputation 216
5.4.4 Synthèse de l'analyse de la vision stratégique de la haute direction 217
5.5 Synthèse globale de l'analyse des résultats 220
CHAPITRE 6 DISCUSSION DES RÉSULTATS 222
6.1 Retour sur les principaux résultats 223
6.2 Confrontation des résultats avec la littérature 224
6.2.1 Confrontation des lacunes actuelles des processus avec l'état de l'art 225
6.2.1.1 Confrontation : Gouvernance de données 225
6.2.1.2 Confrontation : Sécurité 227
6.2.2 Confrontation des défis et opportunités des IDDs avec l'état de l'art 228
6.2.2.1 Confrontation : Défis des IDDs 228
6.2.2.2 Confrontation : Opportunités des IDDs 229
6.2.3 Confrontation des solutions d'identifiants décentralisés avec l'état de l'art 231
6.3 Explication des écarts et des confirmations 231
6.4 Interprétation globale et recommandations 233
6.4.1 Réponse à l'objectif #1 – Identifier les lacunes des systèmes actuels 234
6.4.2 Réponse à l'objectif #2 – Évaluer les défis et opportunités liés à l'intégration des IDDs 234
6.4.3 Réponse à l'objectif #3 – Comprendre la vision stratégique de la haute direction 235
6.4.4 Réponse à l'objectif transversal – Comparer les processus traditionnels et décentralisés 235
6.5 Recommandations 236
6.5.1 Recommandation #1 – Hyperledger Indy 237
6.5.2 Recommandation #2 – Solution KERI 239
6.5.3 Synthèse des recommandations 240
6.6 Limites de la recherche 241
6.7 Contributions de la recherche à la science 242
CHAPITRE 7 CONCLUSION 244
7.1 Résumé de la recherche et principaux résultats 244
7.2 Pistes pour les recherches futures 245
ANNEXE A LETTRE DE RECRUTEMENT 248
ANNEXE B FORMULAIRE DE CONSENTEMENT 249
ANNEXE C GUIDE D'ENTREVUE - EMPLOYÉ.E.S DE LA GIAC 254
ANNEXE D GUIDE D'ENTREVUE - EMPLOYÉ.E.S DU CRM 256
ANNEXE E GUIDE D'ENTREVUE - HAUTE DIRECTION 258
ANNEXE F GUIDE D'ENTREVUE - EXPERT.E.S BLOCKCHAIN 260

ANNEXE G COMPLÉMENTS À LA REVUE DE LITTÉRATURE 262
Stockage de données 262
Gestion des données maîtresses (MDM) 263
Interface de programmation d'application (API) & Open API 265
SAP 266
Salesforce 270
Vagues d'adoption au changement 272
Chiffrement symétrique 274
Chiffrement asymétrique 277
Chiffrement symétrique versus asymétrique 279
Tokenisation 281
Authentification monofactorielle 284
Authentification double facteur (2FA) 285
Authentification multifactorielle (MFA) 286
Protocole d'authentification dans les SBT 289
Protocole Security Assertion Markus Language (SAML) 289
Protocole Fast IDentity Online (FIDO) 290
Protocole Kerberos 292
Contrôle d'accès discrétionnaire (DAC) 293
Contrôle d'accès obligatoire (MAC) 294
Contrôle d'accès basé sur les rôles (RBAC) 294
OAuth & OAuth 2.0 295
Authentification unique (SSO) 296
OpenID 298

ANNEXE H Documents et certifications 300

BIBLIOGRAPHIE 302

LISTE DES FIGURES

Figure 1 Modules du système MDM (Haneem et al., 2017b, p. 4).....264

Figure 2 Fonctionnement des API (Molaro, 2024, p. 20).....265

Figure 3 Évolution du CRM traditionnel vers le CRM durable (Ferrer-Estévez et Chalmeta, 2023, p. 5) 21

Figure 4 Fonctions de base de SAP CRM (Yi Wu et Fengping Wu, 2011, p. 3) 267

Figure 5 Interface Fiori (SAP, 2025).....268

Figure 6 Communication des services web via PI (Cao et al., 2010, p. 458).....269

Figure 7 Modèle de service pour salesforce.com (Koli et al., 2023, p. 2).....271

Figure 8 Architecture de salesforce.com (Koli et al., 2023, p. 3).....272

Figure 9 Modèle d'identité isolé (Jøsang et Pope, 2005, p. 4) 23

Figure 10 Modèle d'identité fédéré (Jøsang et Pope, 2005, p. 4) 25

Figure 11 Diagramme du processus de chiffrement par bloc (DES) (Ratnadewi et al., 2018, p. 3).....275

Figure 12 Présentation du PAN (Stapleton et Poore, 2011, p. 92).....281

Figure 13 Architecture de base de la tokenisation (Mogull, 2010, p. 9) 282

Figure 14 Architecture des systèmes de tokenisation (Díaz-Santiago et al., 2016, p. 3).....283

Figure 15 Flux de tokenisation (Stapleton et Poore, 2011, p. 95).....284

Figure 16 Taxonomie des services cloud de sécurité (Dubey et Rai, 2021, p. 41).....28

Figure 17 Évolution des méthodes d'authentification (Ometov et al., 2018, p. 3) 29

Figure 18 Vulnérabilités dans l'authentification par mot de passe (Farik et al., 2024, p. 2).....285

Figure 19 Caractéristiques de la biométrie (Syed Idrus et al., 2013, p. 9).....287

Figure 20 Principaux défis opérationnels du MFA (Ometov et al., 2018, p. 9).....288

Figure 21 Chronologie des standards d'identification et authentification (Kiourtis et al., 2023, p. 38) ...289

Figure 22 Concepts SAML de base (Kiourtis et al., 2023, p. 38) 290

Figure 23 Architecture FIDO de haut niveau (Kim et al., 2018, p. 3).....291

Figure 24 Vue d'ensemble des actions Kerberos (El-Emam et al., 2009, p. 2) 293

Figure 25: Flux haut niveau de OAuth 2.0 (Kiourtis et al., 2023, p. 39).....296

Figure 26 Vue d'ensemble du SSO (Bazaz et Khalique, 2016, p. 18) 297

Figure 27 Flux d'autorisation OpenID à haut niveau (Kiourtis et al., 2023, p. 39).....299

Figure 28 Toutes les applications et accès sont gérés avec des réseaux et répertoires (Vries et Stjernlöf, 2023, p. 7).....33

Figure 29 Plan de ce à quoi ressemblerait l'étape 1 (Vries et Stjernlöf, 2023, p. 8).....35

Figure 30 Plan de ce à quoi ressemblerait l'étape 2 (Vries et Stjernlöf, 2023, p. 9).....36

Figure 31 Plan de ce à quoi ressemblerait l'étape 3 (Vries et Stjernlöf, 2023, p. 10).....37

Figure 32 Paramètres de l'application Okta (Vries et Stjernlöf, 2023, p. 29).....38

Figure 33 Développement technologique du secteur bancaire (Gupta et Gupta, 2018, p. 76) 40

Figure 34 Fonctionnement d'une blockchain (Crosby et al., 2016, p. 10).....41

Figure 35 Approches principales pour adresser les défis de transparence (Sedlmeir et al., 2022, p. 11)...42

Figure 36 Caractéristiques de la TBC (Florea et al., 2022, p. 2).....43

Figure 37 Chronologie des idées clés trouvés chez Bitcoin (Narayanan et Clark, 2017, p 2) 45

Figure 38 Structure d'un bloc (Zheng et al., 2017, p. 558) 47

Figure 39 Composition d'une chaîne de blocs (Nakamoto, 2008, p. 5).....48

Figure 40 La structure des données du registre dans l'horodatage lié (Narayanan et Clark, 2017, p 6) 51

Figure 41 Proof of work (Nakamoto, 2008, p. 3).....54

Figure 42 Portée des différents types de blockchain (Ahmed et al., 2022, p. 7).....59

Figure 43 Cycle de vie des contrats intelligents en 4 phases majeures (Zheng et al., 2020, p. 5).....61

Figure 44 Applications des contrats intelligents (Zheng et al., 2020, p. 13).....62

Figure 45 Taxonomie de la DeFi (Alamsyah et al., 2024, p. 11).....64

Figure 46 Structure de base d'un NFT (Parry et Ellul, 2024, p. 4).....66

Figure 47 Opportunités offertes par l'intégration des NFTs et de l'IAS (Parry et Ellul, 2024, p. 12) 67

Figure 48 Défis de l'intégration des NFTs et IAS (Parry et Ellul, 2024, p. 18) 68

Figure 49 Modèle centré sur l'utilisateur (Jøsang et Pope, 2005, p. 7).....71

Figure 50 Comparaison des modèles de gestion de l'identité (Chan et al., 2025, p.6) 72

Figure 51 Modèle décentralisé de gestion de l'identité (Chan et al., 2025, p.6) 73

Figure 52 Défis de l'identité décentralisée (Dib et Toumi, 2020, p. 33) 74

Figure 53 Trois acteurs principaux de l'IAS (Hendrickson, 2025) 77

Figure 54 Trois pilliers de l'IAS (Hendrickson, 2025) 78

Figure 55 Composantes d'un système basé sur l'IAS (Ahmed et al., 2023, p. 5) 79

Figure 56 Architecture d'un identifiant décentralisé (Chan et al., 2025, p.9) 81

Figure 57 Architecture de l'IAS (Dib et Toumi, 2020, p. 26) 83

Figure 58 Cadre d'IAS parmi les acteurs d'IIV, c-à-d les acteurs, les fournisseurs d'identité et les vérificateurs (Ahmed et al., 2022, p. 11) 85

Figure 59 Flux de travail (Dib et Toumi, 2020, p. 27) 86

Figure 60 Exemple d'un cas d'utilisation de Verified.Me (Boysen, 2021, p. 3) 88

Figure 61 Flux de travail cliniques & processus de vérification bidirectionnelle de MediLinker (Harrell et al., 2022, p. 6) 91

Figure 62 Comparaison des projets d'IAS (Chan *et al.*, 2025, p. 24) 94

Figure 63 Solution d'architecture Polygon ID 95

Figure 64 Architecture KERI (Boi et al., 2024, p. 163) 97

Figure 65 Architecture globale (Boi et al., 2024, p. 164) 98

Figure 66 Message d'évènement d'interaction de base (Smith, 2021, p. 50) 99

Figure 67 Évènement de délégation (Smith, 2021, p. 50) 99

Figure 68 Cas d'utilisation et acteur de la GIA (Kuperberg 2020, p. 2) 105

Figure 69 Cas d'utilisation adapté de Kuperberg (2020) 107

Figure 70 Liste des sous-codes Défis IDDs 119

Figure 71 Liste des codes dans NVivo 120

Figure 72 Interaction client-banque (tirée depuis les entretiens semi-dirigés) 126

Figure 73 Processus KYC à la banque Piltover à l'aide de (Parra Moyano et Ross, 2017, p. 2) 128

Figure 74 Processus de création d’un profil client dans SAP et mise à jour des informations client dans MDM (tirée depuis les entretiens semi-dirigés) 128

Figure 75 Processus simplifié d'appel à MDM (tirée depuis les entretiens semi-dirigés) 129

Figure 76 Architecture haut niveau de l’interaction entre outils (tirée depuis les entretiens semi-dirigés) 129

Figure 77 Thèmes transversaux codifiés 130

Figure 78 Trilemme des TI (C3L Security, 2019) 145

Figure 79 Graphique des vagues d'adoption lors d'un lancement de produit/service (Duchesne, 2021) 200

Figure 80 Illustration de la confrontation de la littérature avec les résultats et leur produit (création propre) 225

LISTE TABLEAUX

Tableau 1 Primitives cryptographiques offrant un service donné (ANSSI, 2020, p. 38) 280

Tableau 2 Classification de la typologie blockchain (Ahmed et al., 2022, p. 8) 58

Tableau 3 Profil des participants 112

Tableau 4 Sommaire des entretiens réalisés 117

Tableau 5 Grille d'analyse de départ 122

Tableau 6 Codifications et références des problèmes de gouvernance de données 143

Tableau 7 Codification des références de la sécurité 150

Tableau 8 Codification et références de la réticence au changement 155

Tableau 9 Synthèse des lacunes actuelles 155

Tableau 10 Codifications et références des Défis des IDDs - Implémentation 166

Tableau 11 Codifications et références des Défis des IDDs - Humain 170

Tableau 12 Codifications et références des Opportunités des IDDs - Amélioration des processus 178

Tableau 13 Codifications et références des Opportunités des IDDs - Expérience utilisateur 183

Tableau 14 Codifications et références des Opportunités des IDDs - Solutions 188

Tableau 15 Synthèse des défis et opportunités de l'intégration des IDDs 193

Tableau 16 Codification et références du positionnement stratégique 203

Tableau 17 Codification et références du pilotage interne de l'adoption technologique 212

Tableau 18 Codification et références de l'environnement de gouvernance stratégique 219

Tableau 19 Synthèse de la vision stratégique de la haute direction 219

LISTRE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

API	Interface de programmation d'application
ARC	Agence du Revenu du Canada
B2B	Banque-à-banque
B2C	Banque-à-client
BO	Banques ouvertes
CBDC	Monnaies numériques issues de Banques Centrales
CRM	Gestion de la relation client
CRS	Common Reporting Standard
DApps	Applications décentralisées
DLT	Technologie de registres distribués
DNS	Système de nom de domaine
DPKI	Gestion des clés totalement décentralisée
eGOV	Services gouvernementaux en ligne
FATCA	Foreign Account Tax Compliance
FT	Financement du terrorisme

GIA	Gestion de l’identité et des accès
GIAC	Gestion de l’identité et des accès client
IAS	Identité auto-souveraine
IDA	Identifiants autonomes
IDAC	Identifiant auto-certifiant
IDD	Identifiant décentralisé
IIV	Informations d’identification vérifiables
IoT	Internet des objets
KYC	Connaissance client
LCBA	Lutte contre le blanchiment d’argent
MDM	Gestion des données maîtresses
MFA	Authentification multifactorielle
NAS	Numéro d’assurance sociale
P&L	Profit & Loss
P2P	Pair-à-pair
PKI	Infrastructure à clé publique
PoS	Preuve d’enjeu

PoW	Preuve de travail
RAMQ	Régime d'assurance maladie du Québec
SaaS	Software as a Service
SIA	Système d'identité autonome
SSO	Single Sign-On
TBC	Technologie blockchain
TI	Technologies de l'information
UX	User Experience / Expérience client
VP	Vice-Président.e
ZKP	Zero-Knowledge Proof

RÉSUMÉ

À l'ère du numérique, la gestion de l'identité constitue un enjeu central pour les institutions financières. Les processus traditionnels de vérification client, tels que le Know-Your-Customer (KYC), s'avèrent de plus en plus coûteux, inefficaces et vulnérables face aux risques de fraude, de fuites de données et à la complexité des obligations réglementaires. Dans ce contexte, la technologie blockchain et ses composantes émergentes, soit les identifiants décentralisé (IDD), l'identité auto-souveraine (IAS) et les informations d'identification vérifiables, offrent des perspectives prometteuses pour repenser la gestion de l'identité numérique dans le secteur bancaire. Cette recherche s'inscrit dans cette dynamique d'innovation en explorant la manière dont l'intégration des IDDs pourrait transformer les pratiques actuelles de gestion de l'identité et des données clients dans une banque canadienne. Cette étude de cas approfondie vise à : 1) mettre en évidence les faiblesses du processus actuel de gestion de l'identité ; 2) analyser les opportunités et les défis liés à l'intégration des IDD ; 3) explorer la vision stratégique de la haute direction en réponse à la réingénierie des processus de gestion de l'identité. Les résultats obtenus visent à mettre en lumière les perceptions, défis et opportunités perçus par les acteurs internes et externes d'une banque canadienne, ainsi que les leviers stratégiques d'adoption potentielle des identifiants décentralisés. L'étude s'inscrit dans le cadre conceptuel proposé par Kuperberg (2020), lequel mobilise la notion d'affordance telle que formulée par Gibson (1977) dans un perspective sociotechnique, afin d'interpréter la capacité de la blockchain à soutenir une réingénierie des processus bancaires liés à la gestion de l'identité. Sous une approche qualitative interprétativiste et inductive, cette recherche s'appuie sur des entretiens semi-dirigés menés auprès d'employés et membres de la haute direction d'une banque ainsi que d'experts blockchain. Les données recueillies ont été analysées selon un codage thématique itératif pour finalement faire émerger des recommandations concrètes et contextualisées pour guider l'adoption graduelle et stratégique des identifiants décentralisés au sein du secteur bancaire canadien.

Mots-clés : *identité numérique, blockchain, identifiants décentralisés, identité auto-souveraine, informations d'identification vérifiables, KYC, banque canadienne, CRM, transformation numérique*

ABSTRACT

In the digital age, identity management has become a critical issue for financial institutions. Traditional client verification processes, such as Know-Your-Customer (KYC), are increasingly costly, inefficient and vulnerable to fraud, data breaches and the complexity of evolving regulatory requirements. In this context, blockchain technology and its emerging components, decentralized identifier (DID), self-sovereign identity (SSI) and verifiable credentials, offer promising opportunities to rethink digital identity management in the banking sector. This research contributes to this innovation dynamic by exploring how the integration of DIDs could transform current identity and customer data management practices in a Canadian bank. Under a qualitative approach and a single case study, the research aims to: 1) identify gaps in the current identity management process; 2) analyze the opportunities and challenges associated with DID integration; 3) explore the strategic vision of the bank's leadership regarding identity process reengineering. The outcomes of this research aim to highlight the perceptions, challenges and opportunities perceived by internal and external actors of a Canadian bank, as well as potential strategic drivers for DID adoption. The study is grounded in Kuperberg's (2020) conceptual framework, which is based on Gibson's (1977) sociotechnical affordances of blockchain, to interpret the capacity of these technologies to support a reengineering of banking processes related to identity management. Guided by an interpretivist and inductive paradigm, the study relies on semi-structured interviews conducted with employees and executives of a bank along with blockchain experts. The collected data were analyzed through iterative thematic coding, ultimately leading to practical and contextualized recommendations to support gradual and strategic adoption of decentralized identifiers within the Canadian banking sector.

Keywords : *digital identity, blockchain, decentralized identifiers, self-sovereign identity, verifiable credentials, KYC, Canadian bank, CRM, digital transformation*

INTRODUCTION

Dans un monde économique en pleine numérisation, les grandes banques canadiennes sont confrontées à une vague de changements et vont devoir réexaminer leurs façons de faire pour rester compétitives et sur le marché. Cette numérisation s'est rapidement accélérée avec la crise sanitaire de 2020. « Pour la majorité des secteurs économiques au Québec, la crise sanitaire a eu des répercussions humaines et financières, tant sur les activités courantes et sur l'exploitation que sur la clientèle et sur les employés. » (Grenier *et al.*, 2021, p. 1). À cet effet, la numérisation des processus, entendue comme l'intégration de technologies numériques dans les activités organisationnelles (Singhal *et al.*, 2024, p. 2), constitue une priorité pour les grandes banques canadiennes, celles-ci n'étant pas à l'abri de nouveaux évènements perturbateurs, tels que la pandémie de COVID-19 ou encore les tensions liées à la guerre tarifaire entre le Canada et les États-Unis. L'objectif d'une banque est d'offrir à ses clients un service rapide, sans erreur et de qualité (Gupta et Gupta, 2018, p. 75) et pour ce faire, la stratégie d'une banque doit permettre d'améliorer l'efficacité, l'élargissement de l'accès aux services financiers et la promotion de l'inclusion financière (Singhal *et al.*, 2024, p. 2-3). Dans ce contexte, il est judicieux de distinguer les différents types de banques. Les banques traditionnelles sont des institutions financières à but lucratif offrant une gamme complète de services aux particuliers et aux entreprises (Adams, 2023). Les banques centrales, en revanche, sont des entités publiques responsables de la politique monétaire et de la stabilité financière d'un pays (Heakal, 2023). D'autres types de banques existent, tels que les banques coopératives, mais nous allons nous concentrer sur le premier des types précédents.

L'arrivée de technologies émergentes telles que l'intelligence artificielle (IA) et la blockchain remet en question les pratiques traditionnelles et ouvre de nouvelles perspectives pour que les banques puissent interagir avec leurs clients de façon innovante. L'efficacité et la sécurité sont indispensables. La gestion des données des clients, un pilier fondamental de l'activité bancaire, est particulièrement impactée par ces changements. La cybersécurité ainsi que la protection et l'utilisation éthique des données des clients, comme les informations d'identification du client, sont devenues primordiales pour réduire la menace grandissante de cyberattaques (Rjoub *et al.*, 2023, p. 18). Le contexte postpandémique met en lumière le besoin de trouver des solutions modernes et pérennes pour relever les défis contemporains de la sécurité des données, de la transparence des transactions et de l'efficacité des processus. L'évolution rapide des technologies blockchains (TBC) est une solution envisageable qui encourage les échanges pair-à-pair (P2P) sans avoir recours à des intermédiaires centralisés en vue d'améliorer la confidentialité des transactions

et des données (Alamsyah *et al.*, 2024, p. 1). Cette approche décentralisée transforme la manière dont les informations et les actifs sont gérés en adoptant une structure plus fiable, transparente, accessible et ayant un rapport coût-efficacité plus intéressant (Alamsyah *et al.*, 2024, p. 1). Reconnaissant le potentiel des TBCs pour faire évoluer les pratiques courantes de gestion de l'identité et de l'information, la majorité des banques centrales ont engagé des recherches approfondies sur ces technologies, notamment à travers le développement de monnaies numériques de banque centrale (MNBC). Dans ce contexte, le fait que l'identité de l'utilisateur soit associée à chaque MNBC (Kayrouz, 2021, p. 3) constitue un exemple concret permettant d'envisager, plus largement, la capacité des TBCs à soutenir l'échange d'informations d'identité entre les institutions bancaires et les individus, tout en maintenant un contrôle accru de ces informations par l'utilisateur, ce qui est susceptible de renforcer la confiance des clients. Les banques traditionnelles canadiennes pourraient tirer parti de l'expertise des banques centrales en explorant davantage les applications de cette nouvelle technologie dans leurs propres systèmes. Bien que certains projets blockchain aient été initiés dans les banques canadiennes, plusieurs ont été suspendus. Il est donc opportun de réexaminer les initiatives précédemment délaissées et de s'inspirer des projets blockchain en place, comme Polygon ID chez HSBC (Polygon, 2023), afin de positionner les banques canadiennes comme des banques novatrices. La portée des TBCs s'étend bien au-delà des cryptomonnaies et des MNBC englobant des domaines tels que la gestion de l'identité numérique, la sécurité des transactions, l'amélioration de l'efficacité des systèmes et bien d'autres (Crosby *et al.*, 2016, p. 13-16).

Dans le prolongement des transformations technologiques évoquées précédemment, le processus de connaissance client ou *know-your-customer* (KYC) constitue un point d'ancrage opérationnel central de l'évolution des pratiques bancaires en matière de gestion de l'identité. Bien que certaines banques aient lancé des initiatives blockchain, la plupart des banques continuent d'utiliser des méthodes de vérification client désuètes (Mamun *et al.*, 2020, p. 1). Soumises à des réglementations gouvernementales strictes, les banques doivent s'assurer, par le biais du KYC, de l'identification, de la vérification et du suivi de leurs clients tout au long du processus d'affaires, faisant de ce processus un pilier structurant de leur activités (Mamun *et al.*, 2020, p. 1; (Malhotra *et al.*, 2022, p. 2). Ainsi, il convient de s'assurer que le modèle KYC mis en œuvre fasse évoluer le KYC traditionnel, historiquement assumé de manière isolée par chaque institution, vers une approche de KYC partagé reposant sur un réseau interbancaire. Dans ce modèle, chaque banque demeure responsable des informations KYC qu'elle produit et téléverse, tandis que la mutualisation de ces données au sein d'une infrastructure commune permet d'identifier et de diffuser plus rapidement, à l'échelle du réseau, les cas présentant un niveau de risque accru (Kulkarni et Singh,

2019, p.37). Parallèlement, plusieurs concepts issus de l'identité décentralisée, tels que les identifiants décentralisés (IDD), l'identité auto-souveraine (IAS) et les informations d'identification vérifiables (IIV) émergent comme les concepts clés les plus prometteurs pour permettre aux clients de contrôler et de gérer leurs données d'identité de manière plus sécurisée et autonome (Bharadwaj *et al.*, 2023, p. 1 & 9 ; Feulner *et al.*, 2022, p. 4 ; Sedlmeir *et al.*, 2021, p. 3). L'intégration de ces technologies dans les systèmes de gestion de la relation client (CRM) et de gestion de l'identité et des accès client (GIAC) dans les banques marquerait un tournant significatif dans la façon dont les banques interagissent avec leurs clients. Cette évolution numérique a également déclenché une transformation fondamentale dans les attentes et les comportements des clients. Ceux-ci sont à la recherche, de bénéfices associés aux technologies blockchain, avec une plus grande transparence, rapidité, automatisation et réduction de coûts dans leurs interactions avec les banques. « Les transactions bancaires traditionnelles peuvent entraîner des frais allant jusqu'à $50 USD, alors que les réseaux blockchain peuvent réduire les coûts à moins de $0.01 USD par transaction. La mise en œuvre pourrait permettre d'économiser jusqu'à 27 milliards de dollars d'ici 2030 sur les transactions internationales. » (Myronov, 2024, p. 2).

Le présent projet s'appuie sur une étude de cas menée au sein d'une seule banque canadienne, envisagée comme un point d'entrée empirique permettant d'examiner les conditions organisationnelles, les contraintes et les enjeux associés à l'intégration des TBCs dans la gestion de l'identité numérique. Bien que ces technologies ouvrent des perspectives prometteuses pour la transformation des processus existants et l'émergence de modèles de services financiers plus transparents, efficaces et centrés sur la clientèle, leur mise en œuvre soulève des défis importants en matière de conformité réglementaire, d'adaptation des infrastructures informatiques et de développement des compétences organisationnelles. Si la pleine valeur des dispositifs d'identité numérique fondés sur la blockchain repose sur une logique inter-organisationnelle impliquant un réseau de banques, cette recherche ne vise pas à analyser un tel réseau dans son ensemble, mais plutôt à comprendre, à l'échelle d'une organisation, les conditions de possibilité, les limites et les tensions que pose leur adoption. À ce titre, les enseignements issus de cette étude de cas ne prétendent pas à une généralisation directe, mais offrent des éléments de réflexion transférables quant aux bénéfices potentiels et aux défis liés à la mise en œuvre des TBCs dans la gestion de l'identité au sein du secteur bancaire canadien, notamment en ce qui concerne l'interopérabilité, la gouvernance et la protection des données (Akram et Sen, 2022 ; Parate *et al.*, 2023).

Le premier chapitre est dédié à la définition de la problématique, à la formulation de la question de recherche ainsi qu'à la présentation des objectifs. Le deuxième propose une revue de la littérature qui examine d'abord les systèmes bancaires traditionnels et leurs limites en matière de gestion de l'identité numérique, avant d'explorer les fondements techniques de la technologie blockchain et d'analyser l'émergence des systèmes bancaires décentralisés à travers les identifiants décentralisés (IDDs), l'identité auto-souveraine (IAS) et les informations d'identification vérifiables (IIVs), en mettant en lumière les solutions concrètes actuellement en développement ou en déploiement dans le secteur bancaire. Le troisième chapitre expose le cadre conceptuel qui fonde notre analyse, tandis que le quatrième chapitre décrit en détail la méthodologie de recherche, incluant le cadre d'échantillonnage, les méthodes de collecte de données et leur traitement. Le cinquième chapitre présente l'analyse des résultats issus des entretiens semi-dirigés, en structurant l'interprétation des données autour des principales thématiques identifiées et des sous-questions de recherche. Enfin, le sixième chapitre engage une discussion critique des résultats en les confrontant aux éléments du cadre théorique, en examinant leurs implications pour la transformation des pratiques de gestion de l'identité numérique dans le secteur bancaire et en ouvrant sur les recommandations pratiques découlant de cette étude.

CHAPITRE 1

PROBLÉMATIQUE, QUESTIONS ET OBJECTIFS DE LA RECHERCHE

Ce chapitre explore le potentiel de la technologie blockchain dans la gestion de l'identité numérique au sein des banques canadiennes. Nous commençons par définir la problématique principale de la recherche. La question de recherche est ici décomposée en sous-questions pour comprendre les aspects sous-jacents de l'intégration des technologies blockchain dans la gestion de l'identité numérique et de ses effets sur le secteur bancaire canadien. Enfin, les objectifs spécifiques de la recherche sont présentés.

Dans un monde hyperconnecté, les individus exposent davantage leurs informations personnelles faisant en sorte que la gestion et le contrôle de l'identité numérique prennent de plus en plus d'importance dans le quotidien (Dieye *et al.*, 2023). Plus d'un milliard de personnes dans le monde n'ont toujours aucun moyen de prouver leur identité soulignant l'urgence d'agir (Beduschi, 2019). Bien que l'identité soit passée de la forme physique à la forme numérique, les solutions existantes pour la vérification de l'identité numérique ne sont pas satisfaisantes, tant pour les utilisateurs que pour les institutions financières (Feulner *et al.*, 2022). L'évolution des réglementations financières impose aux banques des obligations strictes en matière de connaissance client (KYC) et de lutte contre le blanchiment d'argent (LCBA). Le cadre législatif canadien, régi notamment par la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (LRPCFAT), oblige les institutions financières à vérifier et conserver des informations précises sur leurs clients afin de prévenir à leurs activités illicites. Actuellement, le secteur bancaire, qui doit jongler avec la gestion de l'identité de ses clients et le respect des réglementations sectorielles et gouvernementales, est un acteur important de la gestion d'identité. Celui-ci peut agir en tant qu'émetteur d'identité et de service d'identité numérique tout en fournissant ses propres services via des processus d'identification et d'authentification[1] (Ahmed *et al.*, 2023). Par exemple, les banques canadiennes permettent à leurs clients d'utiliser leur identité numérique bancaire pour accéder aux services en ligne de l'Agence du Revenu du Canada (ARC), ce qui simplifie les processus d'identification et d'authentification pour divers services gouvernementaux. Cependant, les défis réglementaires et légaux posés par l'adoption de la blockchain, accentués par les incertitudes juridiques et les variations des exigences réglementaires à travers les différentes juridictions, compliquent cette intégration (Khanna et

[1] Certains développement conceptuels et techniques relatifs à ce thème ont été placés en annexe afin d'alléger la lecture du corps du mémoire. Le lecteur peut se référer à l'Annexe G pour un approfondissement de ces notions.

Haldar, 2023). Les systèmes d'information (SI) dans le secteur bancaire ne sont pas encore optimaux dans la gestion de l'identité des clients, car les processus traditionnels existants de connaissance client manquent de confidentialité et de sécurité (Malhotra *et al.*, 2022) et cette faiblesse est exacerbée par la charge de conformité réglementaire en constante évolution, rendant l'adhésion complexe et gourmande en ressources (Khanna et Haldar, 2023).

La relation entre la gestion de l'identité numérique et les pratiques bancaires a été étudiée de près par les chercheurs et ceux-ci ont fourni des informations précieuses sur les défis et les opportunités liés aux processus de vérification de l'identité et à la gestion des données des clients et de leur identité. Dans le même ordre d'idées, Rees (2024) affirme l'importance des mesures de vérification pour la gestion de l'identité pour tenir la fraude à distance et instaurer la confiance parmi les clients. Les régulateurs exigent parallèlement que les banques connaissent leurs clients pour LCBA et le financement du terrorisme (FT). Pour ce faire, lors d'un premier contact entre un client et une banque, le processus KYC est immédiatement lancé pour obtenir les informations de vérification, vérifier l'identité, l'historique financier et les antécédents du client (Moyano *et al.*, 2019). C'est un processus qui sert de fondation à toute interaction entre un client et une banque pour non seulement garantir la conformité réglementaire, mais assurer la pérennité de la relation (Parra Moyano et Ross, 2017). « Les banques traditionnelles se doivent d'être conformes aux lois et régulations pour prévenir la fraude et en particulier les réglementations KYC sans quoi des sanctions peuvent être appliquées. Plusieurs pays au monde ont récemment été pénalisés, et ce à la hauteur de 26 milliards USD pour non-conformité. » (Sharma *et al.*, 2023, p.21) Il est évident que le processus KYC cause des problèmes autant pour les clients que les banques. « Soit les utilisateurs doivent fournir une preuve de leur identité, soit les prestataires de services font appel à des tiers pour effectuer la vérification de leurs utilisateurs. Cela nécessite un effort disproportionné et entraîne des coûts élevés pour la vérification. » (Schäffner, 2019, p.14)

De plus, les processus traditionnels de KYC sont souvent manuels, longs et sujets à des erreurs qui au bout du compte entraîne des retards dans l'intégration des clients en plus de coûts supplémentaires opérationnels (Mamun *et al.*, 2020). Fuites d'informations, fraude, FT, criminalité et bien d'autres sont au cœur des enjeux et risques liés à une mauvaise gestion de l'identité numérique et ont remis fortement en cause les divers problèmes de sécurité de partage de données client (Samal et Pradhan, 2019). Assurer la sécurité et la confidentialité de ces données, considérant l'augmentation grandissante des risques de violations de données et de cyberattaques, est un défi majeur à considérer (Mamun *et al.*, 2020). Certes,

dans le modèle bancaire traditionnel, la confidentialité est assurée en limitant l'accès aux informations aux parties impliquées et aux intermédiaires de confiance (Nakamoto, 2008), mais cette centralisation laisse place à des vulnérabilités et inefficacités qui font augmenter les risques de failles de sécurité et de fraudes (Peters et Panayi, 2016). Bien entendu, les exigences réglementaires en matière de conformité KYC évoluent constamment, mais représentent un fardeau de conformité significatif pour les banques (Mamun *et al.*, 2020). Il est donc primordial pour les banques d'avoir un processus KYC efficace, sécuritaire et à jour. Des processus KYC défaillants exposent les banques aux risques de fraudes comme le blanchiment d'argent ou l'usurpation d'identité ce qui pourrait ternir la réputation des banques en plus d'engendrer des pénalités réglementaires (Mamun *et al.*, 2020). L'intégration de concepts blockchain dans les processus KYC, en dépit de son coût initial élevé lié entre autres à la compatibilité des systèmes existants, offre une solution durable pour sécuriser et automatiser la vérification de l'identité réduisant ainsi le risque de fraudes tout en maintenant la conformité réglementaire de manière plus efficace et transparente (Ratnawat *et al.*, 2022). Nonobstant des difficultés liées aux processus de vérification de la connaissance client, celles-ci engendrent un fort coût pour les banques privées considérant que ces processus KYC sont obsolètes et génèrent des coûts de l'ordre de $1 500 à $3 000 pour le processus KYC d'un seul client pour finalement atteindre une trentaine de millions de dollars annuellement par banque (Fenergo, 2023) pour un total de 500 millions de dollars US pour toutes les banques (Parra Moyano et Ross, 2017). La durée du processus KYC pose également un problème. Des processus KYC de longue durée affectent l'expérience client et cause une perte potentielle de confiance (Mamun *et al.*, 2020). C'est désormais une flagrante réalité de considérer que la gestion de l'identité numérique des clients est cruciale pour les banques privées afin de se conformer aux normes et standards de connaissance du client ainsi que de se protéger contre la fraude et la criminalité (Samal et Pradhan, 2019). Les institutions financières s'appuient sur des pièces d'identité physique comme la carte d'assurance maladie (RAMQ) ou les passeports afin d'identifier et valider les informations de leur clientèle (Sedlmeir *et al.*, 2021). S'appuyer sur ces pièces d'identité n'est pas suffisant pour les individus, car une fois que leurs informations sont partagées, ceux-ci n'ont souvent pas le contrôle ni la propriété directe sur la gestion de leur propre identité (Tan *et al.*, 2023). Par ailleurs, la propriété des données constitue un enjeu important, car elle implique le défi de garantir aux utilisateurs, sous consentement éclairé, le droit et le contrôle sécurisé de leurs informations personnelles (Kumar et Anand, 2020), ce qui n'est pas nécessairement le cas lorsque les clients sont introduits dans les systèmes informatiques au début de la relation client-banque ou lorsqu'ils interagissent avec diverses institutions financières. Ceci met en évidence une fragmentation problématique avec les systèmes d'identité numérique actuels qui peinent à soutenir une véritable

interopérabilité entre les organisations. La nécessité d'aborder cette question de confiance et de coopération inter-organisationnelle devient alors apparente soulignant un aspect critique de la gestion des identités numériques dans le secteur bancaire. Ce qui est préoccupant aussi c'est que les problèmes de confidentialité des données et la gestion sécurisée des informations sensibles des clients nécessitent une attention accrue afin de rencontrer le seuil acceptable de sécurité (Batubara *et al.*, 2018). Les banques doivent ainsi jongler leur entre l'impératif de respecter des réglementations strictes et la nécessité de moderniser leurs systèmes de gestion d'identité numérique, ce qui freine l'innovation et la transformation numérique du secteur.

Pour bien comprendre les identités numériques, il est important de mettre la table sur les modèles d'identités numériques existants. L'évolution de l'identité numérique s'est développée selon quatre modèles : l'identité centralisée, l'identité fédérée, l'identité centrée sur l'utilisateur et l'identité décentralisée (IDD). L'identité centralisée repose sur une autorité unique qui crée, gère et stocke les informations d'identification des utilisateurs (Alanzi et Alkhatib, 2022, p. 3). De nature centralisée, ce modèle détient un point unique de défaillance qui tend à être vulnérable aux cyberattaques, il soulève des problèmes de confidentialité en raison du contrôle complet des données des utilisateurs par l'entité centrale et il manque de portabilité, puisque les identifiants créés ne sont souvent valables que dans l'écosystème du fournisseur, et cela est applicable à toutes les identités gérées au sein de ce modèle (Keller, 2024, p.3). À l'inverse, le modèle d'identité fédérée permet à plusieurs entités de partager un système d'authentification commun tout en conservant une autonomie partielle. Ce modèle est largement utilisé par les gouvernements et les grandes entreprises où une base de données centrale contrôle les accès et l'authentification des utilisateurs. Le système de connexion unique (Single Sign-On, SSO), où les utilisateurs peuvent accéder à plusieurs services en ligne avec un seul jeu d'identifiants généralement géré par un fournisseur centralisé (ex : se connecter avec son compte Meta pour accéder à Facebook, Messenger, Instagram, etc.) (Keller, 2024, p.3), offre une grande commodité et gère à la fois les justificatifs (identifiants) utilisateur pour l'authentification et les autorisations (Chan *et al.*, 2025, p.6). Cependant, tout comme le modèle centralisée, les utilisateurs doivent toujours faire confiance au fournisseur d'identité (Chan *et al.*, 2025, p.6). « L'identité centrée sur l'utilisateur remet aux individus plus de contrôle sur les données d'identités, car ils peuvent choisir l'information qu'ils souhaitent partager avec les fournisseurs de services. Toutefois, ce modèle ne résout pas complètement les problèmes de confiance et de centralisation, surtout s'il n'y a qu'une seule entité centrale qui détient les données » (Keller, 2024, p.4). Enfin, l'identité décentralisée, contrairement aux autres modèles présentés et grâce à la technologie

blockchain, permet aux individus d'être propriétaires de leurs données (Keller, 2024, p.4) sans intermédiaire centralisé. Bien que ce modèle présente des avantages notables en matière de confidentialité et de contrôle des données, il souffre également de limitations. L'un des principaux défis de l'identité décentralisée est la complexité de gestion des clés cryptographiques. Chaque utilisateur est responsable de son identité numérique, ce qui peut être plus compliqué à comprendre pour les utilisateurs non technophiles. Au Canada, il n'existe actuellement pas de norme universelle garantissant une interopérabilité entre différentes banques. Cela complique l'intégration de ces solutions dans les services numériques bancaires existants et réduit leur efficacité à grande échelle.

Certes, les processus KYC traditionnels sont coûteux et inefficaces, mais la technologie blockchain offre des solutions prometteuses (Kathrin et Riedel, 2021). La blockchain offre un moyen de stocker les informations d'identité de manière décentralisée, sécurisée et transparente tout en offrant une résistance supérieure aux tentatives d'attaques (Mamun *et al.*, 2020) bien que des failles peuvent tout de même exister selon l'implémentation. Hyperledger, une plateforme « open-source » de technologies blockchain visant à développer des solutions d'entreprises décentralisées, a déjà fait ses preuves comme solution aux problèmes reliés au KYC. En effet, des « résultats expérimentaux ont démontré qu'un système blockchain alimenté via Hyperledger peut accélérer les transferts de validation KYC, relever les inefficacités résultant de la répétition de tâches similaires, sécuriser le partage de données, être rentable et, en fin de compte, apporter de la transparence au système KYC existant. » (Sharma *et al.*, 2023, p.21) De plus, « les vérificateurs n'ont plus besoin de collecter des informations personnelles et stocker dans des silos, ce qui élimine les coûts reliés à la collecte et au stockage de données[2] volumineuses, en plus de rendre inutile l'accès aux cybercriminels. » (Schäffner, 2019, p.39) Bien que cette technologie promette de régler de nombreux problèmes reliés à l'identité, la sécurité des transactions demeure une préoccupation majeure et urgente pour les banques. L'identité numérique doit viser à garantir l'authenticité des transactions et à protéger les données sensibles des clients. Ces données sont notamment stockées dans un système de gestion des données et affichées dans l'outil technologique de l'organisation servant à gérer la relation avec le client, soit le CRM. Ce système permet d'offrir un meilleur service, de gérer les interactions client-banque, de les analyser et d'automatiser certaines tâches, telles que le suivi des ventes et la gestion des campagnes (Wailgum, 2017). Les systèmes de gestion de la relation client utilisent les informations sensibles recueillies auprès des clients pour générer des offres et campagnes marketing (Newton *et al.*,

[2] Voir Annexe G pour plus d'informations

2023). D'après Newton et al. (2023), l'expérience client est étroitement liée au CRM et relève d'une importance significative pour de nombreux contextes dont le secteur bancaire. Pourtant, le CRM souffre de plusieurs difficultés en lien avec l'identité (Canadian Business, 2001). Dans l'univers du commerce en ligne actuel, le fait d'avoir une base de données avec les informations client n'est plus suffisant et il est rendu nécessaire de se concentrer sur des relations durables sur le long terme (Wailgum, 2017). En intégrant la blockchain dans les systèmes CRM, le secteur bancaire pourrait améliorer substantiellement la confiance et l'expérience client notamment par la création d'un réseau blockchain IDD mutualisé au sein d'un consortium de banques. Cette collaboration interbancaire permettrait une gestion unifiée et sécurisée des identités numériques qui renforcerait la confiance entre les institutions et leurs clients. Considérant également que les informations d'identification vérifiables peuvent être stockées sur la blockchain via des contrats intelligents par exemple, le CRM jouirait des bénéfices de cette technologie tout en offrant une méthode qui rend le contrôle et la propriété des données aux clients (Newton *et al.*, 2023 ; N'Goala *et al.*, 2019 ; Sedlmeir *et al.*, 2021).

L'émergence de la technologie blockchain, avec les cryptomonnaies, les jetons non-fongibles (NFT), le Web 3.0 ou autre, se manifeste de plus en plus avec ses avancées et conceptions pratiques. La blockchain peut se définir comme étant une technologie de grand livre distribué immuable qui élimine le besoin d'une entité centrale (Malhotra *et al.*, 2022) gérant le flux de données dans le but de faciliter le partage sécurisé d'informations (Wardhana *et al.*, 2020). Parmi les nouvelles avancées technologiques dans le domaine de la technologie blockchain, l'identité décentralisée (IDD), l'identité auto-souveraine (IAS) et les informations d'identifications vérifiables (IIV) sont mises de l'avant lorsqu'il s'agit de gestion d'identité numérique. Alors que les IDD permettent la création d'identifiants uniques et décentralisés, l'IAS enrichit ce concept en donnant aux utilisateurs le contrôle total sur ces identifiants. Les IIV quant à elles ajoutent une couche de protection en offrant une méthode de validation de l'identité qui protège la vie privée. En somme, les identifiants décentralisés cryptographient les informations personnelles et confidentielles d'un individu (IIV) dans un modèle de gestion de l'identité numérique décentralisée permettant d'être propriétaire de ses propres données (IAS) sur un réseau décentralisé. Contrairement à la plupart des systèmes d'identité numérique, les IDD, IAS et IIV rendent aux utilisateurs le plein contrôle de leur identité numérique (Bharadwaj *et al.*, 2023). Ces protocoles blockchain se doivent d'être fiables et forts en terme de couplage entre l'identité numérique et l'identité physique pour assurer une confiance robuste auprès des utilisateurs (Bharadwaj *et al.*, 2023). La technologie blockchain, et ses différentes applications comme les IDD, IAS et IIV, sont à portée de main et constituent une avancée potentielle dans la manière dont le

secteur bancaire gère et sécurise les identités numériques. Dit simplement, les IDD, IAS et IIV constituent une avancée en permettant respectivement aux utilisateurs de contrôler directement leurs identités numériques, de donner aux individus le pouvoir de gérer et partager leurs informations d'identité de manière autonome en protégeant leur vie privée et de fournir une méthode cryptographiée pour prouver l'identité sans divulguer plus d'informations que nécessaire en assurant un contrôle sélectif des données partagées. Ces technologies résolvent les problèmes liés à la fragmentation des données, à la duplication des identités, aux vérifications du KYC, au manque de contrôle des utilisateurs sur leurs informations et à la vulnérabilité des systèmes centralisés aux fuites de données et à la fraude. Elles surpassent en effet les systèmes actuels en offrant une approche décentralisée où les utilisateurs ont un contrôle sur leurs données personnelles et où la dépendance « aveugle » envers les institutions centrales est réduite considérablement. Dans le contexte d'un réseau blockchain interbancaire basé sur les IDD, IAS et IIV, la responsabilité de la gestion de l'identité numérique repose principalement sur les utilisateurs, car ce sont eux qui contrôlent et partagent leurs informations. Avec cette nouvelle responsabilité et sachant que les utilisateurs devront écrire eux-mêmes leurs informations sur la chaîne, il convient dès lors de s'interroger sur le « last mile », c'est-à-dire la dernière étape critique du processus de gestion de l'identité qui valide l'information au moment où elle devient utilisable. Dans le cadre de cette recherche, la question se traduit ainsi : la validation relève-t-elle de chaque banque pour ses propres clients ou nécessite-t-elle un mécanisme de consensus interbancaire afin de garantir l'intégrité des identités numériques appelées à circuler entre institutions ?

Toutefois, en dépit de ses nouveaux apports, le manque de compétences et de connaissances pour la mise en œuvre de la technologie blockchain dans les banques représente un défi de taille (Mafike et Mawela, 2022). Les organisations font face à une résistance au changement en raison de la nature perturbatrice de la blockchain, qui nécessite un changement de gouvernance dans la gestion des processus et des transactions, conduisant à une résistance au sein de la structure et des procédures internes des banques (Martino, 2019). C'est de toute évidence une technologie qui nécessite des connaissances techniques pour adresser les problèmes liés à l'évolutivité, la sécurité et l'interopérabilité entre différentes implémentations de la blockchain et les systèmes d'information existants (Mafike et Mawela, 2022). La complexité de l'intégration de la technologie blockchain avec les SI existants des banques, engendre souvent des coûts élevés et une refonte des processus (Kumar et Raghavendra, 2022). L'intégration des identifiants décentralisés dans les infrastructures bancaires existantes représente un défi complexe notamment en raison des problèmes d'interopérabilité et de scalabilité des solutions blockchain. Les

banques canadiennes utilisent actuellement des infrastructures centralisées et cloisonnées, ce qui rend difficile l'intégration d'une solution basée sur une technologie distribuée comme la blockchain et la compatibilité avec les systèmes d'information existants. L'interopérabilité entre différentes blockchains et les systèmes de gestion des identités des banques est encore un défi non résolu (Choudhari *et al.*, 2021, p. 1). La diversité des plateformes et réseaux blockchain existants, telles que Hyperledger Fabric, Ethereum et Corda, en plus des collaborateurs et parties prenantes complexifie l'adoption d'un standard unique qui pourrait être intégré de manière harmonieuse dans les systèmes bancaires en raison de leur hétérogénéité structurelle (Vasuki et Rajashree, 2023, p. 5). Par ailleurs, la nécessité d'un consensus interbancaire sur les normes et protocoles d'échange d'identité numériques est importante pour assurer une adoption généralisée. Une solution interbancaire de gestion des identités numériques devrait garantir une comptabilité avec les systèmes existants tout en respectant les réglementations strictes du secteur bancaire et financier. En outre, les problèmes de performance et de scalabilité de la blockchain peuvent limiter son adoption dans des environnements bancaires où le volume des transactions et les requêtes d'authentification doivent être traitées à grande vitesse (Vasuki et Rajashree, 2023, p. 5). Certaines solutions, comme les blockchains privées ou hybrides, sont explorées pour pallier les limites d'une blockchain publique plus lente, mais elles introduisent d'autres problématiques comme la gouvernance et la centralisation partielle. Sur le plan organisationnel, la mise en œuvre des IDD nécessite une refonte des processus internes et une formation approfondie du personnel ouvrant la porte à une résistance au changement au sein des institutions. De plus, la réglementation canadienne, notamment la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), impose des règles strictes sur la gestion et la protection des données personnelles rendant difficile la conciliation entre l'aspect immuable décentralisé de la blockchain et la conformité des réglementations (Vasuki et Rajashree, 2023, p. 5). En effet, l'impossibilité d'effacer ou de modifier les données inscrites sur un réseau blockchain poserait un problème de conformité si le droit à l'oubli européen, une disposition clé du Règlement général sur la protection des données (RGPD) (Campbell, 2023, p. 99), serait en vigueur au Canada.

Au-delà des aspects techniques et réglementaires, l'adoption des IDD et l'IAS dépend fortement de leur acceptabilité par les clients et les institutions bancaires. La résistance au changement, autant du côté des clients que des banques, constitue un frein supplémentaire à l'adoption de ces technologies (Campbell, 2023, p. 99). D'une part, les clients sont habitués aux modèles d'identification traditionnels, où une institution centrale (ex : une banque) gère leur identité. Leur donner un contrôle total sur leur identité, via un portefeuille numérique cryptographique, introduit une responsabilité nouvelle et peut être perçue

comme une contrainte considérant la pleine gestion des clés de sécurités (Satybaldy *et al.*, 2024, p. 19). D'autre part, les banques elles-mêmes peuvent être réticentes à adopter un modèle d'identité décentralisé, car il remet en question leur rôle de gardien des identités. Actuellement, l'identité d'un client est un actif stratégique pour une banque, qui lui permet de contrôler l'accès aux services financiers et de fidéliser sa clientèle. Avec une IAS, les clients pourraient facilement transférer leur identité d'une institution à une autre réduisant ainsi la fidélisation bancaire en plus d'intensifier la concurrence (Campbell, 2023, p. 99). Enfin, les risques liés aux erreurs humaines doivent être prises en compte (Sreenath *et al.*, 2024, p. 389). Si un client perd accès à son portefeuille numérique d'IDD, il peut être extrêmement difficile, voire impossible, de récupérer ses informations, ce qui crée une barrière psychologique à l'adoption et engendre le besoin d'une sorte d'une clé de sauvegarder pratique (Satybaldy *et al.*, 2024, p. 19). Ces enjeux soulignent l'importance d'une transition progressive vers un modèle d'IDD avec un accompagnement des clients et des institutions pour favoriser une adoption fluide et sécurisée.

En identifiant les perspectives des différents auteurs dans leurs recherches, il devient clair que la gestion de l'identité numérique est une question à multiples composantes qui nécessite une approche équilibrée concernant principalement les aspects procéduraux et opérationnels. La gestion de l'identité numérique est problématique et, si la tendance se maintient, mettra les institutions financières canadiennes dans une position plus qu'inconfortable par rapport à leur crédibilité auprès des clients. En ce sens, les méthodes employées pour gérer l'identité numérique des clients nécessitent une révision pressante, mais elle se doit d'être efficace et répondre aux besoins manquants actuels.

La problématique est ici formulée à l'échelle du secteur bancaire canadien afin de situer les enjeux structurels liés à la gestion de l'identité numérique. L'analyse empirique qui en découle s'appuie toutefois sur l'étude approfondie d'une seule institution bancaire, considérée comme un terrain permettant d'observer concrètement la manière dont ces enjeux généraux se manifestent dans les pratiques organisationnelles. Ce positionnement analytique vise à articuler une problématique sectorielle à une investigation située, sans viser une généralisation des résultats, mais en cherchant à éclairer les dynamiques et contraintes susceptibles d'être rencontrées dans des contextes comparables.

Ce projet de recherche est de nature qualitative. Il marie les technologies blockchain avec les problèmes inhérents à la gestion de l'identité numérique et au processus traditionnel de connaissance client dans le secteur bancaire canadien. L'étude repose sur l'analyse et la modélisation du processus actuel de gestion

de l'identité au sein d'une banque canadienne, utilisée comme cas d'étude afin d'examiner comment ces enjeux sectoriels se manifestent concrètement dans un contexte organisationnel donné. Ce processus est ensuite comparé à un modèle intégrant les apports potentiels des TBCs. La question de recherche est la suivante : Comment la gestion de l'identité numérique dans le secteur bancaire canadien peut-elle être transformée par l'intégration d'identifiants décentralisés dans son système de gestion de la relation client ?

Les sous-questions de recherche à se poser s'articulent autour de trois axes :

1. Quelles sont les lacunes du processus actuel de gestion de l'identité et des données des clients?
2. Quelles sont les défis et opportunités à long terme liés à la réingénierie des processus bancaires pour intégrer les identifiants décentralisés?
3. Quelle est la vision stratégique de la haute direction sur les identifiants décentralisés?

Les trois sous-questions sont conçues pour aider à répondre à la question principale en explorant plusieurs dimensions de la transformation potentielle de la gestion de l'identité numérique. La première sous-question permet d'établir un diagnostic du processus actuel dans la banque étudiée en identifiant les défis et les points faibles qui pourraient bénéficier d'une amélioration. Ensuite, la deuxième sous-question permet de comprendre l'impact d'une réingénierie des processus causé par l'intégration d'identifiants décentralisés. Enfin, la troisième sous-question explore la vision stratégique de la haute direction sur l'intégration des identifiants décentralisés pour aider à comprendre comment cette technologie peut être alignée avec les objectifs à long terme de la banque. En abordant ces trois angles, nous sommes en mesure de fournir une réponse plus complète à la question principale en évaluant à la fois l'état actuel, les améliorations possibles, les défis et la vision à haut niveau de l'adoption de la TBC dans la gestion de l'identité numérique.

L'objectif principal de cette recherche est d'explorer et de comprendre en profondeur comment l'intégration des identifiants décentralisés, basés sur la technologie blockchain, peut transformer la gestion de l'identité numérique dans le secteur bancaire canadien. Cette étude se base sur une approche qualitative, car elle vise à examiner la perception des acteurs clés du secteur, soit les employés, membres de la haute direction et experts en blockchain, afin d'identifier l'impact d'une réingénierie des processus existants. Pour atteindre cet objectif général, plusieurs objectifs spécifiques ont été définis en lien avec les sous-questions de recherche.

Le premier objectif est d'identifier et analyser les lacunes des systèmes actuels de gestion de l'identité et des données des clients au sein d'une banque canadienne. Cet objectif vise à comprendre les insuffisances des processus traditionnels notamment en matière de sécurité, de coûts et d'expérience utilisateur. Il s'agit d'examiner comment la banque canadienne étudiée vérifie et stocke actuellement les identités des clients, quels sont les risques associés (ex : usurpation, fraude, fuite des données, etc.) et dans quelle mesure ces problématiques influencent l'efficacité des opérations bancaires. Une attention particulière est portée aux défis liés à la centralisation des données et aux implications pour la protection de la vie privée des clients. Le deuxième objectif consiste à évaluer les défis et opportunités liés à l'intégration des IDDs dans les processus bancaires. Cet aspect de la recherche vise à explorer les implications d'une transition vers un modèle basé sur un réseau blockchain, tant du point de vue technique qu'organisationnel. Il s'agit d'examiner les contraintes liées à l'adoption des IDDs notamment en ce qui concerne l'interopérabilité avec les systèmes existants, la scalabilité, la résistance au changement et la complexité de mise en œuvre. En parallèle, l'étude analyse les bénéfices attendus sur des éléments tels que les impacts sur les processus existants et la confiance des clients. Le troisième objectif est d'explorer la vision stratégique de la haute direction sur l'intégration des identifiants décentralisés et d'évaluer comment cette technologie peut être alignée avec les priorités stratégiques de la banque. Cet objectif vise à comprendre dans quelle mesure les décideurs perçoivent les IDDs comme une solution viable à long terme et quels sont les facteurs déterminants dans leur prise de décision. L'accent sera mis sur les enjeux de gouvernance, les impacts sur l'évolution des modèles d'affaires de la banque et sur l'amélioration en continu des solutions technologiques utilisées. Cette analyse évalue si la banque étudiée considère les IDDs comme un levier d'innovation et de compétitivité ou comme une technologie encore trop immature ou risquée pour être adoptée à grande échelle. Enfin, un objectif transversal de cette recherche est de comparer les processus actuels de gestion de l'identité numérique aux processus améliorés par l'intégration des IDD. Cette comparaison permet de comprendre concrètement comment une transformation et un réingénierie des processus, appuyées par l'intégration des IDD, peuvent être envisagées dans un cadre bancaire, en mettant en évidence les points de friction ainsi que les bénéfices potentiels. En intégrant les perspectives des parties prenantes interrogées, l'analyse débouche sur des recommandations exploitables en vue d'une adoption éventuelle des IDD dans le secteur bancaire canadien.

Ainsi, en répondant à ces différents objectifs, cette recherche comprend une analyse approfondie des implications de l'identité décentralisée dans le cadre bancaire en tenant compte des dimensions

techniques, organisationnelles, humaines et stratégiques. L'aspect réglementaire est abordé, mais n'est pas analysé en profondeur en raison du cadre unique de la banque étudiée. Elle offre plutôt un éclairage sur les conditions nécessaires à une adoption réussie de cette technologie et contribue à la réflexion sur l'avenir de la gestion de l'identité numérique dans le secteur financier.

CHAPITRE 2
REVUE DE LA LITTÉRATURE

Le présent chapitre se consacre à la revue de littérature sur les thèmes centraux de ce travail de recherche, soit : la gestion de l'identité numérique, les systèmes CRM et les processus KYC, les technologies blockchain et leur application à l'identité décentralisée dans le secteur bancaire. L'objectif analytique est de décomposer et comprendre le fonctionnement actuel des processus de gestion de l'identité numérique, ainsi que d'explorer la transformation potentielle de ces processus à travers l'intégration des IDD. Cette analyse détaillée explorera les modifications requises pour l'adoption des TBCs en identifiant les avantages, les défis et les implications de cette réingénierie avec un accent particulier sur leur application aux processus GIAC et aux systèmes de CRM. En explorant les écrits scientifiques, cette revue vise à cerner les implications des IDD, IAS et IIV pour les banques canadiennes dans la gestion de l'identité numérique de leurs clients. Ce cadre théorique enrichira la compréhension des problématiques rencontrées par les banques du secteur et fournira une base solide pour analyser comment l'adoption des identifiants décentralisés pourrait transformer le paysage bancaire canadien.

Les documents recueillis sont principalement des articles scientifiques revus par les pairs, des études de cas, des articles en ligne et de la littérature grise publiées depuis 1998 jusqu'à 2025. Les recherches ont été limités aux écrits en anglais et en français traitant de l'identité numérique, de la TBC et du secteur bancaire. La recherche a été effectuée à travers plusieurs bases de données, dont ABI/INFORM Collection, Google Books, Google Scholar, IEEE Xplore, JSTOR, MDPI, ResearchGate et Scopus. Ces outils ont permis d'approfondir l'exploration bibliographique sur des notions émergentes, telles que les identifiants décentralisés, la preuve à connaissance nulle (ZKP) ou les modèles d'identité auto-souveraine, et de croiser les résultats avec ceux issus des bases de données traditionnelles. Nous avons combiné des mots-clés comme « digital identity », « blockchain », « decentralized identifiers », « self-sovereign identity », « verifiable credentials », « banking », « IAM », « ZKP », « KYC » et « CRM ». La recherche a été itérative et affinée à mesure que les premiers résultats permettaient d'identifier des courants théoriques, des auteurs clés et des cas d'usage pertinents. Près de 296 articles ont été présélectionnés dont 150 écrits ont été retenus pour une analyse plus approfondie après une évaluation initiale basée sur des critères d'inclusion et d'exclusion appliqués lors de la lecture des résumés, tels que la pertinence du sujet, la qualité de la méthodologie, le type d'ouvrage et l'alignement avec les objectifs de la recherche. Au terme du processus,

la totalité des documents ont été conservés et classés dans Zotero, incluant les sources académiques, techniques, professionnelles, afin de constituer une base de connaissance exhaustive et structurée.

Des recherches complémentaires ont également été menées à l'aide d'outils d'intelligence artificielle. En ce sens, nous reconnaissons avoir utilisé les modules Scholar GPT et Consensus, sur la plateforme ChatGPT d'Open AI afin d'identifier des sources récentes, pertinentes et parfois moins accessibles via les canaux traditionnels. De plus, nous reconnaissons également l'utilisation des modèles ChatGPT-4o et ChatGPT-4.5 pour le processus d'idéation et le soutien à la rédaction dans la revue de littérature. Les résultats des invites ont été utilisés pour nous aider dans : la structuration des idées et des thèmes abordés, la traduction de concepts clés, la simplification de sujets plus techniques, la suggestion d'amélioration, l'obtention de termes plus appropriés, la recherche de champs sémantiques, l'approfondissement des connaissances sur certains thèmes, la conformité du texte au contexte, le ciblage de passages d'articles plus pertinents, la reformulation de propos dans un style plus académique et l'affinement du texte dans un langage plus épuré. J'ai employé les requêtes du style suivant : « Trouve moi des articles qui touche le sujet X en lien avec le sujet Y ou qui explique son historique et sa provenance », « Agis en tant que chercheur de haut niveau et suggère-moi des structures pour la section X abordée dans la revue de littérature », « Que pourrais-je améliorer ici : [insertion d'un passage de mon sujet écrit] », « Quel thème me manque-t-il dans cette section ? », « Traduis le concept suivant [insertion du passage] et explique-le simplement pour que je puisse comprendre », « Champ sémantique du terme X », « Rédige un texte explicatif sur X », « Approfondi sur le sujet X », « Est-ce que ce sujet est pertinent pour mon mémoire ? », « Adapte les propos de l'auteur au contexte bancaire », « À l'aide des documents PDF ci-joint, trouve moi les passages en lien avec le sujet X », « Améliore le texte suivant pour le contextualiser dans mon cadre [insertion de mon passage] », « Fais un résumé de ce texte et identifie les passages les plus passages pertinents pour X », « Ajuste le texte suivant rendre plus étoffé », etc.

Toutefois, malgré des recherches abondantes, il existe peu de littérature qui fournisse des retours d'expérience concrets de banques qui ont intégré ces nouvelles technologies blockchain ou qui ont considéré l'intégrer dans leurs processus. Pour combler cette lacune, nous nous sommes tournés vers des sources non académiques qui documentent les projets en cours, tel que l'initiative de HSBC qui développe une solution d'identité décentralisée avec Polygon ID (Polygon, 2023). Ces sources ont été mobilisées de manière critique pour illustrer les tendances actuelles et les intentions stratégiques d'acteurs majeurs du secteur bancaire.

Ce chapitre s'organise en trois grandes sections principales. La première (2.1) présente le fonctionnement des systèmes bancaires traditionnels, en mettant l'accent sur la gestion des données clients, les outils CRM, les mécanismes d'authentification, d'autorisation et de sécurité. La deuxième section (2.2) expose les fondements techniques, cryptographiques et opérationnels de la technologie blockchain, ses applications et ses limites. Enfin, la troisième section (2.3) est consacrée aux systèmes bancaires décentralisés et à la gestion de l'identité à travers les identifiants décentralisés, le modèle d'identité auto-souveraine, les informations d'identification vérifiables et les solutions concrètes actuellement observés, en projet pilote ou déployés. L'ensemble de la revue de littérature vise à construire un socle théorique robuste pour comprendre comment les principes de l'identité décentralisée pourraient réinventer les pratiques actuelles en matière de gestion de l'identité et des accès des clients bancaires dans les institutions canadiennes.

2.1 Systèmes bancaires traditionnels

Les banques d'hier, mieux connues sous le nom de systèmes bancaires traditionnels, ont vu le jour en 1817 au Canada. Ces SBT [3] canadiens constituent l'infrastructure centrale de la gestion des opérations financières et de la relation client au sein des institutions financières. Depuis plusieurs années, ces systèmes assurent le stockage, le traitement et la sécurisation des données des clients. Toutefois, avec l'évolution des technologies et des menaces informatiques, la gestion des données et la sécurisation des échanges d'informations sont devenues des enjeux pour les banques. L'objectif de cette section est de présenter une vision d'ensemble des SBT en mettant l'accent sur les composantes nécessaires pour situer la gestion de l'identité numérique : d'abord la gestion des données clients, puis l'historique de la gestion de la relation, avant d'aborder la gestion de l'identité et des accès, les mécanismes de sécurisation des échanges et enfin les solutions technologiques mobilisées pour opérationnaliser ces fonctions.

2.1.1 Gestion des données des clients dans les SBT

La gestion des données constitue un enjeu central dans les SBT, notamment en raison des exigences réglementaires encadrant la protection des renseignements personnels. Au Canada, des cadres tels que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRDE) et la Loi 25, de même que le Règlement général sur la protection des données (RGPD) à l'échelle internationale, imposent aux institutions financières des obligations strictes quant à la collecte, au traitement et au

[3] SBT est un acronyme de systèmes bancaires traditionnels

stockage des données clients. Ces cadres normatifs structurent les choix organisationnels et technologiques des banques, qui mettent en place des politiques, des mécanismes et des systèmes visant à assurer leur conformité. Dans cette perspective, la gestion des données clients n'est pas seulement une exigence réglementaire, mais elle alimente aussi les systèmes opérationnels qui soutiennent l'interaction avec la clientèle, au premier rang desquels figurent les technologies de gestion de la relation client.

2.1.2 Gestion de la relation client[4]

À partir des années 1990, l'intérêt grandissant envers la gestion de la relation client se fait de plus en plus ressentir (Ngai, 2005, p. 1). En 1997, le marché du « customer relationship management » (CRM) s'élevait à 1.4 milliards de dollars et se serait décupler en 6 ans seulement (Lau, 2005, p. 24). « Le CRM permet aux entreprises d'obtenir une vue intégrée et unifiée de leurs clients grâce à des outils analytiques. Il leur offre également la possibilité de gérer les relations clients de manière homogène, indépendamment du canal de communication utilisé, et il optimise la performance des processus impliqués dans la gestion des interactions avec les clients » (Ferrer-Estévez et Chalmeta, 2023, p. 3). Considérant ce que le CRM réfère aux pratiques, processus et technologies utilisées tout au long du cycle de vie des clients, la technologie utilisée à l'époque n'était pas encore suffisamment sophistiquée pour offrir une expérience personnalisée auprès des clients (Alolayan et Al-Kaabi, 2020, p. 1-3). L'apparition des services bancaire mobiles a permis de rapprocher les clients aux entreprises au moyen d'applications accessibles en tout temps. Cette nouvelle entrée de flux de données a amélioré la collaboration entre les départements de vente et de marketing pour développer de nouvelles stratégies de vente basées sur des informations critiques (Alolayan et Al-Kaabi, 2020, p. 3). Les entreprises peuvent désormais offrir des services personnalisés à leurs clients(Alolayan et Al-Kaabi, 2020, p. 1-3), ce qui encourage l'adoption de technologies CRM pouvant traiter l'information ciblée au besoin du client.

[4] L'usage de l'acronyme anglophone a été employé pour faciliter le pont avec le système SAP CRM

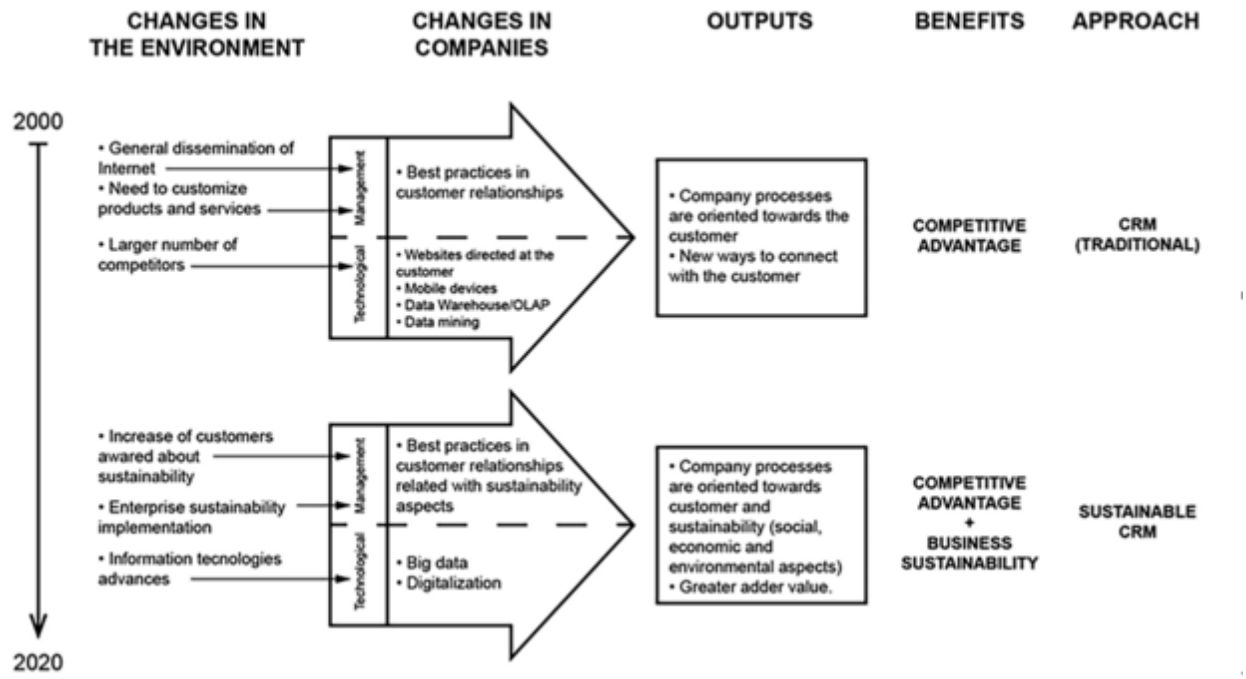


Figure 1 Évolution du CRM traditionnel vers le CRM durable (Ferrer-Estévez et Chalmeta, 2023, p. 5)

La figure illustre l'évolution du CRM entre 2000 et 2020 en réponse aux changements de l'environnement économique, technologique et social. Elle met en évidence le passage d'un CRM traditionnel à un CRM durable en intégrant des dimensions de durabilité aux pratiques de gestion des relations clients (Ferrer-Estévez et Chalmeta, 2023, p. 5). Au début des données 2000, plusieurs transformations ont influencé les entreprises, notamment la généralisation d'Internet, la nécessité de personnaliser les produits et services ainsi que l'augmentation du nombre de concurrents. Face à ces changements, les entreprises ont adopté les meilleures pratiques en matière de gestion des relations clients, en s'appuyant sur des innovations technologiques telles que les sites web dédiés aux consommateurs, l'utilisation accrue des appareils mobiles, les solutions de stockage et d'analyse des données comme les entrepôts de données. Ces initiatives ont permis aux entreprises d'orienter leurs processus vers le client, tout en développant de nouvelles façons d'interagir avec lui. Le principal bénéfice de cette approche a été l'avantage concurrentiel qui renforce la position des entreprises sur le marché en améliorant leur capacité à répondre aux attentes des consommateurs. Ce modèle correspond au CRM traditionnel centré avant tout sur l'optimisation des interactions client-entreprise via des technologies numériques. À partir de 2020, l'émergence de nouvelles tendances ont modifié les attentes des consommateurs et la manière dont les entreprises abordent la gestion de leurs relations clients pour atteindre un CRM durable qui favorise autant l'avantage

concurrentiel que la durabilité des relations d'affaires (Ferrer-Estévez et Chalmeta, 2023, p. 5). Les résultats de cette transition ont conduit à des bénéfices durables, mais il faut aussi noter que « généralement 50%-60% des projets CRM sont un échec en raison du manque de discipline des gestionnaires et un manque de définition des processus d'affaires. » (Nahar et Dhaka, 2014, p. 4). Ainsi, les solutions technologiques CRM, tels que SAP[5] et Salesforce[6], se doivent de s'appuyer sur des mécanismes d'identification, d'authentification et de gestion des droits d'accès pour encadrer l'usage des données clients et sécuriser les interactions, ce qui conduit directement à la gestion de l'identité et des accès.

2.1.3 Gestion de l'identité et des accès des clients (GIAC) dans les SBT

Dans les SBT, la gestion de l'identité et des accès structure la manière dont les clients et les employés accèdent aux services et conditionne à la fois la sécurité, la conformité et la fiabilité des interactions numériques. La littérature sur l'identité numérique aborde notamment les modèles d'identité, ainsi que les mécanismes d'authentification, d'autorisation et de sécurisation des échanges. Afin d'ancrer ces éléments dans le contexte bancaire, la section débute par une définition de l'identité numérique, puis présente les principaux modèles mobilisés dans les environnement traditionnels.

2.1.3.1 Définition de l'identité numérique

L'identité numérique est définie comme un ensemble représentatif de données sur Internet qui capture des aspects essentiels d'une personne dans diverses interactions et transactions en ligne avec des implications significatives pour l'individu et la société (Aiello *et al.*, 1998). D'après Aiello et al. (1998), il est essentiel d'avoir un moyen d'annuler une identité numérique en cas de compromission, tout comme dans le cas d'une carte de crédit volée, illustrant ainsi l'importance de disposer de systèmes de gestion d'identité performants. Dans notre société mondialement interconnectée, la gestion de l'identité numérique est fondamentale pour établir et maintenir des relations de confiance (Damiani *et al.*, 2003). En effet, considérant que l'identité numérique représente une manifestation visuelle d'une vraie identité pouvant être utilisée dans des interactions électroniques avec d'autres personnes et machines, la fraude d'identité devient un enjeu majeur pour les secteurs publics et privés soulevant, dès lors, le besoin de trouver des systèmes de gestion de l'identité efficaces (Phiri et Agbinya, 2006). « En 2023 seulement, la

[5] Voir Annexe G pour plus d'informations

[6] Voir Annexe G pour plus d'informations

Section des crimes économiques du Service de police de la Ville de Montréal a ouvert sept fois plus de dossiers, ce qui représente une hausse alarmante de 629%, de fraudes en deux ans. » (Renaud, 2024) L'identité numérique est en somme « un moyen de vérifier et d'authentifier les clients de manière sécurisée et efficace, permettant ainsi aux institutions financières de mieux gérer les risques liés à la fraude et au blanchiment d'argent » (Feher, 2021).

2.1.3.2 Modèle d'identité centralisé

Premièrement, la littérature nous explique que « ce modèle a évolué avec le temps, en passant premièrement par le modèle centralisé d'identité isolé (SILO), et est désormais le modèle le plus répandu » (Alanzi et Alkhatib, 2022, p. 3). Le modèle d'identité numérique centralisée repose sur une entité unique, généralement un fournisseur d'identité ou une institution gouvernementale, qui agit également en tant que fournisseur de services en contrôlant la gestion et la vérification des utilisateurs (Alanzi et Alkhatib, 2022, p. 3). Dans ce système, les informations d'identité sont stockées dans une base de données centralisée et sont accessibles par le fournisseur d'identité lorsqu'un utilisateur tente de se connecter à un service (Sim *et al.*, 2019, p. 31). Par exemple, un client se connecte sur son compte bancaire en ligne au moyen d'un nom d'utilisateur et d'un mot de passe pour consulter son historique de transactions sur sa carte de crédit.

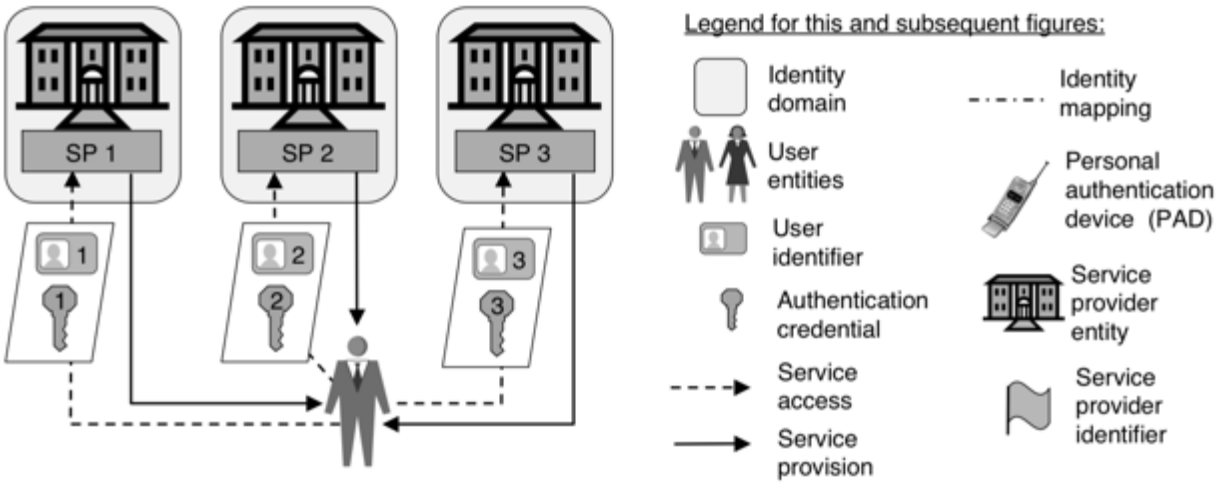


Figure 2 Modèle d'identité isolé (Jøsang et Pope, 2005, p. 4)

Cette approche est simple et adoptée à grande échelle par de nombreuses organisations publiques et privées, notamment les banques, les administrations gouvernementales et les grandes entreprises technologiques (Alanzi et Alkhatib, 2022, p. 3). L'architecture de ce modèle repose sur une combinaison de systèmes techniques et d'affaires, politiques, processus et protocoles[7] standardisés, tel que SAML (Alanzi et Alkhatib, 2022, p. 6)., qui sont utilisés pour « établir les identités, les gouverner et synchroniser la collecte, l'usage des informations d'identité et de les protéger (Bazarhanova, 2020, p. 21). L'un des principaux avantages du modèle centralisé réside dans sa facilité de mise en œuvre et son accessibilité autant pour les institutions que pour les utilisateurs. En possédant un identifiant unique géré par un fournisseur de confiance, les utilisateurs peuvent accéder à plusieurs services de ce même fournisseur. Les fournisseurs d'identité centralisés ont la capacité d'intégrer des mesures de sécurité avancées, telles que l'authentification multifactorielle et la biométrie, afin de renforcer la protection contre les accès frauduleux. Ces systèmes permettent également un contrôle rigoureux des accès et une gestion efficace des permissions ce qui est particulièrement important dans des secteurs comme le bancaire ou l'administration publique. Dans le secteur bancaire, l'identité centralisée joue un rôle clé dans la vérification de l'identité des clients notamment dans le cadre des processus KYC. Grâce à cette approche, les banques peuvent assurer un niveau de sécurité tout en facilitant l'accès aux services en ligne pour leurs clients. Par ailleurs, les autorités réglementaires imposent des exigences en matière de gestion de l'identité numérique auquel le modèle centralisé permet aux entreprises de s'y conformer plus facilement en centralisant la collecte et la gestion des données. Toutefois, ce modèle « souffre de risques potentiels qui menacent la vie privée des utilisateurs et diminuent la transparence du système en raison de sa dépendance à la centralisation dans le contrôle et la gestion des données des utilisateurs » (Alanzi et Alkhatib, 2022, p. 2).

Malgré l'émergence de nouveaux modèles d'identité numérique, le modèle centralisé demeure un standard dominant dans de nombreux secteurs en raison de sa simplicité et de sa capacité à répondre aux exigences réglementaires. Son adoption généralisée et son intégration avec des technologies avancées en font un modèle clé dans l'écosystème numérique actuel, bien qu'il soit appelé à évoluer pour s'adapter aux nouvelles attentes en matière de protection des données et de respect de la vie privée.

[7] Voir Annexe G pour plus d'informations

2.1.3.3 Modèle d'identité fédéré

Le modèle d'identité numérique fédérée a été étudié sous plusieurs aspects : la gestion de l'identité fédérée dans le cloud, ses défis et ses problèmes liés à la sécurité dans le cloud computing (Bazarhanova, 2020, p. 22). Contrairement au modèle centralisé, celui-ci repose sur un système dans lequel plusieurs fournisseurs d'identité collaborent avec des fournisseurs de services pour authentifier un utilisateur (Alanzi et Alkhatib, 2022, p. 3) sans que celui-ci ait à gérer de multiples identifiants et mots de passe. Selon Alanzi et Alkhatib (2022), « le fournisseur d'identité est la partie responsable de la création de l'identité de l'utilisateur, de l'authentification et des informations d'identification nécessaires. L'utilisateur dépend du fournisseur d'identité pour émettre des informations d'identification liées à son identité et les authentifier auprès du fournisseur de service. » Par exemple, lorsqu'un utilisateur souhaite voir son contenu Youtube, un fournisseur de service, qui lui est propre, l'individu doit rentrer son compte Google avec son mot de passe. Il en est de même avec Meta, si un utilisateur souhaite se connecter à un service comme Facebook, Messenger, Instagram ou WhatsApp, celui-ci doit se connecter au moyen de ses accréditations Meta.

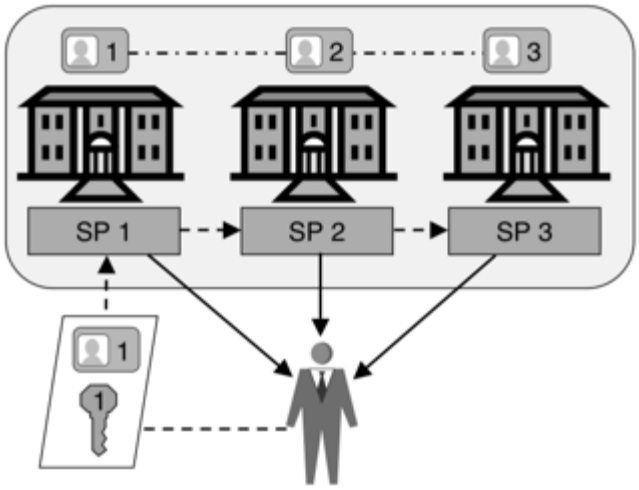


Figure 3 Modèle d'identité fédéré (Jøsang et Pope, 2005, p. 4)

Il y a ici une grande dépendance sur la confiance des utilisateurs auprès des fournisseurs. Les fournisseurs d'identité font affaire avec plusieurs fournisseurs de service dans ce modèle et les données sont répandues au travers de tous ces fournisseurs de services (Sim *et al.*, 2019, p. 31). Les différents acteurs, tels que les gouvernements, les banques ou les entreprises, doivent s'assurer d'exercer leur pouvoir en bonne et due forme au moment d'échanger les informations d'authentification avec d'autres parties prenantes.

L'architecture repose généralement sur des protocoles standardisé, tels que SAML ou OpenID[8] Connect, qui assurent l'interopérabilité, au niveau de l'échange d'informations, entre différentes plateformes et services (Sim *et al.*, 2019, p. 31) Dans le domaine de la santé, plusieurs pays, comme l'Australie, la Suède et le Canada ont mis en place des systèmes d'identification fédérés permettant aux citoyens d'accéder à leurs dossiers médicaux, via une authentification unique, souvent en s'appuyant sur des identifiants bancaires ou gouvernementaux (Ramamoorthi *et al.*, 2024, p. 5-9). Cette approche réduit la fragmentation des identités numériques, avec l'unicité de l'identité, et améliore l'interopérabilité des systèmes tout en respectant les exigences de protection des données personnelles (Ramamoorthi *et al.*, 2024, p. 2). En effet, au lieu de stocker toutes les informations d'authentification sur une seule base de données centralisée, chaque fournisseur d'identité conserve ses propres enregistrements et les partage uniquement sur demande et avec consentement explicite de l'utilisateur (Ramamoorthi *et al.*, 2024, p. 2). L'utilisateur garde le contrôle sur ses identifiants et il peut choisir quels services peuvent accéder à ses informations L'utilisateur garde le contrôle sur ses identifiants et il peut choisir quels services peuvent accéder à ses informations réduisant ainsi la collecte excessive de données (Ramamoorthi *et al.*, 2024, p. 2) réduisant ainsi la collecte excessive de données. Dans le secteur financier, le modèle fédéré est particulièrement utile pour répondre aux exigences réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Une des principales raisons pour lesquelles de nombreux gouvernements et organisations adoptent le modèle fédéré réside dans sa capacité à améliorer la protection des données personnelles. Plutôt que de multiplier les bases de données contenant des informations sensibles sur les individus, ce modèle minimise les risques de violations de données en limitant l'exposition des informations d'authentification. De plus, dans certains pays, comme l'Australie, des modèles d'adhésion basé sur le consentement implicite ont permis d'augmenter significativement le taux d'adoption des systèmes d'identité fédérés atteignant jusqu'à 90 % des utilisateurs (Ramamoorthi *et al.*, 2024, p. 2).

Le modèle d'identité fédéré offre une alternative efficace et sécurisée au modèle centralisé en permettant une meilleure gestion des identités numériques. Son adoption croissante dans des secteurs sensibles, comme la santé et la finance, démontre son efficacité à répondre aux enjeux contemporains, de cybersécurité et de protection des informations personnelles. Cependant, son implémentation nécessite

[8] Voir Annexe G pour plus d'informations

une coopération étroite entre les acteurs impliqués, une standardisation accrue des protocoles d'authentification et une sensibilisation des utilisateurs aux bénéfices de ce système.

2.1.4 Mécanismes de sécurisation des échanges de données dans les SBT

La sécurisation des échanges de données dans les SBT repose principalement sur des mécanismes de chiffrement [9], de gestion clés et d'authentification. Dans un contexte où les systèmes étaient historiquement centralisés, la protection des informations se faisait à travers des contrôles d'accès basés sur des paramètres confidentiels tels que des mots de passe, mais ces méthodes se sont rapidement révélées insuffisantes face aux nouvelles menaces liées aux réseaux informatiques comme l'interception des communications, l'introduction des messages malicieux, la retransmission des messages valides précédemment transmis et la perturbation des messages envoyés (Popek et Kline, 1979, p. 3-9). Face à ces menaces, le chiffrement est apparu comme la solution incontournable du moment pour assurer la confidentialité des échanges. Les algorithmes de chiffrement traditionnel fonctionnent sur la base d'une clé secrète partagée entre l'expéditeur et le destinataire pour assurer que seuls les détenteurs de cette clé peuvent déchiffrer les messages échangés (Popek et Kline, 1979, p. 4). Ainsi, il existe deux grands types de chiffrement ou cryptographie : symétrique et asymétrique. Ces mécanismes visent principalement la confidentialité et l'intégrité des échanges. Or, la sécurisation d'un système bancaire ne repose pas uniquement sur la protection des communications, mais elle suppose aussi de vérifier l'identité des entités qui accèdent aux services, ce qui conduit à la question de l'authentification.

[9] Voir Annexe G pour plus d'informations

2.1.5 Méthodes d'authentification des clients dans les SBT

Afin de situer l'authentification parmi les fonctions de sécurité mobilisées dans les environnements numériques (y compris lorsque des composantes infonuagiques s'ajoutent aux systèmes d'information bancaires), la figure ci-présente synthétise les services de sécurité couramment utilisées.

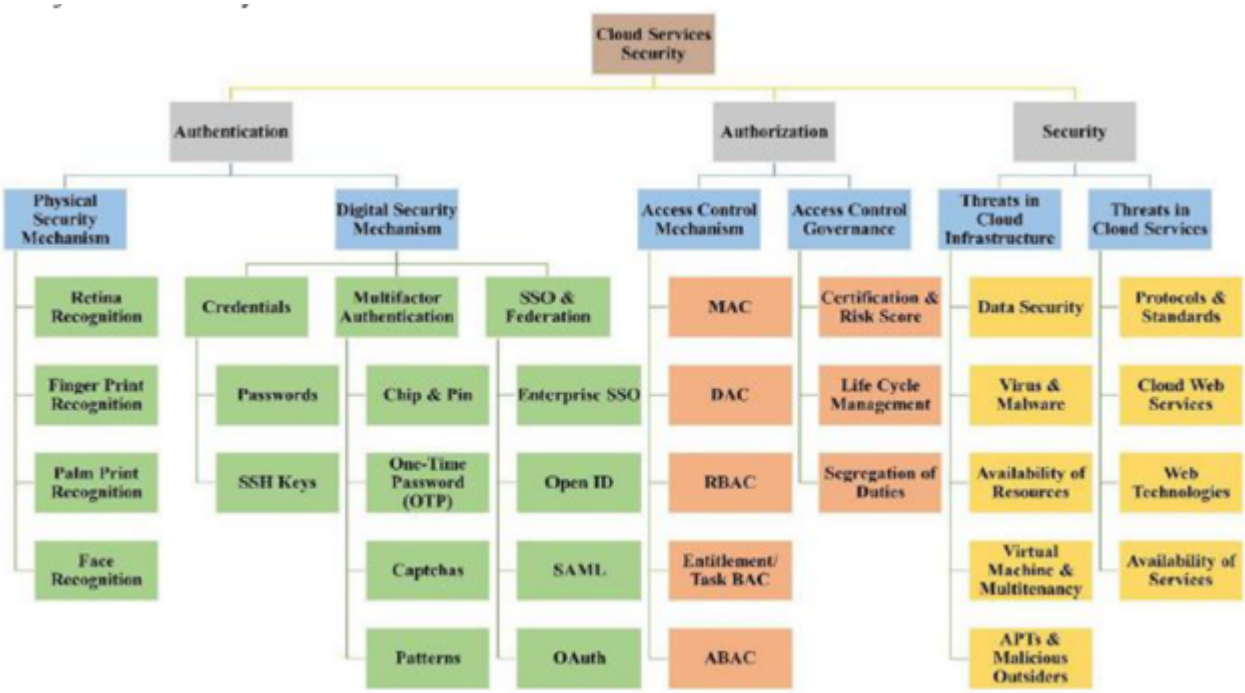


Figure 4 Taxonomie des services cloud de sécurité (Dubey et Rai, 2021, p. 41)

« Bien que les signatures numériques soient importantes, il faut se rendre compte qu'il doit toujours exister un mécanisme d'authentification garanti par lequel un individu est authentifié auprès du système […]. Ce qu'il faut c'est un moyen fiable d'identifier un utilisateur assis à un terminal, une méthode plus puissante que les systèmes de mot de passés utilisés aujourd'hui » (Popek et Kline, 1979, p. 24). Dans les SBT, l'authentification constitue la première ligne de défense contre l'accès non autorisé aux ressources critiques. Elle permet de vérifier qu'une entité, typiquement un utilisateur humain, est bien celle qu'elle prétend être, condition préalable à toute forme d'autorisation. Elle repose sur des fondements conceptuels bien établis, mais dont la mise en œuvre suscite toujours des défis techniques, humains et économiques. Il convient toutefois de distinguer les concepts connexes : l'identification (la déclaration d'identité), l'authentification (la preuve de cette identité) et l'autorisation (l'attribution des droits d'accès) (Syed Idrus *et al.*, 2013, p. 3). L'authentification se situe donc après l'identification, lorsque le système exige du demandeur qu'il démontre qu'il est effectivement le titulaire de l'identité présentée (Syed Idrus *et al.*, 2013, p. 3). Le processus d'authentification suit généralement une séquence bien définie de quatre

étapes : 1) l'état initial non authentifié, 2) la requête d'accès à un service, qui déclenche la procédure d'authentification, 3) l'état authentifié avec ouverture de session et 4) la déconnexion volontaire ou automatique, ramenant le système à son état initial. (Syed Idrus *et al.*, 2013, p. 4). Ce processus peut être gradué selon des niveaux de confiance, ce qui permet d'adapter les exigences d'authentification au type de ressource sollicitée, un mécanisme particulièrement pertinent dans un contexte bancaire où les actions sensibles (ex : virement, modification de profil, gestion des autorisations) requièrent un degré de sécurité plus élevé que la simple consultation de solde. La force d'un système d'authentification repose non seulement sur la robustesse du mécanisme sous-jacent, mais aussi sur son acceptabilité et sa facilité d'usage, sans quoi les utilisateurs sont tentés de le contourner ou d'en compromettre les principes. Cette tension constante entre sécurité, ergonomie et coût rend nécessaire une évaluation rigoureuse des différentes approches (Syed Idrus *et al.*, 2013, p. 10). Ainsi, nous aborderons les différentes méthodes d'authentification utilisées dans les SBT. Les systèmes d'autres fois et même encore aujourd'hui incluent l'authentification : monofactorielle, double facteur et l'authentification multifactorielle.

Figure 5 Évolution des méthodes d'authentification (Ometov et al., 2018, p. 3)

2.1.6 Méthodes d'autorisation des clients dans les SBT

Dans la continuité du processus d'authentification, l'autorisation constitue la deuxième brique du contrôle d'accès [10] dans les SBT. Tandis que l'authentification permet d'établir l'identification de l'usager, l'autorisation détermine si un usager, préalablement authentifié, peut accéder à une ressource ou effectuer une transaction spécifique. Elle est basée sur « des calculs de principes dont l'identité est considérée comme acquise » (Chapin *et al.*, 2008, p. 2). Dans les SBT, le processus d'autorisation repose historiquement sur des modèles d'accès relativement rigides, tels que le contrôle d'accès discrétionnaire, le contrôle d'accès obligatoire et le contrôle d'accès basé sur les rôles. Ces modèles de contrôle d'accès,

[10] Voir Annexe G pour plus d'informations

bien que fonctionnels dans des environnements cloisonnés, « s'intéresse davantage aux politiques de contrôle d'accès non triviales, comment les spécifier, leur signification et à la manière de doter les principes de confiance des informations d'identification nécessaires pour les satisfaire » (Chapin *et al.*, 2008, p. 2).

En somme, nous avons distingué l'authentification, qui établit l'identité d'un usager, et l'autorisation, qui encadre les droits qui lui sont accordés. Dans les SBT, ces deux fonctions sont mises en œuvre de manière intégrée à travers des mécanismes de contrôle d'accès et des pratiques de gouvernance qui visent à assurer la sécurité, la traçabilité et la conformité. La section suivante présente les solutions technologiques qui opérationnalisent concrètement ces principes dans les infrastructures bancaires.

2.1.7 Solutions existantes de la GIAC dans les SBT

Les sections précédentes ont décrit les mécanismes fondamentaux de l'authentification et de l'autorisation, soit le contrôle d'accès, ainsi que les protocoles et standards qui les soutiennent dans les SBT. Pour comprendre comment ces principes sont concrètement appliqués dans les banques, il convient d'examiner les solutions technologiques intégrées qui permettent de les mettre en œuvre à grande échelle. Ces solutions de gestion de l'identité et des accès incarnent des architectures matures, souvent hybrides, conçues pour répondre à la fois aux exigences de sécurité, de conformité réglementaire et d'efficacité opérationnelle. En centralisant l'authentification, la gestion des rôles et la surveillance des accès, elles constituent des piliers de l'infrastructure de sécurité dans les banques. Cette section s'intéresse à trois solutions largement déployées dans le secteur bancaire : Active Directory (AD), Azure AD et Okta.

2.1.7.1 Active Directory (AD)

Active Directory constitue l'une des solutions les plus largement adoptées dans les SBT pour la gestion centralisée des identités, des ressources et des politiques de sécurité. Développée par Microsoft et intégrée à Windows Server depuis les années 2000, AD permet aux organisations de contrôler de manière cohérente et sécurisé l'ensemble des éléments de leur infrastructure informatique : utilisateurs, groupes, terminaux, imprimantes, services applicatifs ou encore documents partagés (Binduf *et al.*, 2018, p. 1). L'architecture d'AD repose sur une structure physique composée de locations et serveurs et une structure logique hiérarchique, divisée en forêts (« continent »), arbres (« pays »), domaines (« état ») et unités organisationnelles (« ville ») (Binduf *et al.*, 2018, p. 2). Cette organisation structurelle reflète la structure fonctionnelle de l'institution bancaire, facilitant ainsi la délégation administrative et l'application

différenciée des politiques d'accès en fonction des unités ou des services (Binduf *et al.*, 2018, p. 2). Grâce aux services de domaine, les administrateurs peuvent définir des stratégies de groupe, gérer les comptes utilisateurs, attribuer des permissions et contrôler les mécanismes d'authentification à partir d'un point central (Binduf *et al.*, 2018, p. 4). Dans un environnement bancaire où la conformité, la traçabilité et la séparation des tâches sont des impératifs réglementaires, cette capacité de contrôle granulaire et centralisé constitue un bel atout. L'un des rôles les plus critiques d'AD dans le contexte bancaire réside dans son mécanisme d'authentification, assuré principalement par le protocole Kerberos (Binduf *et al.*, 2018, p. 5-6). AD prend également en charge des fonctionnalités de sécurité, telles que le chiffrement des communications via IPSec ainsi que la gestion des alertes et des audits via le Change Auditor (Binduf *et al.*, 2018, p. 5). Cependant, malgré ses nombreuses fonctionnalités, AD n'est pas exempt de vulnérabilités. Son déploiement mal maîtrisé peut exposer l'organisation à des attaques internes ou externe. Parmi les failles identifiées figurent l'usage excessif de comptes administrateurs, les configurations faibles des mots de passe de compte de service et de leurs permissions octroyées ou encore la persistance de versions obsolètes de Windows Server exposées à des attaques par exécution de code à distance ou déni de service (Binduf *et al.*, 2018, p. 3-4). De telles failles sont critiques dans un environnement bancaire, où une compromission du domaine AD pourrait entraîner un accès non autorisé à des données financières sensibles ou perturber l'ensemble des opérations numériques.

En conclusion, Active Directory s'impose comme une solution de gestion de l'identité et des accès utile pour les SBT en raison de sa capacité à centraliser la gestion des identités, à intégrer des mécanismes d'authentification et à assurer une gouvernance des accès. Son efficacité repose toutefois sur une mise en œuvre rigoureuse, une surveillance continue et une politique de sécurité proactive, sans quoi les bénéfices potentiels peuvent être gravement compromis.

2.1.7.2 Azure Active Directory (Azure AD)

Azure AD, proposé par Microsoft et intégrée à Microsoft 365, constitue une solution centralisée et extensible de gestion des identités et des accès, conçue pour répondre aux exigences complexes des infrastructures hybrides typiques du secteur bancaire (Rodriguez et Johnson, 2019, p. 1447). En tant que service infonuagique, Azure AD assure l'authentification, l'autorisation et le contrôle des identifiants utilisateurs dans des environnements aussi bien locaux que cloud (Rodriguez et Johnson, 2019, p. 1448). Contrairement à l'Active Directory traditionnel, limité aux ressources locales et fondé sur des protocoles comme Kerberos, Azure AD s'appuie sur des protocoles plus modernes comme SAML, OAuth 2.0 et OIDC,

ce qui permet une compatibilité étendue avec les applications en ligne, mobiles ou hébergés dans le cloud (Rodriguez et Johnson, 2019, p. 1448). Cela permet aux banques de gérer de manière unifiée les identités des clients, employés, sous-traitants ou partenaires, indépendamment du contexte d'accès ou du support utilisé. Les composants structurants d'Azure AD, soit les tenants (l'organisation), utilisateurs (entités principales), groupes (gère les permissions) et rôles (actions autorisées), offrent une granularité de contrôle pour moduler les droits d'accès selon les fonctions, départements ou localisations des utilisateurs (Rodriguez et Johnson, 2019, p. 1449). En combinant ces composantes avec le RBAC, les institutions financières peuvent appliquer de manière cohérente le principe du moindre privilège, en attribuant uniquement les droits nécessaires à l'exécution des tâches. Azure AD propose aussi de gérer les identités numériques avec un seul jeu d'identifiants en appliquant des mécanismes d'authentification tels que le SSO[11] et le MFA (Rodriguez et Johnson, 2019, p. 1448).

L'un des atouts majeurs d'Azure AD réside dans sa capacité à intégrer des environnements hybrides, notamment via l'outil Azure AD Connect, qui permet de synchroniser les identités entre l'AD local et l'annuaire Azure (Rodriguez et Johnson, 2019, p. 1449). Cette interconnexion assure une continuité d'accès aux ressources, qu'elles soient locales ou cloud, avec une authentification homogène, ce qui est pertinent dans les banques qui conserve encore des systèmes hérités tout en migrant progressivement vers des solutions logicielles de service. La sécurité est également renforcée grâce à des politiques d'accès conditionnelles, qui modulent l'accès selon des critères dynamiques tels que la localisation, le type d'appareil, le niveau de risque ou le comportement de l'utilisateur (Rodriguez et Johnson, 2019, p. 1450). En matière de gouvernance, la gestion de l'identité privilégiée et l'accès juste à temps permettent de gérer les identités de manière contrôlée et temporaire, limitant l'exposition des rôles sensibles à des périodes précises et à des utilisateurs dûment autorisés (Rodriguez et Johnson, 2019, p. 1451).

Enfin, grâce à ses fonctionnalités d'intégration à l'aide d'APIs avec les applications tierces via OAuth ou OIDC, Azure AD permet aux banques de centraliser la gouvernance des accès à des écosystèmes applicatifs plus complexes, y compris les plateformes entreprise-à-entreprise et entreprise-à-client (Rodriguez et Johnson, 2019, p. 1454). Cette capacité à gérer les identités externes et internes dans un cadre unifié en fait un levier stratégique de modernisation de l'infrastructure identitaire bancaire.

[11] Voir Annexe G pour plus d'informations

2.1.7.3 Okta

Okta, fondé par Todd McKinnon et Frederic Kerrest, deux anciens employés de Salesforce, en 2008, s'est imposé comme une solution infonuagique de gestion de l'identité et des accès qui a rapidement gravi les échelons dans le marché (Vries et Stjernlöf, 2023, p. 3-4). Le concept de Zero Trust, tel qu'intégré par Okta, repose sur l'idée que ni les utilisateurs ni les dispositifs, internes ou externes à l'organisation, ne doivent être considérés comme digne de confiance par défaut (Vries et Stjernlöf, 2023, p. 6). Chaque accès doit être contrôlé, surveillé et limité selon le principe du moindre privilège, ce qui signifie accorder uniquement les permissions nécessaires, au moment opportun, pour exécuter une tâche précise comme accéder à un certain document de l'organisation (Vries et Stjernlöf, 2023, p. 6). Ainsi, Okta encapsule les concepts de GIAC et de Zero Trust pour se développer en quatre étapes de maturité qui traduisent la transformation progressive des pratiques des identités et des accès au sein des organisations : 0) la fragmentation de l'identité, 1) la GIA unifiée,2) l'accès contextuel, 3) l'effectif adaptif (Vries et Stjernlöf, 2023, p. 6-10).

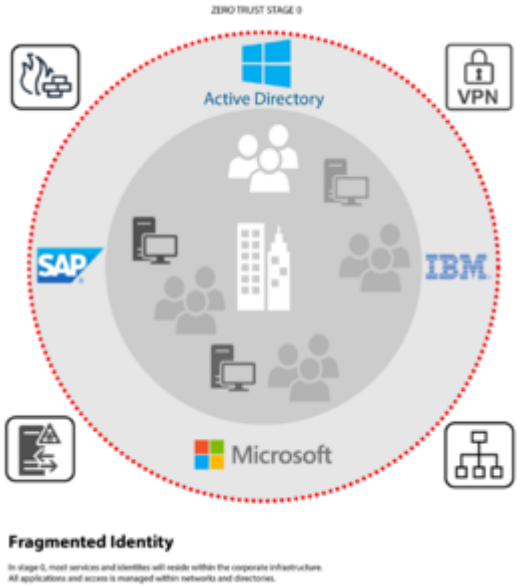
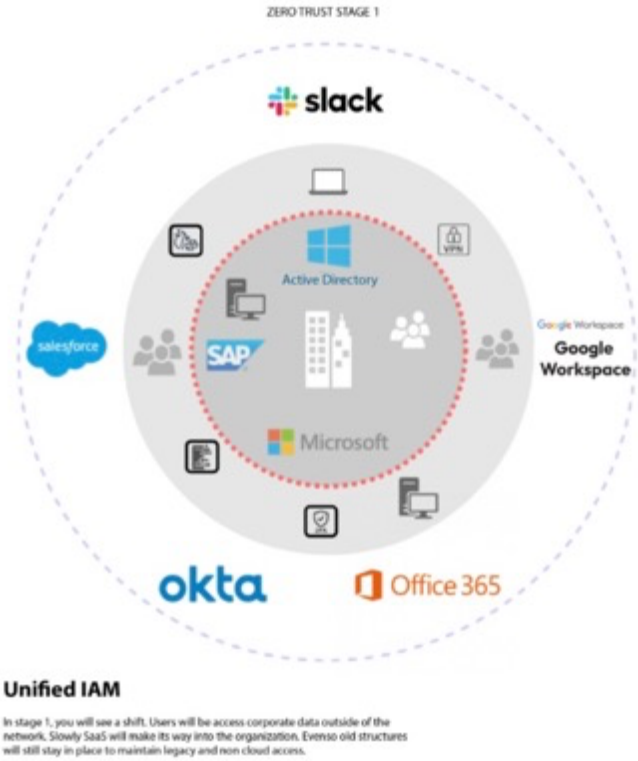


Figure 6 Toutes les applications et accès sont gérés avec des réseaux et répertoires (Vries et Stjernlöf, 2023, p. 7)

La première étape, dite identité fragmentée, correspond à une situation typique des infrastructures bancaires traditionnelles, où les applications et systèmes sont cloisonnés derrière un pare-feu d'entreprise (Vries et Stjernlöf, 2023, p. 7). L'authentification y est centralisée via des systèmes comme Active Directory, mais chaque application ou service, tel que SAP, impose des connexions distinctes (Vries et Stjernlöf, 2023, p. 7). Les utilisateurs doivent gérer plusieurs identifiants et la sécurité repose essentiellement sur des

barrières périmetriques classiques comme les VPN ou les pare-feu (Vries et Stjernlöf, 2023, p. 7). À ce stade, les identités ne sont ni unifiées ni contextualisées, rendant difficile le contrôle d'accès dynamique et granulaire.

La deuxième étape, la gestion unifiée des identités, introduit une première consolidation grâce au SSO et à la mise en œuvre d'un MFA et l'unification des identités au sein d'un répertoire global permet de simplifier la gestion des accès (Vries et Stjernlöf, 2023, p. 8). Ici, l'organisation commence à adopter des services SaaS[12], tout en maintenant des systèmes hérités sur site (Vries et Stjernlöf, 2023, p. 8). Okta agit alors comme un pont entre ces deux mondes, facilitant la gouvernance des identités et l'application des politiques de sécurité transversales. L'utilisateur peut désormais s'autehtifier une seule fois avec le SSO et accéder à une multitude de services internes et externes de façon fluide (Vries et Stjernlöf, 2023, p. 8).



[12] SaaS est un acronyme pour Software as a Service

Figure 7 Plan de ce à quoi ressemblerait l'étape 1 (Vries et Stjernlöf, 2023, p. 8)

La troisième étape, l'accès contextuel, pousse plus loin la logique Zero Trust en intégrant des paramètres dynamiques dans les décisions d'accès. (Vries et Stjernlöf, 2023, p. 9). L'accès aux ressources est conditionné par des éléments tels que le lieu, l'appareil, l'heure ou encore le comportement utilisateur (Vries et Stjernlöf, 2023, p. 9). Cette granularité permet d'appliquer des politiques d'accès spécifiques à chaque situation (Vries et Stjernlöf, 2023, p. 9). L'automatisation commence à jouer un rôle central dans la détection des anomalies et l'application des règles et les API[13] deviennent des vecteurs critiques de contrôle des accès inter-systèmes (Vries et Stjernlöf, 2023, p. 9). L'organisation peut ainsi évaluer le niveau de risque associé à chaque tentative de connexion et adapter les exigences d'authentification en conséquence (Vries et Stjernlöf, 2023, p. 9).

Enfin, la quatrième étape, l'effectif adaptif, représente le stade le plus avancé du modèle. L'organisation dispose alors d'une architecture GIA entièrement automatisée, intégrant des applications tierces comme le « Mobile Device Management », les « Cloud Access Security Brokers » ou les systèmes de gestion des événements de sécurité (Vries et Stjernlöf, 2023, p. 10). Les politiques sont enrichies de mécanismes d'authentification dynamiques, sans mot de passe, qui s'ajustent en fonction du risque évalué en temps réel (Vries et Stjernlöf, 2023, p. 10). L'utilisateur est invité à prouver son identité par des moyens variés selon les circonstances et l'accès est contrôlé en permanence selon le principe du moindre privilège, renforcé par une consolidation des journaux et une gouvernance unifiée (Vries et Stjernlöf, 2023, p. 10).

[13] Voir Annexe G pour plus d'informations

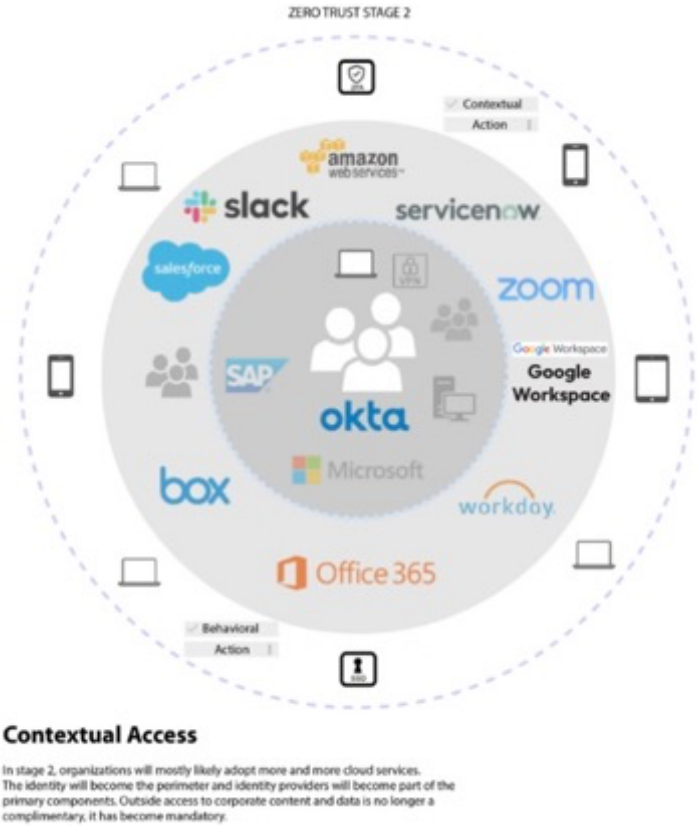


Figure 8 Plan de ce à quoi ressemblerait l'étape 2 (Vries et Stjernlöf, 2023, p. 9)

Figure 9 Plan de ce à quoi ressemblerait l'étape 3 (Vries et Stjernlöf, 2023, p. 10)

En intégrant Okta, les banques peuvent bénéficier d'une visibilité accrue sur les accès et les activités des utilisateurs. Il est possible au travers d'Okta, et son intégration avec AD, d'importer des utilisateurs depuis une application comme Google ou SAP vers Okta afin de pouvoir associer les utilisateurs à des utilisateurs existants dans Okta (Vries et Stjernlöf, 2023, p. 29). Ainsi, Okta permet également l'usage de groupe d'utilisateurs, soit les groupes Okta (méthode de regroupement standard), les groupes répertoires (attachés aux groupes Okta) et les groupes applications (assignées aux utilisateurs) (Vries et Stjernlöf, 2023, p. 32).

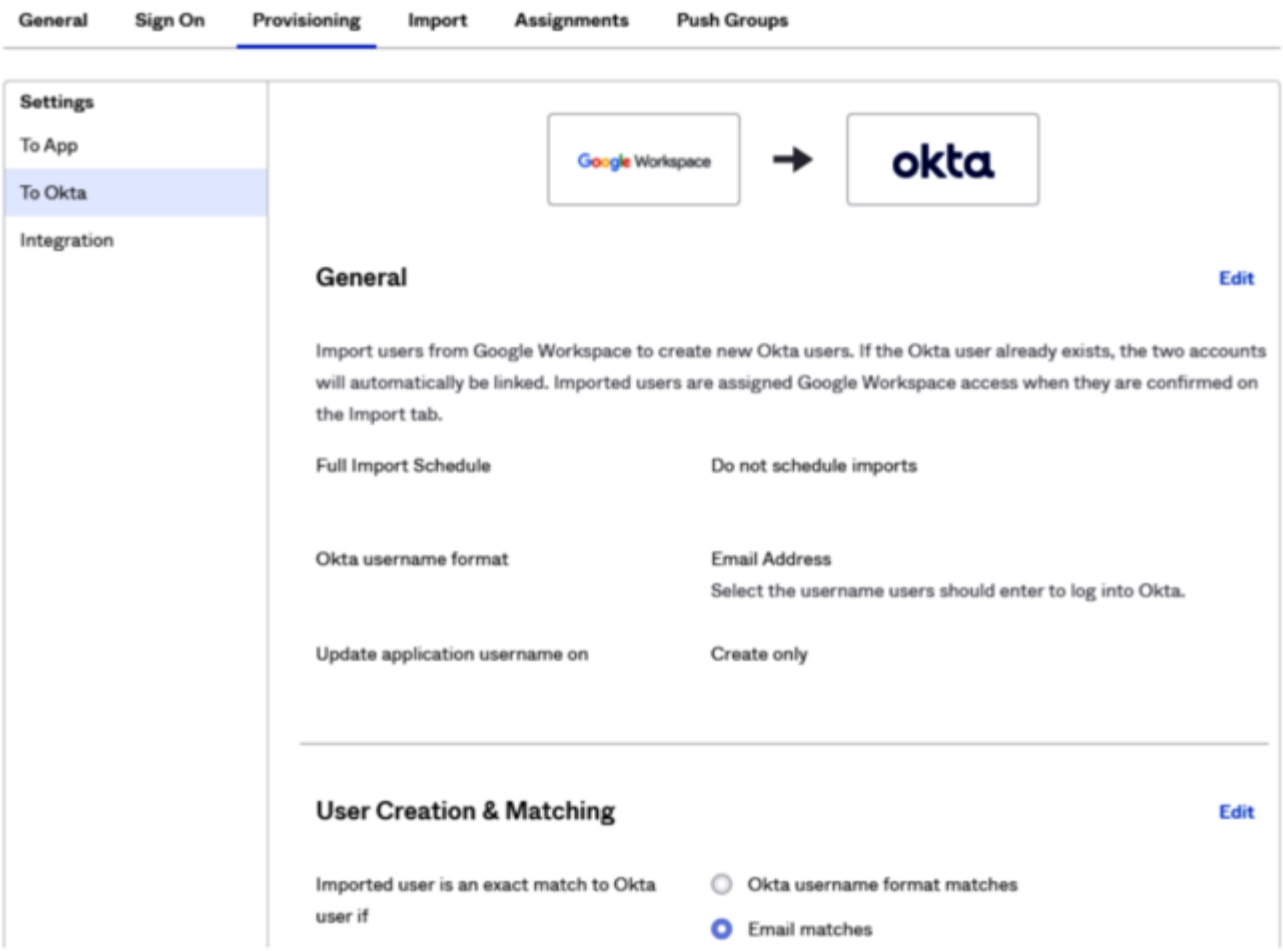


Figure 10 Paramètres de l'application Okta (Vries et Stjernlöf, 2023, p. 29)

2.2 Technologie blockchain (TBC)

Après avoir exploré les systèmes bancaires traditionnels, nous nous tournons maintenant vers le futur, soit les systèmes bancaires décentralisés. Afin de comprendre les systèmes bancaires propulsés par la blockchain, nous allons tout d'abord nous pencher sur la technologie blockchain en soit qui est le vecteur derrière le concept de décentralisation. La blockchain, souvent décrite comme une technologie disruptive, s'érige comme étant le pilier de l'avenir de l'écosystème numérique contemporain. Depuis la publication du livre blanc de Satoshi Nakamoto en 2008, cette technologie s'est rapidement imposée comme un mécanisme innovant de gestion de données distribuées, sécurisées et infalsifiables. Initialement associée aux cryptomonnaies, notamment le Bitcoin, son champ d'application s'est progressivement élargi pour englober une multitude de domaines, tels que la finance décentralisée (DeFi), les jetons non-fongibles (NFTs), et plus récemment, la gestion de l'identité numérique. La TBC et ses nombreuses applications potentielles ne sont pas une solution universelle et présentent des limites qu'il convient de considérer. Elle propose diverses applications technologiques susceptibles de répondre à certaines problématiques spécifiques, mais son efficacité et son applicabilité doivent être évaluées avec prudence et contextualisées selon les besoins et contraintes existants.

C'est pourquoi la section ici présente vise à explorer les fondements techniques, cryptographiques et structurels de la blockchain, nécessaires à la compréhension de ses implications et de ses cas d'usages avancés. Elle débute par une présentation de l'historique et des principes de base de la technologie, en mettant en lumière la structure d'un bloc, la logique de chaînage et les notions clés de décentralisation et d'immutabilité. Ensuite, notre attention sera portée aux mécanismes cryptographiques décentralisés sous-jacents, incluant les fonctions de hachage, les arbres de Merkel et les preuves à divulgation nulle de connaissance[14]. La typologie des blockchains, le trilemme de la blockchain, les algorithmes de consensus ainsi que les contrats intelligents seront aussi abordés. L'objectif est d'offrir une compréhension globale de la TBC afin de mieux saisir son potentiel dans des domaines critiques tels que la gestion de l'identité numérique alimentée par la TBC, qui fera l'objet d'un développement spécifique dans la prochaine section.

[14] Sera référé en tant que Zero Knowledge Proofs ou ZKP

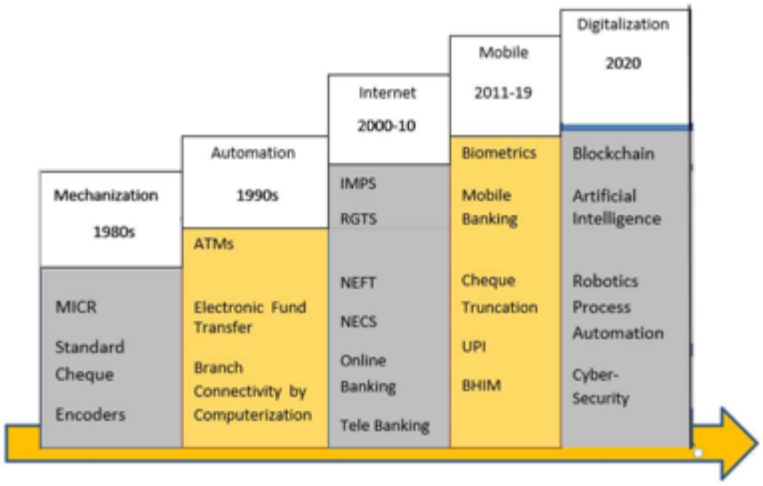


Figure 11 Développement technologique du secteur bancaire (Gupta et Gupta, 2018, p. 76)

2.2.1 Fondements et principes de la technologie blockchain (TBC)

La technologie blockchain est née dans un contexte de défiance vis-à-vis des institutions traditionnelles de gestion de la confiance, telles que les banques. Elle constitue une réponse radicalement nouvelle à la question de la confiance dans les environnements numériques en ce qui a trait à l'intégrité des échanges, la traçabilité des transactions et la sécurité des données sans avoir à se reposer sur un tiers de confiance (Gupta et Gupta, 2018, p. 76). À ces défis, la technologie blockchain répond par une combinaison ingénieuse de principes mathématiques, économiques et de technologies cryptographiques (Gupta et Gupta, 2018, p. 76), d'architecture distribuée et de mécanisme de validation collective pour créer un registre décentralisé, certifié et incorruptible (De Filippi, 2018, p. 43). La blockchain peut être envisagée comme un registre chronologique d'évènements, composés de blocs (Gupta et Gupta, 2018, p. 76) liés entre eux par des fonctions de hachage (Nakamoto, 2008, p. 1). Chaque bloc contient un ensemble de transactions, un horodatage et un pointeur vers le bloc précédent (Gupta et Gupta, 2018, p. 76-77 ; Sousa *et al.*, 2022, p. 7). Toute tentative de modification d'un bloc entraînerait une rupture de la chaîne, détectable immédiatement grâce à la non-correspondance des empreintes numériques (De Filippi, 2018, p. 48). Ce mécanisme permet de garantir l'immutabilité du registre : une fois une information enregistrée sur la chaîne, elle ne peut plus être modifiée ni effacée sans revalidation par l'ensemble du réseau, rendant toute falsification coûteuse voire impossible (De Filippi, 2018, p. 48). Ce registre est maintenu par un

réseau pair-à-pair[15] (Alamsyah *et al.*, 2024, p. 6), dans lequel chaque participant, ou nœud, détient une copie du registre complet (De Filippi, 2018, p. 51). Les décisions concernant l'ajout de nouveaux blocs sont prises collectivement via un mécanisme de consensus (Crosby *et al.*, 2016, p. 7), le plus souvent fondé sur la preuve de travail (« Proof of Work »), bien que d'autres modèles, comme la preuve d'enjeu (« Proof of Stake »), aient depuis vu le jour (De Filippi, 2018, p. 69). L'intérêt fondamental de cette architecture réside dans sa capacité à distribuer la confiance plutôt que de faire reposer l'intégrité du système sur un acteur unique (point de défaillance unique), la blockchain délègue cette responsabilité à l'ensemble des participants du réseau.

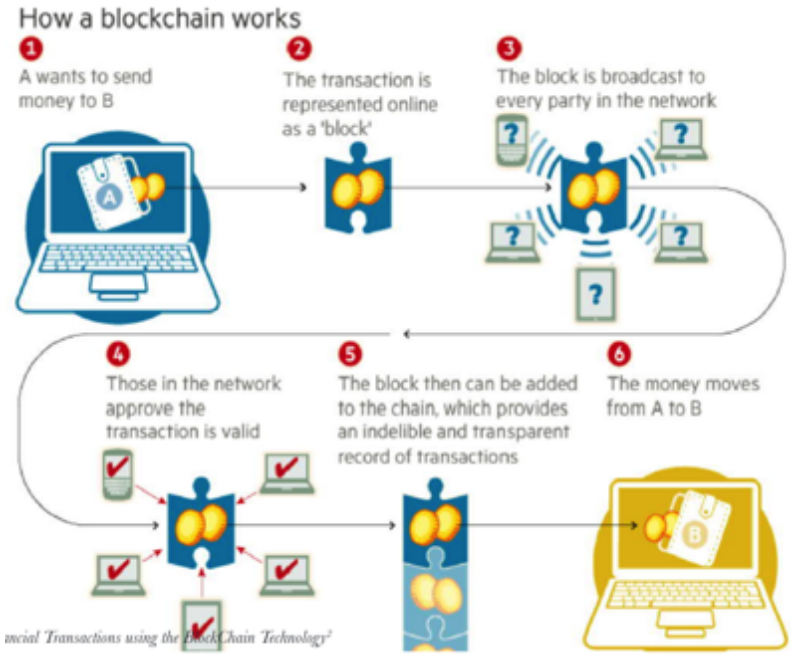


Figure 12 Fonctionnement d'une blockchain (Crosby et al., 2016, p. 10)

L'un des traits les plus remarquables de la blockchain réside dans la garantie simultanée de transparence et de sécurité. Toutes les transactions sont visibles publiquement, dans le cas des blockchains publiques, mais sont pseudonymisées, car les utilisateurs sont identifiés par leurs clés publiques (De Filippi, 2018, p.

[15] Le terme pair-à-pair sera référé comme P2P dans l'ensemble du document

62-63). Ce modèle soulève néanmoins des défis importants en matière de confidentialité, car même si l'identité de l'utilisateur n'est pas connue, la totalité de ses transactions passées et présentes est accessible sur la chaîne, ce qui permet potentiellement de reconstituer ou identifier des profils avec leurs activités publiques (De Filippi, 2018, p. 42). Par exemple, un individu dévoile ouvertement sa clé publique, n'importe qui peut accéder à l'historique des transactions de cette clé publique et associer cette clé à cette personne (De Filippi, 2018, p. 42). Cette limite a motivé le développement de blockchains axées sur la confidentialité, telles que Monero ou ZCash, qui introduisent des techniques cryptographiques avancées, comme les signatures en anneau ou les Zero Knowledge Proofs (De Filippi, 2018, p. 42-43). La nature immuable de la blockchain lui confère également une fonction probatoire. En stockant des « hashes »[16] de documents ou de fichiers, il devient possible de prouver leur existence à un moment à un moment donné, sans avoir à divulguer leur contenu. Ce principe est notamment utilisé dans les applications de type preuve d'existence, où la blockchain agit comme un notaire distribué, assurant l'authenticité et la datation des données (De Filippi, 2018, p. 52).

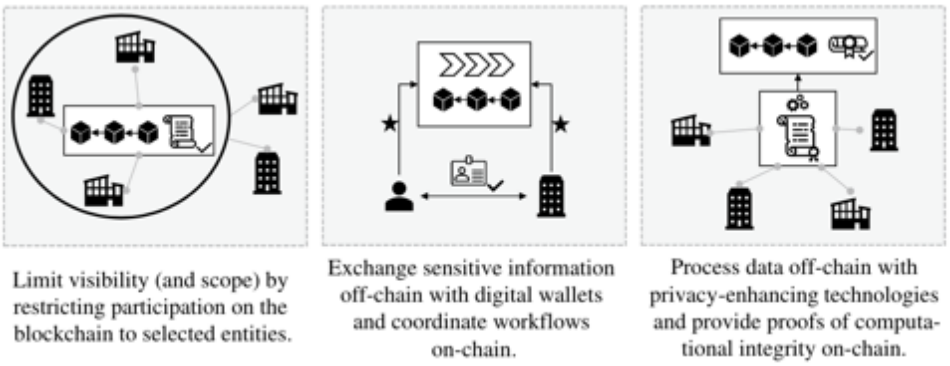


Figure 13 Approches principales pour adresser les défis de transparence (Sedlmeir et al., 2022, p. 11)

En outre, la blockchain introduit un nouveau modèle de temporalité dans les systèmes distribués. Alors que les réseaux P2P classiques peinent à établir un ordre chronologique des évènements, la blockchain résout ce problème en horodatant chaque bloc au moment de sa validation pour établir une séquence temporelle incontestable et répondant ainsi à la question cruciale dans tout système : « Qui fait quoi et

[16] Le terme Hashes réfère aux empreintes numériques

quand ? » (De Filippi, 2018, p. 52). Il faut toutefois souligner que la blockchain ne constitue pas une solution universelle. Son efficacité est intimement liée au coût des ressources qu'elle mobilise, par exemple, la consommation énergétique du protocole de consensus PoW[17] (De Filippi, 2018, p. 48). De plus, les blockchains sont souvent limitées en termes de scalabilité en raison de leur capacité de traitement. Enfin, la blockchain est soumise à une tension structurelle entre ouverture et contrôle. Les blockchains publiques, par leur nature ouverte, sont inclusives et résistantes à la censure, mais plus coûteuses et moins performantes. Les blockchains privées, en revanche, permettent un contrôle plus fin des accès et une meilleure efficacité, mais au prix d'une centralisation plus marquée, ce qui peut affaiblir certaines promesses fondamentales de sécurité et de transparence (De Filippi, 2018, p. 62-67).

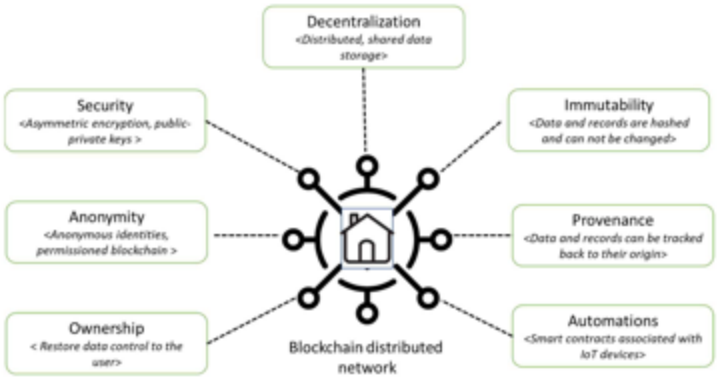


Figure 14 Caractéristiques de la TBC (Florea et al., 2022, p. 2)

2.2.1.1 Historique de la blockchain

La publication du livre blanc par Satoshi Nakamoto en 2008 a donné naissance à la technologie blockchain au travers de la cryptomonnaie nommée Bitcoin. Cette publication a introduit l'idée d'un système décentralisé de transactions P2P qui s'est concrétisée en tant que DLT[18] avec des caractéristiques distinctives telles que les blocs, les chaînes, le hachage cryptographique et le mécanisme de consensus de preuve de travail, proposant une solution au problème de double dépense dans les systèmes de paiement

[17] PoW est un acronyme pour Proof of Work ou Preuve de travail

[18] DLT est un acronyme pour technologie des registres distribués

électroniques sans intermédiaires (Nakamoto, 2008, p. 1). Lancé en 2009, le réseau Bitcoin constitue la première implémentation fonctionnelle de la TBC. Pendant plusieurs années la blockchain a été associée exclusivement au Bitcoin et aux cryptomonnaies. Ce n'est qu'à partir de 2014, avec l'arrivée de Ethereum notamment, que des usages alternatifs ont commencé à émerger avec la prise de conscience que cette technologie pouvait servir à bien d'autres fins que le simple transfert de valeur (De Filippi, 2018, p. 60). Contrairement aux systèmes bancaires actuels, il n'y a pas d'autorité centrale qui gouverne le Bitcoin. Ce sont les utilisateurs, également appelés « miners », de la blockchain qui sont au pouvoir de cette blockchain grâce à leur capacité machine qui résout des calculs complexes en vue d'élire le prochain mineur qui ajoutera un nouveau bloc à la chaîne. Le protocole du Bitcoin fonctionne sur un réseau décentralisé de machines (appelés nœuds), où chaque nœud contient une copie de l'ensemble de la chaîne de blocs, soit l'historique des transactions (Nakamoto, 2008, p. 1). Quelques années plus tard, en 2014, Vitalik Buterin publient une recherche qui a mené à la création d'Ethereum, soit une plateforme blockchain qui utilise des applications décentralisées (AppsD) sur un réseau P2P sans autorité centrale contrôlant la majorité de ses opérations (Zheng *et al.*, 2021, p. 1) et des contrats intelligents (De Filippi, 2018, p. 61-62). L'objectif était de diversifier l'utilisation de la blockchain au-delà des transactions de jetons pour inclure la logique programmable et le calcul distribué (Buterin, 2014). Elle fût donc conçue comme une plateforme de développement d'applications décentralisées, proposant un langage de programmation Turing-complet, Solidity, et une machine virtuelle dédiée, « l'Etheureum Virtual Machine », qui exécute les contrats intelligents de façon distribuée (De Filippi, 2018, p. 61-62). Buterin a depuis grandement amélioré son idée initiale qui a de nos jours plusieurs applications dans l'écosystème blockchain. Dans cette foulée de diversification et d'expansion des applications blockchain, les implications économiques de ces technologies ont également commencé à être scrutées de plus près. Ethereum a non seulement démontré la viabilité des contrats intelligents et des DApps, mais a aussi illustré comment la blockchain pourrait se servir de plateformes décentralisées pour des innovations complexes qui transcendent les simples échanges de cryptomonnaies. Cette capacité à programmer des accords et à exécuter automatiquement des contrats basés sur des conditions prédéfinies ouvre des avenues prometteuses pour automatiser les processus administratifs et financiers tout en réduisant les délais et les coûts associés à ces transactions.

Face à ces opportunités, Catalini et Gans (2016) observent les effets économiques de la blockchain dans leur article en soulignant comment la blockchain pourrait réduire les coûts de transaction, remplacer les intermédiaires et affecter les structures de marché. Ceux-ci concluent que la blockchain viendrait bouleverser les modèles d'affaires traditionnels et créerait de nouvelles opportunités économiques en

soulignant que la DLT réduit l'asymétrie de l'information, permet les échanges P2P et encourage les innovations dans les écosystèmes décentralisés (Catalini et Gans, 2016, p. 6). Le Bitcoin, l'Ethereum et leurs blockchains sous-jacentes ont accéléré et étendu le développement d'applications décentralisées telles que les monnaies numériques, les contrats intelligents, les systèmes de vote, la gestion des identités numériques et bien plus encore même si ces concepts existaient déjà avant l'avènement des blockchains (Narayanan et Clark, 2017, p 19-25).

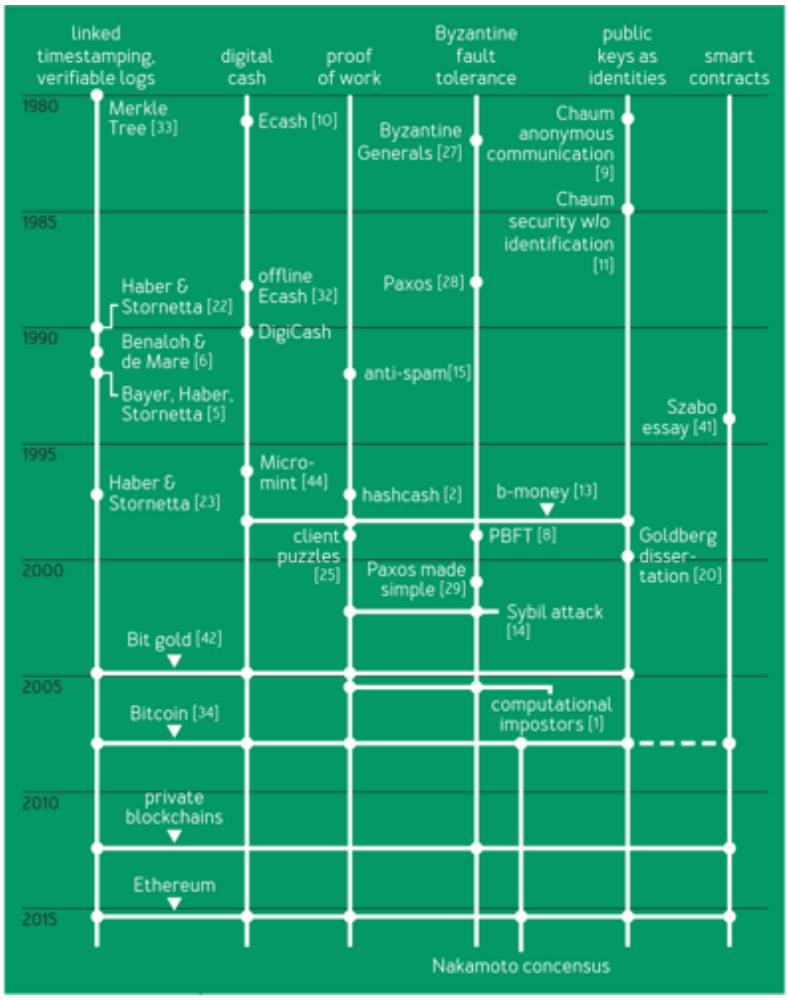


Figure 15 Chronologie des idées clés trouvés chez Bitcoin (Narayanan et Clark, 2017, p 2)

Historiquement, chaque vague d'innovation a été accompagnée de nouveaux questionnements. Le passage de la blockchain monétaire à la blockchain programmable a soulevé des défis en matière de sécurité, d'interprétation juridique des contrats intelligents et d'intégration avec des systèmes extérieurs via les oracles (De Filippi, 2018, p. 58). La question de la gouvernance, elle aussi, a pris de l'ampleur avec l'émergence des blockchains privées, dans lesquelles l'accès au registre et à son écriture est restreint à des acteurs identifiés, comme dans Hyperledger Fabric ou Corda (De Filippi, 2018, p. 65-66). Ainsi, l'histoire de la blockchain n'est pas linéaire, mais marquée par des tensions constantes entre ouverture et contrôle, transparence et confidentialité, innovation technique et enjeux sociaux. Elle reflète une dynamique évolutive, dans laquelle chaque génération itérative de la TBC cherche à résoudre les paradoxes hérités des précédentes pour étendre le périmètre des applications possibles.

2.2.1.2 Structure d'un bloc et chaîne de blocs

Au cœur du fonctionnement de toute blockchain se trouve une architecture de données : la chaîne de blocs (blockchain). Bien que souvent évoquée de manière abstraite, cette structure repose sur des éléments techniques précis qui assurent à la fois la cohérence interne du registre distribué et la fluidité des opérations entre participants. Comprendre la structure d'un bloc, ainsi que la logique de chaînage qui sous-tend l'ensemble, est essentiel pour appréhender la robustesse de cette technologie dans le cadre des systèmes distribués comme ceux qui seront utilisés dans le contexte bancaire ou plus particulièrement en gestion de l'identité.

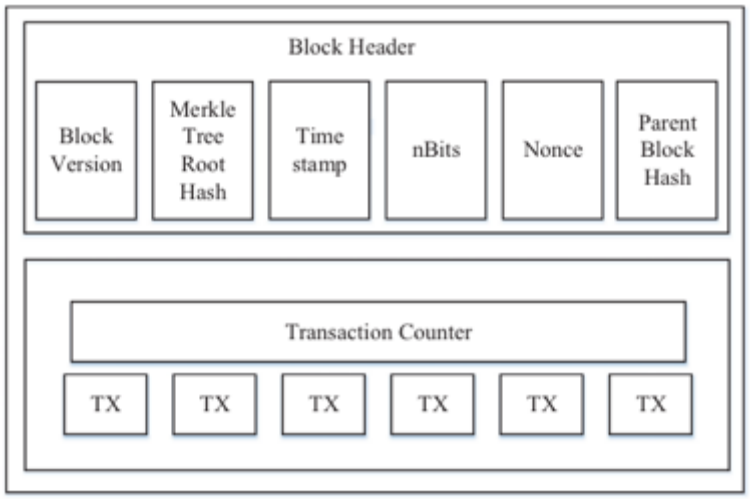


Figure 16 Structure d'un bloc (Zheng et al., 2017, p. 558)

Le tout premier bloc, appelé bloc « genesis », ne possède évidemment pas de prédécesseur et constitue l'ancrage initial de la chaîne (Zheng *et al.*, 2017, p. 558). À partir de là, chaque nouveau bloc vient s'ajouter à la suite, selon une logique séquentielle irréversible qui inscrit durablement les évènements dans une temporalité partagée par l'ensemble du réseau. Chaque bloc constitue une unité d'information composée d'une en-tête (header) et d'un corps (body). L'en-tête contient notamment le hash du bloc précédent, un horodatage, un nombre pseudo-aléatoire (nonce), le nBits[19], la version du bloc, ainsi que la racine d'un arbre Merkle résumant l'ensemble des transactions du bloc courant (Nakamoto, 2008, p. 2-6 ; Zheng *et al.*, 2017, p. 558). Ce chaînage par empreintes cryptographiques crée une dépendance formelle entre blocs successifs, de sorte qu'un changement dans l'un d'eux, même minime, affecterait nécessairement toute la chaîne qui lui succède. Ainsi, la priorité est accordée au bloc qui a été créé, ou miné, en premier pour pallier au problème de double dépense (Nakamoto, 2008, p. 2). Chaque transaction dans l'historique de la chaîne de blocs doit être annoncée publiquement pour que les participants de la chaîne puisse approuver collectivement sur un seul et unique historique de la chaîne (Nakamoto, 2008, p. 1). Le corps du bloc contient quant à lui la liste complète des transactions validées depuis le bloc précédent (Zheng *et al.*, 2017, p. 558). Cette liste est précédée d'un compteur indiquant le nombre de transactions incluses pour structurer davantage le format du bloc interne (Zheng *et al.*, 2017, p. 558). Ces transactions, une fois regroupées, sont condensées cryptographiquement dans l'en-tête du bloc par un mécanisme de

[19] Seuil de difficulté à atteindre pour valider un bloc

construction racinaire. La création d'un nouveau bloc répond à un ensemble de règles protocolaires dont le respect conditionne son ajout à la chaîne. Lorsqu'un nœud du réseau propose un bloc, celui-ci doit être conforme à certaines spécifications techniques (taille maximale, format, validité des transactions) et être accompagné d'une preuve cryptographique, selon le mécanisme de consensus utilisé. Le bloc n'est accepté que s'il respecte la règle de continuité avec le bloc précédent, identifié via son hash, et s'il est jugé valide par l'ensemble des nœuds du réseau (Crosby *et al.*, 2016, p. 7 & p. 10). Cette règle de construction séquentielle assure que chaque nouvelle unité vient s'insérer de manière ordonnée à l'extrémité de la chaîne existante pour former une ligne temporelle irréversible.

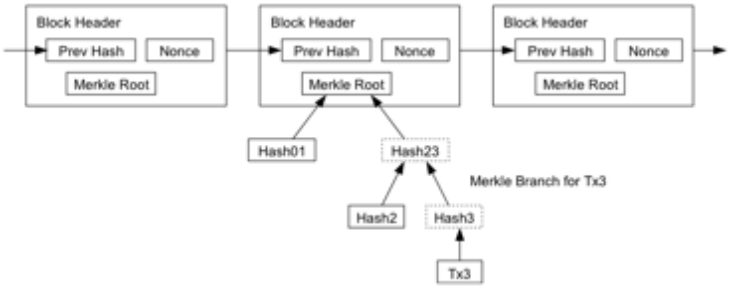


Figure 17 Composition d'une chaîne de blocs (Nakamoto, 2008, p. 5)

En somme, la structure en chaîne des blocs ne se limite pas à une disposition séquentielle d'informations, mais incarne un mécanisme fondamental de sécurisation et de synchronisation de la donnée distribuée. Elle permet à chaque acteur du réseau de vérifier de manière autonome l'intégrité de l'ensemble du réseau pour assurer que les nouvelles données s'intègrent selon une logique temporelle, vérifiable et inviolable.

2.2.1.3 Notions de décentralisation et d'immutabilité

Deux concepts structurants se distinguent fondamentalement la blockchain des bases de données traditionnelles : la décentralisation et l'immutabilité. Ces propriétés, bien qu'étroitement liées, s'ancrent

dans des principes techniques et philosophiques distincts et participent ensemble à la promesse d'un système sans autorité centrale, résilient, fiable et auditable.

La décentralisation désigne d'abord l'absence d'un tiers de confiance centralisé contrôlant le système (Zheng *et al.*, 2017, p. 558). Contrairement aux bases de données classiques, administrées par une entité unique, la blockchain repose sur une architecture distribuée dans laquelle chaque nœud du réseau conserve une copie complète ou partielle du registre en temps réel (De Filippi, 2018, p. 47-48). Cette réplication assure non seulement la continuité du service en cas de défaillance, pas de point de défaillance unique, d'un nœud, mais rend également toute tentative de manipulation unilatérale inefficace. Le contrôle et la validation des transactions sont effectuées collectivement, via une preuve cryptographique, pour permettre de répartir la confiance entre les participants (Crosby *et al.*, 2016, p. 9). Cette architecture P2P supprime la dépendance envers un administrateur unique et réduit le risque de censure, de corruption ou de compromission. Chaque modification proposée au registre est évaluée par l'ensemble du réseau et seule une majorité convergente permet son intégration. Ainsi, dans des blockchains publiques comme Bitcoin ou Ethereum, la décentralisation est non seulement technique, mais aussi politique, dans la mesure où aucune entité unique ne peut à elle seule influencer le devenir du réseau. L'immutabilité, quant à elle, est la conséquence directe de la structure chaînée des blocs et du modèle de consensus adopté. Une fois qu'un bloc est validé et ajouté à la chaîne, il devient pratiquement impossible d'en altérer le contenu (Zheng *et al.*, 2017, p. 559) sans devoir recalculer tous les blocs suivants et obtenir l'accord de la majorité du réseau. Plus un bloc est profond dans la chaîne, c'est-à-dire plus il est suivi de blocs confirmés, plus il devient difficile à modifier, car cela nécessiterait une puissance de calcul supérieure à celle de l'ensemble du réseau combiné. Ce principe garantit une forme de permanence unique, car une fois enregistrée, l'information ne peut être supprimée ni falsifiée, sauf à mobiliser une quantité de ressources considérable, rendant l'attaque économiquement dissuasive.

Enfin, la combinaison des propriétés de décentralisation et d'immutabilité fait de la blockchain un cadastre numérique distribué, garantissant l'intégrité temporelle et logique des enregistrements. Cette garantie structurelle permet d'envisager des usages dans des secteurs où la preuve de d'antériorité, l'absence de falsification et la traçabilité sont critiques tel qu'en gestion d'identité.

2.2.2 La cryptographie et la sécurité

La sécurité de la blockchain repose sur un socle cryptographique robuste, conçu pour assurer la confidentialité, l'intégrité, l'authenticité et la résilience des données dans un environnement distribué et sans autorité centrale. Contrairement aux systèmes traditionnels qui s'appuient sur des entités centralisées pour assurer la fiabilité des transactions et le contrôle d'accès aux données, la blockchain délègue cette responsabilité à des mécanismes mathématiques et informatiques. Elle intègre ainsi des techniques avancées de cryptographie pour établir une infrastructure de confiance décentralisée. À la base de cette architecture se trouvent trois piliers techniques : les fonctions de hachage, les arbres de Merkle et les preuves cryptographiques.

2.2.2.1 Fonctions de hachage

Les fonctions de hachage cryptographique est utilisée pour condenser toute donnée (texte, fichier, transaction) en une empreinte numérique fixe et unique appelée « hash » contenant un horodatage (Di Pierro, 2017, p. 93). Ces fonctions sont au cœur de la sécurité et l'intégrité des chaînes de blocs. Elles transforment une entrée de taille arbitraire en sorte de longueur fixe, appelée empreinte numérique, de manière irréversible (Di Pierro, 2017, p. 93). Une telle transformation assure que même un léger changement dans les données d'entrée produira une empreinte radicalement différente, ce qui permet de détecter toute tentative de modification ou de falsification de l'information. Sur le plan technique, la fonction SHA256 est structurée pour opérer sur des messages d'une taille inférieure à 2^{64} bits et produit un hachage de 256 bits (Fu *et al.*, 2020, p. 5). Elle fonctionne par itérations successives divisées en étapes : remplissage (« padding »), fragmentation du message en blocs, initialisation des registres, transformation par boucles de calcul et agrégation des résultats (Fu *et al.*, 2020, p. 10). Le cœur de l'algorithme repose sur une série de 64 cycles d'opérations bit à bit, d'additions modulaires et de permutations logiques complexes sur des registres intermédiaires (Fu *et al.*, 2020, p. 5). Cette structure permet non seulement de garantir la sécurité de l'empreinte produite, mais également d'optimiser le traitement parallèle sur des architectures matérielles spécialisées, comme les circuits FPGA (Fu *et al.*, 2020, p. 5-6).

Cependant, l'efficacité computationnelle de ces fonctions devient un enjeu critique, particulièrement dans les blockchains à haut débit de transactions. Des recherches récentes ont proposé des architectures proactives reconfigurables (PRCA) afin d'améliorer la performance du hachage sans compromettre sa sécurité (Fu *et al.*, 2020, p. 1). Ces architectures utilisent des pipelines parallèles pour exécuter simultanément plusieurs cycles de l'algorithme, réduisant ainsi le délai global de traitement (Fu *et al.*, 2020,

p. 5). De plus, l'intégration de stratégies comme les « Carry-Save Adders » permet de raccourcir les chemins critiques de calcul pour renforcer la vitesse d'exécution (Fu *et al.*, 2020, p. 5). Outre la rapidité, la résilience face aux attaques est un autre critère à considérer. Une bonne fonction de hachage doit présenter une résistance élevée aux collisions, c'est-à-dire la capacité à éviter que deux entrées distinctes produisent la même sortie. En pratique, la probabilité d'une collision dans SHA256 demeure négligeable, de l'ordre de 1 sur 2^{128}, ce qui signifie qu'un attaquant aurait besoin de ressources computationnelles astronomiques pour compromettre l'intégrité d'un système basé sur cette fonction.

Ainsi, les fonctions de hachage jouent un rôle doublement stratégique dans les systèmes blockchain, car elles assurent l'intégrité des données en empêchant toute falsification non détectée, tout en servant de mécanisme fondamental à la structure même de la chaîne de blocs. Leur optimisation, à travers des dispositifs matériels spécialisés ou des algorithmes hybrides, demeure un enjeu central pour l'évolution des blockchains vers usages intensifs et critiques.

2.2.2.2 Arbre de Merkle

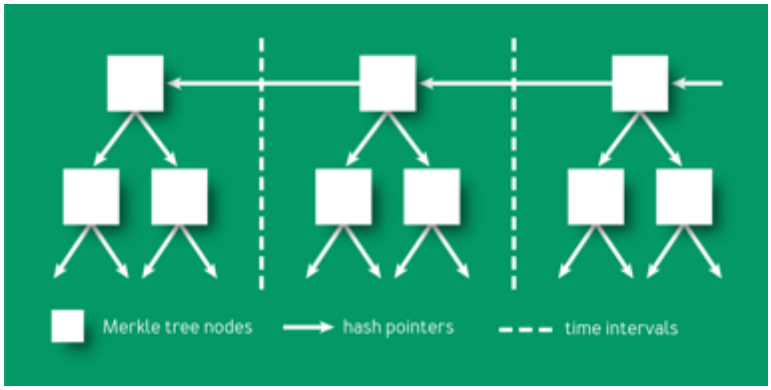


Figure 18 La structure des données du registre dans l'horodatage lié (Narayanan et Clark, 2017, p 6)

L'arbre de Merkle est une composante fondamentale de la structure interne d'un bloc dans une blockchain. Il s'agit d'un arbre binaire dans lequel chaque feuille représente une transaction et chaque nœud interne contient une empreinte de hachage dérivée de ses deux enfants (Narayanan et Clark, 2017, p 7). Cette structure a été initialement proposée par Ralph Merkle dans les années 1980 comme un mécanisme de

validation efficace des ensembles de données et (Narayanan et Clark, 2017, p 7). L'idée d'utiliser un arbre de Merkle au sein d'un bloc permettrait notamment de grouper un ensemble de transactions sous une seule racine de hachage pour conserver la possibilité de prouver l'inclusion d'une transaction sans devoir révéler l'intégralité des données (Narayanan et Clark, 2017, p 6-7). Une fois qu'un utilisateur connaît la racine de l'arbre, stockée dans l'en-tête du bloc, il peut valider l'intégrité d'une transaction spécifique en ne recevant qu'un petit sous-ensemble de nœuds, soit un chemin de hachage entre la feuille concernée et la racine. Bien que le concept ait été proposé bien avant l'avènement de Bitcoin, son potentiel n'a été pleinement reconnu qu'avec la montée en puissance des blockchains.

2.2.2.3 Preuves cryptographiques et Zero-Knowledge Proofs (ZKP)

La cryptographie, discipline centrale de la sécurité informatique, se concentre sur le développement de protocoles qui empêchent les tiers d'accéder aux données privées (Sirvent, 2022, p.1). Ses origines remontent à l'Antiquité, mais c'est avec l'ère du numérique que son importance s'est accentuée considérant l'évolution de l'art du chiffrement des messages à une science complexe intégrant des mathématiques avancées pour sécuriser les communications et les données (Katz et Lindell, 2007, p. 3 ; Sirvent, 2022, p. 1). Les applications de la cryptographie incluaient la sécurisation des transactions numériques et la préservation de la confidentialité des communications sur Internet (Diffie et Hellman, 1976, p. 11). Cette science utilise divers outils tels que les algorithmes de chiffrement symétrique et asymétrique, soit les fonctions de hachage et les signatures numériques pour assurer l'intégrité, la confidentialité et l'authentification des données électroniques. Le développement rapide de la cryptographie numérique, s'étendant au-delà du simple chiffrement des messages pour incorporer des concepts mathématiques complexes, a posé les bases pour des avancées révolutionnaires dans la sécurisation des données. Parmi ces innovations, le Massachusetts Institute of Technology (MIT) a joué un rôle important en inventant le concept de Zero-Knowledge Proof (ZKP).

Le ZKP est « un protocole cryptographique qui permet à une partie de prouver à une autre (vérificatrice) qu'une affirmation est réelle et vraie sans révéler la véracité de l'affirmation elle-même et des informations sous-jacentes » (Groth, 2011, p. 1). Un premier exemple serait « un *prouveur* veuille prouver qu'il ou elle connaît la solution d'un Sudoku sans révéler quelconque information qui pourrait faciliter la résolution du Sudoku au vérificateur » (Sedlmeir *et al.*, 2022, p. 10). Un autre exemple, un patient pourrait procéder à une demande d'assurance sans ambiguïté dans un hôpital pour ainsi vérifier son identité et accéder à des soins sans avoir à partager ses informations personnelles (Akram et Sen, 2022, p. 3). Ce

paradigme s'avère utile pour protéger la vie privée dans des environnements distribués où les données sont accessibles à tous les participants du réseau. L'intégration des ZKP à la blockchain vise à concilier transparence et confidentialité. En effet, si les blockchains offrent une immutabilité précieuse pour la vérification des identités, elles soulèvent également des préoccupations de confidentialité, étant donné que les données sont enregistrées publiquement (Sedlmeir *et al.*, 2022, p. 5). Les ZKP permettent alors de prouver la possession d'attributs personnels, par exemple être majeur ou citoyen d'un pays donné, sans révéler ces attributs eux-mêmes (date de naissance ou numéro d'assurance sociale) pour préserver la vie privée des utilisateurs.

Cela joue un rôle crucial dans la TBC en général, mais plus pertinemment dans la gestion de l'identité numérique dans le secteur bancaire. En appliquant les ZKP dans les systèmes existants, la TBC renforce la confidentialité et la sécurité des données d'identité numérique en permettant aux utilisateurs de préserver leurs informations en dehors des bases de données centralisées des banques. Ainsi, les ZKP constituent une innovation cryptographique déterminante dans la conciliation entre confidentialité des données et vérifiabilité des informations sur la blockchain.

2.2.3 Mécanismes de consensus et validation des transactions

Au cœur des systèmes blockchain repose un enjeu fondamental, soit de parvenir à un consensus sur l'état du registre distribué dans un environnement sans autorité centrale. Le consensus consiste à faire en sorte que tous les participants du réseau s'accordent sur une version unique et valide de la chaîne de blocs, même en présence d'acteurs malveillants, de latence de réseau ou de partitions temporaires. Dans les systèmes traditionnels, cette fonction de coordination est assurée par une entité centrale ou une infrastructure de confiance. À l'inverse, dans la blockchain, cette coordination est assurée collectivement par des nœuds assumés honnêtes et fiables via des mécanismes crypto économiques appelés protocoles de consensus (Narayanan et Clark, 2017, p 11). Les mécanismes de consensus permettent de sélectionner le prochain bloc à ajouter à la chaîne et de s'assurer que toutes les transactions qu'il contient sont valides. Pour que ces mécanismes soient efficaces, ils doivent satisfaire plusieurs propriétés : la résistance aux fautes byzantines[20], la finalité, soit garantir qu'un bloc validé ne sera pas révoqué, et l'efficacité énergétique et temporelle. Deux paradigmes principaux ont émergé dans l'univers des blockchains

[20] Réfère à la résistance aux comportements déviants ou malveillants

publiques : la preuve de travail, utilisée notamment dans Bitcoin, et la preuve d'enjeu, utilisée chez Ethereum, Cardano et d'autres blockchains de nouvelle génération.

2.2.3.1 Preuve de travail (PoW)

La preuve de travail a premièrement été introduite en 1992 par Cynthia Dwork et Moni Naor avec comme objectif de dissuader les spams, les dénis de service et les attaques Sybil (Narayanan et Clark, 2017, p 11). Elle constitue le premier mécanisme de consensus déployé à grande échelle en 2008 via Bitcoin et Satoshi Nakamoto (Nakamoto, 2008, p. 3). Pour ajouter un bloc à la chaîne, un nœud doit démontrer qu'il a accompli un certain travail computationnel, c'est-à-dire qu'il a résolu une énigme mathématique difficile à calculer et qui devient de plus en plus difficile plus la moyenne mobile ciblant un nombre de blocs par heure est élevée (Nakamoto, 2008, p. 3). Concrètement, chaque mineur tente de trouver une valeur de nonce qui, combinée aux données du bloc, produit un hachage, avec SHA 156, inférieur à une certaine cible définie par le réseau pour continuellement augmenter la difficulté de l'énigme mathématique si elle devient trop simple (Nakamoto, 2008, p. 3). Cette opération est aléatoire et repose sur des essais successifs, ce qui rend le processus coûteux en énergie (De Filippi, 2018, p. 48). La première entité à trouver une solution valide diffuse le bloc au reste du réseau, qui vérifie sa validité et, en cas de d'accord, l'ajoute à la chaîne octroyant ainsi une récompense au mineur du bloc (Nakamoto, 2008, p. 3-4). La PoW garantit l'intégrité du réseau en rendant économiquement dissuasive toute tentative d'attaque (De Filippi, 2018, p. 48). Pour modifier une transaction passée, un acteur malveillant devrait non seulement refaire le travail de hachage pour ce bloc, soit résoudre l'énigme mathématique coûteuse en énergie, mais aussi pour tous les blocs subséquents (De Filippi, 2018, p. 48).

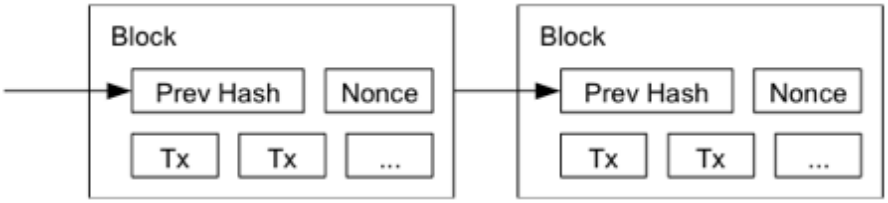


Figure 19 Proof of work (Nakamoto, 2008, p. 3)

Toutefois, la PoW a été critiquée pour son inefficacité énergétique, car les millions de calculs réalisés par les mineurs ne servent qu'à trouver une solution arbitraire sans valeur utilitaire (Catalini et Gans, 2016, p. 32-33). « Si les résultats de l'exploitation minière étaient également utiles à d'autres fins (par exemple, si les calculs permettaient de trouver de grands nombres premiers), le coût marginal de l'exploitation minière serait plus faible, car une partie du coût serait absorbée par les bénéfices que le mineur peut tirer de la vente des solutions à ces problèmes » (Catalini et Gans, 2016, p. 33). En outre, la centralisation du minage dans certaines régions du monde, où l'électricité est peu coûteuse, soulève des préoccupations géopolitiques et écologiques, venant également à l'encontre du principe fondamental de la blockchain, soit la décentralisation.

2.2.3.2 Proof of Stake (PoS)

Face aux limitations du modèle PoW, notamment en matière de consommation énergétique et de scalabilité, le mécanisme de preuve d'enjeu a émergé comme une alternative crédible et plus efficiente. Introduite pour la première fois par la cryptomonnaie Peercoin en 2012 qui utilisait une forme hybride de consensus (PoW & PoS), le PoS s'est depuis imposé dans plusieurs projets majeurs dont Ethereum 2.0 énergie (De Filippi, 2018, p. 41). Le mécanisme de preuve d'enjeu cherche à atteindre le consensus en fonction de la quantité de cryptomonnaie détenue par un participant plutôt que par sa puissance de calcul (Zheng *et al.*, 2017, p. 560). Dans ce modèle, l'idée centrale repose sur l'hypothèse que les détenteurs de grandes quantités de jetons seraient naturellement incités à maintenir l'intégrité du système, car ils en subissent directement les conséquences (BitFury Group, 2015, p. 6). Contrairement à la PoW, où les mineurs doivent résoudre des énigmes cryptographiques complexes, PoS sélectionne le créateur du prochain bloc selon des critères tels que la quantité de jetons en jeu (« Stake »), l'ancienneté des pièces ou encore des algorithmes de randomisation. Par exemple, Peercoin introduit un mécanisme où les pièces les plus anciennes et les plus nombreuses augmentent la probabilité de création d'un bloc, valorisant ainsi l'ancienneté comme facteur de confiance (BitFury Group, 2015, p. 9-10). L'un des enjeux principaux de PoS réside dans le risque d'accroissement des inégalités, puisque les entités déjà riches peuvent potentiellement consolider leur position dominante dans le réseau, phénomène souvent décrit comme le « rich get richer » (Zheng *et al.*, 2017, p. 557). Pour pallier ce déséquilibre, des variantes ont été proposées, telle que le « Delegated Proof of Stake », où les détenteurs de jetons élisent un nombre limité de validateurs chargés de produire et valider des blocs (Zheng *et al.*, 2017, p. 560). Ce modèle représentatif permet d'accélérer le traitement des transactions (Zheng *et al.*, 2017, p. 560). D'un point de vue comparatif, la PoS est reconnue pour sa faible consommation énergétique par rapport à la PoW, mais demeure

vulnérable à des attaques comme le « Nothing at Stake Problem », où des validateurs pourraient soutenir plusieurs chaînes concurrentes sans coût réel (BitFury Group, 2015, p. 12-13). Enfin, bien que le PoS réduise considérablement la consommation énergétique, son efficacité et sa résilience dépendent fortement du design du protocole, des incitations économiques et de la diversité des parties prenantes impliquées dans la validation des blocs.

2.2.4 Dimensions systémiques, opérationnelles et applicatives de la blockchain

Après avoir établi les fondements techniques, cryptographiques et protocolaires de la TBC, cette section aborde ses dimensions systémiques et opérationnelles, ainsi que ses déclinaisons applicatives concrètes. L'objectif est d'examiner comment la TBC, au-delà de ses mécanismes internes, s'inscrit dans des environnements numériques complexes, où des choix d'architecture, de gouvernance et d'usages déterminent sa portée et ses limites. L'analyse s'ouvre sur le trilemme de la blockchain, concept structurant qui met en lumière l'équilibre difficile à atteindre sur les fondations de la TBC. Elle se poursuit avec la typologie des blockchains et les contrats intelligents. Enfin, les sous-sections consacrées à la finance décentralisée et aux jetons non-fongibles illustrent les principales avenues d'implémentation de la TBC en tant qu'infrastructure pour de nouveaux modèles économiques, numériques et surtout décentralisés.

2.2.4.1 Trilemmes

Les innovations technologiques, qu'elles relèvent des systèmes traditionnels ou des systèmes décentralisés, sont souvent confrontées à des contraintes structurelles irréductibles qualifiée comme un trilemme. Ces trilemmes expriment l'impossibilité de maximiser simultanément trois dimensions fondamentales, forçant les concepteurs à faire des arbitrages. La présente sous-section propose d'explorer deux trilemmes importants affectant la transformation numérique des systèmes bancaires, soit celui des TI et celui de la blockchain.

2.2.4.1.1 Trilemme des TI

Le trilemme des TI, tel que présenté par C3L Security (2019), met en lumière les tensions entre trois dimensions fondamentales : la sécurité, la fonctionnalité et l'utilisabilité (simplicité). La sécurité désigne les mesures prises pour protéger les applications, systèmes et périphériques contre les accès non autorisés (C3L Security, 2019). La fonctionnalité correspond à l'étendue des tâches qu'un système doit accomplir, c'est-à-dire sa richesse opérationnelle et sa capacité à répondre aux besoins métier (C3L Security, 2019). L'utilisabilité renvoie, quant à elle, à la facilité avec laquelle les utilisateurs peuvent interagir avec le

système, incluant l'ergonomie, la simplicité, l'intuitivité et l'efficacité perçue dans l'utilisation quotidienne (C3L Security, 2019). Ce trilemme souligne qu'il est extrêmement difficile, voire impossible, d'optimiser les trois simultanément. Ainsi, une solution hautement sécurisée peut restreindre la convivialité ou limiter les fonctionnalités, tandis qu'un système axé sur la performance fonctionnelle ou la facilité d'usage risque de compromettre sa robustesse en matière de protection des données. Ce trilemme est particulièrement pertinent dans le contexte bancaire, où les institutions doivent constamment arbitrer entre le renforcement des mécanismes de contrôle, la fluidité des opérations numériques et l'expérience utilisateur. Il permet de mieux comprendre les défis liés à l'implémentation de technologies émergentes qui ambitionnent de renforcer la sécurité ou de simplifier les processus.

2.2.4.1.2 Trilemme de la blockchain

Le trilemme de la blockchain constitue un enjeu fondamental auquel sont confrontées les plateformes de registre distribué, puisqu'il reflète une tension entre trois objectifs critiques dont seulement deux sont atteignables : la scalabilité, la sécurité et la décentralisation (Werth *et al.*, 2023, p. 146). Ce trilemme repose sur le constat empirique selon lequel il est difficile pour une blockchain de maximiser simultanément ces trois propriétés, car chacune d'elles entre structurellement en conflit avec les deux autres.

Améliorer la scalabilité, c'est-à-dire la capacité à traiter un grand nombre de transactions par seconde tout en maintenant un faible temps de latence, implique souvent de restreindre le nombre de nœuds participants à la validation, tel que Ethereum avec le PoS, ce qui nuit à la décentralisation (Werth *et al.*, 2023, p. 147-150). En effet, certaines blockchains adoptent le mécanisme de consensus PoS en désignant un nombre limité de validateurs afin de réduire la communication réseau et augmenter la performance pour améliorer la scalabilité au détriment du niveau de distribution du pouvoir (Werth *et al.*, 2023, p. 147-150). La décentralisation, pour sa part, repose sur l'absence d'autorité centrale et sur la participation active d'un grand nombre de nœuds indépendants, où la confiance règne, au consensus du réseau (Werth *et al.*, 2023, p. 147-150). Or, plus les nœuds sont nombreux et indépendants, plus il devient difficile de coordonner efficacement leurs actions, ce qui limite les capacités de passage à l'échelle (scalabilité). De surcroît, maintenir un haut niveau de décentralisation peut fragiliser la capacité du système à assurer la sécurité, notamment lorsqu'un trop grand nombre de nœuds sont peu fiables ou mal synchronisés. La sécurité, enfin, vise à garantir la confidentialité, l'intégrité, la résistance aux attaques, par exemple les attaques de 51% ou la défaillance byzantine, ainsi que la disponibilité des transactions même en présence

de comportements malicieux (Werth *et al.*, 2023, p. 147-150). La confidentialité se rapporte au fait de garder l'information secrète au moyen de méthodes d'encryptions pour ne pas révéler leur identité (Werth *et al.*, 2023, p. 147). L'intégrité, quant à elle, se rapporte à la cohérence des données, leur authenticité et leur précision, tandis que la disponibilité assure que l'état de la chaîne est toujours lisible et disponible (Werth *et al.*, 2023, p. 148).

Ce trilemme impose donc un arbitrage stratégique à chaque plateforme blockchain, qui doit prioriser deux des trois attributs selon son cas d'usage. En définitive, aucune solution actuelle ne permet de maximiser simultanément les trois dimensions du trilemme.

2.2.4.2 Typologie de blockchains : publique, privée, avec et sans permissions

Les blockchains peuvent être classées selon deux axes : d'une part, l'ouverture du réseau (public ou privé et d'autre part, le régime de permissions qui détermine qui peut lire ou écrire sur le registre (avec ou sans permissions) (Peters et Panayi, 2016, p. 5). Cette typologie, bien que schématique, permet de distinguer les logiques de gouvernance et les finalités sous-jacentes.

	Public (Permissionless)	**Private (Permission-based)**	**Hybrid**	**Consortium**
Benefits	Independence Transparency Trust	Access control Performance	Access control Performance Scalability	Access control Scalability Security
Drawbacks	Performance Scalability Security	Trust Auditability	Transparency Upgrading	Transparency
Use cases	Cryptocurrency Document validation	Supply chain Asset ownership	Medical records Real state	Research Banking Supply chain
Transaction Throughput	LOW (<= 100 Transactions per second)	High (> 100 Transactions per second)	High (> 100 Transactions per second)	High (> 100 Transactions per second)
Consensus Participation + Mechanism	All the miners PoW/PoS	Particular organization + Practical Byzantine Fault Tolerance (PBFT) / Ripple	Voting based mechanism + PBFT/ PoA/Tendermint	A selected set of nodes + Voting based mechanism
Infrastructure	Highly Decentralized	Distributed	Distributed	Decentralized
Example	Bitcoin, Ethereum, Litecoin.	Hyperledger Fabric, Quorum, SoluLab.	IBM Food Trust	Energy Web Foundation, R3.

Tableau 1 Classification de la typologie blockchain (Ahmed et al., 2022, p. 8)

Dans une blockchain publique nécessairement sans permissions, telle que celle de Bitcoin ou Ethereum, toute personne peut librement accéder au réseau, lire et écrire des transactions (Kumar et Anand, 2020, p. 6), et participer au mécanisme de consensus (De Filippi, 2018, p. 62-63). Ces blockchains se caractérisent par une gouvernance décentralisée qui favorise la confiance entre acteurs qui ne se connaissent pas, mais entraîne également certains compromis étroitement liés à la cryptomonnaie associée et au mécanisme de consensus de la chaîne (De Filippi, 2018, p. 63). À l'opposé, les blockchains privées avec permissions instaurent un modèle fondé sur la centralisation du pouvoir décisionnel. Elles restreignent l'accès au réseau à un groupe prédéterminé d'acteurs (De Filippi, 2018, p. 63), qui sont souvent connus et authentifiés à l'avance. Ces blockchains sont fréquemment utilisées dans un contexte organisationnel ou inter-organisationnel (Peters et Panayi, 2016, p. 5), par exemple entre plusieurs banques ou entreprises partenaires, afin de conserver un certain contrôle sur les opérations du réseau. Les blockchains privées permettent une efficacité accrue dans la validation des transactions et dans le traitement des blocs, puisque le consensus peut être obtenu par des mécanismes plus légers tels que le vote majoritaire ou l'approbation d'un consortium. Entre ces deux extrêmes se situent les blockchains de consortium (ou blockchain hybrides), qui combinent des éléments des deux typologies avec une présélection de nœuds (Peters et Panayi, 2016, p. 6). Les infrastructures de consortium sont généralement permissionnés mais l'autorité n'est pas centralisée dans une seule entité. Les hypbrides, quant à elles, peuvent être permissions ou non permissionnées. Au contraire, plusieurs organisations coopèrent à la validation des blocs selon un mécanisme de gouvernance partagé.

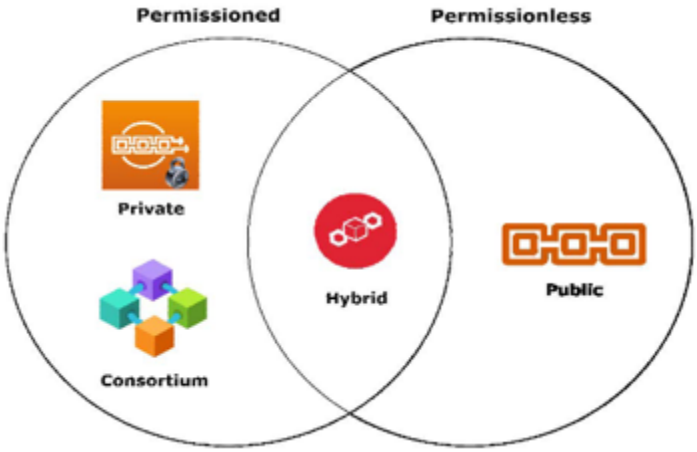


Figure 20 Portée des différents types de blockchain (Ahmed et al., 2022, p. 7)

La distinction entre avec ou sans permissions dépasse toutefois la simple question de l'accès au registre. Elle soulève des enjeux liés à la gouvernance, à la confiance et à la résilience. Dans un réseau sans permissions, l'absence d'identification préalable des validateurs accroît l'ouverture, mais rend plus difficile la mise en œuvre d'incitatifs à participer à valider la chaîne et exige un mécanisme de consensus qui puisse pallier aux incitatifs (Peters et Panayi, 2016, p. 6). Inversement, les blockchains permissionnées, en établissant des conditions d'accès et de participation, permettent d'instaurer des mécanismes contractuels et juridiques clairs entre parties identifiées et autorisées, mais perd dans l'aspect décentralisation.

En somme, le choix entre une blockchain publique ou privée, ouverte ou restreinte, doit être guidé par les objectifs fonctionnels du système, les exigences en matière de transparence ou de confidentialité, ainsi que les contraintes juridiques ou réglementaires du domaine ciblé Ce choix est déterminant dans le cadre de la gestion de l'identité numérique ou des infrastructures financières décentralisées, où les arbitrages entre contrôle, sécurité et inclusion doivent être soigneusement calibrés.

2.2.4.3 Définition et fonctionnement des contrats intelligents

Les contrats intelligents sont des programmes informatiques autonomes déployés sur la blockchain, conçus pour s'exécuter automatiquement dès que des conditions prédéfinies sont remplies (Doğan et Karacan, 2023, p. 5 ; Gautam, 2020, p. 114). Bien que leur conceptualisation remonte à Nick Szabo dans les années 1990 (Zheng *et al.*, 2020, p. 1), leur mise en œuvre concrète s'est matérialisée avec Ethereum, qui a introduit un langage de programmation Turing-complet permettant de coder une logique contractuelle flexible et exécutable de manière décentralisée (Buterin, 2014, p. 1 ; Peters et Panayi, 2016, p. 7). Ces contrats, enregistrés sur une blockchain, sont exécutés et approuvés par l'ensemble des nœuds du réseau pour assurer que les accords soient dument remplis et accomplis (Doğan et Karacan, 2023, p. 5).

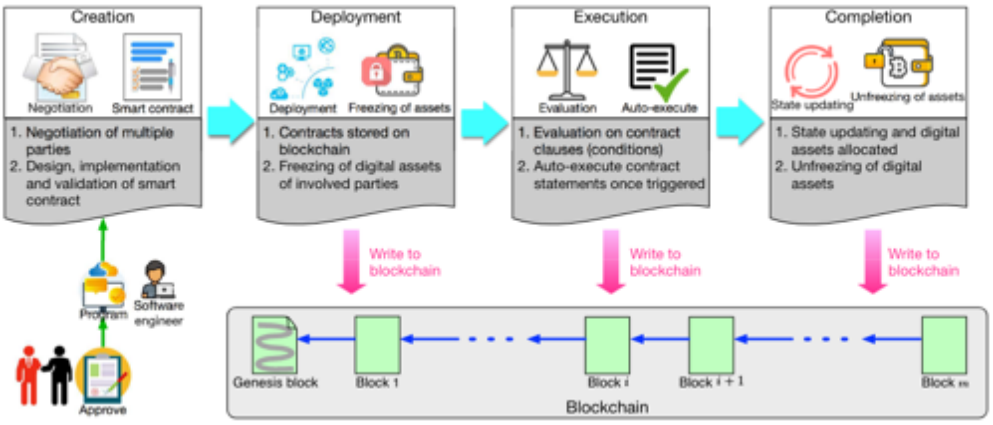


Figure 21 Cycle de vie des contrats intelligents en 4 phases majeures (Zheng et al., 2020, p. 5)

Le cycle de vie d'un contrat intelligent comprend quatre étapes principales. D'abord, lors de la création, les parties concernées négocient les termes du contrat, qui sont ensuite rédigés par des juristes avant d'être traduits en langage informatique par des développeurs (Zheng *et al.*, 2020, p. 3). Ensuite, à l'étape du déploiement, le contrat est enregistré sur une blockchain, où il devient immuable et verrouille temporairement les actifs numériques des parties impliquées (Zheng *et al.*, 2020, p. 4). Vient ensuite l'exécution, où les clauses du contrat sont automatiquement déclenchées dès que les conditions sont remplies, générant des transactions validées et inscrites dans la blockchain (Zheng *et al.*, 2020, p. 4). Finalement, à l'étape de clôture, les états des parties sont mis à jour, les actifs débloqués et toutes les informations sont enregistrées de manière permanente sur la blockchain (Zheng *et al.*, 2020, p. 4). Concrètement, un contrat intelligent fonctionne comme une structure conditionnelle dans laquelle les clauses sont inscrites dans le code et leur exécution est automatiquement déclenchée par l'occurrence d'un événement ou la réception d'une information, soit des conditions prédéfinies (Doğan et Karacan, 2023, p. 5). Par exemple, dans un contexte de commerce électronique décentralisé, un contrat peut être programmé pour effectuer un transfert de fonds à la livraison d'un bien sans qu'aucune autorité centrale ne supervise l'opération. Cette capacité à exécuter des conditions contractuelles de manière autonome permet d'améliorer et accélérer la productivité en automatisant de nombreux processus, de désintermédier ces processus, ainsi que de réduire les chances de désaccord et les coûts de transaction (Kayani et Hasan, 2024, p. 5). Un autre des avantages des contrats intelligents réside dans leur résistance à la censure et à la fraude. Une fois enregistrés sur la blockchain, ils ne peuvent être ni modifiés ni supprimés, sauf si leur code prévoit une clause d'autodestruction ou de mise à jour (Peters et Panayi, 2016, p. 7).

Figure 22 Applications des contrats intelligents (Zheng et al., 2020, p. 13)

Cependant, malgré leurs promesses, les contrats intelligents comportent plusieurs limitations et risques. Premièrement, la scalabilité implique que selon le nombre de contrats et d'utilisateurs, plus il est important, plus il sera difficile voire infaisable de traiter chaque transaction (Peters et Panayi, 2016, p. 7). Deuxièmement, les développeurs des contrats intelligents et les utilisateurs doivent être confiants de l'exactitude du code du contrat avant de le déployer considérant non seulement le résultat du contrat, mais aussi le gas[21] encouru (Peters et Panayi, 2016, p. 7). Troisièmement, sur le plan juridique, les contrats intelligents posent un problème quant à leur reconnaissance dans les systèmes de droit (Peters et Panayi, 2016, p. 7-8). Leur nature automatique ne permet toujours pas d'intégrer des clauses subjectives, comme celles nécessitant l'appréciation d'un juge ou d'un arbitre (Peters et Panayi, 2016, p. 7-8). Cela soulève des interrogations sur leur compatibilité avec les principes traditionnels du droit des contrats, notamment en matière de consentement, de capacité juridique ou de résiliation unilatérale. Enfin, les contrats intelligents peuvent avoir des effets collatéraux involontaires dans des systèmes interconnectés. Dans certains cas, l'interaction entre plusieurs contrats ou entre contrats et plateformes externes peut engendrer des résultats inattendus, voire des failles systémiques.

[21] Gas réfère au frais d'exécution d'un contrat intelligent

En résumé, les contrats intelligents offrent une automatisation puissante et transparente des relations numériques, mais nécessitent une vigilance accrue quant à leur conception, leur intégration dans l'environnement juridique existant et leur interaction avec le monde extérieur. Leur potentiel est indéniable, notamment dans des contextes bancaires décentralisés et de gestion d'identité numérique, mais leur déploiement doit s'accompagner d'une compréhension fine de leurs contraintes techniques et juridiques.

2.2.4.4 Finance Décentralisée (DeFi)

La finance décentralisée, communément désignée sous le terme DeFi, désigne un écosystème d'applications financières construites sur des technologies blockchain qui visent à reproduire ou étendre les services financiers traditionnels sans intermédiaire centralisé (Alamsyah *et al.*, 2024, p. 1). Elle représente une transformation radicale du paysage financier mondial en redéfinissant les modes de création, de distribution et d'utilisation des services financiers (Alamsyah *et al.*, 2024, p. 4). Ce paradigme repose sur une infrastructure ouverte, reposant sur des réseaux décentralisés de contrats intelligent, où le logiciel remplace les institutions financières traditionnelles en assurant l'exécution automatisée, transparente et immuable des opérations (Alamsyah *et al.*, 2024, p. 4-5). À la différence des systèmes financiers traditionnels, la DeFi n'est pas tributaire d'intermédiaires centralisés, mais propose une architecture ouverte, auto-souveraine et résistante à la censure (Alamsyah *et al.*, 2024, p. 4) qui permet à tout utilisateur disposant d'un portefeuille numérique et d'une connexion Internet de participer à l'écosystème financier. Grâce à la TBC, les protocoles DeFi offrent une gamme diversifiée de services, incluant les prêts et les emprunts, la gestion d'actifs, les stablecoins, la tokenisation[22], les paiements, l'assurance et plus encore (Alamsyah *et al.*, 2024, p. 4). En réduisant les coûts de transaction et en éliminant les barrières liées à la vérification des identités ou à la solvabilité, la DeFi favorise une plus grande inclusion financière notamment dans les régions où l'accès aux services bancaires est limité (Alamsyah *et al.*, 2024, p. 3). Elle permet également aux individus de se connecter directement entre eux pour conclure des transactions financières sans passer par une institution centralisée, ce qui réduit les frais et les délais d'exécution (Alamsyah *et al.*, 2024, p. 6). Sa capacité à composer, c'est-à-dire la possibilité d'assembler, plusieurs protocoles ou services interopérables permet la construction d'application financières complexes (Alamsyah *et al.*, 2024, p. 4). Cette propriété a permis l'émergence d'innovations comme le « yield farming », qui combine les stablecoins, le token de gouvernance et les pools de liquidité pour

[22] Voir Annexe G pour plus d'informations

générer des rendements (Alamsyah *et al.*, 2024, p. 4). Les contrats intelligents jouent un grand rôle dans le fonctionnement de la DeFi, car ils codifient les règles de chaque transaction et en assurent l'exécution sans intervention humaine (Alamsyah *et al.*, 2024, p. 6), par exemple, le remboursement d'un frais ou la fin d'une période de mise en jeu (« staking »). La DeFi, reposant sur modèle transactionnel P2P, donne la possibilité aux utilisateurs d'échanger entre eux, mais en s'appuyant sur la sécurité offerte par la blockchain et la transparence des contrats intelligents.

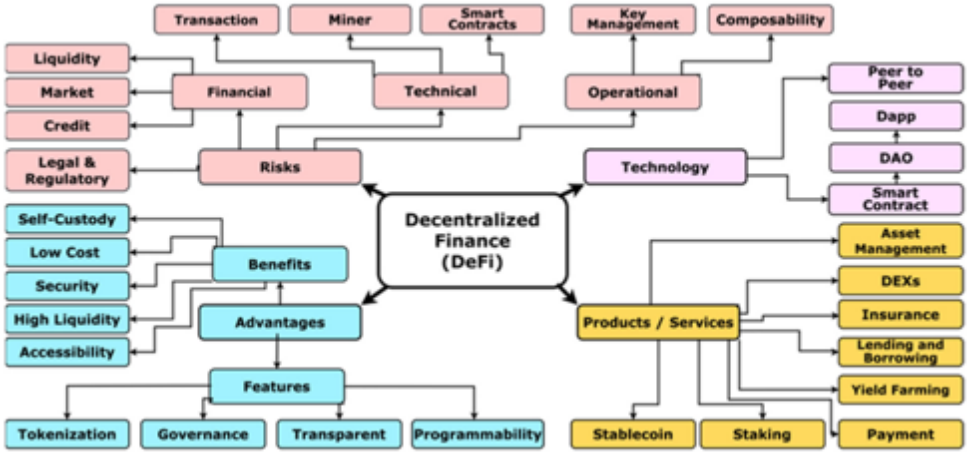


Figure 23 Taxonomie de la DeFi (Alamsyah et al., 2024, p. 11)

Bien que prometteuse, la DeFi est exposée à une série de risques techniques, financiers, opérationnels et réglementaires qui compromettent sa stabilité et son adoption à plus grande échelle. Parmi les menaces techniques les plus préoccupantes figurent les failles dans les contrats intelligents, souvent exploitées pour siphonner les fonds des utilisateurs, comme le montrent l'incident impliquant Qubit Finance qui a coûté 80 millions USD (Alamsyah *et al.*, 2024, p. 22). Du côté financier, les risques se trouvent plutôt au niveau de la liquidité, du marché et du crédit (Alamsyah *et al.*, 2024, p. 23). Les utilisateurs peuvent se voir manquer de fonds pour compléter une transaction, face faire à un déclin de la valeur de leurs actifs en raison de la volatilité des marchés et la possibilité que la partie avec qui un individu fait affaire ne puisse pas rencontrer ses obligations (Alamsyah *et al.*, 2024, p. 23). Les risques opérationnels, tels que la mauvaise gestion des clés, rendent également l'écosystème vulnérable à des pertes irréversibles (Alamsyah *et al.*, 2024, p. 24). Finalement, l'absence de cadre réglementaire clair et la possibilité

d'interventions étatiques brusques soulèvent des incertitudes légales majeures, surtout dans un contexte où les protocoles DeFi peuvent être utilisés à des fins illicites (Alamsyah *et al.*, 2024, p. 24).

En conclusion, la finance décentralisée s'inscrit comme une innovation majeure au sein de l'écosystème blockchain, car elle redéfinit l'accès aux services financiers à travers des mécanismes automatisés, ouverts et sans intermédiaires. En tirant parti des contrats intelligents, la DeFi permet la création d'une infrastructure financière programmable, flexible et mondiale. Toutefois, les risques multiples énoncés rappellent que son développement exige des garanties accrues à aller chercher en matière de sécurité et de gouvernance. Pour assurer une adoption durable et inclusive, il est donc essentiel d'élaborer des mécanismes robustes de gestion des risques tout en préservant les principes fondamentaux de la décentralisation.

2.2.4.5 Jetons non-fongibles (NFTs), Redevances et actifs numériques

L'émergence des jetons non-fongibles représente une évolution importante dans le champ de la tokenisation numérique rendue possible par la technologie blockchain (De Filippi, 2018, p. 85-86). En 2021, le marché des NFTs a explosé pour atteindre plus de 17 milliards de dollars en transactions (Bellagarda et Abu-Mahfouz, 2022, p. 1). Puis, l'année suivante en 2022, un total de 25 milliards de dollars en NFT ont été transigés avec notamment les CryptoPunks qui faisaient fureur (Falk *et al.*, 2022, p. 1).Ces jetons uniques, non interchangeables, permettent de représenter un actif numérique dans des domaines comme l'art, la musique, la gestion de l'identité et les objets de collection (Bellagarda et Abu-Mahfouz, 2022, p. 1-2 ; Parry et Ellul, 2024, p. 2). Contrairement aux fichiers numériques classiques, les NFTs reposent sur l'immutabilité et la décentralisation de la blockchain pour assurer l'unicité et l'inaltérabilité des actifs représentés (Parry et Ellul, 2024, p. 3). Ils garantissent dès lors la non-fongibilité, la propriété, l'authenticité, la rareté, la transférabilité, l'attribution au créateur et la transparence par l'enregistrement de la preuve de propriété sur les systèmes numériques décentralisés (Parry et Ellul, 2024, p. 5). La structure est représentée par des attributs tel que l'identifiant unique, l'adresse la méthode de transfert, les métadonnées, incluant des informations descriptives hors-chaîne et le code sur-chaîne définissant les règles et fonctionnalités (Parry et Ellul, 2024, p. 4).

Dans le domaine de l'art numérique, par exemple, ils permettent à un artiste d'associer une œuvre à un NFT unique, de le transférer et de la commercialiser sans compromettre sa rareté, suivant un modèle comparable aux éditions limitées dans le monde physique. D'un point de vue technique, c'est donc un

token numérique composée en trois classes : le NFT lui-même, ses métadonnées et les contrats intelligents intégrés (Parry et Ellul, 2024, p. 4). Avec les contrats intelligents, un artiste peut déployer le contrat et obtenir des redevances sur ses créations, et ce à chaque fois que son actif numérique change de propriétaire via une vente (Falk *et al.*, 2022, p. 1).

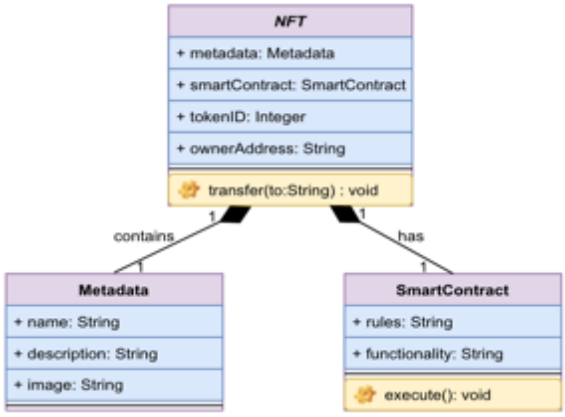


Figure 24 Structure de base d'un NFT (Parry et Ellul, 2024, p. 4)

Les NFTs peuvent également prendre plusieurs formes selon leur usage : des tokens d'identité, des tokens justificatifs, des tokens d'accès, des tokens d'attributs et des tokens de réputation (Parry et Ellul, 2024, p. 6-7). Parmi les cas d'usage émergents, les NFTs jouent un rôle croissant dans la gestion de l'identité avec le concept d'identité auto-souveraine (IAS), une approche qui vise à redonner à l'utilisateur la maîtrise de son identité numérique , puisqu'ils « encapsulent l'identité d'un individu dans le réseau blockchain » (Parry et Ellul, 2024, p. 6-7). Le fonctionnement d'un système d'identité auto-souveraine basé sur des NFTs repose sur des principes d'agence (propriété de l'identité, consentement, transparence, divulgation minimale et portabilité), d'autonomie (interopérabilité, inclusivité, accessibilité, usage et sécurité) et d'intégrité (authenticité, non-répudiation, résilience et vie privée) (Parry et Ellul, 2024, p. 7-8). Un utilisateur peut agréger ses différentes identités et attributs sous forme de NFT, tout en gardant le plein contrôle sur leur divulgation ou leur réutilisation. Les opportunités offertes par cette intégration sont multiples. D'abord, elle permet de bâtir des systèmes d'identité décentralisés qui renforce la souveraineté de l'individu sur ses propres données (Parry et Ellul, 2024, p. 11-12). Ensuite, l'usage de NFTs dans un cadre d'IAS peut favoriser l'inclusion numérique en rendant l'identité portable à travers différentes plateformes

(Parry et Ellul, 2024, p. 12). Enfin, les NFTs permettent de générer des nouvelles avenues de revenus en monétisant les actifs numériques (Parry et Ellul, 2024, p. 12).

Cependant, l'implémentation des NFTs dans un cadre d'IAS peut porter certains défis. Des obstacles techniques, comme la gestion sécurisée des clés privées ou l'absence de normes d'interopérabilité, compliquent leur adoption (Parry et Ellul, 2024, p. 17). À cela s'ajoutent des risques juridiques liés à la reconnaissance légale des identités décentralisés ou aux droits de propriété intellectuelle ou sur la confidentialité des données personnelles (Parry et Ellul, 2024, p. 18). Par ailleurs, la complexité technique et l'absence de standards peut freiner leur adoption par le grand public (Parry et Ellul, 2024, p. 17-19). Il est donc essentiel de développer des interfaces intuitives et des cadres réglementaires adaptés pour permettre à ces solutions de réaliser leur plein potentiel.

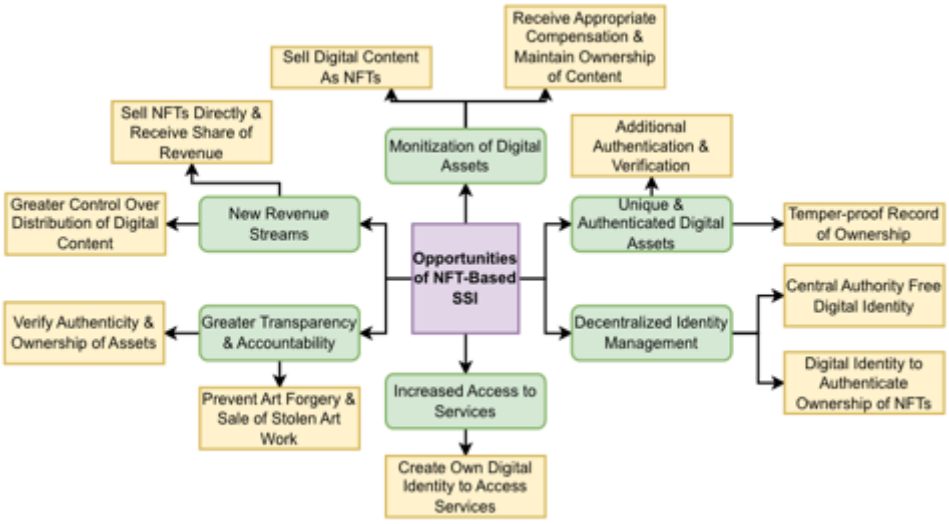


Figure 25 Opportunités offertes par l'intégration des NFTs et de l'IAS (Parry et Ellul, 2024, p. 12)

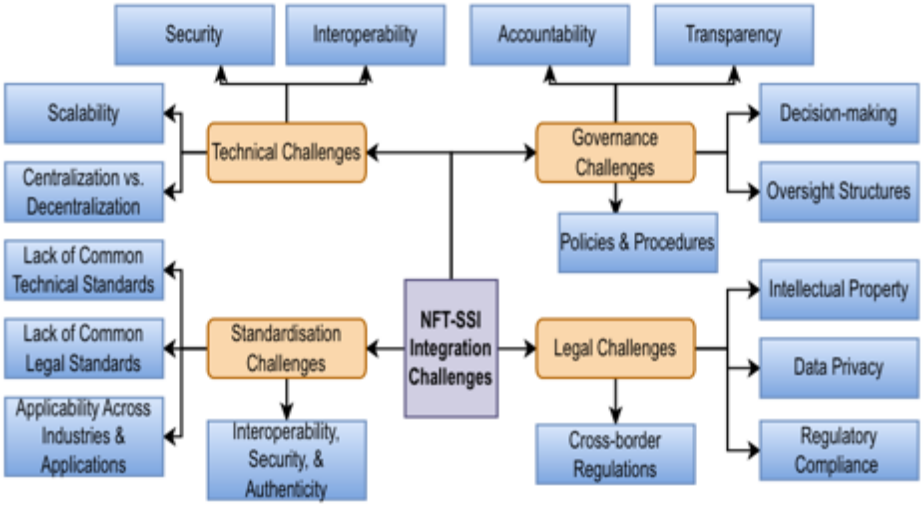


Figure 26 Défis de l'intégration des NFTs et IAS (Parry et Ellul, 2024, p. 18)

2.3 Systèmes bancaires décentralisés (SBD)

Maintenant que la table est mise sur la technologie blockchain, nous pouvons nous pencher sur les avancées récentes en matière de TBC qui ont rendu possible l'émergence de nouveaux modèles de service bancaires reposant sur des architectures distribuées et sans autorité centrale : les systèmes bancaires décentralisés. Les systèmes bancaires décentralisés constituent l'alternative la plus récente aux infrastructures des systèmes bancaires traditionnels en tirant parti des caractéristiques fondamentales de la blockchain, soit la transparence, l'immutabilité, la scalabilité, la sécurité et la décentralisation, pour repenser les logiques de gestion des identités, d'authentification, d'autorisation et de contrôle d'accès dans l'environnement numérique. Dans les écosystèmes propulsés par la blockchain, la confiance n'est plus déléguée à des institutions, mais distribuée entre les acteurs du réseau. Les rôles traditionnellement assurés par les institutions financières, comme la vérification de l'identité, l'authentification et l'autorisation des accès aux services ainsi que la gestion des droits, sont désormais assurés de manière distribuée à l'aide de protocoles cryptographiques et de mécanismes de consensus. Dans un contexte sans intermédiaire de confiance, garantir que les bonnes personnes accèdent aux bons services devient une priorité. Pour y répondre, nous allons explorer les modèles de gestion identitaire émergentes. Ainsi, la présente section explore ces nouvelles dynamiques à travers une revue progressive des composantes de la gestion des identités et accès dans les SBD. Elle débute par une présentation des modèles identitaires les plus répandus dans ces environnements avant d'aborder les innovations techniques concrètes. Elle se conclut par une revue des principales solutions existantes intégrant ces principes dans les SBD pour offrir un cadre complet de compréhension sur l'évolution de la gestion des identités à l'ère de la décentralisation bancaire.

2.3.1 Gestion de l'identité et des accès des clients (GIAC) dans les SBD

La transformation progressive des infrastructures bancaires vers des modèles décentralisés implique une redéfinition complète des mécanismes de gestion de l'identité, d'authentification et de contrôle d'accès. Dans les systèmes bancaires traditionnels, ces fonctions, généralement centralisés ou fédérés, sont assurées par les institutions bancaires elles-mêmes ou par des fournisseurs de services d'identité. Ces derniers détiennent l'autorité exclusive de valider l'identité des utilisateurs, de gérer les processus de connexion et de définir les droits d'accès à des ressources ou à des services. Cette centralisation présente toutefois plusieurs limitations tels qu'une vulnérabilité accrue aux attaques informations (un seuil point de défaillance), une faible interopérabilité entre institutions et une asymétrie de pouvoir dans la gestion des données personnelles.

Dans les systèmes bancaires décentralisés, la gestion de l'identité et des accès des clients doit être repensée pour fonctionner sans intermédiaire de confiance centralisé. Le paradigme change radicalement, car les utilisateurs deviendront les principaux gestionnaires de leurs identifiants, tandis que les mécanismes de validation s'opèreront de manière distribuée à travers des registres blockchain et des protocoles cryptographiques. Cela requiert des solutions techniques innovantes capables de concilier sécurité, confidentialité, simplicité, interopérabilité et conformité réglementaire. L'élément identitaire, qui représente la base de toute opération d'authentification, est au cœur de cette nouvelle approche. Dans un système bancaire décentralisé, l'identité d'un individu n'est plus émise ou conservée par un tiers, mais générée de manière autonome par l'utilisateur lui-même. L'authentification s'effectue alors par la possession prouvée de clés privées sans avoir à communiquer d'informations personnelles sensibles à un serveur central. Le contrôle d'accès, quant à lui, est assuré par des mécanismes programmables tels que les contrats intelligents, qui définissent, valident et enregistrent les règles d'accès de manière transparente et immuable. Cette approche permet d'automatiser la gestion des droits selon des conditions prédéfinies pour conserver une traçabilité complète non falsifiable des actions effectuées. Enfin, l'absence de hiérarchie dans l'architecture des SBD implique la mise en œuvre de standards ouverts pour assurer l'interopérabilité entre différentes entités du réseau. Cela passe par l'utilisation de formats normalisés pour les identifiants, les métadonnées d'identité et les mécanismes d'échange d'information, comme sera développé dans les sections suivantes.

Ainsi, la GIAC dans les SBD devient non seulement un enjeu de sécurité à adresser, mais aussi une condition essentielle pour garantir la confiance, la souveraineté des utilisateurs et la fluidité des interactions financières. Nous allons donc commencer par observer les modèles d'identité qui sont au cœur des solutions décentralisées.

2.3.1.1 Modèle centré sur l'utilisateur

L'identité numérique centrée sur l'utilisateur repose sur un paradigme dans lequel les individus ont un contrôle total sur leurs informations d'identité (Bharadwaj *et al.*, 2023, p. 6). Contrairement aux modèles centralisés ou fédérés, ce modèle permet aux utilisateurs de choisir leur fournisseur d'identité en qui ils ont confiance pour stocker, gérer et partager leurs attributs d'identification (Alanzi et Alkhatib, 2022, p. 3) directement à partir d'un portefeuille numérique sécurisé, comme un téléphone intelligent, dans le domaine de l'utilisateur éliminant ainsi la nécessité d'un intermédiaire pour l'authentification. Cette approche est renforcée par l'émergence des portefeuilles numériques d'identité qui offrent aux

utilisateurs une autonomie accrue dans la gestion de leurs données personnelles. « Dans les solutions suivant le modèle centré sur l'utilisateur, les informations d'identité nécessaires sont récupérées directement depuis le domaine de l'utilisateur, [lues à partir d'un téléphone intelligent], et transmises au fournisseur de service lors de chaque processus d'authentification. Toutefois, le fournisseur d'identité est généralement toujours présent, servant uniquement d'intermédiaire entre le fournisseur de service et le jeton contenant les informations d'identité » (Podgorelec *et al.*, 2022, p. 2).

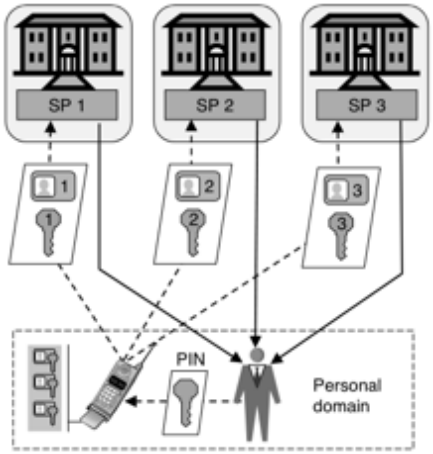


Figure 27 Modèle centré sur l'utilisateur (Jøsang et Pope, 2005, p. 7)

Ce modèle s'inscrit en rupture avec les approches traditionnelles qui privilégient la commodité pour les fournisseurs de services au détriment de l'expérience utilisateur (Jøsang et Pope, 2005, p. 7), engendrant des systèmes peu ergonomiques, comme l'illustrent la prolifération des mots de passe. Bien qu'il soit qualifié de centré sur l'utilisateur, il ne garantit pas une pleine souveraineté. En effet, même si l'utilisateur peut gérer sa propres identité grâce à des services comme OpenID ou OAuth, la propriété et le contrôle ultime de l'identité demeurent entre les mains du fournisseur de service centralisé (Bharadwaj *et al.*, 2023, p. 6). Cela limite l'autonomie réelle de l'utilisateur, puisque l'émission, la révocation ou la portabilité de l'identité nécessitent l'intervention du fournisseur initial (Bharadwaj *et al.*, 2023, p. 6). Sachant cela, la portabilité est tout de même une avancée dans ce modèle (Bharadwaj *et al.*, 2023, p. 6), car les identifiants peuvent être réutilisés entre différents services numériques sans création d'identités distinctes pour chaque plateforme via OpenID. Le compromis, en revanche, est que l'utilisateur ne détient pas les clés

cryptographiques associées à son identité, à la différence des modèles comme l'IAS. Il est donc plus juste de considérer le modèle centré sur l'utilisateur comme une étape de transition entre les systèmes purement centralisés/fédérés et les approches décentralisées.

En somme, le modèle d'identité numérique centré sur l'utilisateur représente une évolution significative vers une gestion plus autonome et sécurisée des identités numériques. Avec l'essor des portefeuilles d'identité et des solutions basées sur la blockchain, ce modèle pourrait devenir une alternative viable aux approches traditionnelles. Toutefois, son succès dépendra de la mise en place d'une infrastructure robuste, d'une adoption large par les institutions et d'une réglementation adaptée pour garantir un équilibre entre sécurité et accessibilité.

2.3.1.2 Modèle décentralisé

L'évolution des modèles d'identité numériques témoigne un déplacement graduel du contrôle, initialement concentré entre les mains d'autorités centrales, vers une autonomie de plus en plus accrue des utilisateurs. Marquée par une décentralisation progressive des mécanismes de gestion de données et d'authentification, cette transition aboutit à un modèle où l'utilisateur devient le principal gestionnaire de son identité. À son aboutissement, le modèle d'identité décentralisé se distingue par sa capacité à éliminer les points de défaillance unique, à renforcer la résilience des systèmes et à redéfinir les fondements de la confiance numérique.

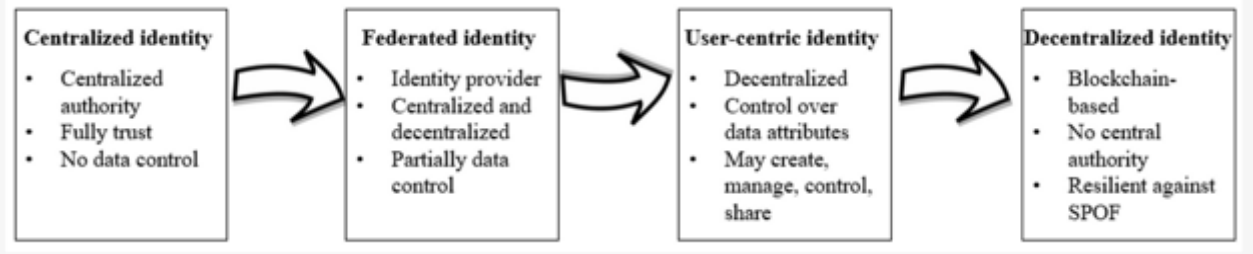


Figure 28 Comparaison des modèles de gestion de l'identité (Chan et al., 2025, p.6)

Contrairement au modèle centralisé et fédéré qui s'appuie sur des tiers de confiance pour vérifier et stocker les identifiants, le modèle décentralisé permet aux utilisateurs de posséder et de gérer

complètement leur identité (Bharadwaj *et al.*, 2023, p. 6). Dans cette logique, l'identité des participants du modèle décentralisé s'approprient une identité distribuée. L'identité distribuée désigne un mode de gestion de l'identité numérique fondé sur un réseau de pairs, où chaque nœud du réseau joue un rôle équivalent (Bharadwaj *et al.*, 2023, p. 6). « L'identification, l'autorisation et les droits d'accès sont alors délégués collectivement par une communauté d'individus » (Bharadwaj *et al.*, 2023, p. 6). Chaque participant peut ainsi agir comme émetteur et vérificateur d'une identité numérique pour accéder aux services d'autres nœuds du système (Bharadwaj *et al.*, 2023, p. 6). Les solutions traditionnelles, reposant sur des bases de données centralisées, constituent des cibles de choix pour les pirates informatiques. En revanche, avec une approche décentralisée, les identités sont stockées de manière distribuée sur plusieurs nœuds de la blockchain (Rana *et al.*, 2019, p. 27), rendant donc toute tentative de compromission bien plus difficile, comme nous l'avons expliqué avec le mécanisme de preuve de travail par exemple. De plus, en supprimant les intermédiaires, les risques de fraude et d'usurpation identité sont considérablement réduits en raison de l'aspect immuable et transparente du registre distribué (Rana *et al.*, 2019, p. 27). Dans le domaine bancaire, il pourrait permettre aux clients de prouver leur identité, de manière sécurisée sans passer par un intermédiaire pour accélérer les processus de vérification KYC.

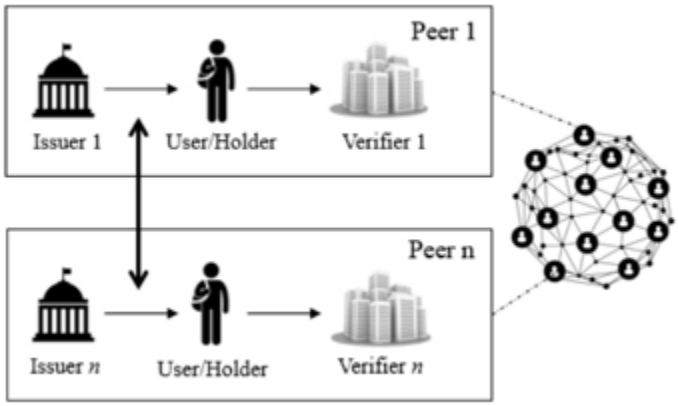


Figure 29 Modèle décentralisé de gestion de l'identité (Chan et al., 2025, p.6)

En conclusion, le modèle d'identité numérique décentralisé représente une avancée majeure par une gestion sécurisée et autonome des identités numériques. Grâce à des technologies, comme la blockchain et les identifiants décentralisés, il permet d'offrir une meilleure protection des données et une plus grande interopérabilité entre les services. Cependant, son adoption généralisée nécessitera des efforts en matière

de standardisation, d'éducation des utilisateurs et d'adaptation des réglementations afin de garantir un équilibre entre sécurité, confidentialité et accessibilité.

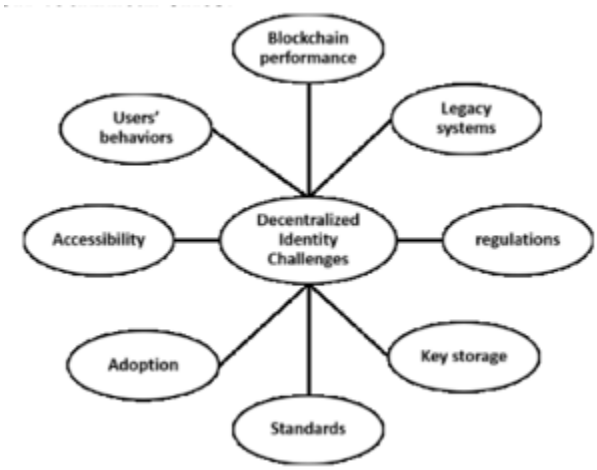


Figure 30 Défis de l'identité décentralisée (Dib et Toumi, 2020, p. 33)

2.3.2 Identité décentralisée

Les identifiants décentralisés (IDD), l'identité auto-souveraine (IAS) et les informations d'identification vérifiables (IIV) ont été identifiés comme les solutions plus prometteuses pour faciliter les opérations bancaires en lien avec la gestion de l'identité numérique. La transformation numérique dans le secteur bancaire a été définie comme un processus global d'adoption de technologies numériques pour transformer les activités et les modèles économiques des banques traditionnelles. En ce sens, la transformation numérique dans le secteur bancaire a été alimenté par la nécessité d'améliorer l'expérience client, d'optimiser les processus internes et de rester compétitif sur un marché en constante évolution. L'intégration de technologies innovantes, telles que l'IA, l'Internet des Objets (IoT), le Big Data et la blockchain, a complètement perturbé le secteur bancaire (Kour, 2023, p. 1). Cela a permis aux banques canadiennes d'optimiser leurs processus, d'améliorer la sécurité des données et d'offrir des services plus personnalisés à leurs clients. De ce fait, la transformation numérique dans le secteur bancaire a ouvert la voie à des modèles commerciaux innovants, tels que les banques ouvertes, qui reposent sur des interfaces de programmation d'application ouvertes pour permettre l'interaction avec des tiers.

De toute évidence, les banques canadiennes peuvent tirer parti de l'adoption des IDD, IAS et IIV en termes de sécurité et d'efficacité des processus de gestion de l'identité, car ces innovations offrent une alternative à la gestion de l'identité centralisée moderne. Ces trois concepts clés issus de la TBC sont tous des changements de paradigme pour l'industrie bancaire canadienne. Une innovation de cette magnitude peut aider les banques canadiennes à favoriser la crédibilité et la confiance, renforcer les efforts envers les indications émises par les régulateurs et, en fin de compte, ouvrir la porte à une large gamme de nouvelles possibilités de croissance et d'innovation dans les espaces numériques en constante évolution. En ce sens, les IDD interbancaires, c'est-à-dire un identifiant répandu à travers toutes les banques, représentent une avancée considérable pour le secteur financier en facilitant des échanges plus sécurisés et transparents entre les institutions. Ces systèmes permettent non seulement d'harmoniser les processus d'authentification à travers différentes banques, mais aussi d'améliorer la gestion de la conformité et de la réglementation. Un exemple notable de cette technologie en action est le projet entrepris par HSBC en collaboration avec PolygonID visant à développer une solution d'identité décentralisée. Ce projet illustre comment les IDD peuvent être utilisées pour simplifier les processus KYC et en améliorant l'expérience client. Cependant, l'adoption de IDD dans le secteur bancaire n'est pas sans défis. Bien que ces systèmes offrent des avantages considérables en termes de coût et d'efficacité, ils exigent une attention accrue aux stratégies de gestion de risques, notamment en matière de protection des données et respect de la vie privée, ce qui peut compliquer leur intégration à l'échelle interbancaire (Mohite *et al.*, 2023, p. 54). Les banques doivent être prêtes à investir dans des technologies avancées et dans la formation de leur personnel pour tirer pleinement profit des possibilités offertes par les IDD interbancaires. Au-delà de ces investissements, les banques canadiennes doivent également respecter les régulations strictes en matière de protection des données et de la vie privée comme la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE) et la Loi 25, soit les nouvelles dispositions protégeant la vie privée des Québécois pour les banques québécoises.

Afin de mieux comprendre les composantes clés de cette nouvelle approche en gestion de l'identité, la présente section est structurée autour de trois sous-parties complémentaires : le modèle d'identité auto-souveraine, les identifiants décentralisés et les informations d'identification vérifiables. Chacune de ses composantes sera explorée afin de mettre en lumière leur rôle respectif, leur interconnexion et leur potentiel d'application dans le secteur bancaire à l'ère de la technologie blockchain.

2.3.2.1 Identité auto-souveraine (IAS)

L'identité auto-souveraine, ou « Self-Sovereign Identity » en anglais, constitue une déclinaison avancée du modèle centré sur l'utilisateur, car elle repose sur des principes de décentralisation où l'utilisateur peut délivrer des preuves cryptographiques de son identité (Sim *et al.*, 2019, p. 32). Elle émerge à la croisée des modèles d'identité numériques, centrée sur l'utilisateur et décentralisée, mais pousse plus loin (Allen, 2016) pour « permettre aux utilisateurs d'exister indépendamment d'un service » (Bharadwaj *et al.*, 2023, p. 6). « Alors que les solutions d'identité centrées sur l'utilisateur dépendent encore des fournisseurs d'identité centraux, le SSI vise à rendre l'utilisateur pleinement souverain de ses identifiants (Podgorelec *et al.*, 2022, p. 2). Elle constitue une réponse concrète aux limites structurelles des systèmes traditionnels d'identité qui souffrent de fragmentation, d'intermédiation excessive, de risques accrus de vol d'identité et d'une absence de portabilité. L'IAS s'inscrit dans la continuité des droits numériques fondamentaux tels que le droit à la vie privée, à l'autodétermination informationnelle et à l'intégrité numérique. Elle promeut un déplacement radical du pouvoir, historiquement entre les mains des États, entreprises ou institutions, vers l'individu lui-même, désormais en mais en mesure de détenir son identité numérique dans un portefeuille numérique (Bharadwaj *et al.*, 2023, p. 7) et de créer, gérer et partager leurs identités numériques (Chan *et al.*, 2025, p. 8). En l'absence d'une autorité administrative et puisque les utilisateurs sont en plein contrôle de leurs identités, les utilisateurs eux-mêmes sont attachés avec leurs identifiants, au moyen d'un chiffrement asymétrique, pour établir un pont entre l'identifiant et la clé publique afin que quiconque puisse lire et vérifier l'identifiant sur la chaîne (Sim *et al.*, 2019, p. 32). Ainsi, en utilisant l'identifiant lié à son portefeuille numérique, il est possible d'interagir en ligne et d'accès à des service, et ce sans céder le contrôle de ses informations personnelles (Ahmed *et al.*, 2022, p. 10).

Afin de garantir le contrôle de l'utilisateur et l'équilibre entre transparence, équité, le soutien des biens communs avec la protection de l'individu, l'approche d'IAS repose sur onze principes fondamentaux formulés par Christopher Allen en 2016 (Allen, 2016). Premièrement, les identités numériques doivent être connectées à un individu réel physique ou à une entité vérifiable (Existence) (Allen, 2016). Deuxièmement, les individus ont l'autorité ultime sur leurs identités numériques, c'est-à-dire s'y référer, de les mettre à jour ou de les cacher (Contrôle) (Allen, 2016). Troisièmement, les individus doivent toujours avoir accès à leurs propres identités pour retrouver toute données relatives à son identité (Accès) (Allen, 2016). Quatrièmement, les opérations algorithmiques et la gestion des systèmes d'IAS doivent être transparentes (Transparence) (Allen, 2016). Cinquièmement, les identités numériques devraient être éternelles pour permettre aux individus de les conserver au fil du temps sans entrer en conflit avec le

« droit à l'oubli » (Persistance) (Allen, 2016). Sixièmement, les informations et services reliés à l'identité doivent pouvoir être transférable sans effort entre différentes juridictions (Portabilité) (Allen, 2016). Septièmement, les systèmes d'IAS doivent permettre le plus possible l'usage des identités sur différentes plateformes et obtenir une reconnaissance internationale (Interopérable) (Allen, 2016). Huitièmement, le consentement de l'utilisateur avant l'utilisation et le partage des informations relatives à son identité (Consentement) (Allen, 2016). Neuvièmement, les individus devraient minimiser la divulgation de leurs données strictement nécessaires (Minimisation) (Allen, 2016). Dixièmement, la protection des droits des utilisateurs doivent toujours être respectée (Protection) (Allen, 2016). Finalement, les réclamations doivent être vérifiables (Prouvable) (Dieye *et al.*, 2023, p. 2).

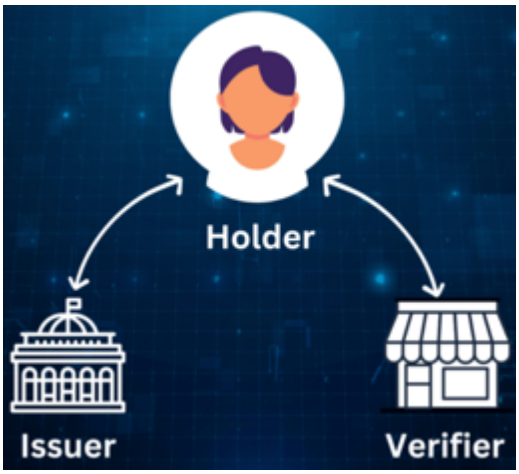


Figure 31 Trois acteurs principaux de l'IAS (Hendrickson, 2025)

Par ailleurs, le modèle d'IAS implique trois grands acteurs. D'abord, le titulaire d'identité, le « holder », soit l'utilisateur final, est celui qui possède et gère ses identifiants (Hendrickson, 2025). Ensuite, l'émetteur d'attestations, le « issuer », est une entité reconnue (ex : université, banque, gouvernement) qui émet une information d'identification vérifiable liée à un attribut (ex : diplôme, compte bancaire, passeport) pour des fins de validations (Hendrickson, 2025). Enfin, le vérificateur, le « verifier », est l'organisation ou l'entité qui consulte ces informations d'identification pour valider l'identité ou l'attribut présenté par le titulaire (Hendrickson, 2025). La triangularité de ces acteurs est à la base de toute interaction entre les différents acteurs dans le cadre d'une structure d'IAS. Ces interactions reposent, elles-mêmes, sur trois

piliers fondamentaux de l'IAS : les identifiants décentralisés, les informations d'identification vérifiables et la blockchain (Hendrickson, 2025).

Figure 32 Trois pilliers de l'IAS (Hendrickson, 2025)

L'adoption d'un modèle d'IAS présente des bénéfices substantiels pour les individus, les entreprises et les institutions. En premier lieu, l'IAS redonne à l'utilisateur, tel que mentionné, la pleine propriété de ses données personnelles et de ses identifiants numériques (Fedrecheski *et al.*, 2020, p. 1). L'immutabilité, un des principes de l'IAS, des informations liées à l'identité peut être assurée par les signatures numériques de tiers, comme les imprimantes fédérales et les universités, pour certifier la validité de documents (Sedlmeir *et al.*, 2022, p. 9-10). Toutefois, l'immutabilité en elle seule n'est pas suffisante pour les documents d'identité par exemple, car il faut s'assurer de l'authenticité de l'information au moment de la rédaction (Sedlmeir *et al.*, 2022, p. 10). En tant qu'exemple, une preuve de vaccination Covid-19 n'est pas une preuve suffisante d'identité (Sedlmeir *et al.*, 2022, p. 10), elle ne sert qu'à certifier une vaccination. C'est pour cette raison qu'au lieu d'utiliser la blockchain pour stocker une partie ou l'entièreté des informations d'identité d'un individu, plusieurs projets ont décidé d'utiliser des registres distribués hors-chaîne comme substitut pour des informations de l'ordre public (Sedlmeir *et al.*, 2022, p. 10) afin d'assurer que la vaccination puisse être à tout moment mise à jour. À cet effet, l'application de la blockchain est utile pour les informations personnelles sensibles, car elle impose que les échanges d'informations se fassent uniquement de pair-à-pair (Sedlmeir *et al.*, 2022, p. 10), et ce avec un minimum d'informations partagées. En deuxième lieu, sur le plan organisationnel, l'IAS facilite l'authentification et l'identification inter-organisationnelle, améliorant ainsi la souveraineté et l'interopérabilité des données (Sedlmeir *et al.*, 2022, p. 10). L'échange bilatéral d'informations authentiques devrait être un prérequis (Sedlmeir *et al.*, 2022, p. 10) entre les banques. Considérant son principe de transparence, il serait bénéfique pour les banques de cibler les cas de fraude, blanchiment d'argent ou de financement du terrorisme plus

rapidement et se partager ces informations instantanément via un réseau blockchain interbancaire. Cela permettrait de réduire les coûts liés à la gestion des identités et à la vérification des utilisateurs, en automatisant les processus d'authentifications via des certificats cryptographiquement vérifiables (Sedlmeir *et al.*, 2022, p. 10). Dans d'autres cas, les informations posées sur le réseau blockchain interbancaire pourraient être choisies de façon à choisir ce qui mérite d'être transparent ou moins transparent (Sedlmeir *et al.*, 2022, p. 10). Néanmoins, même si l'IAS présente un degré de transparence plus élevé, il n'est pas suffisamment prêt pour des niveaux d'audits à grande échelle ou pour des cas où il n'y a pas d'entité qui valide un échange, puisqu'il n'y a pas encore de solution d'IAS en qui toutes les parties prenantes ont confiance (Sedlmeir *et al.*, 2022, p. 11). En dernier lieu, l'IAS renforce la cybersécurité en limitant les risques de compromission liés aux bases de données centralisées ainsi que les appels frauduleux (Ahmed *et al.*, 2023, p. 4). Dans un système d'IAS, même si une plateforme est attaquée, les identités stockées localement par les utilisateurs restent intactes (Ahmed *et al.*, 2022, p. 18). En stockant les données sensibles des clients hors-chaîne, il devient moins dangereux pour les informations d'identification vérifiables d'être exposées à des risques de fraude alors que les preuves d'intégrité et d'authenticité quant à elles sont sur-chaîne afin de maintenir la vie privée des clients (Ahmed *et al.*, 2023, p. 4-7).

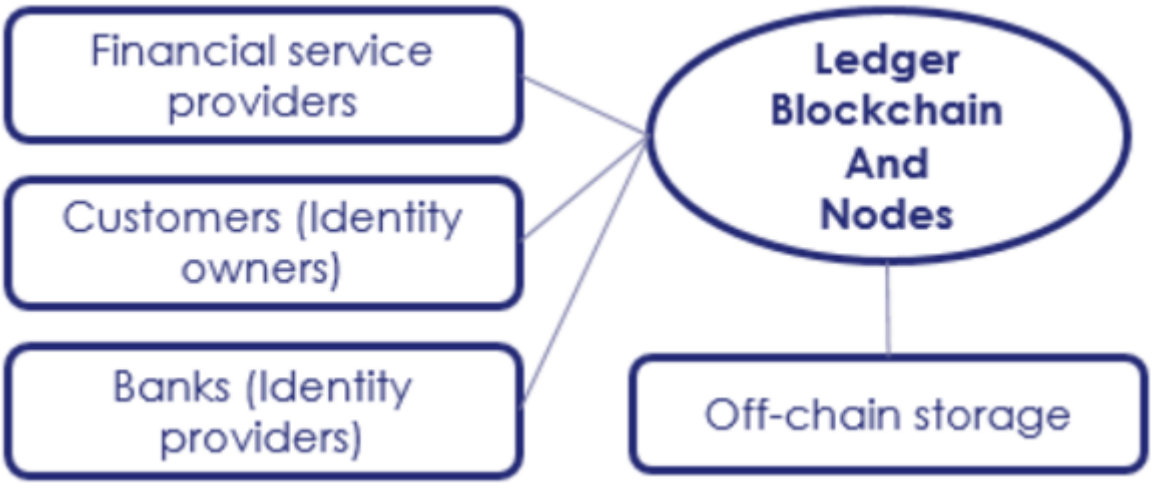


Figure 33 Composantes d'un système basé sur l'IAS (Ahmed et al., 2023, p. 5)

Malgré ses promesses, l'IAS soulève des défis de l'ordre techniques, juridiques et réglementaires. Techniquement parlant, l'un des plus gros enjeux concerne l'interopérabilité entre les différentes implémentations et normes d'IAS. Sans standardisation effective, les risques de fragmentation et d'incompatibilité entre écosystèmes sont élevés. Le statut légal du modèle d'IAS, n'étant pas encore universellement reconnu (Sedlmeir *et al.*, 2022, p. 11), limite l'adoption de l'IAS dans des environnements réglementés comme le secteur bancaire. La charge de responsabilité transférée à l'utilisateur peut devenir problématique. Contrairement aux modèles traditionnels où les institutions encadrent la gestion des données et des identités, le modèle d'IAS implique une bonne gestion des clés privées et publiques (Ahmed *et al.*, 2022, p. 40). Des risques de perte de clés pourrait mettre fortement en péril l'identité numérique considérant qu'il est presque impossible de récupérer les clés privées perdues (Ahmed *et al.*, 2022, p. 18). À cela s'ajoute une dimension sociale : tous les utilisateurs ne disposent pas du même niveau de littératie numérique. Une adoption à grande échelle nécessite un important travail d'éducation, de normalisation et de création d'interfaces « user friendly » pour garantir l'inclusivité du modèle d'IAS. Finalement, bien que l'IAS remette le plein contrôle de l'identité aux utilisateurs, il demeure tout de même une dépendance auprès des fournisseurs d'identité et de services. Le système n'est pas complètement décentralisé, puisqu'il s'appuie sur les mêmes bases que le modèle d'identité centré sur l'utilisateur.

En conclusion, ce modèle répond aux préoccupations croissantes en matière de protection de la vie privée, en particulier, dans un contexte où la surveillance numérique et les violations de données sont devenus des enjeux majeurs. Par exemple, certaines institutions bancaires, comme HSBC, commencent à expérimenter des solutions d'identité numériques décentralisées, tel que Polygon ID, où les clients contrôlent directement leurs informations de vérification d'identité sans passer par une base de données centralisée (Polygon, 2023). En remettant entre les mains des individus le contrôle de leurs données personnelles, l'IAS remet en question les paradigmes traditionnels de gestion de l'identité dominés par les autorités centrales. Si son architecture technique, ses principes et ses fondements s'alignent avec les valeurs d'autonomie, vie privée et sécurité, sa mise en œuvre, quant à elle, demeure confrontée à des défis importants. Néanmoins, l'essor d'initiatives concrètes montre que cette vision est en voie se concrétiser à plus grande échelle.

2.3.2.2 Identifiants décentralisés (IDD)

L'un des principes fondamentaux découlant du modèle d'identité auto-souveraine est l'utilisation des identifiants décentralisés (IDD). Proposé par le World Wide Web Consortium (W3C), les IDDs permettent d'identifier de manière unique chaque entité (personne, chose, entité abstraite, etc.) (Dixit *et al.*, 2022, p. 336). Ils permettent de lier une identité numérique à un individu sans passer par une autorité centrale de gestion. Un IDD est donc un identifiant unique, persistant et auto-administré, généré de manière cryptographique par l'utilisateur lui-même (Chan *et al.*, 2025, p.8). Ce mécanisme permet aux utilisateurs de se créer un identifiant dont ils ont la maîtrise exclusive.

La figure 56 montre l'architecture d'un IDD décentralisé. Cette architecture inclut plusieurs composantes : un identifiant unique (IDD), un document IDD, une méthode IDD et les informations d'identification vérifiables (Brunner *et al.*, 2020, p. 62). La création et l'utilisation d'identifiants décentralisés implique plusieurs participants clés : le fournisseur de services blockchain, l'émetteur d'identité, les utilisateurs et la blockchain elle-même (Bharadwaj *et al.*, 2023, p. 9). Le fournisseur de services est responsable de sélectionner le réseau blockchain pour fournir à l'émetteur d'identité une solution qui facilite les fonctionnalités nécessaires au processus de création d'identité pour l'utilisateur (Bharadwaj *et al.*, 2023, p. 9).

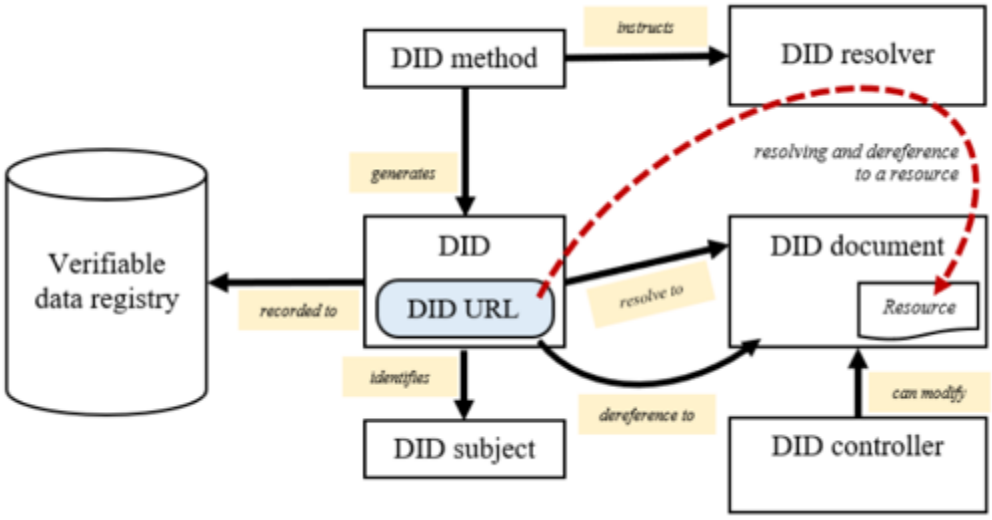


Figure 34 Architecture d'un identifiant décentralisé (Chan et al., 2025, p.9)

Lors de la création d'un ou plusieurs IDDs, ceux-ci incluent dans chacune d'elles une clé publique, partageable publiquement avec d'autres entités, et une clé privée, qui elle doit être conservée par l'utilisateur seulement (Brunner *et al.*, 2020, p. 62). De plus, cet IDD est en réalité une chaîne de caractères, soit les métadonnées, qui est résolue en un document IDD (Chan *et al.*, 2025, p.8). À titre d'exemple, un IDD pourrait prendre la forme suivante : *did:examplechain:123456789* (Chan *et al.*, 2025, p.8). Au sein du document IDD se trouve des informations clés telles que l'IDD, les clés publiques de l'utilisateur, les méthodes d'authentification et les points d'accès (Chan *et al.*, 2025, p.8). L'objectif du document IDD est de donner des informations additionnelles relié à l'IDD pour décrire la structure des clés, les protocoles requis pour l'authentification, les services de points d'accès pour interagir avec l'entité identifiée, l'horodatage pour fins d'audit et une signature JSON numérique (Dib et Toumi, 2020, p. 25). Le document associé à un IDD est ainsi la clé de voûte de l'identité numérique dans un environnement décentralisé. Le document IDD se traduit donc comme étant une interface établissant le canal de communication avec le propriétaire du IDD (Dib et Toumi, 2020, p. 25). La méthode IDD, dans son cas à elle, permet de définir la façon dont le document IDD sera résolu, écrit et mis à jour (Bai et Bisht, 2022, p. 5). À cet effet, tout comme un lien URL, la méthode doit indiquer vers quel réseau distribué il sera résolu pour pouvoir récupérer l'IDD (Brunner *et al.*, 2020, p. 62) grâce au résolveur IDD. En effet, le résolveur IDD permet de retrouver le document IDD associé à un identifiant en utilisant le nom de méthode et l'identifiant spécifique, ce qui rend le système interopérable entre différents réseaux et implémentations. Cette structure repose alors sur des algorithmes cryptographiques, qui permettent d'ancrer l'identifiant à sa clé publique, pour ainsi faciliter l'authentification d'un individu grâce à son IDD, et ce à travers plusieurs applications (Chan *et al.*, 2025, p.8).

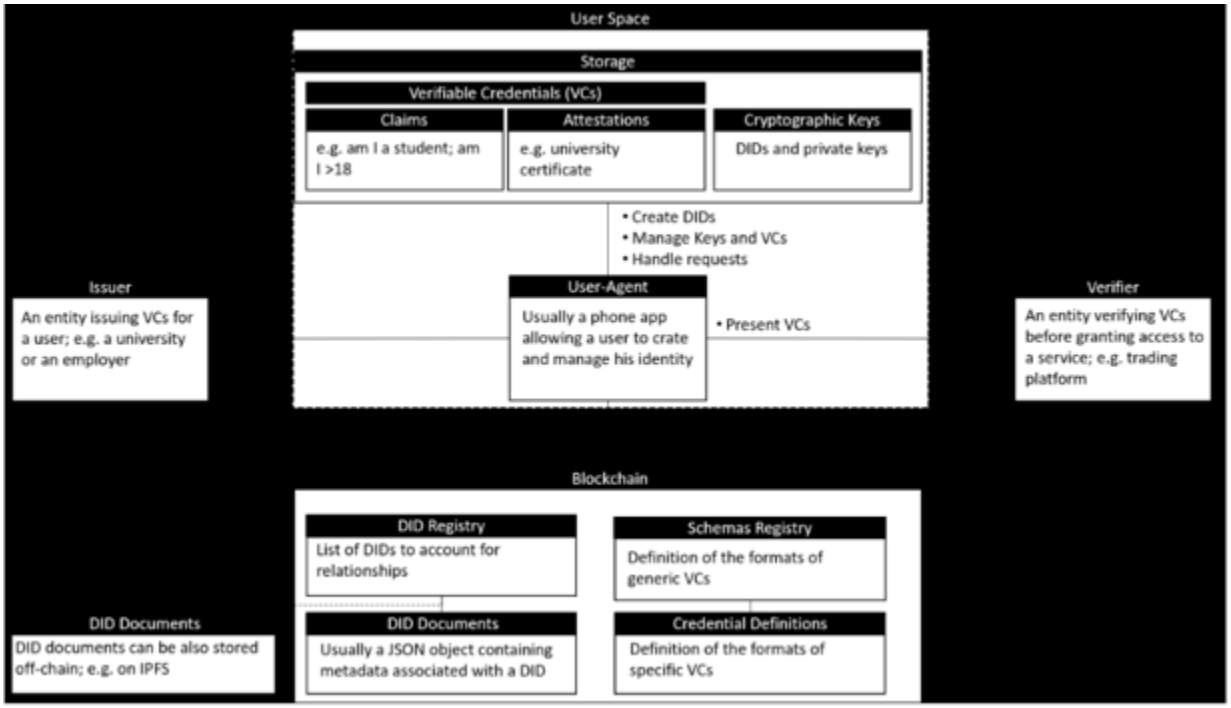


Figure 35 Architecture de l'IAS (Dib et Toumi, 2020, p. 26)

Dans le cadre de l'IAS, les IDDs sont essentiels au bon fonctionnement de l'écosystème, car ils sont la contrepartie cryptographique des informations d'identification vérifiables. D'une part, les IIVs sont stockées hors-chaîne, tel que le démontre la figure 57, tandis que les IDD sont quant à eux sur-chaîne (Dib et Toumi, 2020, p. 26). Lorsqu'un fournisseur d'identité émet une IIV, comme une université, il y joint l'IDD public pour ensuite l'enregistrer sur la chaîne. Les IIVs partagées par l'utilisateur sont ensuite vérifiées par un entité vérificatrice et celle-ci validera l'identité au moyen de l'IDD (Ahmed *et al.*, 2022, p. 11). De manière plus concrète, l'utilisation d'un IDD permet à un individu d'accéder à un service en prouvant qu'il possède les attributs requis par le biais d'attestations vérifiables qui certifie qui l'individu est réellement (Dieye *et al.*, 2023, p. 2).

« Prenons l'exemple de l'obtention d'un prêt hypothécaire auprès d'une institution financière. Dans le scénario actuel, il faut plusieurs itérations de vérifications de pièce d'identité pour prouver l'identité d'un client et son historique de crédit. Cela entraîne un délai considérable pour débloquer les fonds du prêt hypothécaire au client. La raison principale de ce délai d'exécution élevé est l'exigence de conformité en matière de KYC imposée par les institutions financières. Les systèmes KYC actuels comportent de

nombreux contrôles et nécessitent de nombreuses interventions manuelles. Grâce à l'IDD, les institutions financières peuvent vérifier l'identité du client et les exigences KYC via les identifiants qui partagent la clé privée de l'utilisateur (stockée dans son portefeuille) et la clé publique (depuis la blockchain) » (Bharadwaj *et al.*, 2023, p. 9).

En conclusion, les IDD favorisent une nouvelle approche de la gestion de l'identité autant pour les clients que les institutions financières. Ce contrôle accru, remis aux client et utilisateurs, est permis par les portefeuilles numériques dans lesquels les utilisateurs conservent leurs clés privées et leurs IIVs. Grâce à ce mécanisme, les individus peuvent accéder à différents services, qu'ils soient bancaires, gouvernementaux, de santé ou autre, à l'aide de leurs identifiants décentralisés auto-détenteurs et auto-souverains validés cryptographiquement.

2.3.2.3 Informations d'identification vérifiables (IIV)

Les informations d'identifications vérifiables, ou « Verifiable Credentials » selon la terminologie du W3C, représentent la dernière composante du modèle de l'IAS. Il s'agit de données structurées, cryptographiquement sécurisées, qui attestent les attributs relatifs à une entité, qu'il s'agisse d'une personne physique ou d'une organisation, émises par une autorité reconnue et pouvant être validées par une tierce partie (Ahmed *et al.*, 2022, p. 10). Concrètement, les IIVs prennent la forme de certificats numériques contenant un ensemble de déclarations portant sur l'utilisateur, par exemple son nom, sa date de naissance, sa citoyenneté et autres (Brunner *et al.*, 2020, p. 62). Ces données sont signées par l'émetteur via sa clé privée, ce qui garantit leur authenticité. La validité de la signature est ensuite vérifiable au moyen de la clé publique associée à l'IDD de l'émetteur (Fedrecheski *et al.*, 2020, p. 2). L'ensemble de ce processus permet de maintenir une intégrité forte des données tout en assurant une indépendance vis-à-vis des serveurs d'autorités centralisées.

Le processus d'interaction entre les parties repose sur une architecture à trois pôles : le fournisseur d'identité, le détenteur d'identité et le vérificateur, comme illustré dans la figure 58. D'abord, le fournisseur d'identité émet une IIV et enregistre son IDD public sur un registre de données vérifiables (Ahmed *et al.*, 2022, p. 10). Ensuite, l'utilisateur, ou le détenteur, reçoit cette IIV et la stocke dans son portefeuille numérique (Ahmed *et al.*, 2022, p. 10-11). Il en garde la pleine propriété et le contrôle, pouvant décider quand et à qui présenter ses données (Ahmed *et al.*, 2022, p. 10-11). Lorsqu'un service demande une preuve d'identité ou un attribut spécifique, le détenteur peut créer une présentation

vérifiable de l'IIV, c'est-à-dire une version partielle et ciblée de l'attestation, ne révélant que les données strictement nécessaires (Brunner *et al.*, 2020, p. 62). Le vérificateur, de son côté, interroge le registre de données pour valider l'authenticité de l'IIV et de l'émetteur à l'aide du IDD publié (Ahmed *et al.*, 2022, p. 10-11). Ce mécanisme repose sur des techniques cryptographiques telles que les ZKP permettant de prouver une information sans la divulguer intégralement (Fedrecheski *et al.*, 2020, p. 2). Ce processus offre une granularité dans la divulgation des informations, appelée divulgation sélective, qui protège la vie privée tout en assurant la validité de la vérification (Ahmed *et al.*, 2022, p. 10-11).

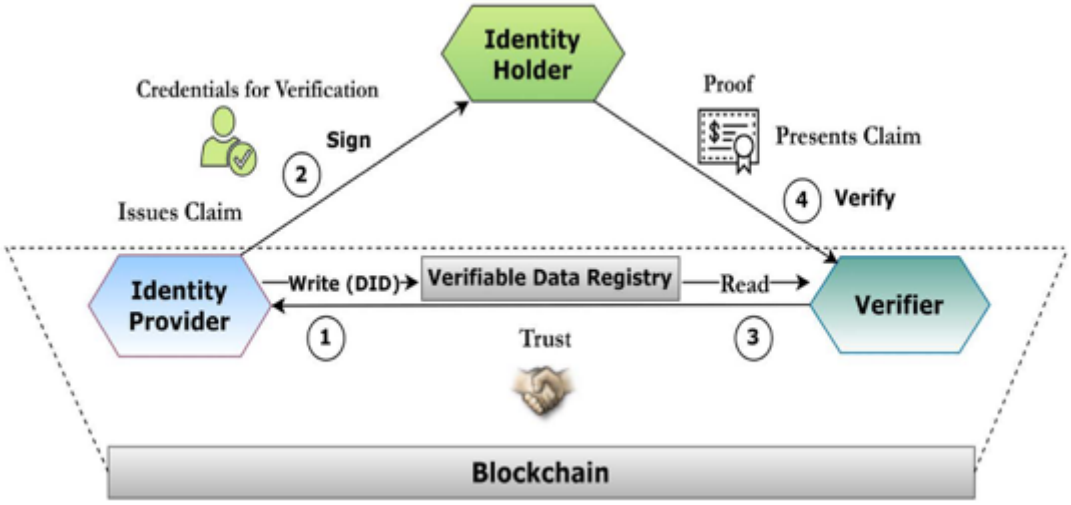


Figure 36 Cadre d'IAS parmi les acteurs d'IIV, c-à-d les acteurs, les fournisseurs d'identité et les vérificateurs (Ahmed et al., 2022, p. 11)

En outre, contrairement aux documents physiques, les IIVs peuvent être utilisées de manière flexible sans duplication des processus de vérification. Par exemple, lorsqu'un utilisateur change d'adresse, il peut mettre à jour son IIV localement et diffuser automatiquement cette mise à jour auprès des services connectés (Dib et Toumi, 2020, p. 24). Les IIVs permettent ainsi de réduire considérablement les frictions dans les échanges d'informations d'identité. Cela dit, les IIVs ne suppriment pas complètement le rôle des tiers de confiance. Comme pour les documents traditionnels, seule une entité reconnue peut émettre une attestation ayant une valeur juridique ou contractuelle. Par exemple, seul un gouvernement peut légalement émettre un passeport, un numéro d'assurance sociale ou une carte d'assurance maladie. L'autorité d'émission conserve également un droit de révocation sur ces informations d'identification (Dib et Toumi, 2020, p. 24).

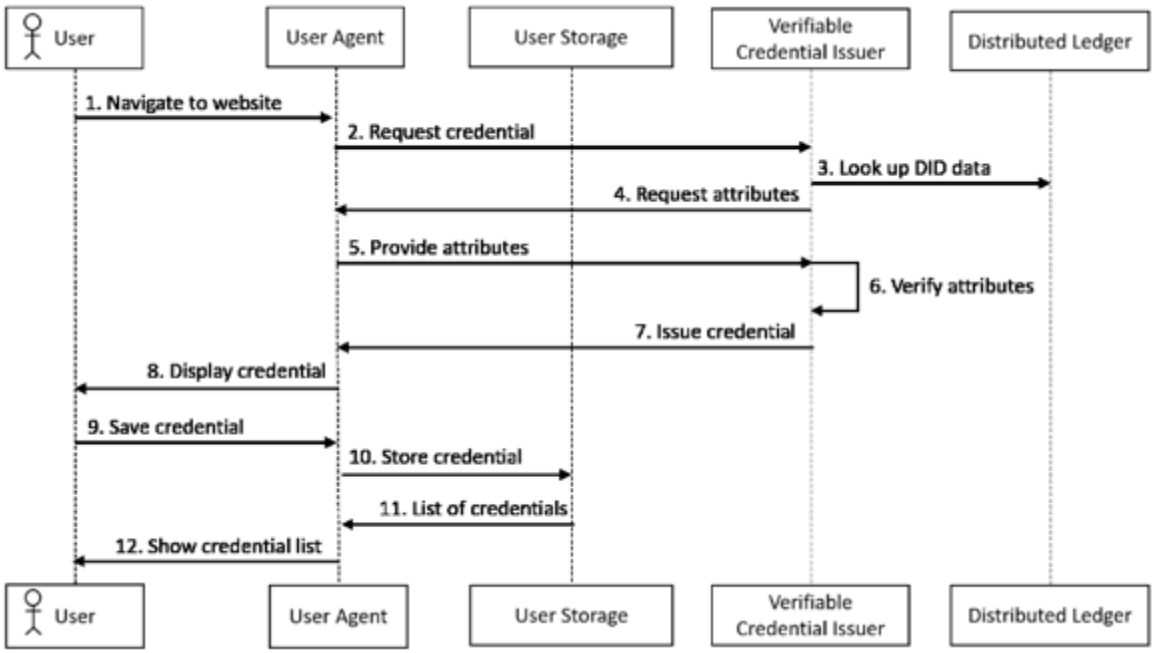


Figure 37 Flux de travail (Dib et Toumi, 2020, p. 27)

En résumé, les IIVs offrent un moyen fiable, sécurisé et privé de valider une information identitaire dans une architecture décentralisée. Ils représentent le vecteur central des interactions entre les différents acteurs de l'écosystème d'IAS et incarnent le passage d'une logique de preuve documentaire multiple à une preuve singulière cryptographique, où l'utilisateur garde le plein contrôle de ce qu'il partage, quand et avec qui. L'intégration des IDD, de l'IAS et des IIVs révèle une synergie puissante pour renforcer l'authenticité et la souveraineté des identités numériques. Dixit et al. (2022) expliquent que les IDD servent de fondation pour les systèmes IAS en facilitant une gestion décentralisée par le contrôle direct des utilisateurs sur les identifiants numériques. Cette fondation est cruciale pour assurer la vie privée, l'interopérabilité et la persistance des identités dans divers environnements numériques.

2.3.3 Solutions existantes de la GIAC dans les SBD

À la lumière des principes fondateurs de l'identité auto-souveraine, les solutions techniques permettant de concrétiser une gestion de l'identité décentralisée se sont multipliés. Ces solutions, qui s'appuient sur la technologie de registres distribués et les standards émis par le W3C tels que les identifiants décentralisés et les informations d'identification vérifiables, visent à implémenter les valeurs fondamentales de la blockchain vis-à-vis de la gestion de l'identité dans notre quotidien. Dans un contexte bancaire, où la

vérification d'identité est un préalable critique à la conformité réglementaire et à la bienveillance des opérations, les systèmes traditionnels arrivent à bout de leurs solutions et celles-ci deviennent de plus en plus désuètes. C'est dans l'optique de renouvellement des approches que des solutions ont émergé pour pallier aux problèmes actuels. Parmi toutes les plateformes ayant une solution existante, nous allons nous concentrer sur : Verified.Me Hyperledger, Sovrin, Polygon ID, Microsoft Entra Verified ID et KERI. Bien qu'issues de milieux variés (ex : fondations à but non lucratif, consortiums open-source, etc.), ces initiatives partagent un même objectif : permettre une authentification fiable, qui respecte la vie privée et interopérable à l'échelle mondiale.

Les sous-sections suivantes analyseront chacune de ces solutions. Pour chaque technologie, nous présenterons son origine, son architecture, son mécanisme de gestion des IDD et des VC, son approche en matière de protection de la vie privée (ex : ZKP, P2P, etc.), son modèle d'identité préconisée ainsi que les cas d'usages bancaires concrets auxquels elle se prête. En mettant l'accent sur l'adoption réelle et leurs bénéfices, nous chercherons à évaluer le pour et le contre pour déterminer dans quelle mesure ces plateformes peuvent répondre à nos objectifs de recherche.

2.3.3.1 Verified.Me

Verified.Me est une solution d'identité numérique développée par SecureKey Technologies en collaboration avec un consortium de grandes institutions financières canadiennes telles que la Banque de Montréal (BMO), la Banque Canadienne Impériale de Commerce (CIBC), Desjardins, la Banque Nationale du Canada, la Banque Royale du Canada (RBC), la Banque Scotia et la Banque TD (Boysen, 2021, p. 1-3). Verfied.Me utilise la plateforme blockchain Hyperledger pour le transfert sécurisé d'informations (Malhotra *et al.*, 2022, p. 28). Par sa gouvernance multisectorielle, ce projet incarne une approche pragmatique d'implémentation de l'identité auto-souveraine (Boysen, 2021, p. 2). L'objectif principal de Verified.Me est de permettre aux citoyens canadiens de partager de manière sécurisée des informations d'identification personnelles (IIP) avec des fournisseurs de services (Boysen, 2021, p. 4). Le système repose sur une architecture hybride, combinant à la fois les paradigmes d'identité fédérée et d'identité auto-souveraine, pour des fins de vérification d'identification numérique (Boysen, 2021, p. 4). Cette approche permet une interopérabilité entre multiples fournisseurs, services récepteurs et systèmes d'identité décentralisée qui adhèrent au même standards (Boysen, 2021, p. 6). Verified.Me se distingue par son modèle de partage de données triple-aveugle : ni la source de l'information, ni sa destination, ni même l'opérateur du réseau n'ont accès à la totalité des données échangées (Boysen, 2021, p. 5). Ce modèle

s'inspire notamment de l'infrastructure blockchain qui assure les principes établis par Allen : les principes IAS (Boysen, 2021, p. 4). La plateforme permet à un utilisateur de récupérer ses informations d'identification auprès de sa banque par exemple, de les stocker dans une application mobile dédiée, puis de les transmettre sur demande à des services tiers, tels qu'un propriétaire d'immeuble, un organisme gouvernemental ou autre. Conforme aux principes de minimisation, de consentement et de protection de la vie privée, chaque transaction nécessite un consentement explicite et actif de la part de l'utilisateur (Boysen, 2021, p. 3).

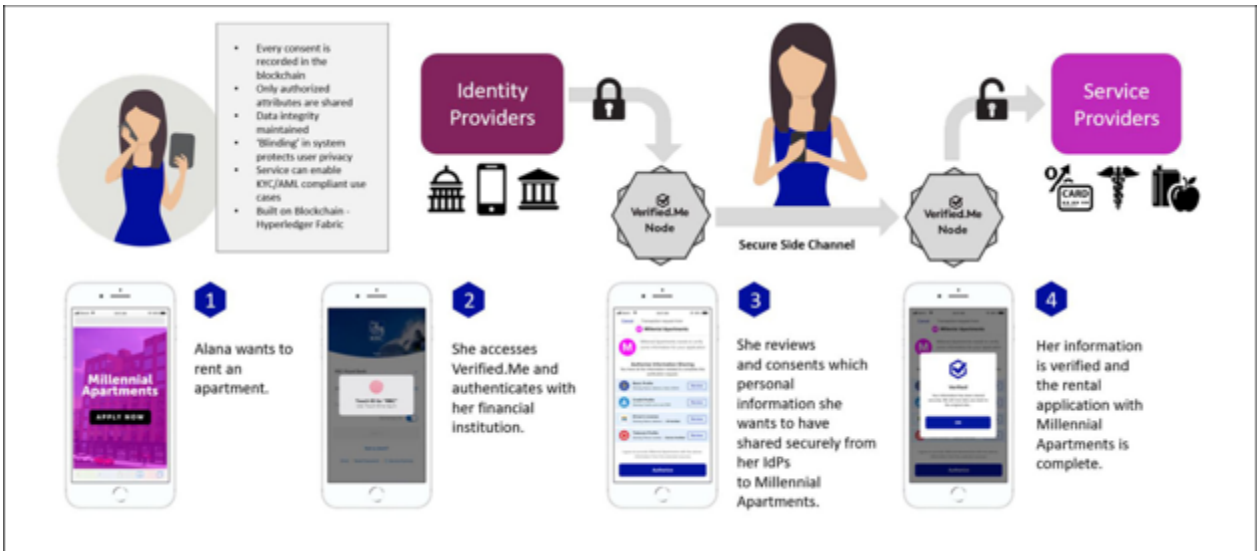


Figure 38 Exemple d'un cas d'utilisation de Verified.Me (Boysen, 2021, p. 3)

En matière de normes et d'interopérabilité, Verified.Me est conforme aux standards établis par le W3C et souhaite adhérer au Decentralized Identity Foundation (Boysen, 2021, p. 6). L'entreprise SecureKey, bien qu'agissant comme opérateur de la plateforme, n'a pas accès aux données des utilisateurs. Elle assume un rôle de facilitateur technologique pour assurer le bon fonctionnement et la sécurité du réseau sans interférer dans les échanges privés. Ce sont les institutions financières qui sont responsables de l'hébergement des composants principaux du réseau et agissent comme l'entité vérificatrice des utilisateurs auprès des fournisseurs de services (Boysen, 2021, p. 6). Considérant le manque d'un cadre de gouvernance entre les fournisseurs d'identité et les fournisseurs de services, Verified.Me prévoit des

règles communes définies par un accord multilatéral entre les parties prenantes (Boysen, 2021, p. 6). Cela permettra de bâtir une confiance mutuelle de protection des renseignements personnels et de conformité aux lois provinciales et fédérales. De plus, Verified.Me s'inscrit dans le cadre du Pan-Canadian Trust Framework (PCTF), une initiative du Digital ID and Authentication Council of Canada (DIACC) visant à établir des standards d'interopérabilité et de confiance pour les solutions d'identité numérique au Canada. La mise en œuvre de Verified.Me révèle également plusieurs enseignements clés. D'une part, le projet démontre la faisabilité d'une solution basée sur l'IAS dans un environnement réglementé comme les banques au Canada. D'autre part, il souligne l'importance d'une gouvernance partagée entre les secteurs publics et privé (Boysen, 2021, p. 6). Toutefois, la solution n'est pas sans défis. La complexité de la coordination intersectorielle, la lenteur relative de l'adoption et l'incertitude en matière de responsabilité figurent au sommet des difficultés à rencontrer (Boysen, 2021, p. 6-7).

En somme, Verified.Me incarne une première étape concrète vers la mise en œuvre d'une infrastructure d'identité décentralisée viable, respectueuse des standards internationaux et adaptée aux spécificités du marché canadien. Elle offre un modèle soucieux de la vie privée et reproductible pour d'autres juridictions cherchant à concilier innovation technologique, respect de la vie privée et exigences réglementaires.

2.3.3.2 Hyperledger

Hyperledger constitue un projet de la fondation Linux visant à promouvoir le développement de technologies blockchains à des fins applicatives (Doğan et Karacan, 2023, p. 5). Il s'agit d'un écosystème open-source regroupant plusieurs frameworks, outils et bibliothèques destinés à construire des applications blockchain robustes, modulaires et interopérables (Doğan et Karacan, 2023, p. 5). Dans le contexte spécifique de la gestion de l'identité et des accès des clients (GIAC) dans les systèmes bancaires décentralisés, trois projets Hyperledger méritent une attention particulière : Hyperledger Indy, Hyperledger Aries et Hyperledger Fabric.

Tout d'abord, Hyperledger Indy est une plateforme uniquement conçue pour les identités numériques décentralisées et les informations d'identification vérifiables avec une approche basé sur le modèle d'identité auto-souveraine (Doğan et Karacan, 2023, p. 5). Dérivée initialement du code source développé par Evernym en 2012, elle a été confiée à la Sovrin Foundation en 2018 avant d'être intégrée à Hyperledger (Bharadwaj *et al.*, 2023, p. 14). Indy repose sur un registre distribué public et permissionné (Abdelgalil et Mejri, 2023, p. 6), destiné à stocker les identifiants décentralisés (IDDs), les schémas de données, les

définitions d'accréditation et les registres de révocation (Harrell *et al.*, 2022, p. 3). Ce système permet aux utilisateurs de générer et de gérer leurs propres IDDs, d'autoriser l'accès à leurs informations et d'effectuer des mises à jour ou révocation selon leurs besoins (Bai et Bisht, 2022, p. 5). Elle est offre une solution alternative au KYC via une infrastructure à clé publique décentralisée (Malhotra *et al.*, 2022, p. 15). Étant alignée avec les standards du W3C, la plateforme favorise l'interopérabilité avec d'autres réseaux et solutions blockchain (Abdelgalil et Mejri, 2023, p. 6).

Ensuite, pour faciliter les communications entre agents et la gestion des flux de justificatifs, Hyperledger Aries joue un rôle complémentaire à Indy. De nature open-source (Mazzocca *et al.*, 2025, p. 8), Il offre une interface à Indy en plus d'un ensemble d'agents et d'APIs (RESTful) pour le stockage, la transmission et la vérification d'information d'identification vérifiables (Harrell *et al.*, 2022, p. 5). Plusieurs agents sont disponibles pour les environnements mobiles ou serveurs, comme Aries Cloud Agent – Python, Aries Framework .NET ou Aries Static Agent - Python, tous deux intégrant Indy SDK (Mazzocca *et al.*, 2025, p. 8). Ce sont des agents qui peuvent déployer en production et respectivement être utilisés pour toutes les applications non-mobiles, bâtir des agents mobiles ainsi que pour configurer des agents (Mazzocca *et al.*, 2025, p. 8). Aries intègre également des bibliothèques compatibles avec plusieurs langages de programmation pour bâtir des applications d'identité décentralisée (Mazzocca *et al.*, 2025, p. 8). Hyperledger Ursa complémente davantage ces bibliothèques en proposant des bibliothèques cryptographiques partagées qui permettent d'éviter les redondances entre projets Hyperledger et de standardiser l'implémentation de primitives cryptographiques (Doğan et Karacan, 2023, p. 5). Ensemble, ils renforcent la robustesse et la cohérence des systèmes construits à partir des différents composants Hyperledger.

Enfin, bien que Fabric ne soit pas spécifiquement conçu pour la gestion d'identité, il demeure pertinent dans les architectures hybrides. Développé par la Linux Foundation (Abdelgalil et Mejri, 2023, p. 6) en collaboration avec IBM en 2015, Hyperledger Fabric est un registre distribué permissionné, modulaire et extensible, qui supporte l'exécution de contrats intelligents, appelés « chaincode », le contrôle d'accès granulaire et une faible latence transactionnelle pour les applications en entreprise (Doğan et Karacan, 2023, p. 5-6 ; Malhotra *et al.*, 2022, p. 27). Son modèle de gouvernance décentralisée est adapté aux consortiums interbancaires, car il permet, par exemple, de gérer des règles d'accès à des données d'identité en fonction du rôle des participants.

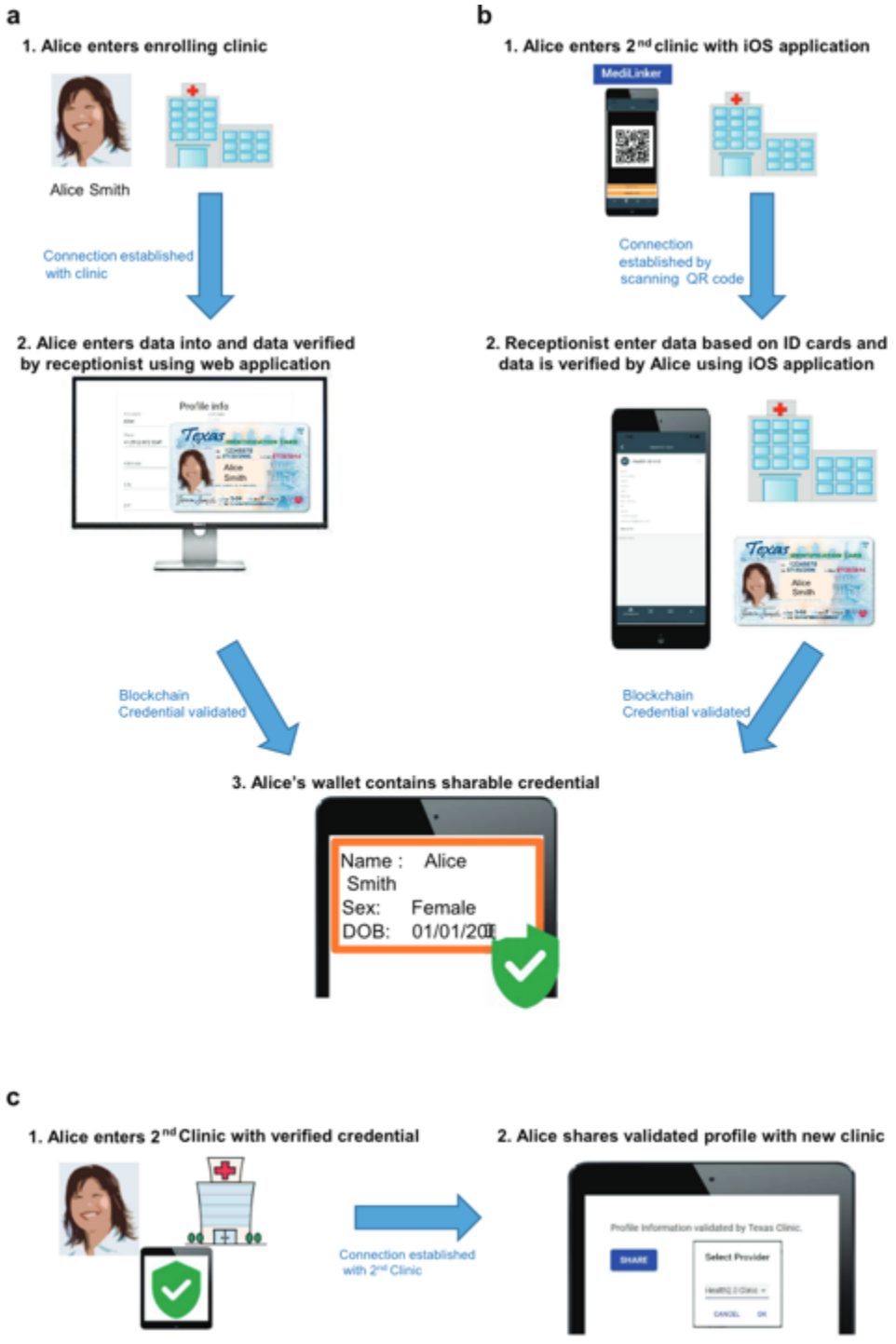


Figure 39 Flux de travail cliniques & processus de vérification bidirectionnelle de MediLinker (Harrell et al., 2022, p. 6)

Bien qu'il n'existe pas de solution actuelle dans le domaine bancaire, le système MediLinker, conçu pour la gestion d'identités dans le domaine de la santé, illustre la capacité d'Hyperledger à répondre aux exigences d'interopérabilité, de sécurité, de confidentialité et d'autonomie des utilisateurs (Harrell *et al.*, 2022, p. 10). En s'appuyant sur Hyperledger Indy pour la gestion des identités et sur Aries comme couche d'interaction, MediLinker a permis aux patients de contrôler leurs données médicales tout en facilitant leur partage avec les fournisseurs de soins utilisateurs (Harrell *et al.*, 2022, p. 5-10). Ce cas d'utilisation démontre l'applicabilité du modèle d'identité décentralisée dans des environnements sensibles aux enjeux réglementaires pouvant être transposés au secteur bancaire.

En somme, Hyperledger propose un écosystème cohérent et modulaire adapté aux exigences des banques en matière de GIAC. Grâce à l'interopérabilité de ses composants, sa compatibilité avec les standards ouverts et ses capacités de gestion fine des identités, Hyperledger constitue une base technologique solide pour le développement de solutions bancaires décentralisées centrées sur l'utilisateur.

2.3.3.3 Sovrin

Sovrin constitue l'un des premiers réseaux à avoir été spécifiquement conçu pour répondre aux exigences du modèle d'identité auto-souveraine, en s'appuyant sur une infrastructure décentralisée et des standards ouverts. Bâti sur le registre distribué permissionné Hyperledger Indy, Sovrin incarne une solution de référence open-source pour la gestion des identités numériques décentralisées dans les systèmes bancaires décentralisés du futur. Le réseau Sovrin, basé sur un modèle d'identité auto-souveraine qui propulse les concepts d'identifiants décentralisés et d'informations d'identification vérifiables, repose sur une architecture publique permissionnée et facilite la création, la gestion et la vérification des identités (Parry et Ellul, 2024, p. 15). Cela signifie que, bien que toute personne puisse interroger le registre, au moyen de transactions de lecture, seules des entités préapprouvées, appelées « stewards », ont le droit d'écrire sur la chaîne (Ahmed *et al.*, 2022, p. 13). Ces stewards sont sélectionnés par un conseil de fiduciaires selon un processus de gouvernance établi dans le Sovrin Trust Framework (Ahmed *et al.*, 2022, p. 13 ; Bharadwaj *et al.*, 2023, p. 14). Ils peuvent écrire, distribuer et répliquer l'identité des nœuds autorisés selon le consentement de l'utilisateur grâce à la preuve de divulgation nulle ou sélective (ZKP) (Bai et Bisht, 2022, p. 6). Cette gouvernance décentralisée permet d'assurer la robustesse du réseau tout en limitant les risques liés à une autorité centrale unique. Chaque entité dans Sovrin génère un IDD, soit une chaîne de caractère unique et persistante associée à une clé publique (Kaneriya et Patel, 2020, p. 3). Puis, les nœuds de validation et d'observation peuvent respectivement effectuer des transaction

d'écriture ainsi que répondre aux demandes de lecture (Kaneriya et Patel, 2020, p. 3). En accord avec les principes fondamentaux de l'IAS, Sovrin ne stocke aucune donnée personnelle sur la chaîne même de manière chiffrée (Kaneriya et Patel, 2020, p. 3). Or, aucune corrélation est possible entre un IDD et une entité participante à la chaîne, puisque l'IDD ne contient que des informations du document IDD, soit des métadonnées publiques, alors que les attributs personnels sont gardés hors-chaîne sur la clé privée (Kaneriya et Patel, 2020, p. 3).

Sovrin utilise le protocole de consensus Plenum (Tobin *et al.*, 2017, p. 16), une variante du protocole de tolérance de défaillance byzantin, pour assurer la validité des transactions. De plus, Sovrin permet la création de plusieurs identités pseudonymes pour un même utilisateur, chacune liée à une paire de clés asymétriques distincte, pour mitiger le risque de corrélation entre les participants et leurs IDD (Sousa *et al.*, 2022, p. 11). Ce principe contribue au droit à l'oubli, à une meilleure performance, la capacité à dissocier l'IDD des individus et à adopter les bonnes pratiques d'Ethereum et du protocole de tolérance de défaillance byzantin (Sousa *et al.*, 2022, p. 11). Malgré ses atouts, Sovrin présentes des limites. L'absence de services d'authentification intégrés, la complexité de son architecture, l'utilisation de primitives cryptographiques un peu plus anciennes et aucun support pour les contrats intelligents sont régulièrement pointées du doigt comme des défis à surmonter (Bai et Bisht, 2022, p. 6). De plus, la dépendance à des entités intermédiaires, bien qu'encadrée par un cadre de confiance, peut remettre en question les principes de consentement et de souveraineté de l'utilisateur (Dib et Toumi, 2020, p. 29).

En résumé, Sovrin constitue une solution pionnière dans la mise en œuvre du modèle d'IAS au sein des systèmes décentralisés. Grâce à sa gouvernance distribuée, Sovrin s'impose comme une référence en matière d'identité numérique. Selon Chan et al. (2025), Sovrin figure au sommet de la liste des projets d'identité auto-souveraine comparés. Elle démontre donc une bonne opportunité pour les entreprises désirant se tourner vers des solutions décentralisées.

Project	Open Source	Blockchain Type	Storage	Future Enhancements	Security Features	Fit for Academic Domain
Sovrin [112]	Yes	Public Permissioned (Hyperledger Indy)	Distributed ledger, on/off-chain storage (e.g., encrypted cloud storage)	Integration with other decentralised networks, enhance privacy features	Decentralised identity ledger, zero-knowledge proofs, strong cryptography	**Excellent**: Strong focus on privacy and verifiable credentials, suitable for academic certificates and transcripts
uPort [111]	Yes	Public (Ethereum)	On-chain for identifiers, off-chain for data (IPFS, encrypted cloud storage)	Enhanced interoperability, scalability solutions	Decentralised identifiers (DIDs), verifiable credentials, smart contracts	**Good**: Ethereum's smart contracts can manage academic credentials, but scalability may be an issue
EverID [92]	No, proprietary	Private, proprietary	Off-chain (secure cloud storage)	Expansion into financial services and healthcare	Biometric verification, secure document storage, multi-factor authentication	**Moderate**: Focus is more on financial services and healthcare
LifeID [92]	Yes	Public (Ethereum)	On-chain for identifiers, off-chain for data (IPFS, encrypted cloud storage)	Improved privacy protocols, wider adoption	Decentralised identifiers (DIDs), verifiable credentials, smart contracts	**Good**: Ethereum-based solution with strong security, suitable for academic credentials
Sora [117]	Yes	Public (Polkadot)	On-chain for identifiers, off-chain for data (IPFS, encrypted cloud storage)	Integration with Polkadot ecosystem, more DeFi applications	Decentralised identifiers (DIDs), verifiable credentials, cross-chain identity	**Good**: Decentralised IDs and verifiable credentials suitable for academic records
SelfKey [92]	Yes	Public (Ethereum)	On-chain for identifiers, off-chain for data (IPFS, encrypted cloud storage)	Cross-chain interoperability enhanced KYC solutions	Decentralised identifiers (DIDs), verifiable credentials, hardware wallet integration	**Good**: Ethereum-based solution with strong identity verification features suitable for academic use
ShoCard [110,113]	No, proprietary	Public (Ethereum)	Off-chain (encrypted cloud storage)	Expansion into more industries, enhanced biometric authentication	Biometric verification, secure document storage, multi-factor authentication	**Moderate**: Primarily focused on financial services and enterprise use cases
WeIdentity [110]	No, proprietary	Public (Consortium, FISCO-BCOS)	On-/off-chain (consortium-managed storage)	Greater integration within the consortium blockchain, enhanced privacy, and security features	Decentralised identifiers (DIDs), verifiable credentials, consortium blockchain security	**Good**: Consortium blockchain offers strong security and privacy, suitable for academic records

Figure 40 Comparaison des projets d'IAS (Chan *et al.*, 2025, p. 24)

2.3.3.4 Polygon ID / Privado ID

Parmi les solutions émergentes de gestion décentralisée de l'identité, Polygon ID, un portefeuille d'identité numérique, se distingue par son ancrage dans l'écosystème Web3 et son utilisation avancée de la cryptographie à connaissance nulle (zkSNARK) (Raipurkar *et al.*, 2023, p. 614). Développé par les créateurs de la blockchain Polygon, cet outil vise à offrir une identité numérique auto-souveraine, privée par défaut, et interopérable avec les applications décentralisées (Raipurkar *et al.*, 2023, p. 614). À la base de Polygon ID se trouve un modèle d'IAS où ce sont les contrats intelligents qui vérifient les identités dans le système (Bharadwaj *et al.*, 2023, p. 14). Les utilisateurs peuvent générer des identifiants décentralisés qu'ils contrôlent eux-mêmes (Luís *et al.*, 2024, p. 3). Ces IDDs sont enregistrés sur la blockchain Polygon et utilisés pour associer des informations d'identification vérifiables émises par des parties tierces, puis stockées localement dans le portefeuille numérique Polygon ID (Luís *et al.*, 2024, p. 3). Ce portefeuille, disponible sur Android et iOS, permet à l'utilisateur de gérer ses IIV de manière sécurisée tout en contrôlant la divulgation des informations (Patil *et al.*, 2024, p. 5). La principale innovation de Polygon ID

réside dans l'application des preuves à divulgation nulle de connaissance (ZKP) (Raipurkar *et al.*, 2023, p. 614). Grâce à cette technologie un utilisateur peut prouver à un fournisseur de services qu'il possède une caractéristique, comme être majeur, sans révéler l'ensemble de ses données personnelles, comme sa date naissance (Raipurkar *et al.*, 2023, p. 614). Polygon ID repose aussi sur deux piliers technologiques principaux : le protocole Iden3, qui structure la logique des identités et des interactions entre agents, et Circom, une boîte à outil de circuits cryptographiques permettant de générer des preuves zkSNARK (Raipurkar *et al.*, 2023, p. 614).

Figure 41 Solution d'architecture Polygon ID (Bharadwaj *et al.*, 2023, p. 14)

Par ailleurs, aujourd'hui l'écosystème de Polygon ID s'inscrit dans une dynamique plus large de développement d'outils d'identité décentralisée. Initialement développé par Polygon Labs, Polygon ID a récemment évolué pour devenir Privado ID et il est désormais encore plus interopérable considérant qu'il n'est plus limité à Polygon (Opiah, 2024). Privado ID propose à la fois une approche résolument tournée vers l'intégration institutionnelle et l'adoption sur-chaîne (Opiah, 2024). Parmi les nouvelles fonctionnalités clés de la plateforme Privado ID figurent la vérification d'identité intégrée aux applications, l'émission d'attestations réutilisables pour des cas d'utilisation comme la vérification d'âge, les processus KYC et les processus de connaissance d'entreprise (Opiah, 2024). Privado ID présente une visualisation graphique du parcours de l'utilisateur avec des démonstrations basées sur la biométrie faciale en 3D

(Opiah, 2024). Toujours basé sur le concept de ZKP, Privado ID se positionne comme un acteur stratégique pour la finance décentralisée. L'entreprise multiplie les partenariats avec des organisation sur et hors-chaîne, notamment à travers des projets pilotes avec plusieurs institutions financières multinationales (Opiah, 2024). Parmi ces institutions, nous y retrouvons les banques HSBC et Deutsche Bank

Ces deux projets pilotes démontrent la pertinence de Polygon ID et Privado ID dans le monde bancaire traditionnel. D'une part, la banque HSBC a annoncé l'intégration de Polygon ID dans sa stratégie d'identité numérique. L'objectif est d'exploiter les ZKP pour permettre l'ouverture de compte interne (Polygon, 2023). « Lorsqu'un client ouvre un compte HSBC, la banque effectue une vérification KYC et crée une preuve d'identité vérifiée, qui peut ensuite être utilisée pour un certain nombre de transactions, notamment à la connexion à un compte HSBC, les achats, la demande de prêt, les crédits carbone, et bien plus encore, afin de l'utiliser auprès d'émetteurs d'identité (agences gouvernementales, services publics, etc.) » (Polygon, 2023). D'autre part, Deutsche Bank, dans une étude de faisabilité menée en collaboration avec Polygon Labs, a exploré l'application de Polygon ID à la gestion de l'identité des clients dans un environnement bancaire multi-juridictionnel. Le rapport a conclu que la preuve de concept offre une réduction des risques réglementaires, une interopérabilité renforcée avec les systèmes KYC/LCBA existants et une souveraineté accrue pour les clients en matière de contrôle de leurs données (Noone *et al.*, 2024, p. 27-32).

En somme, Polygon ID et Privado ID incarne une nouvelle génération de systèmes d'identité décentralisée. Par son architecture modulaire, son respect des normes d'IAS et son orientation vers la confidentialité, il s'inscrit comme une alternative crédible pour les institutions financières soucieuses de redonner à l'individu le contrôle de son identité numérique.

2.3.3.5 Key Event Receipt Infrastructure (KERI)

Le « Key Event Receipt Infrastructure » représente une avancée significative dans l'évolution des systèmes d'identification auto-souveraine en rupture avec la logique des infrastructures de confiance centralisées ou même des registres immuables comme les blockchains publiques. Développé par Samuel M. Smith et ses collaborateurs, KERI propose une infrastructure de gestion des clés totalement décentralisée (DPKI[23]), fondée sur des évènements de changement de clés attestables et sur une vérification par consensus des

[23] DKMI est un acronyme pour « Decentralized Key Management Infrastructure

évènements clés (Jackson et Taiuru, 2023, p. 14). Un objectif fondamental de KERI est de réduire la surface d'attaque inhérente à l'infrastructure de l'Internet actuel, notamment les failles liées aux DNS[24], aux certificats centralisés ou services cloud (Smith, 2021, p. 5). En plaçant la sécurité au niveau des identifiants et de leur gestion autonome, KERI offre une alternative où l'autorité ne dépend plus d'un tiers, tel qu'un fournisseur d'identité, mais de l'utilisateur lui-même et de la cryptographie (Boi *et al.*, 2024, p. 162). Par conséquent, aucune autre source de confiance n'est requise au-delà du détenteur de la clé privée, soit l'utilisateur, et sa paire de clé (Boi *et al.*, 2024, p. 162). KERI est dès lors une méta-plateforme open-source, interopérable avec des applications Web 3.0, de l'Internet des Objets et autres, qui forme une couche de confiance transversale minimalement suffisante à l'Internet (Jackson et Taiuru, 2023, p. 14). Contrairement aux approches classiques fondées sur des identifiants dépendants d'une plateforme ou d'un fournisseur, KERI permet à chaque entité de générer un identifiant auto-certifiant (IDAC), dont la validité est démontrable par une racine de confiance primaire, qui sont fortement liés lors de leur émission à une paire de clés, publique et privée, signée cryptographiquement (Smith, 2021, p. 5). Dans KERI, il existe une deuxième racine de confiance : les témoins. Ceux-ci sont entités tierces choisies librement par le titulaire de l'identifiant pour vérifier, signer et conserver les évènements de clés, en jouant un rôle similaire à celui des notaires (Smith, 2021, p. 58). « Le but d'un témoin est de protéger le titulaire de l'identifiant contre toute exploitation externe de son identifiant » (Smith, 2021, p. 58). Ce modèle vise à répondre aux limites des systèmes de gestion de l'identité centralisés ou même des IAS fondées sur des blockchain, en assurant la portabilité, l'autonomie et la vérifiabilité sans infrastructure de confiance extérieure (Boi *et al.*, 2024, p. 162).

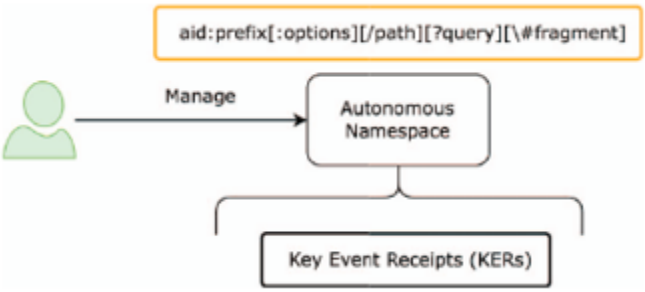


Figure 42 Architecture KERI (Boi et al., 2024, p. 163)

[24] DNS est un acronyme pour système de nom de domaine ou « Domain Name System »

Au cœur de l'infrastructure KERI se trouve l'identifiant auto-certifiant, une chaîne encodée mathématiquement dérivée des propriétés de la cryptographie de la clé publique asymétrique à laquelle il est lié (Smith, 2021, p. 5), rendant toute falsification ou substitution impossible sans possession de la clé privée correspondante. Ces IDACs sont inscrits dans un formalisme d'identifiants autonomes (IDA), qui eux font partie d'un système d'un système d'identité autonome (SIA), pour permettre à l'utilisateur de posséder un contrôle cryptographique exclusif sur l'identité créée (Jackson et Taiuru, 2023, p. 14). Ainsi, les trois propriétés importantes de l'IDAC sont : 1) une racine de confiance cryptographiquement sécurisée et autonome, 2) un contrôle décentralisé via la gestion des clés privées et 3) des identifiants universellement uniques (Jackson et Taiuru, 2023, p. 14). Un des mécanismes fondamentaux de KERI pour garantir la sécurité à long terme des identifiants est la rotation cryptographique des clés. Chaque clé publique associée à un identifiant auto-certifiant est conçue pour être temporaire et une clé suivante est définie à l'avance, pré-rotation, chiffrée puis révélée uniquement lors de l'évènement de rotation afin de mitiger la compromission des clés (ex : perte, vol, oubli) (Jackson et Taiuru, 2023, p. 14). La rotation constitue donc un niveau de protection plus robuste que jamais contre l'usurpation. KERI est donc en mesure de suivre plusieurs évènement clés au travers de messages d'évènements qui incluent notamment la rotation, mais aussi l'Inception, les interactions, le début de délégation et la rotation de délégation (Boi *et al.*, 2024, p. 163).

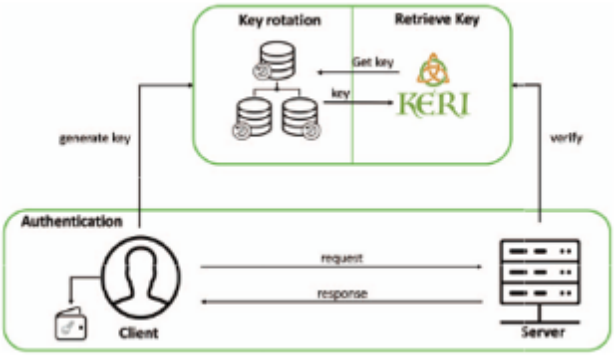


Figure 43 Architecture globale (Boi et al., 2024, p. 164)

KERI permet d'une part l'évènement d'interaction. L'évènement d'interaction est un évènement de clé qui permet de lier des messages ou des actions à un identifiant pour certifier qu'ils ont été produit par l'identifiant sans modifier les clés ou l'état de l'identité (Smith, 2021, p. 49).

Figure 44 Message d'évènement d'interaction de base (Smith, 2021, p. 50)

D'autre part, KERI permet dans ses évènements la délégation d'identifiants, c'est-à-dire la création d'un sous-identifiant par un identifiant parent, avec traçabilité des relations hiérarchiques, pour établir une relation où une entité reçoit l'autorité d'agir au nom d'une autre entité (Smith, 2021, p. 50).

Figure 45 Évènement de délégation (Smith, 2021, p. 50)

Grâce à sa logique d'auto-certification par évènements, KERI peut fonctionner au sein de n'importe quel système capable de stocker et restituer un journal ou un historique. Toutefois, malgré ses avantages conceptuels, KERI soulève des défis. D'abord, sa proposition de s'affranchir complètement des registres et des tiers de confiance implique une complexité technique élevée, tant pour les développeurs que pour les utilisateurs finaux (Keller, 2024, p.6). L'autogestion de la sécurité cryptographique, en particulier la rotation et la conservation des clés, nécessite certaines compétences numériques qui ne sont pas encore maîtrisée par tous. En second lieu, bien que KERI se présente comme une solution souveraine, il reste une tension entre autonomie maximale et dépendance à certaines infrastructures physiques pour stocker les journaux et synchroniser les témoins. Par ailleurs, l'absence de standardisation large rend encore difficile l'adoption de KERI dans les systèmes d'information classiques (Keller, 2024, p.4) . En dépit de sa compatibilité avec le RGPD, certaines critiques portent sur la difficulté de concilier la délégation complexe

d'identifiants et les exigences de transparence ou de révocabilité exigées dans des contextes juridiques sensibles.

En conclusion, KERI s'impose comme une réponse ambitieuse et novatrice aux limites structurelles des systèmes d'identité numérique auto-souveraine fondés sur des blockchain. En proposant une architecture légère, évènementielle et indépendante de toute infrastructure centralisée, il offre un contrôle granulaire sur l'identité et sur la gestion cryptographique des identifiants, tout en répondant aux exigences modernes de portabilité, de conformité réglementaire et d'interopérabilité. Malgré les défis liés à sa complexité technique et à son adoption encore limitée, KERI représente une avancée décisive dans la construction d'un écosystème réellement décentralisé où l'identité n'est plus imposée ni hébergée, mais véritablement possédée par l'individu.

2.4 Conclusion de la revue de littérature

La revue de littérature a permis d'identifier certains avantages et défis associés à l'adoption de la blockchain dans la gestion de l'identité numérique, les processus KYC et les systèmes CRM. Ces avantages incluent une plus grande transparence, une meilleure traçabilité sécurisée des échanges d'informations, une réduction des coûts d'intermédiation, ainsi qu'un renforcement du contrôle par l'utilisateur sus ses données personnelles. Du côté des défis, les enjeux de scalabilité, d'interopérabilité, de gouvernance et d'acceptabilité organisationnelle demeurent importants. Ces constats proviennent majoritairement des réflexions théoriques ou de projets pilotes encore peu matures, ce qui limite la généralisation des résultats à des environnements bancaires complexes et régulés Il apparaît dès lors pertinent de poursuivre les recherches autour des applications concrètes et opérationnelles de la blockchain dans les systèmes de gestion de l'identité décentralisée (IDD, IAS, IIV), en s'appuyant sur des études longitudinales, des retours d'expérience sectoriels et des expérimentations réelles. De plus, l'évaluation de l'impact organisationnel, technologique et humain d'une telle réingénierie des processus bancaires constitue un champ d'investigation encore peu exploré dans la littérature.

Par ailleurs, la littérature existante traite encore de manière marginale des conséquences réglementaires et juridiques liées à l'intégration de la technologie blockchain dans le secteur bancaire canadien. Bien que certaines publications abordent des notions connexes telles que la conformité RGPD, les responsabilités

contractuelles des parties dans les contrats intelligents ou encore les exigences de connaissance client, aucune synthèse ne permet à ce jour de cartographier les risques et obligations réglementaires associés à l'usage de solutions décentralisés dans un cadre bancaire, et encore moins canadien. La méthodologie de cette recherche ne se penchera donc pas sur les implications réglementaires détaillées, notamment celles concernant la conformité aux législations locales et internationales ou le cadre juridique des contrats intelligents par exemple, pour laisser ces dimensions à des études futures centrées sur les enjeux légaux.

Pour conclure, la revue a mis en lumière les limites des approches traditionnelles, centralisées et fédérées, qui dominent encore aujourd'hui la gestion de l'identité, en soulignant leur vulnérabilité en matière de sécurité, leur manque d'interopérabilité et leur incapacité à garantir un contrôle effectif des utilisateurs sur leurs données personnelles. À l'inverse, les identifiants décentralisés, l'identité auto-souveraine et les informations d'identification vérifiables offrent des perspectives prometteuses en matière de traçabilité, de transparence et d'autonomisation des utilisateurs, tout en réduisant certains coûts liés à l'intermédiation et à la vérification de l'identité. Toutefois, la littérature révèle que ces solutions demeurent largement à l'état embryonnaire, de projet pilote ou de démonstration technologique et que leur intégration concrète dans les systèmes bancaires complexes, particulièrement au Canada, soulève de nombreux défis techniques, organisationnels et humains. Ce constant met en évidence la nécessité d'approfondir la recherche sur les modalités d'implémentation réelle de ces technologies dans un contexte bancaire, en tenant en compte des contraintes opérationnelles, des résistances au changement et des enjeux de gouvernance. Cette revue fournit ainsi une base essentielle pour orienter la présente recherche, qui vise à comprendre comment l'intégration des IDD peut transformer la gestion de l'identité numérique au sein d'une banque canadienne. Elle permettra d'identifier les lacunes des processus actuels, d'évaluer les bénéfices et les limites d'une réingénierie fondée sur la blockchain et d'explorer la manière dont les décideurs perçoivent cette transition technologique au regard des objectifs stratégiques de l'institution. En posant ces jalons, la revue éclaire les conditions nécessaires à une transformation réussie et alimente la réflexion sur l'évolution des pratiques d'identité numérique dans le secteur financier.

CHAPITRE 3
CADRE CONCEPTUEL

Ce chapitre explore les fondements conceptuels de la GIA dans le secteur bancaire canadien en mettant l'accent sur les affordances de Gibson et sur l'intégration des IDD. Nous commencerons par définir le concept d'affordances et son rôle dans la manière dont les technologies façonnent les interactions entre les utilisateurs finaux et la banque étudiée. Ensuite, nous analyserons son application dans la GIA, suivi d'une analyse du cadre selon Kuperberg (2020) qui inclut des concepts tels que les IDD, l'IAS et les IIV pour comprendre comment des solutions comme Sovrin et Hyperledger Indy peuvent reconfigurer la gestion de l'identité en permettant aux utilisateurs finaux de prendre contrôle de leurs données personnelles. Ce chapitre servira de base pour développer une grille d'analyse permettant de codifier et d'interpréter les données recueillies lors de la recherche.

3.1 Les affordances de Gibson (1977)

Les affordances sont les possibilités d'action qu'un environnement ou un objet offre à une institution (Gibson, 1977, p. 1). Gibson (1977) introduit ce concept pour décrire la manière dont les êtres vivants perçoivent leur environnement en termes des opportunités d'interaction. Une affordance est une relation entre les propriétés d'un objet et les capacités de l'organisme impliquant que les objets dans l'environnement ne sont pas simplement vus en termes de leurs propriétés physiques, mais aussi en termes de ce qu'ils permettent de faire (Gibson, 1977). En appliquant ce concept à la gestion de l'identité et des accès (GIA) dans le secteur bancaire canadien, les affordances des IDDs se réfèrent aux nouvelles possibilités et fonctionnalités qu'ils offrent aux utilisateurs et aux institutions financières. Dans le cadre de la GIA, les affordances des IDDs offrent des opportunités nouvelles tant au niveau individuel qu'organisationnel. Pour les utilisateurs, ces affordances incluent le contrôle et la propriété des données, la confidentialité et la sécurité. Les clients peuvent posséder et contrôler leurs identités numériques sans intermédiaires grâce à l'IAS et peuvent choisir quelles informations partager et avec qui selon leurs IIV limitant l'exposition de leurs données personnelles. À un niveau organisationnel, les banques bénéficient d'une simplification des processus de vérification d'identité et de conformité, tandis qu'à un niveau inter-organisationnel, ces technologies peuvent transformer les relations interbancaires et les systèmes financiers à grande échelle. Un point qui favoriserait le réseau interbancaire blockchain pan-banque canadien.

3.2 La GIA selon Kuperberg

Kuperberg (2020) explique que la GIA moderne repose sur des concepts clés tels que les IDD, l'IAS, les IIV, le réseau blockchain et l'Identité-en-tant-que-Service (IDaaS). L'IDaaS, solution basée sur l'infonuagique qui offre des services de GIA centralisés et externalisées (Kuperberg, 2020), est couramment utilisée par les banques canadiennes pour faciliter le processus de GIA qui peut être à la longue fastidieuse et coûteuse (OneLogin, s. d.). En effet, les utilisateurs peuvent s'authentifier auprès de leur institution financière au moyen des fonctionnalités de l'IDaaS, c'est-à-dire le *Bring-Your-Own-Identity* : l'authentification multifactorielle (MFA) et le single sign-on (SSO).

Afin de mieux comprendre comment analyser le processus de GIA en intégrant les solutions issues de la TBC, les cas d'utilisation courants de la GIA dans la figure 68 nous montrent toutes les interactions de l'utilisateur final, soit le client, avec les autres acteurs. Ce modèle de cas d'utilisation de la GIA suggère que l'utilisateur final est en relation avec plusieurs acteurs nécessitant des informations qui lui sont propres. Que ce soit une banque, le gouvernement, un notaire, ou autre, tous ces acteurs sont en relation d'une façon ou d'une autre avec l'utilisateur final et celui-ci utilise ses identifiants numériques pour interagir, s'authentifier et partager des informations en fonction des besoins de chaque interaction. En observant le modèle, mise à part le processus KYC et la LCBA, nous pouvons identifier les composants clés suivants : *e-Government services, eID,* Contrôle d'accès, écosystème *Public Key Infrastructure* (PKI) et SSO (Kuperberg, 2020, p. 2).

Premièrement, les services gouvernementaux électroniques (*e-Government services*) nécessitent une identification et une authentification sécurisées pour permettre l'accès aux services publics en ligne. Les citoyens doivent prouver leur identité de manière fiable pour accéder à divers services administratifs. Deuxièmement, les identifiants électroniques (*eID*) sont délivrés par les gouvernements pour faciliter l'identifications en ligne des citoyens. Ces eIDs permettent de prouver son identité de manière sécurisée dans divers contextes numériques. Troisièmement, le contrôle d'accès est utilisé dans la GIA pour protéger les ressources et les données sensibles en garantissant que seules les personnes autorisées puissent y accéder. Finalement, l'écosystème PKI est largement utilisée pour l'authentification, la signature de courriels et de code. Ainsi, en examinant la figure 68 de plus près, nous pouvons constater plusieurs points d'améliorations dont le nombre de points d'interactions entrants et sortants de l'utilisateurs final.

La solution la plus prometteuse pour adresser ces améliorations selon Kuperberg est Sovrin. Sovrin, Hyperledger Indy et Evernym forment une trinité dans l'écosystème de gestion des identités décentralisées (Kuperberg, 2020, p. 15). Sovrin est « un cadre *open-source* d'identité souveraine soutenu par la fondation Hyperledger initialement développé par Evernym » (Kuperberg, 2020, p. 15). Aligné avec ce que l'IAS offre comme affordances à la GIA, l'objectif de Sovrin est de permettre aux individus de posséder et de gérer leurs propres informations d'identité sans dépendre de tiers centralisés. Dans ce cadre, chaque utilisateur peut créer des IDDs uniques pour prouver leur identité de manière privée. Le projet Hyperledger Indy est utilisé et peut être déployé sur une blockchain publique avec permission. Une blockchain publique avec permission est un type de réseau blockchain où les données, dans notre cas ce sont les identités, sont accessibles seulement aux utilisateurs approuvés par un administrateur (Wust et Gervais, 2018, p. 45). Une banque pourra octroyer des accès restreints à ses utilisateurs au moyen de son réseau blockchain public avec permission tel que Sovrin et Hyperledger. Inversement, les utilisateurs finaux, c'est-à-dire les clients, pourront ainsi interagir en toute sécurité avec la banque grâce à leur IDD. Sovrin emploie des IDDs et ce qui est intéressant c'est qu'un individu peut se créer plusieurs identifiants (Kuperberg, 2020, p. 15) qui auront chacune des informations à différents niveaux de confidentialité. Les individus seront en mesure de contrôler le niveau de partage d'informations personnelles à leur guise. Sovrin se base sur « des pseudonymes cryptographiques pour minimiser les corrélations non souhaitées entre les interactions » (Kuperberg, 2020, p. 15). Les interactions et les IIV sont stockées en dehors du registre principal par chaque propriétaire d'identité souveraine (Kuperberg, 2020, p. 15) selon ses différents IDD créés. En somme, Sovrin s'inscrit comme étant la solution la plus prometteuse pour répondre aux besoins d'amélioration de la gestion des identités numériques, une dynamique que nous allons illustrer de manière visuelle en adaptant le modèle proposé par Kuperberg (2020) en y intégrant les spécificités de Sovrin et Indy. Cette adaptation servira de fondement à l'élaboration de notre cadre conceptuel, orienté par les affordances identifiées, afin d'analyser de manière critique la réingénierie des processus de gestion de l'identité numérique.

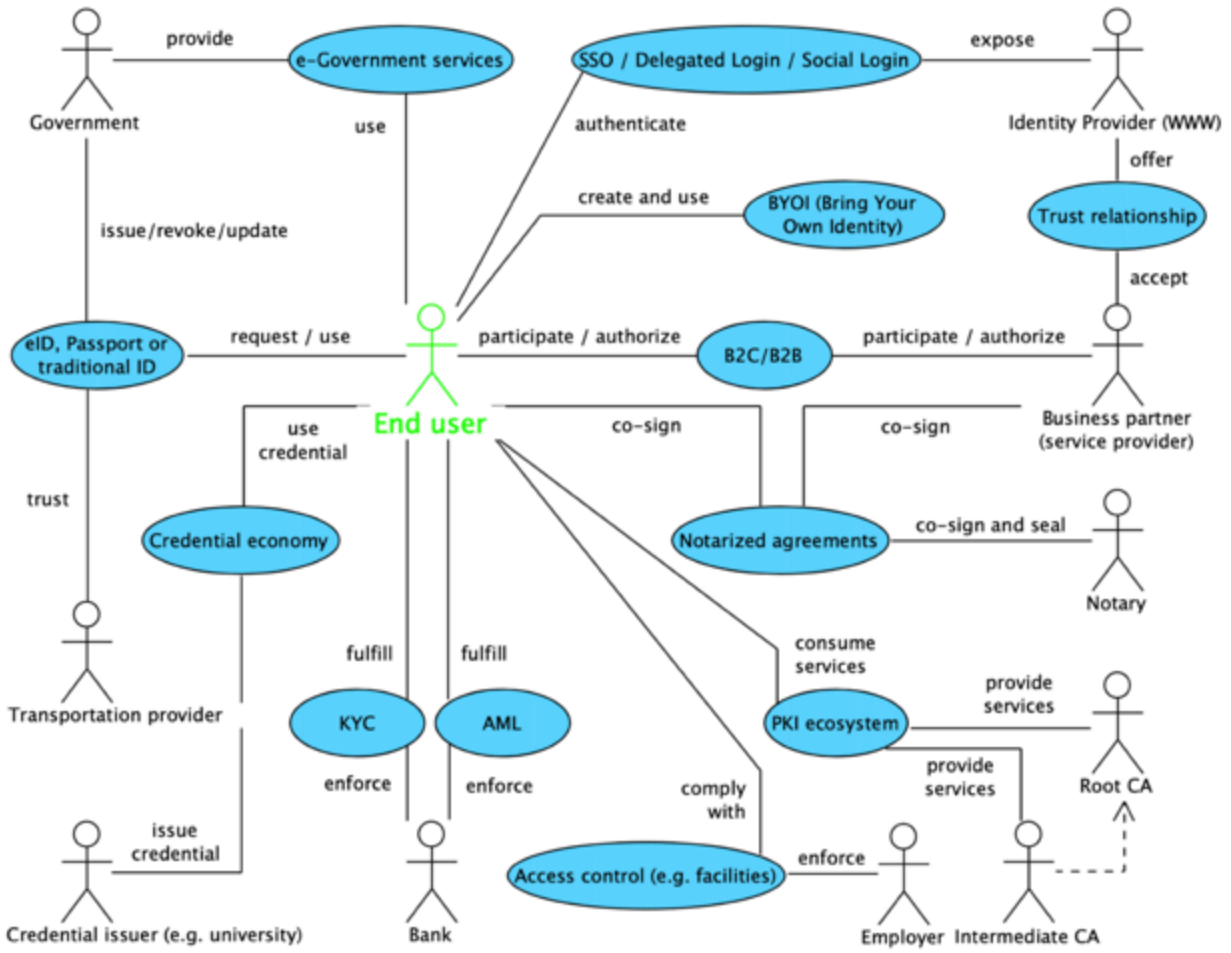


Figure 46 Cas d'utilisation et acteur de la GIA (Kuperberg 2020, p. 2)

3.3 Cadre conceptuel selon l'adaptation du modèle de Kuperberg et des affordances de Gibson

Dans le cadre de notre démarche de recherche, nous avons analysé comment l'intégration des IDD peut transformer ces interactions en considérant autant les affordances et les enjeux d'une possible réingénierie des processus. L'idée consiste à détacher l'utilisateur final de tout points d'entrée et de sorties pour ne conserver qu'un seul lien d'attachement avec son ou ses IDD. Ce dernier a dès lors l'occasion de s'approprier pleinement son identité et de déterminer quel sera le niveau d'information partagée. Sachant que les solutions blockchain présentées comportent encore des limites et enjeux en termes d'adoption lente, de manque de maturité au niveau de la conformité réglementaire, du niveau de sophistication des infrastructures en comparaison des infrastructures existantes et du défi d'acceptation des utilisateurs, une grille d'analyse a été mobilisée afin de codifier les données recueillies en fonction des affordances qu'offre Sovrin et des limites soulevées par Kuperberg (Kuperberg 2020, p. 2). Cette grille est structurée autour des

axes principaux suivants : la conformité réglementaire, l'adoption et la sophistication technologique, et la réingénierie des processus. La conformité réglementaire a été analysée en évaluant comment les solutions répondent aux exigences en matière de protection des données par les utilisateurs finaux et les institutions financières ainsi que les efforts nécessaires pour la formation et la sensibilisation. La sophistication technologique a été analysée en fonction de la robustesse actuelle des solutions, de leur fiabilité et de leur capacité à évoluer et à répondre aux besoins futurs en comparaison des solutions blockchains tel que Sovrin afin d'en évaluer la pertinence dans un contexte bancaire réel. Enfin, la réingénierie des processus a été explorée pour comprendre comment les affordances des IDD peuvent améliorer les interactions utilisateurs et faciliter les processus de GIA et KYC tout en tenant compte des enjeux d'une telle réingénierie.

La figure 69 illustre la manière dont les affordances peuvent être incorporées dans les processus actuels. L'analyse a permis de couvrir les limites et les enjeux du cadre afin de déterminer la viabilité de la solution de Sovrin pour les banques canadiennes. En ce sens, notre analyse s'est particulièrement concentrée sur les encadrés verts de la figure 69, soit les interactions depuis l'utilisateur final et ses IDD avec la banque. La solution adaptée de Kuperberg vise à répondre aux enjeux courants de la GIA en optant pour une possible réingénierie des processus existants pour intégrer des IDD via Sovrin Hyperledger Indy et l'IAS. Dans ce cadre, l'utilisateur final est en mesure de se créer plusieurs identifiants qui lui permettraient de s'authentifier auprès de sa banque, du gouvernement et n'importe quelle autre entité plutôt que de passer par un eID ou l'IDaaS par exemple représenté par des croix rouges dans la figure 69. L'émetteur de justificatifs est remplacé par Sovrin, et la banque, acteur central de notre projet, interagirait avec ses utilisateurs finaux dans la même mesure, mais offrirait une expérience client et un niveau de confiance nettement amélioré. En utilisant des IDD, la banque ne stocke plus de manière centralisée et vulnérable les identités de ses clients.

Par ailleurs, une solution émergente comme KERI, centrée sur la vérification d'événements plutôt que sur la technologie de registres décentralisés, propose également une approche complémentaire qui renforce les principes d'identité auto-souveraine, d'autonomie, de traçabilité cryptographique et de portabilité des identifiants. Bien que notre cadre conceptuel s'appuie principalement sur Sovrin et Hyperledger Indy, l'architecture événementielle de KERI s'inscrit pleinement dans la logique des affordances explorées. Cette solution est ainsi considérée pour couvrir d'autres angles, notamment l'interopérabilité sans dépendance à une infrastructure blockchain, la portabilité et la longévité des identifiants, l'automatisation sécurisée

des cycles de vie d'identité dans une logique de réingénierie des processus, ainsi que l'exploration de modèles de gouvernance distribuée potentiellement plus souples et mieux alignés avec les exigences canadiennes en matière de conformité réglementaire.

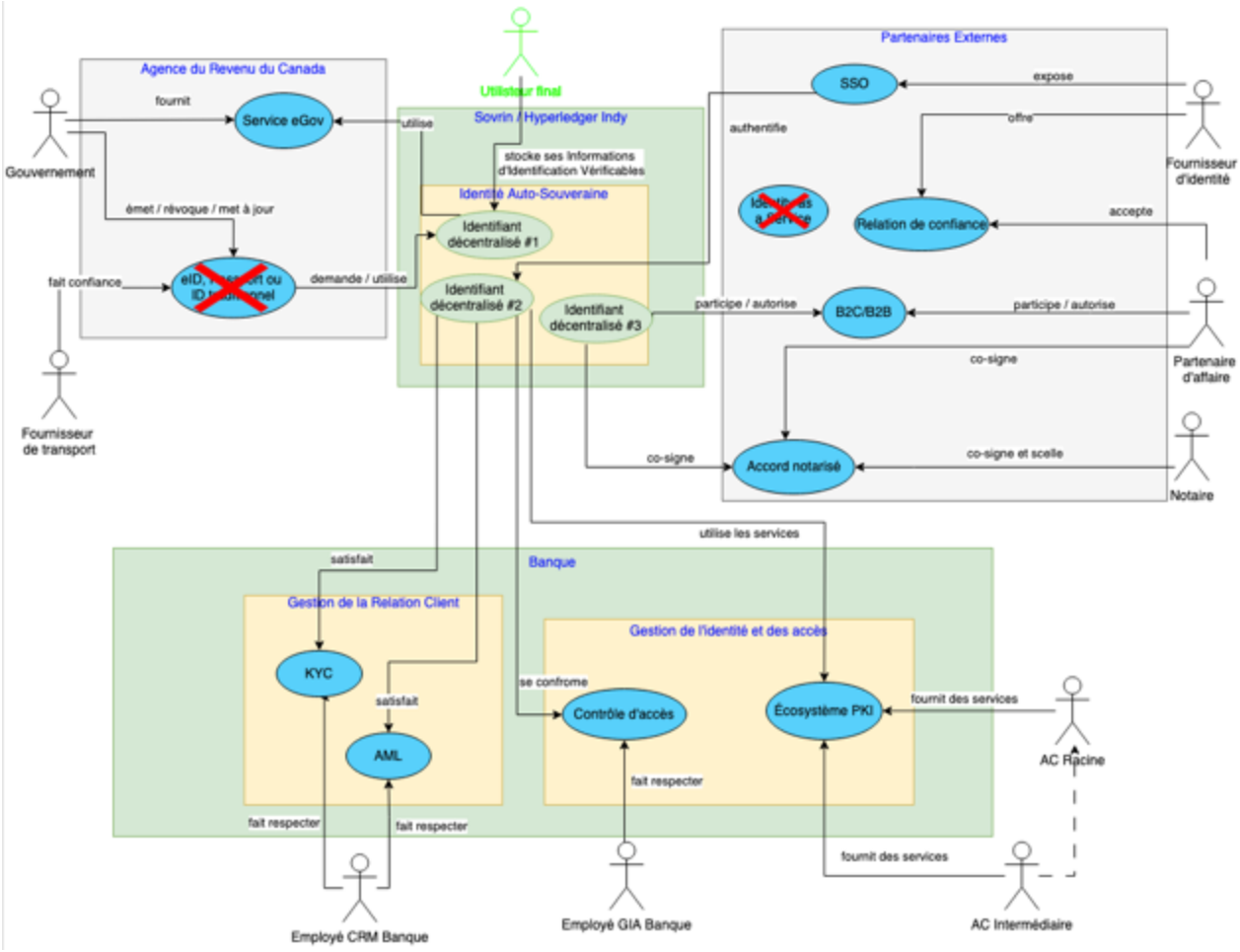


Figure 47 Cas d'utilisation adapté de Kuperberg (2020)

CHAPITRE 4
MÉTHODOLOGIE

Le projet de recherche, composé d'une démarche méthodologique qualitative de nature exploratoire, a été réalisée sous le paradigme interprétativiste en tant que positionnement épistémologique et repose sur l'approche inductive. Ce paradigme, de nature compréhensive, utilise une attitude qui souhaite expliquer le sens que la réalité présente pour les individus dans leurs expériences au quotidien (Pourtois *et al.*, 2006). Ainsi, notre méthodologie est axée sur la tenue d'entretiens semi-dirigés avec des employés et deux membres de la haute direction d'une banque en plus d'experts de la technologie blockchain afin de répondre aux objectifs préalablement définis.

4.1 Étapes et démarche de la recherche

Tout d'abord, le projet de recherche suit une démarche méthodologique qualitative, car notre but est d'explorer le sujet et obtenir la perception directe des participants, en l'occurrence les employés d'une banque canadienne, en vue de comprendre l'expérience humaine et fournir une compréhension riche d'un contexte social complexe (Cloutier, 2024; Gaudet et Robert, 2018). L'étude de cas unique est adaptée pour notre démarche exploratoire, car elle permet d'investiguer un phénomène dans son contexte réel (Yin, 2009). « L'étude de cas unique ne représente pas un échantillon et l'objectif du chercheur est d'élargir et de généraliser des théories plutôt que de les particulariser pour guider des recherches éventuelles et former une étude de cas multiple. » (Yin, 2009) Bien que le projet se concentre sur une seule banque et que l'étude de cas unique ne puisse garantir la généralisation à un secteur d'activité, les résultats obtenus visent plutôt à proposer des pistes interprétatives et à identifier des tendances, des opportunités et des défis liés à l'intégration des IDDs qui pourront ensuite être appliqués ou adaptés à d'autres banques dans le cadre d'un réseau interbancaire plus large. Cette approche aide à anticiper les implications potentielles d'un déploiement à plus grande échelle dans l'ensemble du secteur bancaire canadien. Cependant, il est important de reconnaître que les banques n'ont pas toutes les mêmes chartes et leurs priorités stratégiques peuvent différer même si elles sont soumises à des réglementations communes. Les résultats obtenus sont donc contextualisés à la banque étudiée pour tenir compte des spécificités des processus bancaires et des technologies utilisées en vue de garantir que les recommandations finales tiennent compte des réalités opérationnelles et des contraintes techniques actuelles. En outre, cette étude de cas unique permet de capter la vision stratégique de la haute direction sur l'adoption de ces technologies, un facteur clé dans leur intégration à long terme. De plus, considérant notre contexte, elle est également

pertinente lorsque « les limites entre le phénomène étudié et le contexte ne sont pas clairement évidentes » (Yin, 2009). En ce sens, cette étude nous permet de comprendre les affordances et les enjeux d'une réingénierie des processus visant à intégrer les IDD dans la GIA.

Notre projet de recherche adopte un positionnement épistémologique interprétativiste, car il vise à comprendre comment les employés d'une banque perçoivent et interprètent les défis liés à la gestion des identités numériques. Nous nous concentrons ainsi sur le pourquoi d'une situation (Bulinge, 2014), soit pourquoi une banque adopterait les IDD, IAS et IIV, en se concentrant sur la compréhension des significations et des expériences subjectives que les individus au sein des banques attachent à la réalité sociale, leurs motivations et intentions (Bulinge, 2010). Ce positionnement nous a amené à évaluer comment les employés perçoivent les changements apportés par les nouvelles technologies et quels sens ils attribuent à leurs interactions quotidiennes avec les systèmes et les clients (Schwandt, 2000). Le paradigme interprétativiste est idéal pour ce type de recherche, car il permet d'explorer en profondeur les perspectives actuelles et collectives, ce qui enrichit la compréhension du phénomène étudié par une construction sociale des réalités (Schwandt, 2000). Cette perspective reconnaît que la réalité est perçue et interprétée de manière cohérente avec l'expérience de différents acteurs (Bulinge, 2010) pour tenter de découvrir les ressorts cachés du phénomène (Bulinge, 2014). Ce positionnement est pertinent pour explorer les perceptions, les attitudes et les expériences (Denzin et Lincoln, 2011) des employés et des membres de la haute direction de la banque ainsi que des experts blockchain. Des entretiens semi-dirigés ont donc été tenus afin de collecter des données sur le terrain.

L'approche préconisée est l'approche inductive, car le raisonnement inductif permet d'élaborer des interprétations au fur et à mesure où les données collectées sur le terrain sont analysées (Cloutier, 2024), expliquant comment et pourquoi les technologies blockchain, notamment les identifiants décentralisés, pourraient s'intégrer au secteur bancaire canadien. De surcroît, le paradigme interprétativiste se marie bien avec l'approche inductive, considérant sa nature riche en compréhension de phénomènes sociaux, et a été utilisé pour comprendre comment les individus interprètent leurs interactions avec les technologies blockchain dans des contextes bancaires tout en tenant compte de leur vécu et de leur environnement socio-économique (Kovács et Spens, 2005). L'application de l'approche inductive dans ce présent projet permet d'observer sans préjugés les pratiques actuelles de gestion de l'identité numérique en plus de découvrir des modèles d'usage et des problématiques potentiellement non anticipées par les théories existantes pour finalement comprendre les vrais défis rencontrés par les employés et les clients. Ainsi,

l'analyse des données recueillies, grâce à la tenue d'entretiens semi-dirigés, nous permet de valider nos tendances itératives sur le potentiel de l'utilisation de la technologie blockchain sur la gestion de l'identité numérique dans le secteur bancaire pour enfin formuler des recommandations.

Dans cette section, les étapes de réalisation, étant alignées avec l'approche inductive, seront décrites, puis justifiées. La démarche méthodologique qualitative employée s'appuie sur une collecte de données terrain auprès d'employés et dirigeants d'une grande banque canadienne et auprès d'experts des technologies blockchain lié à la gestion de l'identité numérique. Par ailleurs, l'étude exploratoire du secteur bancaire canadien, visant à définir des questions, concepts, propositions ou modèles (Paré, 2004), est la stratégie centrale de notre recherche, car elle combine à la fois la tenue d'entrevues et un cadre flexible pour examiner de plus près l'impact de l'intégration de la technologie blockchain dans les pratiques de gestion de l'identité numérique (Eisenhardt, 1989). Par la suite, nous expliquerons comment le cadre d'échantillonnage a été mené, quel a été l'instrument de collecte de données, incluant le guide d'entretien semi-dirigés, et la façon dont l'analyse des résultats a été cadrée pour pouvoir les discuter et les interpréter par la suite.

4.2 Cadre d'échantillonnage et recrutement des participants

Tout d'abord, nous tenons à spécifier que le chercheur principal est un employé de la banque étudiée et que cela a facilité l'identification et le recrutement des participants employés. Par ailleurs, le fait que le chercheur principal soit un employé de l'organisation étudiée implique un positionnement particulier qui peut influencer la collecte et l'interprétation des données. En effet, l'observateur n'est jamais totalement neutre et ses perceptions peuvent être orientées par son expérience, ses interactions quotidiennes et sa compréhension préalable au contexte (Kardiner, 1969, p. 81). Cette proximité comporte des facteurs sous-jacents tels qu'un biais d'initié, une familiarité avec certains collègues pouvant faciliter l'accès au terrain, mais aussi influencer la spontanéité des réponses, ainsi qu'un rapport d'autorité avec des supérieurs hiérarchiques pouvant affecter le degré de prudence ou de retenue de certains participants. Afin de limiter ces effets, la participation a été présentée comme strictement volontaire et sans incidence sur la relation d'emploi, l'anonymat a été renforcé par l'usage de pseudonymes et par une minimisation des informations indirectement identifiables. Le chercheur a adopté une posture réflexive tout au long du processus. Dans cette logique, l'analyse s'est appuyée sur une démarche critique visant à confronter les interprétations à des critères d'analyse explicites et à des vérifications internes, afin de réduire l'emprise des perceptions personnelles sur les conclusions. Ainsi, une triangulation des sources de données a été effectuée, croisant

les points de vue de plusieurs répondants avec la littérature existante, et une grille d'analyse a été utilisée pour encadrer l'interprétation.

Concernant le recrutement des répondants, ceux-ci ont été sélectionnés de manière ciblée par l'envoi d'invitations officielles par courriel. Chaque participant a été préalablement informé des objectifs de l'étude, du respect de l'anonymat et de la confidentialité des données recueillies, conformément aux normes éthiques en matière de recherche (Patton, 2014). Le cadre d'échantillonnage repose sur une sélection raisonnée des participants en fonction de leur expérience et de leur expertise directe avec les processus KYC, le système CRM, la cybersécurité, la gestion des identités numériques des clients, la stratégie de la banque ou l'expérience client, ainsi que des technologies blockchain orientées vers les identifiants décentralisés et l'identité auto-souveraine afin de garantir que les données recueillies soient pertinentes et riches en informations contextuelles (Martínez-Mesa *et al.*, 2016 ; Patton, 2002). L'échantillon cible en particulier des employés ayant œuvré en succursales, au sein de l'équipe de gestion d'identité et accès (GIA), dans les systèmes de gestion de la relation client (CRM), ainsi que dans les discussions stratégiques de haut niveau. En complément, des experts externes en technologies blockchain (TBC) ont aussi été interviewés afin d'approfondir les aspects techniques des solutions blockchain envisagées. La taille de l'échantillon a été déterminée par la disponibilité des participants et ajustée progressivement jusqu'à l'atteinte d'une saturation théorique. Quatre employés, deux membres de la haute direction et deux experts blockchain ont été interrogés pour un total de huit personnes, ce qui a permis d'explorer la problématique sous divers angles et d'obtenir des données riches en connaissances réelles, pratiques et applicables.

4.3 Présentation du profil des participants

Le tableau ci-dessous présente l'ensemble des participants à nos entretiens semi-dirigés. Ceux-ci ont été menés auprès d'employés en succursale, de membres des équipes CRM et GIA, de la haute direction de la banque étudiée, ainsi que d'experts externes en TBC. Pour préserver l'anonymat des participants, des pseudonymes leur ont été attribués, comme présenté dans le tableau ci-dessous. Ce tableau résume le profil de nos participants avec leur rôle et expériences, leur provenance ainsi que leur expertise.

Participant	Surnom	Rôle & Expériences	Provenance	Expertise
P1A	Leona	Analyste Fonctionnel CRM, service à la clientèle	Banque	KYC, CRM, UX[25]
P2A	Fiora	Analyste Fonctionnel CRM, support TI	Banque	KYC, CRM
P3A	Teemo	Analyste Qualité CRM, support TI	Banque	CRM, MDM
P4C	Willump	Directeur cybersécurité	Banque	Okta, Azure AD
P5E	Ekko	Expert blockchain, Propriétaire de produit, développeur	Externe	IDDs, Indy, Corda, IAS, IIVs, ZKP, UX
P6E	Kennen	Ingénieur logiciel, développeur	Externe	IAS, KERI, IIVs, IDDs, ZKP
P7H	Ezreal	Haute direction	Banque	Canaux assistés, TI
P8H	Jayce	Haute direction	Banque	Canaux assistés, TI

Tableau 2 Profil des participants

4.3.1 Employés et haute direction de la banque

Parmi les participants internes, quatre employés et deux membres de la haute direction ont occupé des postes variés, incluant des fonctions d'analyste fonctionnel CRM, de service à la clientèle, de support TI, de direction en cybersécurité et de direction principale. Leur expertise couvre les processus KYC, les systèmes CRM, la gestion centrale de données MDM[26], les outils d'authentification Okta et Azure AD ainsi que les canaux assistés en général.

[25] UX est un acronyme pour user experience, donc expérience utilisateur

[26] Voir Annexe G pour plus d'informations

Premièrement, les participants ayant une expérience directe auprès de la clientèle sont essentiels, car leur interaction régulière avec les clients leur confère une compréhension approfondie des besoins, des attentes et des préoccupations en matière de gestion de l'identité numérique. À travers leur rôle, ils participent activement au fonctionnement des processus actuels de la relation client, en particulier en ce qui concerne la collecte et la mise à jour des informations d'identité des clients. Leur perspective est importante pour identifier les limites opérationnelles telles que la redondance des vérifications d'identité, les lacunes du KYC, la complexité des processus existants et bien d'autres.

Deuxièmement, les employés rattachés aux équipes CRM et support TI détiennent une vision détaillée des processus de la relation client, des données clients et de l'identification client. Leur connaissance approfondie des flux d'informations et des mécanismes de gestion des données clients constitue un apport déterminant pour comprendre l'organisation actuelle, ses complexités et son quotidien en arrière-plan. Il s'agit de connaissances solides que nous pouvons ensuite investiguer pour aider à répondre à la première sous-question de recherche en lien avec les lacunes actuelles des processus.

Troisièmement, l'entretien avec l'employé de l'équipe de gestion de l'identité et des accès clients apporte un éclairage technique fondamental sur les pratiques internes de création et de gestion des identités ainsi que de l'authentification des clients. Son expertise permet de mieux saisir les mécanismes sur lesquels repose aujourd'hui la gestion de l'identité numérique au sein de la banque, ainsi que les limites et contraintes auxquels elle est confrontée. Cette perspective est indispensable pour enrichir l'analyse du fonctionnement actuel de la GIA et orienter l'évaluation critique de ses limites, en cohérence avec les objectifs de la première sous-question de recherche.

Finalement, les entretiens avec la haute direction permettent de comprendre la vision stratégique de la banque, la réflexion et les requis stratégiques derrière l'implémentation de nouvelles technologies dont celle des identifiants décentralisés. Leur point de vue et expérience constituent des apports essentiels pour répondre à notre troisième sous-question de recherche axée sur le discernement de la vision stratégique long terme de la banque concernant les nouvelles technologies. Par ailleurs, bien que les participants identifiés ici comme membres de la « haute direction » n'occupent pas les plus hauts niveaux hiérarchiques de l'organisation étudiée, au sens strict du comité exécutif ou de la présidence, ils se situent néanmoins à un niveau stratégique intermédiaire de la gouvernance. Il s'agit du supérieur immédiat du chercheur et son supérieur direct, lesquels participent fréquemment à des instances décisionnelles et à

des rencontres impliquant des cadres de niveau supérieurs, incluant des vice-présidences (VPs) et des premières vice-présidences (PVP). À ce titre, ces acteurs disposent d'une compréhension transversale des orientations stratégiques de la banque et des contraintes organisationnelles associées à leur mise en œuvre. Le participant occupant le niveau hiérarchique le plus élevé parmi les deux jouent un rôle plus direct dans la traduction des orientations stratégique en décisions opérationnelles, ce qui justifie leur mobilisation dans l'analyse de la vision stratégique, sans pour autant prétendre capter la perspective du sommet exécutif ultime de l'institution.

4.3.2 Experts Blockchain

Deux experts spécialisés en blockchain appliquée à la gestion de l'identité ont également été interviewés dans le cadre de cette étude. Bien qu'extérieurs au secteur bancaire, leur expertise est directement pertinente pour notre projet de recherche, car ils disposent d'une expérience concrète avec les principaux éléments technologiques décentralisés mobilisés, notamment les identifiants décentralisés, l'identité auto-souveraine et les informations d'identification vérifiables. À cela s'ajoute les solutions comme Hyperledger Indy, Corda, les ZKP et « Key Event Receipt Infrastructure » (KERI). Leur contribution revêt une importance particulière, dans la mesure où ils apportent une perspective externe de l'organisation étudiée et spécialisée sur la conception, l'intégration et l'application de solutions blockchain dans des contextes de gestion de l'identité numérique de clients bancaires. Il s'agit d'apports significatifs pour répondre à notre deuxième sous-question de recherche.

4.4 Instrument de collecte des données

La collecte des données a été effectuée à travers un guide d'entrevue semi-dirigé. Les étapes de la démarche d'entrevues semi-dirigés se divisent en trois phases : 1) Préparation de l'entrevue 2) Conduite de l'entrevue 3) Synthèse de l'entrevue (Cloutier, 2024a).

4.4.1 Préparation des guides d'entretien

Afin de recueillir des données de qualité en lien avec nos objectifs de recherche, une attention particulière a été portée à la préparation des guides d'entretien. Plutôt que d'utiliser un seul guide uniforme, nous avons conçu plusieurs guides distincts (Annexes C à F), chacun adapté aux spécificités des profils des participants : employés en succursale, employés du CRM, employés de l'équipe GIA, membres de la haute direction et experts blockchain. Cette division sert à maximiser la pertinence et la profondeur des réponses en alignant les questions avec nos objectifs de recherche, l'expérience concrète et le niveau d'implication

des participants dans les différents processus, outils et réflexions. La logique derrière cette segmentation repose sur la nature même de notre problématique. Chaque catégorie de participant possède une perspective unique sur les processus d'identification, les systèmes CRM, la cybersécurité, les exigences KYC et les défis d'adoption de nouvelles technologies telles que les identifiants décentralisés. En ajustant les guides d'entretien à ces réalités, nous avons pu orienter les discussions vers les domaines où chaque participant pouvait offrir une contribution experte et contextuelle, tout en maintenant une trame commune facilitant l'analyse croisée ultérieure des résultats.

Pour l'employé de la GIAC, les questions visaient à explorer son rôle opérationnel quotidien, la description détaillée du processus actuel de création et de gestion des identités, les outils technologiques utilisés, ainsi que sa perception des limites et des risques associés à ces outils, ce qui répond à notre première sous-question de recherche. Bien que l'ensemble des employés et des membres de la haute direction ne connaissent pas les solutions blockchain en lien avec l'identité, voire même les identifiants décentralisés tout simplement, nous avons quand même intégré des questions sur ce sujet au besoin pour tenter de répondre à la deuxième sous-question de recherche. Pour les employés en succursale, nous avons couvert les questions dans le même guide que celui du CRM. Les questions portaient principalement sur le rôle du CRM dans les processus de gestion de la relation client, de vérification client et de partage des données entre services. Nous souhaitions, avec ce guide, mettre en lumière les lacunes actuelles, ce qui répond également à notre première sous-question de recherche. Pour les membres de la haute direction, les questions avaient pour objectif de répondre à notre troisième sous-question de recherche. Il s'agissait de recueillir la perspective stratégique sur l'adoption potentielle d'une nouvelle technologie. Le guide visait donc à comprendre comment une nouvelle technologie comme les IDDs pourrait s'inscrire dans les orientations stratégiques à long terme de l'institution. Enfin, le guide pour les experts blockchain explorait de manière plus technique les limitations des systèmes actuels de gestion de l'identité, les défis techniques et humains d'implémentation, ainsi que les opportunités des IDDs. Ce guide a permis de couvrir principalement notre deuxième sous-question de recherche.

Dans tous les guides, la structure suivait un cheminement logique : une première partie explorait le fonctionnement actuel et ses limites, une seconde partie s'intéressait à l'intégration potentielle des IDDs et à la réingénierie des processus, et une dernière section recueillait les perceptions sur l'acceptabilité organisationnelle et les besoins de formation pour accompagner ce changement. La préparation différenciée des guides a donc permis d'optimiser la pertinence du questionnement, d'assurer une

couverture complète des enjeux liés à l'intégration des identifiants décentralisés et de mieux aligner les réponses obtenues avec les objectifs de recherche.

4.4.2 Entretiens semi-dirigés

La conduite des entretiens semi-dirigés a été réalisée, avec notre compte étudiant, au travers de la plateforme Microsoft Teams en raison principalement de sa fonctionnalité de transcription en direct. Bien que la transcription sur Teams ne soit pas parfaite et nécessite une vérification manuelle approfondie à partir de l'enregistrement audio, elle constitue tout de même une base utile pour amorcer les travaux de transcription et d'analyse. Chaque entretien a ainsi été transcrit, puis analysé à travers un processus de codage thématique itératif, permettant de structurer les données en identifiant les thèmes récurrents et significatifs. Ce travail de codage visait à faciliter l'interprétation ultérieure des résultats en lien avec les objectifs de recherche. L'usage de Microsoft Teams s'est imposé naturellement, étant déjà maîtrisé par les employés de la banque dans leur environnement de travail quotidien. Pour les experts blockchain, c'est plutôt la plateforme Zoom qui été utilisée. Dans ce cas-ci, l'usage de l'IA a été employé pour retranscrire l'entretien. Avec l'outil Otter.ai nous avons pu automatiser la rencontre, puis nous avons manuellement corriger les erreurs que l'IA a pu faire.

L'usage des entretiens semi-dirigés constitue une approche méthodologique centrale dans notre perspective interprétativiste pour répondre aux objectifs de recherche en se concentrant sur des phénomènes complexes (Savoie-Zajc, 2009) comme l'impact de la technologie blockchain dans la gestion de l'identité numérique dans le secteur bancaire canadien. Cet instrument de collecte de données est intéressant pour comprendre les expériences, attitudes et perceptions des participants afin de saisir la richesse des contextes individuels et organisationnels (DiCicco-Bloom et Crabtree, 2006). Les entretiens semi-dirigés offrent une structure flexible qui facilite la discussion et les échanges riches en information. Dans ces circonstances, poser des questions ouvertes permettra aux participants de s'exprimer librement sur leurs expériences tandis que les questions dirigées aideront à concentrer la discussion sur les aspects spécifiques de la recherche (Longhurst, 2003). Ainsi, l'instrument aide à recueillir des données qualitatives sur le sujet de la recherche et en alignant les questions des entretiens avec les objectifs de la recherche, il est possible de déceler les détails cruciaux du point de vue des participants (Travers, 2001). Or, pour répondre efficacement aux objectifs de recherche, chaque entretien explore les thèmes centraux de l'étude comme la gestion de l'identité numérique, la technologie blockchain et le secteur bancaire en plus de l'observation du processus de gestion de l'identité numérique actuel versus le futur et les affordances

et enjeux reliés. Grâce aux perspectives données par les participants, nous avons ensuite été capables de formuler des recommandations pratiques et réalisables, dans la mesure du possible, pour l'adoption de la blockchain dans les pratiques bancaires.

En prévision des entrevues, nous avons rédigé une mise en contexte de deux pages expliquant la solution blockchain Sovrin de façon théorique et conceptuelle. Celle-ci a été envoyée aux répondants souhaitant participer aux entretiens. Nous avons ainsi gagné du temps sur la mise en contexte et chaque participant a été en mesure d'évaluer en quoi et où il pourra être en mesure de contribuer à la recherche.

Catégorie	Banque étudiée	Experts blockchain
Nombre d'entrevues	6	2
Plateforme utilisée	Microsoft TEAMS	Zoom
Durée	50 minutes	
Contact	En personne & Courriel	Référencé par courriel

Tableau 3 Sommaire des entretiens réalisés

4.5 Cadre d'analyse des résultats

Dans le cadre de cette recherche, l'analyse des données recueillies lors des entretiens semi-dirigés a été réalisée en utilisant un codage thématique itératif. Cette méthode identifie et analyse les thèmes principaux liés aux lacunes du processus actuel de gestion de l'identité, aux défis et opportunités de la réingénierie des processus pour intégrer les IDD, ainsi qu'à la vision stratégique de la haute direction. Bien que des aspects réglementaires existent, ceux-ci ne sont pas approfondis dans cette étude, car ils sont abordés dans de futures recherches et font partie des limites de notre recherche. Le codage nous a permis de découvrir des thèmes émergents à partir des données recueillies auprès des participants. Ces thèmes ont ensuite été raffinés, puis liés aux objectifs de la recherche, et ce à travers plusieurs cycles de codages itératifs qui interprète les données en information de qualité. Cette approche itérative nous a aidé à intégrer continuellement les perspectives tirées des répondants pour affiner la compréhension des thèmes tout en s'assurant que les aspects pertinents sont explorés en détails (Braun et Clarke, 2006 ; Fereday et

Muir-Cochrane, 2006). Ce processus de codage thématique itératif est clé pour s'assurer que l'analyse des résultats soit alignée autant avec les thèmes centraux qu'avec les objectifs de la recherche pour refléter fidèlement les expériences et perceptions des participants. Nous avons donc importé les transcriptions dans le logiciel NVivo 15 pour codifier les thèmes principaux. Puis, nous avons utilisé un agent conversationnel d'intelligence artificielle générative (IAG), ChatGPT, pour soutenir certaines étapes de notre analyse, sans substituer l'interprétation humaine. Concrètement, une fois un premier codage réalisé dans NVivo et les thèmes principaux extraits des transcriptions, nous avons soumis à l'IAG ChatGPT des éléments dérivés du codage tels que les listes de codes, des regroupements envisagés et des extraits synthétiques anonymisés, afin d'obtenir : des propositions d'amélioration de regroupement de codes, des suggestions de relations entre thèmes et des pistes de formulation de catégories plus abstraites, à des fins de comparaison et de consolidation. L'utilisation de ChatGPT a été effectuée en mode incognito, dans une logique de prudence, et les décisions finales, soit la création, la fusion, le renommage et la hiérarchisation des codes, ont été prises manuellement par le chercheur à partir des données NVivo récoltées. L'IAG a ainsi agi comme un outil de soutien à la structuration entre le niveau terrain, étant le verbatim et les codes descriptifs, et le niveau abstrait, étant les catégories et les thèmes, tandis qu'un contrôle constant a été exercé afin de valider la cohérence et la pertinence des propositions générales au regard des transcriptions, de la réalité et des objectifs de recherche. En somme, nous avons propulsé notre processus d'analyse manuelle avec l'IAG, en vue d'améliorer la précision et la profondeur de nos interprétations tout en s'assurant de la confidentialité des données traitées.

4.5.1 NVivo 15

Après avoir retranscrit les entretiens semi-dirigés, nous avons importé les transcriptions directement dans NVivo 15. Notre première étape consistait en une relecture approfondie de chaque transcription afin d'acquérir une compréhension holistique des données et d'identifier les schémas initiaux ou les idées récurrentes. Cette immersion initiale a permis la réflexion d'un ensemble préliminaire de thèmes généraux, servant de point de départ à un codage plus ciblé. Ensuite, nous nous sommes engagés dans un processus de codage ligne par ligne plus détaillé. Lorsque nous avons relu chaque transcription dans NVivo, nous avons créé des codes qui représentaient des concepts, des idées ou des expériences spécifiques exprimées par les participants. Ces codes étaient initialement descriptifs et restaient proches du langage utilisé par les participants interrogés. Les fonctionnalités de NVivo permettant de surligner du texte et de relier directement ces annotations à des codes nouvellement ou précédemment crées nous ont facilité l'organisation des thèmes émergents. La nature itérative de l'analyse thématique fait en sorte qu'à mesure

que nous codifions plus de transcriptions, nous affinions continuellement notre schéma de codage ainsi que le nom des codifications et thèmes ressortis. Nous avons examiné régulièrement la liste de codifications en recherchant, parallèlement avec l'IAG, les chevauchements, les redondances ou les possibilités de créer des sous-thèmes plus nuancés grâce à la création de sous-codes. Considérant que nous savions que les thèmes allaient être découpés en trois axes, nous avons préalablement divisé les codes en trois. Puis, au sein de chaque axe, lorsque durant la relecture des transcriptions a été faite, nous avons codifié les thèmes jugés pertinents pour notre analyse. Une fois que les thèmes ont été codifiés, nous avons demandé à ChatGPT de faire des regroupements pour faciliter l'analyse subséquente. À cette étape, seuls des éléments dérivés du codage (ex : listes de code et proposition de regroupements) ont été soumis à ChatGPT. Par exemple, dans la figure 70, les sous-codes complexité d'intégration, conformité réglementaire, coûts, formation, last mile, mise en œuvre, acceptation, résistance au changement IDD, sensibilisation et technophobie avait été identifiés comme thème lors de la première phase d'analyse. En donnant la liste des thèmes initiaux codifiés non regroupés et avec un prompt comme « Agis en tant que chercheur et suggère-moi une logique de regroupements de codes pour faciliter l'analyse des résultats » lancé dans ChatGPT, l'IAG nous a recommandé de mettre les thèmes initiaux sous des sous-codes dans les défis des IDDs afin d'avoir une liste plus claire des thèmes. Nous avons ensuite réfléchi à ce qui allait faire le plus de sens pour finalement obtenir la liste ci-dessous

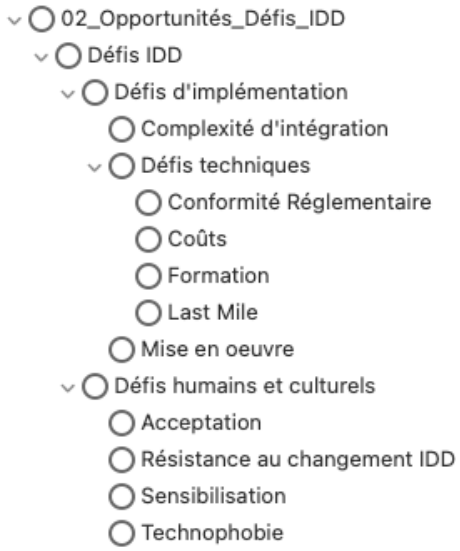


Figure 48 Liste des sous-codes Défis IDDs

Ainsi, avec l'IA, nos annotations, notre schéma de codage, nos révisions, notre esprit critique et analytique, nous avons sur tirer parti des principales fonctionnalités de NVivo pour explorer les relations entre les thèmes soulevés venant potentiellement répondre à nos objectifs de recherche.

Figure 49 Liste des codes dans NVivo

4.5.2 Grille d'analyse pour codage thématique itératif

La grille d'analyse élaborée dans le cadre de cette recherche a permis d'opérationnaliser le cadre conceptuel en fournissant une structure claire et systématique pour le codage thématique itératif des données recueillies lors des entretiens semi-dirigés. Lors du processus d'élaboration de la grille d'analyse, nous avons tout d'abord réfléchi aux thèmes qui seront potentiellement abordés. Ensuite, nous avons utilisé l'intelligence artificielle générative pour nous aider à identifier les indicateurs de thèmes lors de nos entretiens. Pour ce faire, nous avons demandé à ChatGPT avec un prompt comme : « À l'aide de la grille d'analyse de thèmes, aide-moi à trouver des indicateurs qui pourront me permettre de mieux cibler les thèmes à codifier ». L'IAG a donc généré des indicateurs par axe pour mieux cibler les thèmes. Enfin, nous avons intégré le tout dans un tableau pour cibler par axe les thèmes et indicateurs à surveiller.

Tel que mentionné, nous avons découpé nos codes en trois axes et chaque axe d'analyse correspond aux grands thèmes abordés au sein du cadre conceptuel et se décline en objectifs spécifiques, en thèmes à codifier et en indicateurs d'analyse. Le premier axe, relatif aux lacunes du processus actuel de la GIA, visait à identifier les inefficacités et les failles existantes dans la sécurité et la gestion des données d'identité. Les

thèmes codifiés dans cet axe incluent l'efficacité, la sécurité, le fonctionnement des processus KYC et GIA, l'usage du système CRM, ainsi que les interactions et l'expérience client. Les indicateurs utilisés pour l'analyse comprenaient la fréquence des problèmes signalés, les types de failles rencontrées et la satisfaction des utilisateurs. Le deuxième axe portait sur l'exploration des défis et opportunités liés à la réingénierie des processus pour intégrer les IDD. Cet axe poursuivait l'objectif d'analyser les défis techniques, les opportunités d'innovation, les stratégies de formation et les perceptions d'acceptabilité de ces nouvelles solutions. Les thèmes codifiés incluaient notamment les affordances offertes par les IDD, les défis de mise en œuvre, la sensibilisation des clients et des employés, l'acceptation institutionnelle, l'amélioration des processus de GIA, la capacité d'évolution ainsi que la fiabilité perçue des solutions envisagées, telles que Sovrin et KERI. Les indicateurs utilisés concernaient notamment la résistance au changement, les coûts et dettes technologiques anticipés, les niveaux d'acceptation des utilisateurs et les besoins en formation et sensibilisation. Le troisième axe portait sur la vision stratégique de la haute direction en lien avec l'intégration des IDD. Il visait à comprendre comment les dirigeants percevaient les avantages concurrentiels, les implications organisationnelles et les obstacles potentiels associés à l'adoption de cette technologie. Les thèmes codifiés regroupaient la vision stratégique, l'adoption technologique, la gestion du changement et la transformation numérique. Les indicateurs retenus comprenaient la perception de la technologie, la stratégie à long terme envisagée, les implications organisationnelles identifiées et les dynamiques concurrentielles anticipées.

Ainsi, nous avons pris la grille d'analyse de départ pour structurer notre schéma de pensée et codage. Cette grille a servi à identifier les thèmes récurrents et l'IAG a été mobilisée pour soutenir la structuration des regroupements de codes et des indicateurs de thèmes. En structurant l'analyse thématique, la grille a permis d'assurer une couverture systématique des aspects opérationnels, technologiques et stratégiques liés à l'intégration des identifiants décentralisés. Cette approche a renforcé la rigueur analytique du projet et a facilité la production de résultats en lien étroit avec les objectifs de recherche.

Axe principal	Objectif	Thèmes/Affordances à codifier	Indicateurs
Lacune du processus actuel de GIA	Identifier les inefficacités actuelles et les failles dans la sécurité et la gestion des données d'identité	Efficacité Sécurité Processus KYC & GIA Système CRM Interactions clients Expérience client	Fréquence des problèmes signalées Types de failles rencontrées Satisfaction des utilisateurs
Défis et opportunités des IDDs	Analyser les défis techniques, les opportunités d'innovation et les impacts sur les processus Étudier les perceptions liées à l'adoption des IDD et les besoins en formation Comprendre comment les affordances des IDD peuvent améliorer les interactions avec les utilisateurs et faciliter les processus de GIA	Opportunités/ Affordances Défis de mise en œuvre Stratégies de formation Sensibilisation des clients Acceptation des usagers, employés et institution Amélioration des processus Capacité d'évolution Fiabilité	Résistance au changement Coûts/Dette technologique Amélioration de la performance et des interactions Défis d'adoption perçus Besoins en formation et sensibilisation Enjeux perçus Facilitation de la GIA Réduction des points d'entrée Niveau d'acceptation des utilisateurs Défis techniques Fiabilité de Sovrin ou autre
Vision stratégique	Comprendre comment la haute direction perçoit les avantages stratégiques et les obstacles potentiels à l'Intégration des IDD	Vision stratégique Adoption technologique Gestion du changement Transformation numérique	Perception Stratégie à long terme Implications organisationnelle Concurrence

Tableau 4 Grille d'analyse de départ

4.6 Perspective éthique

La confidentialité et le consentement éclairé des participants ont rigoureusement été respectées. La planification et la logistique des entretiens semi-dirigés a tenu compte des disponibilités et contraintes des participants et de la banque. La recherche a respecté les normes éthiques élevées pour maximiser la confidentialité et le consentement éclairé à chaque étape. Le formulaire de consentement en annexe a été transmis à l'avance et a été signé par les participants. Lors de nos entretiens, nous avons réitéré les droits des participants et nous avons également demandé la permission d'enregistrer l'entretien avec chacun d'eux. Ces mesures ont été mises en place pour protéger l'identité des participants. De plus, nous avons documenté les données recueillies, provenant des entretiens, sur un fichier Word pendant comme support de prise de notes pendant chacun de nos entretiens. Ce fichier Word est localisé sur notre compte étudiant privé où personne sauf le chercheur principal y a accès. Nous avons ensuite importé dans NVivo les transcriptions et nous avons donné des surnoms à chacun des participants pour conserver leur anonymat et mitiger la corrélation de leurs propos avec leur personne. Ce fichier est donc conservé sur le serveur infonuagique de l'UQÀM en vue de garantir une meilleure qualité de sécurité de données. L'approche éthique préconisée inclut également la possibilité pour les participants de l'étude de se retirer à tout moment pour garantir leur contrôle sur leur participation (Resnik, 2020).

CHAPITRE 5
ANALYSE DES RÉSULTATS

Ce chapitre présente l'analyse des résultats issus de la collecte de données réalisée sur le terrain dans le cadre de l'étude de cas. En cohérence avec les objectifs de recherche définis au Chapitre 1 et les fondements conceptuels présentés dans les chapitres subséquents, l'analyse s'articule selon trois axes principaux : 1) l'identification des lacunes du processus actuel de gestion de l'identité numérique ; 2) l'exploration des opportunités et des défis associés à l'intégration des identifiants décentralisés (IDDs) et 3) la compréhension de la vision stratégique de la haute direction concernant la réingénierie d'une telle transition. Chaque axe est structuré en sous-sections qui regroupent les thèmes récurrents issus des entretiens semi-dirigés, en s'appuyant sur un codage thématique itératif.

L'objectif n'est pas seulement de décrire les propos recueillis, mais d'en extraire des significations éclairantes, en croisant les perceptions des employés de différents niveaux avec celles des experts externes blockchain, afin de dégager des tendances interprétatives et des recommandations. Cette analyse permet également d'identifier les conditions de faisabilité organisationnelle et technique d'une éventuelle adoption des IDDs dans le contexte spécifique de la banque étudiée. Ce pont entre terrain et théorie prépare ainsi la discussion critique qui sera approfondie dans le chapitre suivant.

Il convient également de rappeler que les résultats présentés dans ce chapitre reposent sur un nombre restreint de répondants, ce qui limite la portée de la triangulation possible. Les analyses proposées doivent être comprises comme des interprétations contextualisées, visant à mettre en lumière des dynamiques et des tensions observées dans le cas étudié, plutôt qu'à produire des généralisations à l'échelle du secteur bancaire.

5.1 Présentation du contexte de l'étude de cas

Pour débuter, nous allons présenter le contexte de la banque étudiée à l'aide des propos recueillis lors de nos entretiens. Dans un contexte de transformation numérique, la banque étudiée s'est engagée à s'adapter aux besoins en constante évolution de leurs clients. Plusieurs départements sont au cœur de cette transformation qui intègrent : les technologies de l'information (TI), les canaux numériques, les canaux assistés, la gestion des identités et des accès, la cybersécurité et bien d'autres. En tant qu'organisation de grande envergure dans l'écosystème financier nord-américain, la banque canadienne

Piltover[27] (le nom Piltover sera utilisé tout au long du processus d'analyse et interprétation des résultats afin de conserver l'anonymat de la banque étudiée et faciliter la lecture), et ses départements critiques à notre étude précédemment mentionnés, se doit d'adapter sa stratégie d'affaires, ses outils technologiques et sa cybersécurité afin de rester compétitive, digne de confiance et conformes aux réglementations. Dans ce contexte, la banque Piltover offre des produits et services en fonction des besoins de leurs clients et assure la communication avec ses clients au travers de canaux numériques tels que leur site web, leurs réseaux sociaux, des courriels électroniques, le clavardage en ligne et les applications mobiles (Entrevue P8H). Les canaux assistés de la banque quant à eux assurent la saine gestion des interactions avec ses clients grâce à aux appels téléphoniques ou vidéoconférence, le service en succursale et le support par courriel (Entrevue P8H).

5.1.1 Interaction avec le client

L'interaction avec les clients débute lorsqu'un client souhaite ouvrir un compte ou effectuer une quelconque activité bancaire auprès de la banque. Pour ce faire, la banque Piltover détient deux procédures différentes qui varie selon le canal assisté. Nous avons pu modéliser ces procédures à partir des informations obtenues des répondants[28] (voir figure 72).

[27] Le nom Piltover sera utilisé tout au long du processus d'analyse et interprétation des résultats afin de conserver l'anonymat de la banque étudiée et faciliter la lecture

[28] Le processus de mise à jour d'information est également possible via le site de la banque ou l'application mobile, mais a été omis volontairement pour faciliter la compréhension simple d'une interaction client-banque

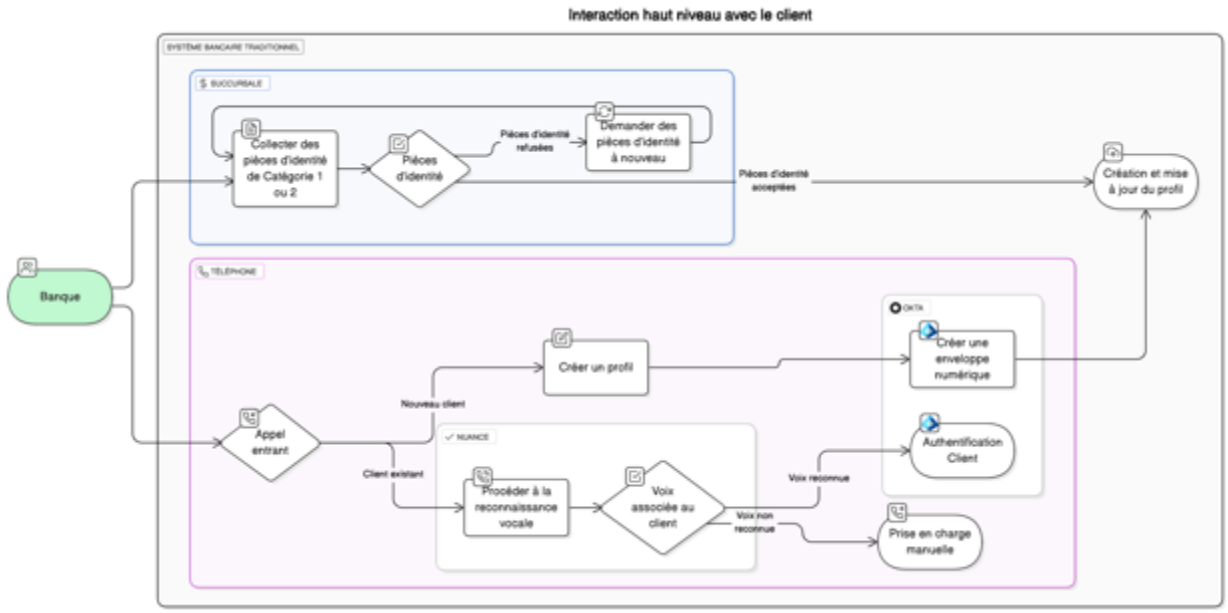


Figure 50 Interaction client-banque (tirée depuis les entretiens semi-dirigés)

D'une part, lorsqu'un client se présente en personne en succursale, la banque demande une ou des pièces d'identité au client dépendamment de certains critères d'acceptation pour l'identifier (Entrevue P3A). Il n'est seulement nécessaire que de donner une pièce d'identité si elle est de catégorie 1, soit une carte d'assurance maladie, un permis de conduire ou un passeport. Dans le cas contraire, il suffira de donner deux pièces d'identité de catégorie 2 pour être éligible, par exemple une carte d'hôpital, une facture d'Hydro-Québec, etc. (Entrevue P3A). La banque demande ces pièces d'identité pour obtenir le nom, le prénom, la date de naissance, l'adresse de résidence et un moyen de communication du client. Tant que le client n'est pas identifié au moyen des pièces d'identité, la banque demandera une pièce d'identité (Entrevue P3A).

D'autre part, lorsqu'un client appelle la banque, il est possible pour un client existant de s'identifier grâce à la biométrie vocale (Entrevue P4C). Nuance, l'outil de gestion de biométrie vocale, s'assure de reconnaître la voix du client lorsqu'il s'identifie au téléphone avec la banque (Entrevue P4C). Si le client

est identifié avec succès par Nuance[29], il sera authentifié par la suite grâce au processus d'authentification d'Okta[30] pour assurer que la personne au bout de la ligne correspond bel et bien au client (Entrevue P4C). Sinon, un agent prendra en charge l'appel et pourra l'authentifier lui-même. Pour un nouveau client, l'interaction avec le client commence par un agent ou un conseiller qui crée le profil du client et crée une enveloppe numérique dans laquelle le client est capable d'aller compléter son processus d'identification en mode libre-service (Entrevue P2A). Cette procédure, propulsée par SafeID un token MFA d'Azure AD et Okta, envoie un lien par texto ou par courriel que le client accède et où il devra scanner des pièces d'identité qui seront ultimement validées par le système de la banque (Entrevue P2A). Dans les deux scénarios, un compte client sera créé ou validé dans Okta, soit la plateforme utilisée pour gérer l'identité numérique des clients, leur authentification et leurs autorisations.

Le processus de création et de mise à jour du profil client (figure 74) débute juste après réception des informations du client avec le processus de connaissance client (voir figure 73[31]) : le KYC. Cette étape obligatoire est un processus réglementé qui oblige les banques à connaître leurs clients avant d'entamer une relation d'affaire avec ceux-ci (Parra Moyano et Ross, 2017, p. 2). Il s'agit tout d'abord pour un agent ou un conseiller de s'assurer de recueillir les informations nécessaires pour authentifier un client pour de futures interactions. Avec ces informations, la banque est en mesure de déterminer si le client sera approuvé ou refusé considérant la qualité des informations d'identification fournie et la vérification de ses antécédents. Un client approuvé pourra continuer le processus de création ou de modification de profil, tandis qu'un client refusé se verra devoir fournir de meilleures preuves justificatives ou bien se faire rejeter comme client de la banque. Il est important pour la banque de connaître leurs clients pour conformité réglementaire, en cas d'audit et pour prévenir des activités illicites tels que le blanchiment d'argent ou le financement du terrorisme.

[29] Microsoft Nuance est un logiciel de reconnaissance vocale. C'est un programme informatique qui peut être entraîné pour reconnaître et identifier des voix spécifiques en analysant les caractéristiques uniques de leur pattern vocal

[30] Ce processus est sensiblement le même pour la connexion sur le site internet ou l'application mobile

[31] La figure 73 a été définie à l'aide de la revue de littérature

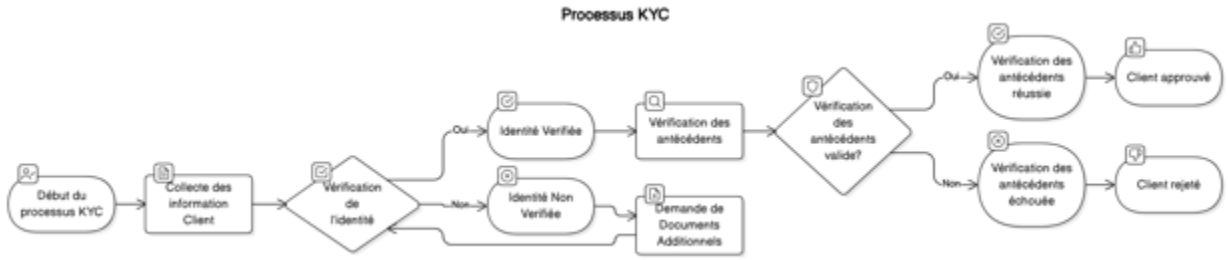


Figure 51 Processus KYC à la banque Piltover à l'aide de (Parra Moyano et Ross, 2017, p. 2)

Une fois les informations validées et la légitimité du client vérifiée, la banque utilise ces informations pour les indexer dans le « customer relationship management » (CRM), SAP CRM, pour pouvoir établir et visualiser un profil client dans le système de la banque (Entrevue P3A). Lorsque les informations sont indexées dans le profil client, le système de gestion des données maîtresses (MDM) est alimenté par ces informations et devient la source de vérité (Entrevue P3A). Si un client met à jour une information personnelle via un des canaux assistés, MDM sera mis à jour selon les nouvelles dernières informations du client (Entrevue P1A). Peu importe la source des nouvelles informations, MDM sera la centrale de données qui assurera la véridicité des données sur un client. Ainsi, tout système autorisé peut appeler MDM via un Fatpub, soit des APIs, ou des tokens pour afficher ou recevoir l'information véridique d'un client (Entrevue P3A). Ces informations seront utiles pour créer des opportunités d'affaires avec le client, soit offrir des produits et services adaptés aux besoins spécifiques de chaque client (Entrevue P2A). La gestion de l'identité numérique des clients ainsi que la gestion de la relation client sont donc au cœur des activités essentielles d'une interaction avec le client.

Figure 52 Processus de création d'un profil client dans SAP et mise à jour des informations client dans MDM (tirée depuis les entretiens semi-dirigés)

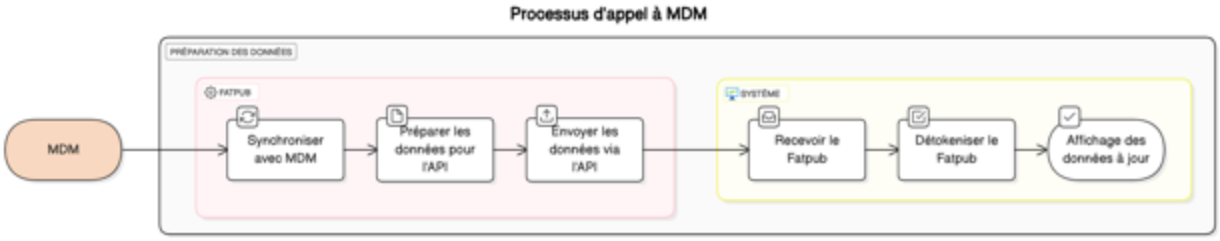


Figure 53 Processus simplifié d'appel à MDM (tirée depuis les entretiens semi-dirigés)

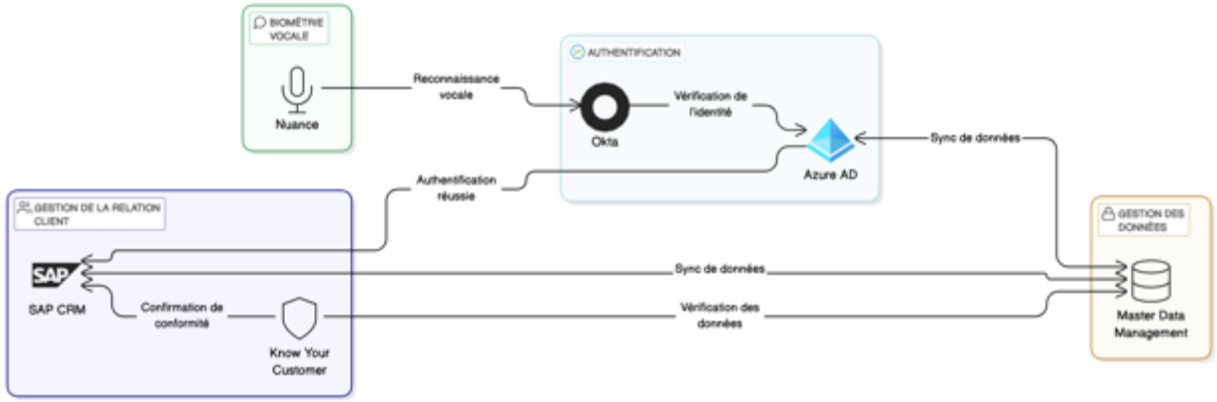


Figure 54 Architecture haut niveau de l'interaction entre outils (tirée depuis les entretiens semi-dirigés)

5.1.2 Présentation des perceptions générales des employés et de la haute direction

Avant de débuter avec l'analyse des réponses des employés et des membres de la haute direction de la banque Piltover, il convient de souligner que nous avons mis en lumière tout au long du processus de codification des transcriptions d'entretiens semi-dirigés des signaux, des indices, des pensées et des perspectives qui aideront la compréhension du positionnement actuel de la banque. Pour ce faire, nous avons utilisé les fonctionnalités de NVivo pour la codification, mais aussi pour la prise de notes grâce à la fonctionnalité d'annotations. Le thème « Thèmes Transversaux » a été codifié à mesure que les entretiens se sont déroulés et ne figurait pas dans nos plans initiaux. Parmi ses sous-thèmes, nous accorderons une importance particulière à la thématique « Perceptions générales ». En effet, il s'agit d'un sous-thème qui n'a pas nécessairement de lien direct avec les axes prédéterminés, mais qui permettra d'orienter la

compréhension des réponses des participants pour les axes à venir. En ce sens, nous avons demandé ce que sont les priorités de la banque aux yeux de nos répondants. Les réponses des participants, qu'il s'agisse d'un employé ou un membre de la haute direction, varient, mais convergent dans l'ensemble pour ultimement refléter la réelle vision de la banque.

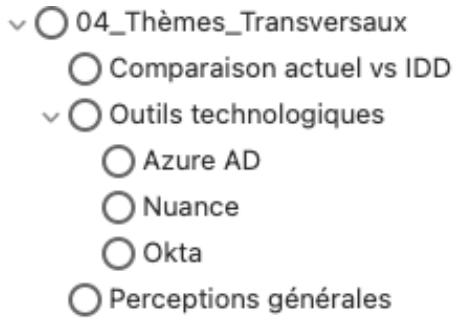


Figure 55 Thèmes transversaux codifiés

Tout d'abord, un premier constat de priorité fût celui de la confiance que la banque représente aux yeux de ses clients. Le niveau de confiance qu'une banque projette, contribue fortement à une relation d'affaire client-banque à long terme. C'est pourquoi un répondant nous partage que la priorité de la banque « c'est la confiance, la stabilité [des] informations clients, d'être l'institution financière à laquelle [les clients] peuvent faire confiance pour dire tout est en sécurité avec nous, puis d'être proche de nos clients » (Entrevue P3A). Un autre point de vue appuie cette observation en soulignant que : « C'est sûr qu'il y a un gros engagement à protéger la donnée des clients [avec] toutes les notions de consentement. » (Entrevue P2A). La banque offre des mesures aux clients, alignées avec la réglementation sur les consentements, pour se positionner comme une entité de confiance et cela s'observe directement au niveau de la sécurité et de la gestion des données clients. Ce souci de conformité et de fiabilité informationnelle est ancré dans la culture organisationnelle et s'exprime autant dans les choix technologiques que dans les politiques internes de protection des renseignements personnels. Puis, ce même répondant nous ajoute que « les priorités de la banque c'est toujours l'acquisition de nouveaux clients, de nouveaux volumes. Par contre, on ne le fait pas au détriment de la qualité des clients et de l'information. Nous sommes sous la loupe constante des instances gouvernementales donc je pense qu'il y a une grande volonté de non seulement avoir de nouveaux clients mais aussi avoir des clients de qualité avec de l'information qui est véridique et vérifiée » (Entrevue P2A). Ce propos souligne bien l'équilibre délicat que la banque cherche à maintenir entre croissance stratégique et rigueur informationnelle. L'idée ici n'est pas de maximiser la quête de

volumétrie client à tout prix, mais plutôt de construire une base client fondée sur l'exactitude et la fiabilité, en respectant les standards réglementaires élevés qui encadrent le secteur financier.

D'autres témoignages convergent plutôt sur l'amélioration continue. La banque montre une volonté de modernisation traduite par une dynamique proactive de transformation numérique tel qu'appuyé par les propos suivants : « On veut se faire une banque plus moderne, technologique, tout ce qui est plus cloud. » (Entrevue P3A). Cette volonté vise à anticiper les besoins des clients de demain en investissant dans l'architecture technologique de la banque, ce qui inclut la migration vers des solutions infonuagiques pour gagner en flexibilité, en rapidité de déploiement et en efficacité opérationnelle. Cette pensée est également reprise par Willump avec les propos suivants : « C'est toujours chercher à s'améliorer » (Entrevue P4C). Une perspective complémentaire sur l'innovation est accentuée par un des membres de la direction qui nous mentionne que « Cette année, c'est la première année que je vois qu'il a vraiment un appétit. Notre président l'a dit, il investit sur toutes les capacités canaux, mais dans des années antérieures, je ne pense pas que le monde voyait les bénéfices d'être sur le mobile. Puis, aujourd'hui c'est 75-80% d'achalandage sur le mobile. » (Entrevue P8H). Cette citation illustre le virage stratégique que la banque amorce vers une approche sur les canaux numériques, et ce en réponse à une évolution des comportements utilisateurs. Le mobile devient un symbole de maturité numérique et d'agilité autant pour la banque que pour les clients.

D'un avis commun et global, les répondants font ressortir l'amélioration continue, la qualité et la confiance comme étant les principales priorités de la banque. Ces trois piliers interreliés forment une ensemble stratégique cohérent que la banque inculque à ses employés et ses clients. Améliorer les processus en continu permet d'assurer une meilleure qualité de service qui elle-même ne doit pas être perçue comme une rupture brutale, mais bien comme un levier au service de la crédibilité, de la sécurité et de la croissance maîtrisée de l'institution.

5.2 Analyse des lacunes du processus actuel de gestion l'identité numérique

L'analyse des lacunes du processus actuel de gestion de l'identité constitue la première étape du processus d'analyse des résultats. Il s'agit ici de l'analyse qui permettra de répondre à notre première sous-question de recherche : Quelles sont les lacunes du processus actuel de gestion de l'identité et des données des clients? Cette section prépare le terrain pour comprendre comment les problèmes qui résonnent dans la banque étudiée font écho aux défis inhérents de la gestion de l'identité numérique, de gestion des

données et au processus traditionnel de connaissance client dans le secteur bancaire canadien. La connaissance des irritants actuels permettra d'identifier les points d'amélioration que la technologie blockchain pourrait éventuellement venir régler. De ce fait, nous avons regrouper les lacunes en trois axes qui ont été soulevées le plus souvent lors de notre codage.

Le premier axe, les problèmes de gouvernance de données, explore les failles structurelles lis à la gestion fragmentée et centralisée des identifiants et des attributs clients. Il est décliné en deux sous-sections : les enjeux de tokenisation et de fraude ainsi que les dysfonctionnements observés dans les systèmes SAP CRM, MDM et les processus KYC. Ensemble, ils mettent en lumière l'opacité et le cloisonnement technologique des systèmes bancaires actuels.

Le deuxième axe, la sécurité, s'intéresse aux tensions persistantes entre la volonté de simplifier les parcours utilisateurs et l'impératif de sécuriser l'accès aux services. Il s'articule en trois dimensions : la recherche d'un équilibre entre simplicité et efficacité au prix de la sécurité, les limites des mécanismes d'authentification actuels et les menaces émergentes liées à l'intelligence artificielle, notamment en matière de falsification d'identité

Le troisième axe, la réticence au changement, met en évidence les barrières humaines et culturelles qui freinent l'adoption de solutions plus innovantes. Deux aspects sont ici développés : la culture organisationnelle souvent ancrée dans une logique de stabilité et de conformité ainsi que les enjeux d'expérience client et employé, qui traduisent une difficulté à concilier transformation numérique, attentes des utilisateurs et engagement interne

Ces trois grands volets constituent une cartographie détaillée des points de friction qui affectent aujourd'hui la gestion de l'identité numérique dans la banque étudiée. Ils forment le fondement à partir duquel nous pourrons, dans les chapitres suivants, évaluer la pertinence des solutions décentralisées comme réponse aux lacunes du système actuel.

5.2.1 Problèmes de gouvernance de données

Tout d'abord, notre schéma de codage pour l'axe de problèmes de gouvernance de données se traduit par l'utilisation des codes suivants dans NVivo : la fraude, la gestion des données et ses outils ou processus sous-jacents (CRM, KYC & MDM). Trois références ont été portés pour la fraude depuis une seule

transcription. Une quinzaine de références sur la gestion des données ont été soulevées, ce qui marque le plus grand nombre de références pour cet axe, alors que CRM suit de près avec treize références. Finalement, deux références ont été annotées pour le processus KYC et quatre pour MDM. Un total de 36 références a été codifié pour le premier axe des lacunes actuelles dans NVivo.

Les membres de la haute direction s'entendent pour dire que la gestion des données n'est pas parfaite à la banque. « On sait que la donnée client est au centre de nos activités. Est ce qu'on l'utilise la bonne façon ? Je pense qu'on a des défis. » (Entrevue P8H) répond Jayce. « Je pense qu'il y a beaucoup d'informations du côté marketing […] qu'on n'utilise peut-être pas ou qu'on utilise moins bien pour le moment » répond à son tour Ezreal (Entrevue P7H).

5.2.1.1 Tokenisation et fraude

Dans le but de protéger les données d'identité, la banque Piltover emploie des mécanismes comme la tokenisation pour atténuer ses vulnérabilités contre la fraude. La tokenisation consiste à substituer les données sensibles par des identifiants sans valeur exploitable, réduisant ainsi la surface d'attaque en cas d'intrusion. Toutefois, nos résultats de terrain révèlent que cette solution, bien que théoriquement robuste, rencontre des limites significatives dans sa mise en œuvre réelle.

Une première faiblesse réside dans la quantité massive d'informations détenues par la banque, qui ne sont pas toutes soumises à un processus de tokenisation. En effet, étant une institution accueillant une quantité substantielle de clients, la banque Piltover « détient beaucoup, beaucoup d'informations » (Entrevue P3A). Fiora renchérit en disant : « [au niveau des limites actuelles], c'est sûr qu'il y a la quantité de données qu'on possède qui n'est pas toute tokenisée évidemment. C'est un risque en soit qu'une partie de l'information ne le soit pas » (Entrevue P2A). Cette observation suggère que même au sein d'infrastructures matures, la sélection des données à tokeniser demeure partielle, laissant place à des zones grises propices à l'exploitation malveillante. La tokenisation est un aspect important de la gestion des données client, car elle suscite une réduction significative des risques liés aux violations de données et une amélioration quant à l'interopérabilité des données entre différents systèmes vis-à-vis des méthodes traditionnelles. C'est pourquoi nous avons pris le temps d'approfondir sur le sujet en analysant la réponse de Fiora lorsque nous lui avons demandé quelles sont les limites actuelles qu'un usager ou qu'un système rencontre au niveau de la gestion des données. Face à cette question, Fiora expose d'abord que :

> « On est capable de voler l'identité pas juste avec une pièce d'identité ou des courriels. Il y a plein d'informations qui sont utilisés partout sur le web qui fait qu'on ne tokenise pas tout et ça peut comporter des risques. Il y a des applications qui ne tokenisent pas ou qui ont des contraintes technologiques qui font en sorte qu'elles ne peuvent pas le faire aussi » (Entrevue P2A).

Ce constat révèle une faiblesse supplémentaire avec la fracture entre les intentions de sécurité exprimées par la banque et sa capacité réelle à protéger au maximum l'ensemble de ses systèmes et données. Un élément de réponse intéressant suivant le discours de Fiora a été retenu où il a été mention de l'aspect budgétaire. L'enjeu budgétaire, souvent occulté dans les discussions, agit comme un frein réel à la sécurisation complètes des systèmes d'information. Fiora confirme cette faiblesse avec lucidité en soulignant que « Il n'y a jamais de limite à ce qu'on peut faire en TI autre que le budget » (Entrevue P2A). Fiora ajoute qu'il serait possible de « tout tokeniser et sécuriser au max tout, mais la réalité fait en sorte que ce qu'on tokenise d'abord ce sont les données de niveau 1. Donc ça ce sont des pièces d'identité, ce sont des numéros de carte, des numéros de compte, des numéros d'assurance sociale. Mais il y a ensuite des données de niveau 2, 3, 4 qui elles ne sont pas tokenisées, mais qui pourraient être utilises à un fraudeur » (Entrevue P2A). La hiérarchisation du risque en lien avec les données tokenisées met en lumière une stratégie de priorisation restreinte où les moyens disponibles déterminent les seuils de sécurité atteignables. Plus préoccupant encore, nos résultats montrent que la menace peut aussi venir de l'interne. Fiora poursuit son discours en déplorant que

> « La fraude c'est souvent fait de l'interne et que malgré qu'un système de tokenisation soit [pratique. Si un utilisateur peut cliquer sur un bouton] pour afficher de l'information, il a accès à l'information. Si c'est fait de manière intelligente, il y a toujours façon d'aller accumuler de l'information sur des individus incluant des données de haut niveau de sécurité, puis [de les exploiter] pour commettre des crimes financiers. Ce n'est pas 100% bulletproof » (Entrevue P2A).

Ce constat illustre la limite d'un modèle de sécurité qui repose exclusivement sur des contrôles techniques sans couplage fort avec des mécanismes de traçabilité, de limitation et de segmentation des droits d'accès et des responsabilités, et ce même si les outils technologiques sont robustes. En revanche, nous remarquons aussi que les problèmes rencontrés par d'autres institutions ont amené les banques, dont la banque étudiée, à revoir ses façons de faire. « Depuis ce temps-là, c'est sûr qu'il y beaucoup, beaucoup, de processus qui ont été mis en place, plus de monitoring qui est fait pour éviter qu'un individu puisse extraire de la donnée massivement facilement. Par contre, comme je disais, un fraudeur, dès qu'il a ton adresse courriel et un mot de passe, il va peut-être capable de commencer à infiltrer des systèmes comme

ton compte bancaire » (Entrevue P2A). Cela montre une faiblesse face aux facteurs externes et que malgré les efforts déployés par la banque, la fragilité demeure, puisque les facteurs externes, comme les réseaux sociaux, ne sont pas sous le contrôle de la banque. Fiora termine en disant que « ce ne sont pas toutes les données qui sont tokenisées, puis sécurisées, mais tout ce qui est jugé absolument nécessaire l'est, puis surtout les personnes qui ont accès à la donnée en tant que tel, et bien on suit et on trace ce qu'ils font. Donc, on est capable de lever des alertes assez rapidement dans le cas où il y aurait des situations potentiellement frauduleuses à l'interne également » (Entrevue P2A).

Enfin, notre expert externe, Ekko, offre une perspective complémentaire sur la faiblesse structurelle du modèle bancaire traditionnel. Il insiste sur l'ampleur des données compromises sur le dark web en disant :

> « Il faut protéger les données personnelles. Il y a beaucoup d'escroqueries, certains prêts sont pris sur votre compte, [et] on ne s'en rend même pas compte. Des millions de données sont disponibles sur le dark web et c'est en raison des cyberattaques. » (Entrevue P5E, traduction libre)

Cette remarque vient élargir le spectre d'analyse au-delà des frontières de l'organisation étudiée, en rappelant que les banques évoluent dans un écosystème numérique menacé globalement par la montée des cyberattaques et l'ingénierie sociale.

Dans son ensemble, cette section montre que la tokenisation, bien qu'efficace sur papier et même en pratique, ne suffit pas à elle seule à garantir une gestion sécurisée des données d'identité. Elle est freinée par des choix budgétaires, des contraintes techniques, des angles morts organisationnels et des limites humaines. La logique défensive actuelle repose encore trop sur des stratégies de protection ponctuelle et de contrôle après-coup, au lieu d'une architecture distribuée, proactive et centrée sur les utilisateurs. Ces constants résonnent fortement avec les faiblesses explorées dans les sections suivantes.

5.2.1.2 Fragmentation des systèmes et processus : SAP CRM, MDM et KYC

La gouvernance des données clients dans le secteur bancaire se doit de reposer sur des systèmes technologiques interopérables, fiables et capables afin de maintenir la cohérence de l'information à travers l'ensemble de l'organisation. Cependant, les résultats de notre enquête terrain révèlent une réalité beaucoup plus différente et complexe, car elle est marquée par une fragmentation notables entre les principaux systèmes utilisés à la banque Piltover, notamment l'outil de gestion de la relation client SAP CRM, le système de gestion de données maîtresses MDM et le processus KYC. Cette fragmentation, loin

d'être un simple enjeu technique, soulève d'importantes préoccupations quant à la fiabilité des données, la charge administrative pour les employés et l'expérience globale du client.

Tel qu'illustré dans la figure 74, SAP CRM et MDM interagissent fréquemment lorsqu'il s'agit des données des clients. MDM est décrit par les employés comme étant le « gardien et maître des informations » (Entrevue P4C) et est la source unique des informations propres au client. Tout système qui met à jour une information client ou souhaite obtenir une information client la plus à jour doit nécessairement passer par MDM. Toutefois, la centralisation des données n'est pas sans faille. Elle figure à nos yeux comme une faiblesse flagrante et nous interrogeons donc les participants sur les problèmes et limites encourus dans SAP CRM et MDM. Leona répond que « l'interaction qu'il y a avec MDM aujourd'hui » constitue une des limites du CRM. « 80-90% des informations qui s'affichent [dans SAP CRM] nous proviennent de MDM. Ces informations, peut-être que MDM les a reçues d'un autre système qu'elle nous partage, qu'elle dispatche par la suite au CRM. » (Entrevue P1A) dit Leona. La dépendance envers MDM ici implique que si MDM reçoit des données qui ne sont pas à jour ou erronées d'un autre système en amont, ces erreurs se propagent jusqu'au CRM, compromettant ainsi la qualité de l'information affichée aux employés. Par exemple :

> « Si le numéro de téléphone d'un client que je reçois [depuis] le dernier Fatpub est différent de ce que j'ai [dans SAP CRM], je le mets à jour. Fatpub c'est un historique de données, un message que je reçois de MDM vers SAP qui contient une concaténation de données » (Entrevue P1A)

Leona souligne donc qu'il « ne faut jamais prendre pour du cash ce qui est affiché dans le CRM, puisqu'il n'est pas owner de cette information. Ce n'est pas certifié l'information qu'il détient, [car] le client a peut-être changé d'adresse entre-temps [depuis la dernière mise à jour] » (Entrevue P1A). L'avis de Leona suggère que l'interaction entre les deux systèmes pose un problème quant à la validité des informations les plus récentes du client. En fonction du ressenti de Leona sur l'interaction entre les systèmes CRM et MDM, nous avons poussé la question plus loin pour déterminer les points d'accrochage plus spécifiques. Il était important pour nous de savoir plus spécifiquement ce qui pose un problème lors d'interactions entre systèmes, car il s'agit d'un élément crucial de la technologie blockchain. L'interopérabilité entre système marque en partie la réussite de l'intégration de la technologie blockchain par sa nature décentralisée. Ainsi, puisque MDM régit et supervise l'ensemble des données reliées au client, les employés sont soumis à des règles spécifiques concernant l'ajout ou la modification d'informations client. Teemo nous indique :

> « Un usager ne peut pas rentrer n'importe quel numéro de référence [dans SAP] pour une pièce d'identité canadienne, parce qu'on est capable de savoir la façon que les pièces d'identité devraient être indexées selon chaque province dans SAP, car SAP lui-même a mis des restrictions afin que les validations prennent place dès l'indexation de cette pièce d'identité. […] Il y a un format à respecter pour les pièces d'identité de catégorie 1. [En revanche, pour les pièces de catégorie 2], on appelle ça un processus double dans SAP [pour vérifier avec deux documents différents] l'adresse et la date de naissance. [Dans ce cas-ci], je peux indexer n'importe quoi comme donnée, parce que SAP ne va pas valider toutes ces pièces d'identité [qui sont de catégorie 2] » (Entrevue P3A)

Nous observons un manque de rigueur entre les pièces de catégorie 1 et 2 qui soulève des préoccupations importantes quant à la qualité et la vérifiabilité des données collectées dans certains contextes.

Outre les règles autour des indexations, nous observons une autre faiblesse quant aux activités que les employés doivent effectuer au moment d'entrer les informations dans le système. Un client qui se présente en succursale ou qui appelle la banque par téléphone, émet à un moment ou un autre une information identificatoire à son sujet que l'employé de la banque doit entendre. Pour plusieurs raisons, l'accent d'une personne, la qualité de la connexion internet ou téléphonique, l'information partagée depuis le client à la personne derrière le comptoir ou la ligne téléphonique peut s'avérer différente qu'elle ne l'est réellement. Dans cette optique, la question demeure autour des limites du CRM. Teemo juge que les indexations manuelles dans SAP sont laborieuses et qu'il y aurait moyen « d'éviter d'entrer manuellement des pièces d'identité pour limiter les erreurs d'entrée manuelles » (Entrevue P3). « Certaines pièces d'identité ont [des] barres code [avec lesquels] on peut faire un scan puis l'indexer pour éviter des erreurs » (Entrevue P3A), affirme Teemo. Cela suggère qu'une partie de la complexité actuelle pourrait être évitée par l'introduction de technologies de numérisation plus robustes qui minimisent l'entrée humaine manuelle. Par ailleurs, notre répondant s'interroge sur la pertinence même de conserver autant de types de pièces d'identité « On accepte beaucoup de pièces d'identité. [Dans SAP], la liste est très très longue. Est-ce que c'est nécessaire avoir toutes ces pièces d'identité là? Je ne sais pas. » (Entrevue P3A), souligne Teemo. Ces impressions nous ont permis de nous questionner sur la validité et véridicité des informations dans les systèmes. Nous nous sommes déjà posé la question des limites du CRM au niveau notamment des interactions entre systèmes SAP CRM et MDM, ainsi que des erreurs d'entrée manuelles à propos des informations client, mais qu'en est-il de l'usage qui en est fait? C'est ce chemin de pensée qui nous a mené à interroger les participants sur l'information qui est affichée dans le profil d'un client. SAP CRM est le vecteur sur lequel les employés se base pour interagir avec leurs clients.

Donc, en ce qui concerne l'information en tant que tel que SAP CRM affiche dans le profil client pour les agents, conseillers financiers et autres employés, nos répondants ont deux visions différentes. Ce questionnement s'est développé du fait que nous voulions savoir si des informations client sont actuellement stockées et affichées à la banque Piltover, mais qu'en réalité ces informations ne soient pas nécessaires. L'usage de protocoles Zero Knowledge Proofs d'une solution blockchain permettrait de divulguer seulement sous certaines conditions proposées par le client ses informations avec la banque. S'il y avait des inconvénients, ou inversement des avantages, pour les clients à avoir ses informations personnelles dans le système centralisé de la banque ou s'il y avait des inconvénients pour les employés eux-mêmes, nous aimerions le savoir. Nous nous sommes dès lors penchés sur la question des informations non pertinentes actuellement dans les systèmes de la banque. D'un côté, Leona est d'avis que « [SAP] affiche des données que je n'ai pas forcément besoin comme usager. Chaque fois que je rentre dans un profil client, je n'ai pas systématiquement besoin de tout ce qu'on affiche comme données clients. » (Entrevue P1) ajoute Leona. Vraisemblablement, l'avis est que les informations stockées dans les systèmes de la banque ne sont pas toutes nécessaires surtout dépendamment de l'usage de la donnée et de l'intention d'interaction avec le client. Un exemple exprimé par Leona est le suivant :

> « Systématiquement, je n'ai pas besoin de connaître son employeur ou son numéro d'assurance sociale. [Que ce soit une information banale ou confidentielle], ces informations qu'on affiche aujourd'hui dans le profil client, l'usager n'en a pas forcément besoin, sauf peut-être à la demande. […] On affiche trop d'informations qui ne sont peut-être pas pertinentes pour ce que je suis en train de faire pour mon client ». (Entrevue P1A)

Il y a donc une surcharge informationnelle qui pourrait être évitée en utilisant par exemple la divulgation sélective de données pour que le client ne mette pas à risque ses données personnelles et pour qu'il puisse jouir des produits et services de la banque selon sa convenance. Ekko va dans le même sens pour sa part en ajoutant ceci lors de notre entretien avec lui :

> « Il faut prendre que les données pertinentes sur les clients. En tant qu'humain on a tendance à prendre toutes les données, mais il n'en est pas nécessaire. Il suffit juste de valider l'existence du client. Il n'est pas nécessaire d'avoir une quantité X de métadonnées sur les clients. Avec une approche minimaliste, on est en mesure de valider le client et son existence. » (Entrevue P5E, traduction libre)

D'un autre côté, Teemo et Fiora s'entendent pour dire « qu'il faut un minimum [d'informations] » (Entrevue P3A) dans le système. Bien que la technologie blockchain apporte des bénéfices pour cacher les renseignements personnels des clients, la banque, quant à elle, a besoin de savoir certaines informations

pour répondre aux besoins de leurs clients. Lorsque Teemo énonce « on catégorise chaque client pour être capable de leur offrir des offres marketing plus précises à certains types de clientèles » (Entrevue P3A), il devient clair que les informations stockées ont une utilité pour la banque. Fiora de son côté s'exprime avec les propos suivants pour renchérir sur la réponse qui nous a été donnée dans l'entretien avec Teemo :

> « Quelqu'un en analytique te dirait qu'il y n'aucune donnée qu'on ne veut pas avoir parce que ça te permet de faire des modèles prédictifs, ça permet de faire du marketing, ça permet de reconnaître des situations à propos du client qui sont peut-être une opportunité de contact ou de conseil, puis finalement d'être capable d'offrir des produits et des services qui soient mieux adaptés à la réalité du client. » (Entrevue P2A)

L'ensemble des données clients, bien qu'elle ne soit pas utilisée quotidiennement par tous, détient quand même une place importante pour les employés en analytique, qui eux se basent sur ces données pour améliorer la valeur offerte par la banque et parallèlement une meilleure personnalisation des services. En revanche, Fiora se pose tout de même la question jusqu'où souhaite-t-on aller? Selon nous, cette réflexion est très importante, car nous comprenons le besoin de conserver certaines données, mais nous souhaitons aussi comprendre ce qui pourrait être optimisé. « Qu'est-ce qu'on a absolument besoin ? » (Entrevue P2A) déclare Fiora. À cette question, la gouvernance des donnés revient à la charge et accentue fortement la problématique sur la manière dont les systèmes de gestion d'information sont actuellement utilisés. L'interrogation de Fiora place la gouvernance de données au cœur des préoccupations stratégiques et opérationnelles de l'organisation.

> « C'est sûr qu'on a besoin de connaître tes pièces d'identité, ton numéro d'assurance sociale pour lier avec ta déclaration de revenus, ton adresse [résidentielle] et ton adresse courriel pour t'envoyer des communications, ton numéro de téléphone. Ton emploi est nécessaire aussi parce que quand on fait des demandes pour des produits de crédit, on veut connaître où tu travailles, ton statut, ton salaire afin d'être capable de faire un bilan financier qui reflète vraiment ta situation financière pour t'approuver ou pas des montant d'octroi. » (Entrevue P2A)

Les répondants ayant une expérience en tant qu'analyste sont en mesure de bien définir les raisons des informations conservées par la banque. Nous soulignons ici le besoin d'une prise de conscience sur la nécessité d'équilibrer la collecte des données et le respect du principe de minimisation. Nous sommes toutefois allés un peu plus loin dans la question en demandant quelles données seraient moins nécessaires. Pour y répondre, Fiora exprime que « c'est dur à dire [et] que cela dépend de comment on se positionne. Nous ne sommes pas non plus Facebook, Google et Instagram qui se partagent la donnée entre eux et qui sont en mesure de déterminer que ton bébé est né et qu'une personne est enceinte. Nous ne sommes pas

aussi bons » (Entrevue P2A). Dans la continuité des choses, nous avions posé la question initialement sur l'utilité des informations qui sont affichées dans le CRM, mais nous voulions également savoir s'il était possible de retirer des informations volontairement du système en tant que client. L'objectif de cette question est de savoir si le client détient aujourd'hui au moins un certain pouvoir de décision sur ses propres données ou si le pouvoir sur les données est complètement détenu par l'institution financière. Les trois répondants à qui nous avons posé la question ont tous répondu que « oui, [mais] jusqu'à un certain point » (Entrevue P2A). Ezreal, un membre de la haute direction, ajoute également que c'est en raison des règles gouvernementales. « Le gouvernement a quand même un grand rôle à jouer sur ce que la banque fait, mais oui à tout moment tu peux demander à ce que tes données écrasées, détruites et avoir une confirmation que ça l'a été fait. Ce sont les nouvelles lois sur les renseignements personnels » (Entrevue P7H). C'est donc dire que le gouvernement, une entité externe à l'organisation, affecte la banque Piltover son cadre réglementaire. Or, même si des facteurs externes impactent négativement la banque et sa gouvernance des données comme c'est le cas avec les réseaux sociaux, ces facteurs peuvent aussi être bénéfiques pour les clients avec les mesures de protection issues du gouvernement. Il convient d'ajouter ici les propos de Leona au sujet des données conservées : « Si [le client] ne détient pas un produit qui nécessite qu'on ait le NAS[32], on ne le garde pas, on ne le demande pas. » (Entrevue P1A). Par exemple :

> « Je fais une demande de financement, je veux un prêt hypothécaire. [La banque] peut me demander une lettre de mon employeur. Cette lettre de mon employeur, une fois que mon processus de demande de prêt hypothécaire est complété, approuvé et que tout est fini. La banque n'a pas à garder ce document-là. [Il se peut que la banque ait à conserver ce document ou un autre] dans le cadre de la conformité réglementaire pendant un minimum de 5 ans dans lequel il y a des délais d'archivage d'informations pour certains documents. Après ces 5 ans, on peut le détruire ou bien jusqu'à ce qu'on termine la relation avec le client, qu'il ne soit plus client de la banque. » (Entrevue P1A)

Conjointement à cette question, le volet de savoir quelles sont les informations détenues par la banque a aussi été posée comme question. Il est intéressant pour nous de savoir si, au-delà du pouvoir de destruction des données clients possédés par la banque, il est également possible de savoir les informations spécifiques au sujet du client, de nous-même, pour identifier les informations exploitables par des criminels ayant accès aux informations. « Les clients peuvent faire des requêtes, une demande à la banque, [pour] savoir c'est quoi les informations que vous détenez [à mon égard] » (Entrevue P1A). Ce constat montre qu'il est possible en tant que client de demander à la banque de détruire ses informations,

[32] NAS est un acronyme pour numéro d'assurance sociale

ce qui témoigne d'un certain pouvoir remis aux clients. Il ne s'agit pas encore d'un pouvoir complet sur sa propre identité et ses données, mais c'est une bonne base.

Toujours dans une optique de gouvernance et de gestion des données, le processus KYC figure parmi toute relation avec un client. Ce processus requiert, tel qu'illustré dans la figure 73, la vérification de l'identité, de documents et des antécédents d'un client. Il s'agit effectivement d'informations identificatoires sur le client afin de déterminer si le client est approuvé ou rejeté par la banque. « Le KYC est le défi principal » (Entrevue P5E, traduction libre), déclare Ekko lorsque nous lui avons demandé quels sont les défis actuels en lien avec la gestion de l'identité. Le processus KYC vient cristalliser plusieurs tensions avec sa lourdeur, redondance, non standardisation et source de frustration.

> « Dans le secteur bancaire, la première étape [d'une intégration client] est le KYC […]. Il y a différentes façons d'effectuer le processus KYC, mais il n'y a pas de mécanisme standardisé. » (Entrevue P5E, traduction libre)

En effet, dans le processus KYC, il arrive également que l'interaction avec le client prenne du temps et impacte l'expérience client. En ce sens, nous avons aussi demandé à nos participants d'identifier, en plus des faiblesses du processus KYC, si c'était un irritant pour les clients de devoir se faire poser plusieurs fois des questions d'identification à plusieurs instances pour vérifier l'identité du client et les réponses sont mitigées parmi les participants. La première approche sur la question du KYC concerne l'identification du client. Que ce soit au téléphone ou en personne, nos résultats présentent l'identification client comme étant ardue en raison de l'incapacité à réellement déterminer si l'individu est la personne qu'elle prétend être. Pour illustrer cette faiblesse, voici un extrait d'un de nos répondants : « le problème [au niveau du KYC] c'est que, surtout pour les appels téléphoniques, tu ne peux pas être sûr que c'est ton client. [Par exemple], peut-être quelqu'un [de proche], un copain ou quelqu'un qui habite à la maison peut avoir accès à ton nom, prénom, adresse […]. Je pense que ce sont des informations très faciles à trouver. » expose Leona. Un client qui appelle la banque doit répondre à des questions de connaissance client, mais ces informations peuvent être disponibles facilement sur internet. Or, le fait de poser des questions fait partie intégrale du processus KYC, mais il demeure que des questions supplémentaire et répétitives sont posées pour pallier à l'incertitude du processus.

Pour faire suite à l'incertitude du KYC, un deuxième élément de réponse concerne la validation du client en soi. Dans ce cas-ci, s'il s'agit vraiment de la bonne personne, mais que le client se fait poser plusieurs fois des questions pour vérifier son identité, alors la frustration monte chez le client. Cette frustration est

causée par la faiblesse du processus KYC et peut impacter négativement l'expérience client. « Cette validation, c'est une question qui [dépend] de la personnalité du client » (Entrevue P1A). Avec cette réponse de Leona, nous comprenons qu'il y a tout de même une ambivalence au niveau des réponses. Pour sa part, Leona souligne :

> « Moi si j'arrive [en succursale] et on me demande toujours est-ce que votre adresse c'est ça? Moi ça ne me dérangerait pas. Mais effectivement, si je viens de changer mon adresse hier [dans le système], c'est très très irritant […]. Mais si tu me reconfirmes rapidement est-ce que c'est la bonne adresse? Moi je ne trouve pas que c'est irritant, mais ça dépend des personnalités. » (Entrevue P1A).

Pour continuer dans la même lignée sur le KYC, Leona affirme que lors du processus en personne, la banque demande une pièce d'identité pour fins d'identification tel que le suggère la figure 70. Toutefois, Leona ajoute qu'il est possible que quelques questions supplémentaires soient posées. De ce fait, « ça peut être très irritant si tu présentes une pièce d'identité, mais ils te posent 36,000 questions pour s'assurer de ton identité. Moi ça m'est arrivé […]. Je pense que la personne a passé 15 minutes à me poser des questions pour bien s'assurer que c'est bien moi. Ça c'est frustrant […]. C'est rendu limite trop d'informations personnelles que je te donne pour m'identifier. » (Entrevue P1A). Non seulement l'expérience client est affectée, élément jugé important selon les priorités de la banque, mais Leona souligne que trop d'informations sont partagées, ce qui remet en question à nouveau l'intérêt de détenir autant d'informations au sujet d'un même client, surtout si l'identification n'est pas simple et efficace. À l'inverse, un de nos répondants nous amène une point de vue différent sur l'importance des nombreuses questions. Ce point de vue suggère qu'il peut être rassurant pour un client de ses faire poser des questions, car sans cela n'importe quel personne pourrait se faire passer pour soi. C'est pour cette raison que Teemo mentionne pour sa part que le client « veut se faire poser des questions parce que si tu ne te fais pas poser des questions il y a un gros problème. Ça peut devenir frustrant quand tu veux transférer de l'argent et on te demande qui vous êtes, à qui, pourquoi? Mais c'est une banque, il faut qu'on garde certaines informations pour le blanchiment d'argent. » (Entrevue P3A). La lutte contre le blanchiment d'argent, évoqué par Teemo à la fin de ses propos, revêt une grande importance, car il nécessite la conservation des informations à cette fin.

En somme, l'ensemble des résultats illustre les limites structurelles d'une architecture d'identité centralisée, fragmentée et peu flexible, qui repose sur une interconnexion imparfaite entre des systèmes comme SAP CRM et MDM ainsi de que sur des processus KYC. Ces faiblesses se traduisent à la fois par des

redondances informationnelles, des erreurs d'entrée manuelles, des doutes sur la validité des données et une surcharge informationnelle qui nuit à la clarté et à la pertinence des interactions client-banque. Si certains répondants reconnaissent l'utilité stratégique des données stockées pour des fins analytiques ou marketing, d'autres remettent en question la nécessité de tout conserver ou afficher. Cette tension entre la nécessité fonctionnelle et le principe de minimalisation reflète l'absence d'une gouvernance des données réellement adaptée aux besoins actuels des clients, tout en exposant la banque à des risques réputationnels et réglementaires. De plus, le processus KYC est particulièrement rigide, non standardisé et parfois vécu comme intrusif par les clients, ce qui accentue le besoin d'un modèle plus fluide, vérifiable et centré sur l'utilisateur. Ces constats suggèrent que l'intégration d'une infrastructure décentralisée fondée sur des principes comme la divulgation sélective ou l'interopérabilité des données d'identité pourrait représenter une réponse structurelle à ces défis, à condition qu'elle soit accompagnée d'une réingénierie profonde des processus internes.

Codification / Thème	Nombre d'entrevues	Références
Fraude	1	3
Gestion des données	5	13
CRM	2	13
KYC	2	2
MDM	2	4

Tableau 5 Codifications et références des problèmes de gouvernance de données

5.2.2 Sécurité

La sécurité est un aspect critique de notre analyse sur les lacunes des systèmes bancaires traditionnels. Elle se place comme étant la lacune qui pourrait potentiellement mener le changement vers de nouvelles technologies. Bien que la sécurité puisse être perçue au niveau du thème précédent, soit la gouvernance des données, ainsi que certains autres thèmes, nous avons décidé de prendre la sécurité à part pour aller

plus loin sur des sujets comme la fraude et l'authentification des clients. Pour ce faire, nous avons codifié les thèmes suivants en lien avec la sécurité : l'authentification, la collaboration avec les fournisseurs, l'intelligence artificielle et la simplicité au prix de la sécurité. L'authentification a été référé à douze reprises depuis trois transcriptions, tandis que son sous-thème collaboration avec les fournisseurs, seulement deux références. L'intelligence artificielle à une reprise, alors que la simplicité et l'efficacité quatre et deux respectivement. Finalement, le nombre de références au profil des clients s'élève à deux références pour une transcription. Un total de 23 références a été porté.

5.2.2.1 Simplicité et efficacité au prix de la sécurité

Dans le secteur bancaire, la recherche de performance opérationnelle impose souvent des arbitrages entre rapidité d'exécution, convivialité des interfaces et solidité des mécanismes de sécurité. Cette tension se manifeste particulièrement lorsqu'il s'agit d'implémenter des nouvelles solutions technologiques. En effet, les exigences de conformité, de fluidité de parcours client et de protection des données cohabitent difficilement dans un univers où les systèmes sont historiquement fragmentés. À cet égard, un de répondants a souligné l'absence de standards techniques communs et la diversité des pratiques d'identification à travers les institutions, ce qui rend la consolidation des efforts de sécurité difficile. L'un des experts interrogés décrit cette situation comme un déséquilibre fondamental entre la diversité des systèmes en place et l'absence d'une couche de coordination unifiée.

> « La sécurité est le plus grand défi du secteur bancaire en raison du nombre de systèmes d'identité différents dans le monde. Les meilleures pratiques actuelles ne sont pas sécures en raison de l'utilisation de technologies tel que le DNS […]. Chaque banque a ses propres règles et organismes de standardisation, et il n'existe pas de couche unifiée. C'est comme s'il manquait le réseau Swift, soit le réseau utilisé par les banques pour communiquer, pour les consommateurs. Une couche similaire est nécessaire pour les transactions B2C[33] » (Entrevue P6E, traduction libre)

Il y a donc une carence structurelle qui se fait sentir. Dans un tel contexte, la quête de simplicité dans les processus internes et l'expérience client devient non seulement un enjeu d'efficacité, mais aussi un facteur aggravant de vulnérabilité, puisqu'elle s'appuie sur des mécanismes d'authentification disparates et souvent obsolètes. En ce sens, tout comme le trilemme de la blockchain qui stipule qu'une blockchain peine à optimiser simultanément la scalabilité, la sécurité et la décentralisation (Werth *et al.*, 2023, p. 146), il existe aussi un trilemme en sécurité TI (Theyse, 2024). La figure 78 illustre que dans toute décision

[33] B2C est un acronyme pour Bank to Customer ou Banque à Client

d'architecture ou de processus technologique, optimiser un de ces piliers signifie inévitablement en compromettre au moins un autre. C'est précisément ce trilemme que vivent quotidiennement les institutions financières. La banque Piltover doit faire des choix stratégiques en ayant en tête ce trilemme et c'est pour cette raison qu'opter pour la simplicité peut impacter négativement la sécurité des opérations. Au sein de la banque Piltover, cette tension entre efficacité opérationnelle et sécurité est omniprésente. Les propos recueillis lors des entretiens révèlent une tendance à privilégier la simplicité au détriment des mécanismes de protection plus robustes. Autrement dit, l'expérience client est largement priorisée à la banque.

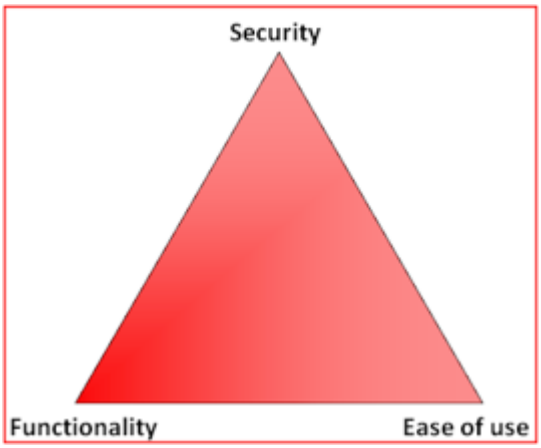


Figure 56 Trilemme des TI (C3L Security, 2019)

Pour le confirmer, nous avons interrogé nos répondants sur ce qui était perçu comme étant le plus important ou impacté des trois. Pour sa part, Fiora confirme ce constat en disant que « c'est sûr que centraliser la donnée c'est un gain d'efficacité » (Entrevue P2A). Ici, l'efficacité est perçue comme une valeur essentielle, car la centralisation permet une meilleure accessibilité des données. Cela signifie que la simplicité est mise de l'avant dans ses propos. De plus, Fiora termine ses propos précédents avec l'exemple suivant : « Quand tu veux ouvrir de nouveaux comptes ou quand tu fais affaire avec une nouvelle entreprise, ça simplifie le processus. D'un autre côté, c'est de la gestion supplémentaire » (Entrevue P2A). Or, en pesant ses propos, Fiora nous fait comprendre que la simplicité est de mise avec la centralisation des données, mais qu'en contrepartie elle demande plus de gestion. Cela témoigne une idéologie procédurale simple, mais dans la pratique, elle s'avère compliquée.

Cette tension entre simplicité et sécurité est perçue avec acuité par d'autres répondants. Leona, adoptant la posture client, exprime une préférence claire pour la sécurité en disant : « moi je pense que comme client je préfère avoir une application sur mon téléphone un petit peu moins sophistiquée mais que je suis sûr à 1,000% que je ne me fais pas frauder » (Entrevue P1A). Sa perspective souligne une méfiance fondée sur les risques liés à la sécurité vis-à-vis des outils numériques actuels. Toutefois, Leona ajoute « Comme client j'aimerais un équilibre, un minimum d'équilibre » (Entrevue P1A), ce qui montre une réflexion parcimonieuse de la stature actuelle à la banque en tant qu'employé et client.

Puis, Willump offre pour sa part une vision lucide de la ligne de crête sur laquelle marche la banque : « la banque veut essayer d'être sécurisée, mais ne veut pas impacter les clients […]. Alors pour moi aujourd'hui, [les processus] sont simples, mais pas forcément sécuritaires. » (Entrevue P4C). Or, ce qui ressort des répondants pour la simplicité et l'efficacité au prix de la sécurité, c'est qu'ils impliquent des défis de sécurité, puisque la banque favorise l'expérience utilisateur. Cette problématique est bien exprimée par le passage suivant indiquant la réalité de certains clients : « Dans les clients qu'on a, il a des gens qui ont un certain âge. Il y a des gens avec des handicaps qui ne sont pas forcément capables d'accéder ou d'utiliser facilement certains outils, donc c'est tout un challenge » (Entrevue P4C). Bien que la centralisation soit un gain en efficacité et que l'expérience utilisateur soit mise de l'avant par la banque, nous nous demandons à quel prix. Les propos des répondants stipulent que la sécurité et l'expérience sont au cœur des décisions de la banque, mais qu'ultimement lorsqu'il s'agit de prioriser entre les différentes dimensions du trilemme Willump tranche sans détour « en 2^{e} ce serait clairement la sécurité » (Entrevue P4C).

En somme, cette section révèle une stratégie d'arbitrage technologique fondée sur une tension constante entre performance perçue et robustesse invisible. La banque Piltover, comme de nombreuses institutions financières, s'efforce de rendre ses processus le plus simple possible pour ses clients. En revanche, cette volonté se heurte à la réalité opérationnelle. En effet, bien qu'essentielle, la simplicité se fait parfois au prix d'une sécurité affaiblie ou d'une complexité de gestion accrue en arrière-plan. La question qui se pose dès lors n'est pas de choisir entre sécurité et simplicité, mais bien de trouver des solutions technologiques capables de réconcilier ces deux impératifs. Les solutions décentralisés tels que les identifiants décentralisés pourraient représenter une voie d'équilibre dans une paysage technologique où le trilemme reste jusqu'ici irrésolu.

5.2.2.2 Enjeux d'authentification

La codification du thème de l'authentification a été principalement discuté avec Willump. Étant à la direction du domaine de la cybersécurité, nous avons posé des questions plus spécifiques sur le processus de gestion des identités afin d'identifier ses lacunes actuelles. Tel qu'illustré dans la figure 70, Okta joue un grand rôle dans la gestion de l'identité et l'authentification des clients. Nous avons donc premièrement posé la question à Willump sur la façon dont Okta est utilisé.

> « Okta c'est la plateforme qu'on utilise pour gérer toute la partie authentification et autorisation. C'est vraiment l'outil qu'on utilise en mode SaaS[34] pour pouvoir gérer les identités. Okta c'est un fournisseur d'identité, donc en effet, il permet de gérer les identités, il permet de définir des droits pour accéder à un certain nombre d'applications. Il contient des identités, mais qui sont déjà stockées ailleurs et on veut pouvoir les réutiliser […]. L'identité est stockée dans Azure AD, mais au travers d'Okta. On appelle un autre fournisseur d'identité pour que quand la personne va essayer de se connecter dans Okta, Okta ne va pas vérifier dans sa base de données si la personne existe, mais va vérifier auprès de l'autre base de données si la personne existe et si ces justificatifs sont corrects. » (Entrevue P4C).

Ce passage met donc en lumière Okta et Azure AD dans le processus de gestion des identités. Cette question nous a permis de comprendre le flux entre Okta et Azure AD pour ensuite pouvoir demander quels sont les principaux défis et limitations rencontrées dans le processus actuel de gestion de l'identité des clients. Le répondant a ensuite exprimé : « Aujourd'hui, toute la partie création de compte ça se passe plutôt bien. Là où on a des enjeux c'est clairement plus au niveau de l'authentification donc les MFA, les facteurs d'authentification multiples, au sens Okta » (Entrevue P4C). Ces MFA font écho aux facteurs connus discutés dans notre revue de littérature où ils doivent nécessairement être soit un élément de connaissance (ex : mot de passe), un élément biométrique (ex : voix) et un élément de possession (ex : codes envoyés sur un téléphone). Il convient de rappeler rapidement ici les différentes façons qu'un client peut interagir avec la banque. Un client peut se présenter en personne dans une succursale, appeler la ligne téléphonique de la banque ou bien naviguer sur internet et se connecter à son compte bancaire. Tel que souligné plus tôt par Leona, un client qui se présente en personne doit présenter une pièce d'identité pour s'identifier. Au téléphone, ça peut aussi être via la reconnaissance vocale ou une enveloppe numérique envoyé par texto ou courriel au client tel que soulevé par Fiora. Sur internet, le client se connecte sur son compte au moyen de son mot de passe et d'un code envoyé sur son téléphone. Ainsi, les lacunes s'articulant autour de l'authentification se passe au niveau des facteurs d'authentification lors

[34] SaaS est un acronyme pour Software as a service

d'une tentative d'interaction d'un client avec la banque. Cette perception est illustrée dans les propos suivants :

> « La biométrie vocale a été mise en place pour s'assurer de rajouter une couche supplémentaire de sécurité. Mais on voit par exemple à côté que les mots de passe, la Banque a du mal à retirer ça ou même à retirer certains autres facteurs comme le téléphone ou les SMS qui sont reconnus comme étant pas suffisamment fiables vis-à-vis des autorités de cybersécurité. Ils ont du mal parce qu'ils se disent que ça impacte les clients. Donc c'est compliqué de faire bouger les choses. C'est ce bout-là qui est le plus gros challenge de notre côté. » (Entrevue P4C).

Ici, un paradoxe se dessine. Alors que certaines méthodes sont connues pour être vulnérables (ex : SMS), celles-ci sont tout de même maintenues pour ne pas déstabiliser les habitudes des clients. Ces propos traduisent donc un fort sentiment accordé à l'expérience utilisateur et cela freine la progression vers une sécurité plus avancée. « La biométrie vocale aujourd'hui n'est pas utilisée comme étant TA clé d'authentification, mais comme étant UNE clé d'authentification. [Aussi], la biométrie vocale, forcément, on a cette limitation que c'est uniquement quand tu appelles [la banque], mais s'il y avait quelque chose de similaire pour n'importe quelle autre fonctionnalité que ce soit le web ou mobile, je pense que ça serait un gros oui [du côté de la banque] » (Entrevue P4C) renchérit Willump. Ce commentaire montre que même les solutions innovantes comme la biométrie vocale restent insuffisantes pour réellement authentifier un client. En parallèle Leona exprime que le MFA n'est pas une source fiable avec les propos : « même le MFA ne peut pas être exact […]. La double identification ce n'est apparemment pas sécuritaire à 100%. » (Entrevue P1A). Dans la même optique que la fraude, « ce n'est pas monsieur tout le monde qui peut frauder avec un minimum d'informations, [mais] les fraudeurs arrivent de plusieurs façons à essayer de trouver des informations. Juste Facebook c'est un bon endroit où voir les informations des gens » (Entrevue P1A). Avec ces propos, nous comprenons que l'authentification multifactorielle perd en sécurité avec les informations sur notre identité traînant un peu partout sur internet, notamment sur les réseaux sociaux, où l'ingénierie sociale peut se faire facilement. En complément des défis MFA, Jayce ajoute aux défis de l'authentification la collaboration avec les fournisseurs d'identité dans ce cas-ci avec les propos :

> « L'authentification à la banque est faite par un groupe trans, donc quand que les gens se connectent au niveau du mobile ou au niveau du transactionnel, c'est une capacité externe avec un roadmap externe. Donc, arrimer les plans ensemble, ça devient un défi. En termes de compréhension du client, ça devient un défi, ces groupes-là ne sont pas *front* avec nous, avec le UX/UI, ils ont une compréhension de la technologie, mais voient moins les impacts clients, ils voient moins les impacts, car ils sont plus en retrait de leur responsabilité en termes de quand ça fonctionne moins bien » (Entrevue P8H).

En somme, l'enjeu d'authentification dans le contexte bancaire dépasse le cadre technique. Il traduit un équilibre instable entre sécurité, confort d'utilisation, crédibilité perçue et collaboration avec les acteurs externes. Bien que des solutions comme la biométrie soient mises en place, leur usage reste insuffisant et doit être complémenter par d'autres méthodes d'authentification. Le frein principal ne réside pas dans la technologie, mais dans la capacité de la banque à réconcilier innovation, conformité et acceptabilité client. Dans un environnement où l'identité devient un actif stratégique, l'authentification mérite d'être reconfigurée en profondeur.

5.2.2.3 Enjeux avec l'intelligence artificielle

Au-delà de l'ingénierie sociale et des outils communs d'hameçonnage, l'intelligence artificielle vient aujourd'hui s'installer dans le portait des risques de sécurité. Les technologies de duplication de voix, de visage et l'utilisation des Deepfakes font partie intégrale des outils de l'intelligence artificielle. De ce fait, nous avons posé la question à Willump pour identifier quels sont les problèmes amenés par l'IA et s'il y a des mesures prises actuellement pour contourner ces problèmes. « On s'est posé les mêmes questions » (Entrevue P4C) confirme Willump. Avant de s'attarder à ce qui est mis en place, observons le processus actuel : « Donc les personnes, quand ils vont appeler, l'agent qui va être au bout de la ligne va poser des questions, va discuter avec la personne, pour voir si au niveau du Matching de la voix tout se passe correctement » (Entrevue P4C). Ce passage met une évidence sur l'utilisation d'un outil qui sait reconnaître les voix. « L'intelligence qu'il y a dans cet outil, [qui] n'est pas du tout dans Okta, c'est un autre outil géré par Microsoft, va analyser la voix et il va donner un score [de comparaison] avec ce qu'il a [déjà] enregistré, (les tics verbaux), et estimer à combien c'est bien la bonne personne. Mais l'outil va juste communiquer une information derrière. Ça reste une action humaine au niveau de la biométrie vocale pour le moment à la banque pour [valider] si c'est la bonne personne ou non » (Entrevue P4C). L'outil dont il est question ici est Nuance et il a été illustré dans la figure 70. Or, pour contrer la montée de ces menaces, la banque a déployé un système de reconnaissance vocale destiné à valider l'identité des clients lors des appels téléphoniques. En ce qui concerne la façon dont la banque se défend contre la menace de l'IA, elle s'y prend par un combat du feu par le feu. Grâce à Microsoft Nuance, les employés sont en mesure de déterminer plus facilement si le client au bout de la ligne est réellement la bonne personne. Il faut toutefois que l'employé effectue une validation manuelle et que ce client soit un client existant dans le système de la banque afin que Nuance puisse reconnaître la voix, les tics, l'intonation, etc. Bien que l'outil témoigne une avancée des anciens systèmes en place, elle comporte tout de même ses limites.

En somme, les participants exposent que les problèmes liés à la sécurité sont au niveau des MFA et tout ce qui englobe les facteurs d'authentification en tant que tel, la collaboration avec les fournisseurs d'identité, l'intelligence artificielle ainsi que la simplicité et l'efficacité au prix de la sécurité. Ces défis et limitations nous montrent que le trilemme TI se traduit dans l'organisation par les choix de la haute direction, le profil des clients ainsi que des technologies de pointe qui sont utilisées par la banque ou même par les criminels qui souhaitent s'infiltrer dans les systèmes.

Codification / Thème	Nombre d'entrevues	Références
Authentification	3	12
Collaboration avec les fournisseurs	1	2
Intelligence artificielle	1	1
Simplicité au prix de la sécurité	2	4
Efficacité	2	2
Profil des clients	1	2

Tableau 6 Codification des références de la sécurité

5.2.3 Réticence au changement

La réticence au changement constitue le dernier sous-code de l'axe sur les lacunes actuelles du processus de gestion l'identité numérique dans un système bancaire traditionnel. Bien que l'expérience utilisateur ait été abordé lors du thème précédent, nous avons ciblé dans cette thématique l'aspect humain du changement. À différent de la résistance au changement, la réticence au changement renvoie davantage à une hésitation ou une inquiétude passagère, souvent liée à l'incertitude ou au manque d'information. En ce sens, nous avons identifié les thèmes suivants concernant la réticence au changement : la culture organisationnelle référée à cinq reprises depuis trois transcriptions, la communication interne référée une fois depuis une transcription, l'expérience des clients référée six fois depuis deux transcriptions et l'expérience des employés référée trois fois depuis trois transcriptions pour un total de quinze références.

5.2.3.1 Culture organisationnelle

Nous souhaitons débuter le thème de la culture organisationnelle en spécifiant qu'il ne s'agit pas une lacune actuelle en soi. Il s'agit plutôt d'un thème qui a des répercussions sur les expériences des clients et des employés. La culture organisationnelle est une toile de fond omniprésente qui forge aussi bien les stratégies d'innovation que les arbitrages opérationnels. Elle exerce un effet d'entraînement sur la manière dont les projets émergent, sont évalués et éventuellement priorisés ou mis de côté. En ce sens, elle représente un levier déterminant dans la capacité d'une organisation à évoluer vers de nouvelles solutions technologiques.

L'avis de nos répondants ont souligné plus tôt que la banque et ses priorités ont des impacts sur la simplicité, l'efficacité et la sécurité. « L'enjeu c'est comment on peut garder ça simple pour le client » (Entrevue P4C) exprime Willump. Cette phrase met en lumière le fait que la simplification des processus pour les clients soit un élément qui fait partie de la culture organisationnelle et, par conséquent, de la prise de décision. La simplicité est un aspect aux yeux de la banque qui doit être priorisé, mais tel que soulevé par Fiora, le budget joue aussi un grand rôle dans les décisions. Les choix technologiques, notamment en matière de transformation numérique, sont souvent ajustés à la lumière de ce critère. Lorsque Fiora mentionnait qu'il serait possible de tout tokeniser, mais que c'est le budget qui dicte les choix de quoi tokeniser en premier, il faut se tourner vers la culture de l'organisation pour identifier les perspectives qui mènent le changement. Ce constant est confirmé par Jayce, qui, tout en reconnaissant l'ouverture à l'innovation, précise que celle-ci dépend de la capacité à démontrer de la valeur.

> « Il y a un appétit au niveau de l'organisation, mais il faut démontrer qu'on a la capacité de livrer, puis d'amener de la valeur. Ça c'est le défi qu'on a comme organisation » (Entrevue P8H).

Ces propos signifient qu'en tant qu'organisation, même s'il existe des nouvelles technologies ou façons de faire, elle reste ouverte au changement, tant et aussi longtemps qu'il y aura une valeur ajoutée. C'est donc dire que la banque fait ses choix vers le changement en fonction de la valeur, des coûts, de la rentabilité et surtout de la capacité à livrer. Il faut donc monter ce qu'on appelle un « business case » pour apporter un changement aux yeux de la haute direction. Avec le passage de Jayce, nous sommes dès lors en mesure d'identifier une réticence au changement et non une résistance au changement. C'est une réticence, car la banque reste ouverte au changement et c'est également un défi, puisqu'il faut monter un business case robuste qui sera porteur du changement. Nous discuterons du business case plus en détails dans la section

Vision Stratégique de notre analyse des résultats. Pour le moment, nous nous concentrerons sur les humains derrière les business case.

En somme, la culture organisationnelle de la banque Piltover agit comme un prisme structurant à travers lequel sont évaluées toutes les décisions de changement, y compris celles touchant la gestion de l'identité numérique. Plutôt que de manifester une résistance fermée à l'innovation, l'organisation fait preuve de réticence stratégique fondée sur la nécessité de démontrer une valeur concrète, mesurable et réaliste avant de s'engager. Bien que cette posture puisse ralentir l'adoption de technologies émergentes, elle n'en demeure pas moins ouverte à des solutions qui s'alignent avec les priorités organisationnelles de confiance, d'expérience client et de rentabilité. La culture organisationnelle devient ainsi un facteur d'arbitrage central dans la trajectoire d'adoption du changement.

5.2.3.2 Enjeux d'expérience client et employé

Pour enchaîner sur les derniers propos du membre de la haute direction, Ezreal affirme pour sa part que « la collaboration inter-secteurs à la banque ce n'est pas la chose la plus simple » (Entrevue P7H). En début d'analyse, nous avions souligné les défis d'interopérabilité entre systèmes. Ici, c'est l'interopérabilité entre humains, équipes, départements et secteurs d'affaires. Ce sont des humains, les employés, derrière les technologies et nous savons maintenant qu'il peut y avoir des difficultés au moment de travailler ensemble en tant qu'organisation lors d'un changement ou même lors de communications à l'interne. L'expérience des employés est impactée par la culture de l'organisation dans la mesure où l'expérience est modelée selon les interactions entre humains.

Du côté des clients, la réalité est que si un changement impacte le client, « c'est compliqué à faire bouger les choses. » (Entrevue P4C). En se fiant aux propos préalablement cités de Willump : « la banque veut essayer d'être sécurisée, mais ne veut pas impacter les clients. » (Entrevue P4C), nous avons tenté de savoir en quoi peut consister cet impact sur le client et son expérience. Est-ce simplement de changer l'interface d'une page web et d'une application mobile ou est-ce plutôt de changer des habitudes comme la façon de se connecter au compte bancaire en ligne ? En ce sens, Willump explique que la banque ne souhaite pas changer le processus des mots de passe par exemple, même si c'est « pour des raisons de sécurité, parce que ce sont les bonnes pratiques. Changez votre mot de passe pour avoir quelque chose de plus long, [la banque] ne veut pas » (Entrevue P4C). Ce témoignage marque solidement la ligne que la banque considère un changement ou un impact sur l'expérience client. La banque n'est pas prête à faire

un changement qui impacterait les habitudes et l'expérience du client. « Nous, à côté, on pousse pour avoir quelque chose de sécure, [mais] on fait avec ce qu'on peut. » rétorque Willump. En outre, Teemo et Leona ont indépendamment exprimé que les clients sont capables de s'adapter aux changements lorsque nous avons demandé si aujourd'hui nous sommes prêts à avoir une nouvelle technologie comme la blockchain :

> « Il faut toujours s'adapter aux nouveaux changements. On sait qu'en 2025, la technologie avance. C'est sûr qu'on ne va pas reculer, c'est toujours de l'avant, c'est toujours de nouveautés, c'est toujours la plus haute technologie. [Surtout] les jeunes. Ils veulent ça les changements. Ils aiment ça la technologie, la simplicité, l'efficacité. Même s'ils n'aiment pas ça, ils n'ont pas le choix de s'adapter. On ne recule pas en arrière, on fait juste avancer. » (Entrevue P3A).

Parallèlement, Leona nous explique son point de vue suivant :

> « Avec les nouvelles générations, oui. Mais on tient compte des anciennes générations encore, aujourd'hui. N'oublie pas que les boomers, ils s'adaptent. Regarde nos parents, ils ont tous un compte Instagram, Facebook, téléphone intelligent et ils s'adaptent quand même aux nouvelles technologies. » (Entrevue P1A).

En somme, la culture organisationnelle de la banque, bien qu'elle ne soit pas une lacune, impacte indirectement l'expérience des employés et des clients de la banque. En adoptant une culture qui priorise l'expérience, la confiance, la sécurité et l'aspect financier dans cet ordre, il est compréhensible que des projets technologiques ne voient pas le jour. Que ce soit en raison du business case, de la valeur ajoutée ou de l'impact direct sur le client, nous constatons une réticence au changement. D'un autre côté, tel qu'exprimé par Teemo et Leona, il ne fait pas sous-estimer les clients. Ceux-ci sont en mesure de s'adapter et ils l'ont déjà prouvé avec les technologies que nous avons aujourd'hui.

5.2.4 Synthèse de l'analyse des lacunes du processus actuel de gestion de l'identité

En conclusion, l'analyse des lacunes actuelles du processus de gestion de l'identité révèle plusieurs domaines critiques nécessitant des améliorations et des tensions entre les objectifs d'efficacité opérationnelle, les exigences de sécurité et les dynamiques organisationnelles. Trois axes principaux structurent cette analyse : la gouvernance des données, la sécurité et la réticence au changement. Sur le plan de la gouvernance des données, les systèmes actuels manquent de cohérence et d'interopérabilité, en particulier l'intégration entre les systèmes SAP CRM et MDM ainsi que les processus KYC. Ce morcellement engendre des risques sécurité important, dont notamment la fraude, et ce malgré la

présence de mécanismes de protection des données comme la tokenisation. En effet, la présence massive des données sur le web rend la gouvernance des données d'identité des clients encore plus compliquée pour la banque. La tokenisation atteint dès lors ses limites rapidement si nous considérons les facteurs externes à la banque. Cette configuration technique des processus empêche l'émergence d'affordances de visibilité systémique, c'est-à-dire la capacité pour les utilisateurs à percevoir clairement les circuits de données, leur validité, ainsi que les responsabilités associées à leur gestion.

Concernant la sécurité, les compromis technologiques effectués au nom de la simplicité, comme l'authentification par mots de passe ou code envoyés par SMS, exposent la banque à des vulnérabilités critiques. Les parcours d'authentification ne soutiennent pas une affordance de cohérence perceptible, ce qui rend l'adoption de comportements sécuritaires adaptés par les clients comme par les employés plus difficiles. La réticence au changement, profondément enracinée dans la culture organisationnelle, freine la volonté de modernisation. En effet, les expériences vécues par les clients sont considérées de près pour évaluer tout changement. Si le changement risque de trop perturber l'expérience actuelle du client, alors la banque décide de ne rien changer, même si c'est pour améliorer les bonnes pratiques. Le changement doit se faire de façon transparente, sans quoi elle se verra vouée à l'échec ou du moins aura plus de difficulté à se vendre. Par conséquent, l'absence d'affordances perçues d'appropriation organisationnelle et technologique limite la capacité des employés et des clients à s'engager activement dans l'usage de nouveaux outils. Parallèlement, la faible affordance perçue de valorisation du rôle du client, telle qu'elle est médiée par le cadre organisationnel, limite leur capacité à se percevoir comme des acteurs clés et habilités du processus d'innovation. Cela engendre un désalignement entre la perception des besoins technologiques et les capacités d'adaptation pourtant perçues chez les employés et démontrées par les usagers eux-mêmes.

Le système actuel échoue dès lors à offrir des affordances cognitives, fonctionnelles et sociales adéquates pour soutenir une gestion fluide, sécurisée et acceptée de l'identité numérique. Cette déficience affecte non seulement la performance opérationnelle, mais également la capacité des acteurs humains à s'orienter, interagir et faire confiance aux technologies en place ou à venir. Ces constats justifient une transition vers des solutions plus intégrées et orientées utilisateurs, notamment celles basées sur l'identité auto-souveraine et les identifiants décentralisées.

Codification / Thème	Nombre d'entrevues	Références
Culture organisationnelle	3	5
Communication interne	1	1
Expérience client	2	6
Expérience employé	3	3

Tableau 7 Codification et références de la réticence au changement

Thème	Sous-thème
Gouvernance de données	• Tokenisation • Fraude • SAP CRM • MDM • KYC
Sécurité	• Simplicité & Efficacité au prix de la sécurité • Authentification • Intelligence artificielle
Réticence au changement	• Culture organisationnelle • Expérience client • Expérience employé

Tableau 8 Synthèse des lacunes actuelles

5.3 Analyse des défis et opportunités liés à l'intégration des IDDs

L'analyse des défis et opportunités liés à l'intégration des IDDs constitue la deuxième étape du processus d'analyse des résultats. Il s'agit ici de l'analyse qui permettra de répondre à notre deuxième sous-question de recherche : Quels sont les défis et opportunités à long terme liés à la réingénierie des processus bancaires pour intégrer les identifiants décentralisés? Pour éclairer cette interrogation, nous avons réalisé des entrevues détaillées avec des spécialistes techniques du domaine de l'identité numérique distribuée et de la technologie blockchain, ayant une expérience pratique dans la mise en œuvre dans le secteur financier. Les personnes interrogées ont principalement été les deux experts blockchain Kennen et Ekko plutôt que les employés et membres de la haute direction de la banque Piltover en raison de leur connaissance approfondie sur le sujet. Bien que la portée de notre recherche se concentre sur la banque Piltover, les employés et dirigeants de la banque n'ont pas suffisamment de connaissances ou même pour certains n'ont jamais entendu parler de la technologie blockchain. Par conséquent, Kennen et Ekko ont été ciblés pour leur maîtrise remarquable de l'architecture de l'identité décentralisée, du développement de systèmes distribués, ainsi que de la transformation numérique dans le secteur financier. Grâce à leur expertise dans des domaines clés, tels que les identifiants décentralisés, l'identité auto-souveraine, les informations d'identification vérifiables, ainsi que des solutions blockchains comme Hyperledger (Sovrin) et le « Key Event Receipt Infrastructure » (KERI), nous sommes en mesure d'analyser les biens faits et les problématiques tant sur le plan technique qu'opérationnel.

L'analyse actuelle des défis et opportunités des IDDs ne vise pas à fournir un aperçu technique des procédures d'identification décentralisée, mais plutôt à mettre en évidence les conséquences, positives et négatives, fondamentales de leur incorporation dans les systèmes bancaires. L'adoption des IDDs ne se limite pas à une simple mise à niveau technologique. Elle soulève des questions cruciales sur la gestion de l'identité client, la souveraineté des données, la conformité réglementaire, la standardisation des infrastructures bancaires et l'évolution de la relation entre les banques et leurs clients. L'analyse repose sur une codification thématique des entrevues, qui permet de mettre en évidence les défis structurels, technologiques et organisationnels récurrents, ainsi que les opportunités stratégiques associées à la mise en œuvre des IDDs dans le secteur bancaire. Cette classification des thèmes sert à évaluer le niveau de consensus entre les deux spécialistes en plus d'analyser les facteurs clés de réussite d'un tel projet, ainsi qu'à identifier des orientations stratégiques pouvant guider les décisions futures des établissements bancaires. En examinant ces différents aspects, nous pourrons mieux saisir les profondes métamorphoses

qu'entraînerait une large adoption des identifiants décentralisés, en évaluant à la fois les obstacles à surmonter et les avantages potentiels à long terme d'une réingénierie des processus.

Avant de débuter l'analyse, nous avons demandé aux participants de nous expliquer leur expertise et expérience avec la technologie blockchain et l'industrie bancaire afin d'adapter les questions à leurs champs de compétence respectifs. En comprenant le profil des experts, nous allons pouvoir adapter nos questions en fonction de leurs forces. D'une part, Kennen est un expert reconnu en matière d'identité distribuée et de technologie blockchain, ayant agi comme architecte et conseiller sur plusieurs projets d'envergure liés aux infrastructures et aux MNBC. Il est également impliqué dans le développement de solutions d'identités fondées sur des approches évènementielles, notamment au sein de l'écosystème KERI. Kennen connaît parfaitement les limitations des méthodes conventionnelles pour établir l'identité et il maîtrise un large éventail de sujets, allant de la cryptographie sophistiquée (ex : rotation de clés, multisignature, preuves de provenance) jusqu'aux aspects sociétaux et économiques. Son discours propose une perspective systémique et prospective sur l'intégration de l'identité auto-souveraine. D'autre part, Ekko compte plus de huit années d'expérience dans la création, le perfectionnement et la supervision de solutions technologiques axées sur la blockchain, principalement dans le domaine bancaire et notamment au Japon. Il a commencé sa carrière en tant que développeur, avant de gravir les échelons pour devenir responsable de produit, ce qui lui a permis d'acquérir une expérience technique, fonctionnelle et orientée affaires complémentaires. Ekko a participé à des projets pilotes dans le contexte bancaire et accompagne aujourd'hui des institutions dans l'intégration concrète des technologies d'identité auto-souveraine. Il se concentre sur les applications bancaires, accordant une attention particulière à l'interopérabilité, à la gestion des données et à l'expérience utilisateur. Il structure son discours autour des avantages concrets des identifiants décentralisés, tels que la réduction des données, le contrôle accru par l'utilisateur, les preuves de divulgation nulle, et ce en abordant leur mise en œuvre dans des écosystèmes technologiques complexes, en considérant les défis de sécurité, d'évolutivité et de coûts.

5.3.1 Défis des IDDs – Implémentation

L'implémentation des identifiants décentralisés dans les systèmes bancaires s'accompagne de défis techniques et organisationnels complexes qui dépassent largement la simple intégration d'un nouveau protocole. Trois sous-thèmes ressortent de l'analyse des entretiens analysés : la complexité d'intégration,

les défis techniques d'une infrastructure d'identité auto-souveraine, ainsi que les enjeux de mise en œuvre et d'interopérabilité.

La complexité d'intégration, référée huit fois depuis deux transcriptions, désigne l'effort requis pour concilier les principes de la décentralisation et de gouvernance distribuée avec les réalités d'architectures bancaires traditionnelles souvent rigides et centralisées. Cette tension se manifeste dans les difficultés d'adaptation des systèmes legacy, dans les réticences à modifier les fondations technologiques existantes et dans la nécessité de garantir la sécurité tout au long du processus. Les défis techniques d'une infrastructure d'IAS, référées 16 fois depuis une transcription, renvoient quant à eux aux limites intrinsèques des protocoles actuels d'identité décentralisée, encore peu standardisées, souvent fragmentées et nécessitant des compétences spécialisées. Le manque de maturité des écosystèmes technologiques, les critiques portées à certaines approches et l'absence d'un modèle d'adoption à grande échelle confirment que l'IAS demeure à ce jour un champ d'exploration plus qu'un standard qui a fait ses preuves. La mise en œuvre opérationnelle ne peut être possible sans une réflexion approfondie sur l'interopérabilité. Référée neuf fois depuis deux transcriptions, la mise en œuvre de l'identité auto-souveraine et des identifiants décentralisés se doit d'appliquer les principes de portabilité et d'interopérabilité si elle souhaite tenir sa promesse de décentralisation.

Ainsi, l'axe d'implémentation technologique révèle des défis multiples qui imposent aux banques de repenser leur architecture, leurs infrastructures et leur mentalité organisationnelle afin de s'orienter vers un modèle nouveau.

5.3.1.1 Complexité d'intégration

L'intégration des identifiants décentralisés dans les systèmes bancaires ne saurait être envisagée sans une prise en compte rigoureuse de la complexité technique et organisationnelle inhérente à une telle transformation. Les propos recueillis révèlent une série d'obstacles liés à la décentralisation, mais plus spécifiquement à son infrastructure, la nature de ses technologies sous-jacentes, aux normes de sécurité et à la gouvernance des réseaux décentralisés. Ces éléments contribuent à freiner l'adoption à large échelle des IDDs dans l'écosystème bancaire canadien.

Le premier aspect évoqué concerne les défis liés à l'infrastructure des IDDs vis-à-vis de celles des banques. Selon Ekko, l'intégration de solutions décentralisées dans les systèmes traditionnels bancaires implique des ajustements de grande ampleur.

> « L'infrastructure *backend* devra probablement changer, car l'intégration avec les systèmes bancaires *Legacy* sera complexe. Il faut qu'il y ait une interopérabilité fluide entre les différentes plateformes dans le *backend* » (Entrevue P5E, traduction libre)

Cette complexité est accentuée par la coexistence d'architectures hétérogènes au sein même des banques, rendant la compatibilité difficile sans refonte profonde des fondations. À cette difficulté s'ajoute la question de la gouvernance des réseaux décentralisés. L'idée même d'un réseau blockchain repose sur la pluralité des nœuds. Ekko rappelle que « un réseau décentralisé ne peut pas reposer sur un seul nœud, car cela reviendrait à centraliser le système. Il n'est donc pas souhaitable qu'une seule banque y participe. Pour véritablement décentraliser, il faut impliquer plusieurs entités » (Entrevue P5E, traduction libre). Sans la présence de plusieurs nœuds, soit plusieurs banques, dans le réseau, l'essence même de la décentralisation est annulée. Cette réalité impose aux banques de non seulement collaborer entre elles, mais aussi d'accepter une forme de mutualisation des standards, ce qui représente un défi culturel et stratégique. Kennen de son côté nuance les propos de Ekko avec ses propos :

> « Une banque pourrait mettre en place certaines de ces technologies, mais cela dépend de la solution choisie. Beaucoup de plateformes sont trop complexes ou trop lourdes pour être déployées par une seule institution, en particulier les plus petites. À l'inverse, certaines solutions comme KERI sont plus simples et permettent une mise en œuvre rapide. Cela dit, la valeur réelle et les économies d'échelle augmente lorsque plusieurs banques collaborent dans un même écosystème. » (Entrevue P6E, traduction, libre)

La migration des données existantes constitue un autre défi complexe. « Les banques possèdent d'importants volumes de données sensibles [difficilement] transférables » (Entrevue P5E, traduction libre) vers un écosystème blockchain décentralisé. Les interactions entre différentes institutions financières au sein d'un même réseau décentralisé complexifient encore davantage les exigences d'interopérabilité. L'exemple soulevé par Ekko nous aide à comprendre :

> « Si plusieurs banques participent à un même réseau et que je souhaite pousser une transaction, disons que je suis de la banque Demacia[35] et que tu es de la banque Noxus[36], et

[35] Demacia est un nom fictif pour anonymiser le nom de la banque mentionnée

[36] Noxus est un nom fictif pour anonymiser le nom de la banque mentionnée

> que tu pousses une transaction, les systèmes doivent suffisamment être fiables et standardisés pour respecter les exigences réglementaires propres à chaque juridiction. » (Entrevue P5E, traduction libre)

En d'autres termes, chaque transaction interbancaire dans un tel réseau décentralisé doit respecter les normes et standards pouvant varier d'une juridiction à l'autre d'où la nécessité d'une architecture souple pouvant s'adapter aux normes. En matière de cybersécurité, l'adoption de la blockchain ne constitue pas en soi une garantie d'immunité. Bien au contraire, Ekko souligne que « s'il y a cinq nœuds, cela signifie cinq points d'entrée potentiels pour une attaque. Il faut donc prévoir des pares-feux adaptés et un cadre de sécurité normalisé avant toute mise en place du réseau » (Entrevue P5E, traduction libre). Cela requiert donc une attention rigoureuse à la sécurisation de chaque point d'accès, ainsi qu'à la conception de mécanismes de protection décentralisées. Cette exposition accrue aux risques technologiques alimente la réticence des banques à adopter ces technologies émergentes. Ekko estime que « si un environnement n'est pas sécurisé, les données hébergées sur le réseau sont exposées, ce qui engendre des risques majeurs. C'est l'une des raisons principales pour lesquelles les banques restent prudentes par rapport à cette technologie. Pourtant, ce sont elles qui lancent les premiers projets pilotes liés à la blockchain. » (Entrevue P5E, traduction libre)

5.3.1.2 Défis techniques d'une infrastructure d'IAS

L'analyse des propos recueillis auprès de nos experts met en lumière plusieurs défis techniques au sujet des identifiants décentralisés et du concept de l'identité auto-souveraine dans le secteur bancaire. Les défis soulevés ne sont pas seulement culturels ou organisationnels, mais ils vont au cœur même des architectures technologiques et remettent en question les paradigmes actuels de conception, de sécurité, de gouvernance et d'évolutivité des systèmes d'information.

Une des toutes premières réponses de Kennen fût au niveau de la différenciation entre sa solution de prédilection KERI versus les protocoles décentralisés habituels. « KERI est un protocole d'identité véritablement décentralisé. La plupart des autres protocoles s'appuient sur des raccourcis ou des systèmes qui ne le sont pas entièrement. » (Entrevue P6E, traduction libre), déclare Kennen. Cette réalité négligée nous amène à penser que les solutions blockchain doivent être décentralisée de bout en bout et ne laisser place à aucune centralisation ou point de défaillance unique. « Plusieurs écosystèmes d'identité prétendent être décentralisés, alors qu'ils utilisent des éléments comme le DNS, qui restent sous le contrôle d'autorités centralisées » (Entrevue P6E, traduction libre), insiste Kennen. En d'autres mots,

certaines architectures dites décentralisées véhiculent une illusion de décentralisation en perpétuant des logiques techniques de centralisation.

Un aspect fondamental à respecter au niveau de l'identité auto-souveraine et des identifiants décentralisés est l'exigence d'un historique d'enregistrement fiable des clés. Selon Kennen, c'est un élément incontournable, car « tout système d'identité décentralisé qui réclame être de nature auto-souveraine, mais qui n'offre pas d'historique vérifiable des clés passe à côté d'un élément fondamental. » (Entrevue P6E, traduction libre). Sans cette fonctionnalité, il est impossible d'assurer la cohérence identitaire au fil du temps, ni sur le plan légal ni sur le plan réputationnel. Kennen ajoute aussi que certains « protocoles d'identité décentralisée offrent la rotation de clés, d'autres ne le font pas » (Entrevue P6E, traduction libre), ce qui signifie que la gestion des clés peut être compliquée à gérer lorsqu'une clé est perdue ou oubliée. En complément, l'hétérogénéité des piles constitue un défi de taille considérant que certains « protocoles d'identité décentralisée permettent de vérifier les justificatifs d'identité, alors que d'autres ne le font pas. » (Entrevue P6E, traduction libre). Cette discontinuité fonctionnelle entre protocoles entraîne un manque de confiance auprès de certaines solutions d'identité décentralisées et des frictions en matière d'interopérabilité.

Un point intéressant amené par Kennen sur les protocoles ZKP a capté notre attention. Il était de notre avis que les preuves de divulgation nulle ou sélective étaient une avancée en matière de gestion des données personnelles par leur nature discrète de partage de données sensibles. Toutefois, Kennen s'étend longuement sur une analyse critique des ZKP, qui nous a fait réfléchir sur leur réel potentiel à préserver la confidentialité.

> « Ce que la communauté des ZKP a tendance à croire, c'est qu'il est possible d'utiliser ce qui s'appelle la divulgation sélective avec un ensemble privé de vérifications et de preuves de données, comme des preuves d'âge adulte, savoir si la personne est de tel ou tel sexe, s'il s'agit d'une personne âgée, si c'est un ancien combattant, etc. Certains disent qu'il faut utiliser les ZKP. Ne divulguez pas vos données. Répondez seulement par oui ou non. Le problème avec ce modèle c'est que les ZKP n'incluent pas la terminologie permettant de contrôler qui a accès à ces données. La raison pour laquelle cela ne fonctionne pas, c'est qu'à l'ère moderne, avec les courtiers de données et le vaste nombre d'attributs de données, il est trivialement facile pour une entreprise d'avoir accès [à des données] sur toi, moi et tout le monde. Dans une étude universitaire publiée en 2020, il était assez facile de réidentifier ou de désanonymiser quelqu'un. Et même si nous avons un ensemble de données entièrement anonymisées, il est possible d'identifier quelqu'un avec un petit nombre d'attributs. L'IA a d'ailleurs rendu ce problème encore pire. » (Entrevue P6E, traduction libre)

Cette critique gagne donc en pertinence dans le contexte actuel dominé par les courtiers en données et l'intelligence artificielle. Pour qu'un système d'identité décentralisé soit à l'abri de ces failles, il faut que l'architecture technique permettent de protéger les transactions et les vérifications entre les utilisateurs. De plus, Kennen rajoute qu'il y a d'autres facteurs à prendre en considération en disant que « nous n'avons même pas encore parlé des problèmes B2C, du piratage biométrique et la façon dont des gens piratent la biométrie. » (Entrevue P6E, traduction libre). Selon Kennen, « les supporteurs des protocoles ZKP ignorent qu'il est facile de réidentifier les gens de façon contextuelle » (Entrevue P6E, traduction libre). Pour mettre en lumière ses propos, Kennen pose un l'exemple qui suit :

> « J'essaie d'acheter du tabac ou une substance qui exige que je sois âgé de 21 ans ou de plus de 18 ans. J'essaie d'acheter une voiture et je dois avoir plus de 25 ans. Il se peut tu divulgues seulement oui ou non, mais en réalité, le numéro de carte de crédit utilisé, les caméras de sécurité … Il y a plusieurs moyens. Il est possible de tout corréler. Il y a cinq ou six courtiers de données au sommet du monde. Ils mettent en corrélation toutes les données en permanence et les vendent aux enchères. Et celui qui les achète veut vous vendre quelque chose. Ils veulent tous vous réidentifier pour vous vendre des choses (Entrevue P6E, traduction libre)

Considérant que les ZKP ne couvrent donc pas totalement la sécurité et la confidentialité d'un individu en raison des facteurs énoncés par Kennen, il faut au minimum que l'organisation sache dans quoi elle s'embarque pour éviter de tomber dans des pièges et vendre du rêve. Dans ce contexte, l'implémentation d'un protocole comme KERI, qui permet une gestion unifiée des identifiants et des preuves vérifiables, nécessite une compréhension et une révision complète de la gestion des systèmes de sécurité et d'identité. C'est pourquoi Kennen souligne que :

> « Si une banque prend réellement au sérieux la question de la sécurité, la mise en œuvre est envisageable si elle est prête à investir. C'est un investissement important et elle requiert une expertise technique poussée. Il faut savoir déployer des composants d'infrastructure, les maintenir et être capable de résoudre les problèmes qui surviennent. Des formations sont disponibles, de la consultation aussi. Cependant, cela reste un processus qui demande du temps. L'infrastructure technologique n'a pas encore atteint le niveau nécessaire [pour une adoption massive]. Certains écosystèmes sont plus avancés que d'autres, mais l'ensemble reste fragmenté. Nous sommes encore loin d'un modèle d'identité numérique consolidée avec une interopérabilité élevée. Les débats, discussions et politiques autour des infrastructures à adopter sont encore très présents et aucune solution ne s'impose clairement à ce jour. » (Entrevue P6E, traduction libre)

Or, le niveau de compréhension technique exigé, bien qu'il puisse être facilité par des formations ou des services de consultation, complique inévitablement l'implémentation d'infrastructures décentralisées. En

effet, la commercialisation de ces infrastructures n'est pas encore assez avancée. Le marché reste fragmenté, les normes restent floues et l'incertitude domine encore. Cette fragmentation rend toute tentative d'alignement stratégique risquée et peu d'exemples concrets permettent actuellement de prouver la viabilité du modèle d'identité auto-souveraine à grande échelle. Il est donc important de comprendre qu'une intégration technologique réussie nécessite une profonde transformation interne, plutôt qu'une simple adaptation superficielle. En ce sens, Kennen recommande « d'abord d'acquérir une compréhension approfondie de la technologie. Ensuite, il faut la déployer dans un environnement sécurisé avant de l'intégrer progressivement au cœur de l'architecture des systèmes existants. » (Entrevue P6E, traduction libre). Nous comprenons qu'il faut une démarche graduelle et que pour intégrer les principes d'IAS dans une architecture bancaire, il faut aussi repenser les fondements même de la sécurité. Tel qu'expliqué par Kennen dans l'extrait suivant, le point de départ de toute réflexion d'un design architectural est crucial et doit être basé sur des principes identifiés en amont d'implémentation.

> « L'identité est au cœur de tout système logiciel, ce qui veut dire qu'elle doit donc être architecturée en fonction de la performance, de la scalabilité et de la sécurité en même temps, et ce en amont. Si ce n'est pas fait en amont, des révisions et réécritures lourdes seront nécessaires par la suite. Il faut donc se familiariser avec les architectures de type IAS, l'approche Zero Trust et les principes sans secrets partagés. Cela implique de concevoir dès le départ un sous-système ou un flux métier capable de tirer parti de ce niveau de sécurité. Il faut également maîtriser les kits de développement pour intégrer des portefeuilles numériques sur les téléphones et navigateurs ou applications. Et finalement, il est indispensable de savoir opérer, surveiller et maintenir en continue toute cette infrastructure, ce qui demande un engagement conséquent en temps et en ressources. » (Entrevue P6E, traduction libre)

Ce constant nous amène à réfléchir sur le besoin de synchronisation entre l'infrastructure et la mentalité de l'organisation. L'organisation doit être en mesure d'appliquer les fondements de l'identité auto-souveraine dans ses valeurs pour ensuite l'appliquer dans ses systèmes. Kennen poursuit ensuite en disant que « la prochaine étape est faire évoluer la technologie parallèlement avec la proposition de valeur […]. En résumé, il faut concevoir chaque activité centrale, chaque transaction ou flux métier, en intégrant l'identité numérique à la base du système […]. L'infrastructure d'identité doit évoluer au même rythme que l'ensemble du système. » (Entrevue P6E, traduction libre). Cela veut donc dire que l'identité doit maintenant être considérée comme l'épine dorsale d'un écosystème numérique interconnecté.

À la lumière de ces éléments de réponse, il devient clair que l'intégration technique des IDDs et des principes d'IAS repose sur un ensemble de conditions strictes passant par la robustesse cryptographique,

la sécurité distribuée, la capacité d'évolutivité, la standardisation interopérable et une gouvernance ouverte. Tant que ces dimensions ne seront pas réunies dans une infrastructure unifiée, les solutions d'identité décentralisée resteront confinées à des expérimentations isolées.

5.3.1.3 Mise en œuvre et interopérabilité

La mise en œuvre et l'interopérabilité des systèmes décentralisés ne se limitent pas à un aspect technique, mais s'avère être un facteur clé de durabilité, de fiabilité et de valeur à long terme. Selon les propos de nos répondants, toute démarche de mise en œuvre se heurte rapidement à un dilemme entre les capacités internes des institutions financières et la nécessité d'intégrer un écosystème distribué, normalisé et collaboratif.

Selon Kennen, la clé du succès à long terme d'un système d'identité décentralisé repose sur la capacité à garantir une identité continue et solide. Il soutient que « il faut une identité durable pour construire une réputation durable. En l'absence de cette continuité, les systèmes d'identité décentralisée deviennent trop complexes à adopter, ce qui explique l'échec de nombreux projets. » (Entrevue P6E, traduction libre). Cette observation met en évidence le fait que l'implantation d'un système d'identité ne peut être réduite à une simple question de technologie. Elle doit se conformer à une approche pouvant prendre en compte la gestion du cycle de vie des identifiants, leur portabilité et leur capacité à franchir les frontières organisationnelles. Le principe d'interopérabilité émerge alors comme une nécessité structurelle plutôt que comme une option. « Plus les systèmes sont interopérables, plus la valeur générée est élevée. » (Entrevue P6E, traduction libre), exprime Kennen. Cette affirmation résonne avec la logique même des technologies décentralisées, car leur valeur ne réside pas dans leur performance individuelle, elle réside dans leur capacité à former un réseau fonctionnel, fluide et distribué. Ainsi, Ekko souligne pour sa part la difficulté suivante : « un enjeu majeur est que tes identifiants doivent être interopérables » (Entrevue P5E, traduction libre). Un système bancaire ayant des IDDs qui ne soient pas interopérables entraînerait une nouvelle forme de fragmentation numérique, qui serait contraire à l'objectif de fluidité promu par les principes d'IAS. Cependant, cette nécessité se heurte à la réalité de la diversité provinciale au Canada. Ekko illustre cette réalité avec l'exemple suivant : « Ma carte de santé de l'Ontario devrait être admissible en Colombie-Britannique. Il devrait être possible d'interpréter qui est la personne. La standardisation est importante. » (Entrevue P5E, traduction libre). Cela est seulement possible dans un écosystème basé sur des normes ouvertes clairement comprises et acceptées par tous. Ces conditions correspondent d'ailleurs aux directives du W3C concernant les identifiants décentralisés.

De ce fait, la dimension réseau devient centrale. Un réseau décentralisé ne peut fonctionner qu'à partir d'un nombre minimal de nœuds connectés. Ekko réitère, à juste titre, que « un réseau ne peut pas reposer sur un seul nœud, cela reviendrait à centraliser le système. Il n'est donc pas souhaitable qu'une seule banque soit impliquée [dans une solution décentralisée]. La décentralisation exige la participation de plusieurs banques ». Plusieurs banques, en effet, sont nécessaires pour rendre les identifiants interopérables. Toutefois, il existe des dangers à une incompatibilité entre les systèmes bancaires. Ekko met en garde les réseaux qui ne sont pas interopérables : « Un fraudeur pourrait facilement profiter du manque d'interopérabilité pour se faire passer pour un client légitime d'une autre banque » (Entrevue P5E, traduction libre). Cette faille met en lumière la nécessité de mettre en place des procédures de vérification croisées permettant d'identifier de manière fiable un individu à travers plusieurs institutions. En ce sens, « l'interopérabilité est précisément le problème principal identifié à ce jour. » (Entrevue P5E, traduction libre).

La mise en œuvre de systèmes d'identité distribuée requiert inévitablement une démarche coopérative entre les banques. Elle exige une gouvernance interbancaire, l'élaboration de normes communes et l'établissement de mécanismes de vérifications distribuées. Elle réclame également une réflexion sur la portabilité des identités, non seulement entre banques, mais aussi entre provinces, juridictions et même services publics. En d'autres termes, l'identité auto-souveraine ne pourra tenir ses promesses que si elle s'appuie sur un système concerté où la confiance est partagée et où les participants se sont commis à collaborer. L'analyse des données issues des entretiens montre que la mise en œuvre des IDDs dans les banques est indissociable de leur interopérabilité. La clé du succès réside dans l'élaboration d'une identité décentralisée, reconnue et utilisable par tous. Ce n'est qu'à ce moment que le potentiel de l'IAS dans le secteur bancaire pourra être pleinement réalisé. Sans cela, les efforts de mise en œuvre risquent de rester marginaux, fragmentés et voués à une adoption limitée.

Codification / Thème	Nombre d'entrevues	Références
Complexité d'intégration	2	8
Défis techniques de l'IAS	1	16
Mise en œuvre/Interopérabilité	2	9

Tableau 9 Codifications et références des Défis des IDDs - Implémentation

5.3.2 Défis des IDDs – Humain

Si l'intégration des identifiants décentralisés soulève des défis technologiques majeurs, leur adoption à grande échelle dépend tout autant, sinon davantage, de leur acceptabilité humaine. À la croisée des logiques techniques et des réalités d'usage, les freins à l'appropriation de l'identité auto-souveraine révèlent des dynamiques profondément ancrées dans les comportements, les habitudes et les représentations des utilisateurs, qu'ils soient clients ou employés. Les entrevues réalisées mettent en lumière deux axes interdépendants de cette problématique humaine : la difficulté d'opérationnaliser la gestion des clés dans la vie quotidienne des gens et la gestion du changement.

Le last mile, référé six fois dans deux transcriptions, constitue un point de friction critique entre l'infrastructure technologique et la réalité des utilisateurs finaux. Loin d'être un détail important d'implémentation, il renvoie à la capacité de l'utilisateur final à accéder, gérer, sécuriser et récupérer son identité dans un environnement souvent perçu comme complexe. La promesse du contrôle total devient ici un fardeau lorsqu'elle n'est pas appuyée par des mécanismes de protection, de récupération et d'assistance adaptés à la diversité des profils des utilisateurs.

En parallèle, la résistance au changement, référée huit fois dans deux transcriptions, émerge comme un phénomène omniprésent dès qu'une innovation touche à la structure d'interaction avec l'usager ou à la stabilité des systèmes en place. Elle ne résulte pas d'un rejet irrationnel de la nouveauté, mais d'un réflexe de protection des repères, d'une gestion du risque perçue et parfois d'un scepticisme fondé face à des technologies encore en phase de maturation. Peu importe comment elle s'exprime, la résistance oblige les concepteurs et les décideurs à penser la manière dont elle sera communiquée aux personnes impactées.

L'adoption dépendra en partie de la capacité des institutions à instaurer un climat de confiance et reconnaître les difficultés dans la trajection du changement.

C'est donc en tenant compte de ces réalités humaines que pourront être envisagées des conditions de déploiement favorables, pérennes et inclusives. Le présent axe propose d'explorer le thème humain des défis liés à l'intégration des IDDs.

5.3.2.1 Last Mile

Un défi incontournable est certainement la question du « last mile », soit la zone critique où la technologie rencontre l'usager final. Bien que l'infrastructure, les protocoles et les normes soient les fondations d'un écosystème d'IAS, la question du last mile est déterminante pour son adoption réelle. C'est pourquoi Kennen met l'emphase sur cet aspect en disant : « La question du last mile est essentielle. » (Entrevue P6H, traduction libre). L'enjeu ne se limite pas à la robustesse cryptographique des identifiants ni à la gouvernance distribuée ou à l'interopérabilité. Elle porte aussi sur la manière concrète dont les individus peuvent interagir avec leur identité numérique, la gérer, la sécuriser et surtout la récupérer en cas de perte ou d'oubli. Kennen accentue ce fait en donnant l'exemple de Bitcoin : « Bitcoin est un excellent exemple : si ce n'est pas votre clé, ce n'est pas votre crypto. C'est pour cela qu'il y a des gens qui paient des millions de dollars pour récupérer leurs mots de passe. » (Entrevue P6E, traduction libre). Bien connue dans l'univers des cryptomonnaies, cette réalité devient problématique au moment de l'appliquer à une identité numérique. En effet, contrairement à un actif financier, l'identité ne peut être émise à nouveau à la légère. Prenons l'exemple d'un passeport perdu ou oublié. Il n'est pas si simple de s'en procurer un nouveau, car c'est le gouvernement qui l'émet. De même, une identité numérique décentralisée revêt d'un niveau de complexité élevé, car elle est censée être unique, persistante et inviolable. Sa perte n'a donc pas qu'une portée technique, mais également une portée juridique, sociale et fonctionnelle. Dans cette optique, l'accessibilité des systèmes d'IAS au grand public implique de concevoir des mécanismes de sécurité préventives et adaptées aux comportement réels des usagers. Kennen insiste sur ce point en nous partageant :

> « Les gens ont tendance à perdre leurs effets personnels. Ils oublient ou ils se font pirater. Il faut donc réfléchir en conséquence. Nous ne pouvons pas espérer que les gens soient habiles avec leurs clés. Et pas seulement cela, les gens veulent les utiliser sur plusieurs périphériques. » (Entrevue P6E, traduction libre)

Or, le modèle d'identité décentralisée ajoute une couche de complexité au système, mais il en est indispensable pour prévenir la perte, le vol ou le piratage des identités. Face à ce problème, notre entretien avec Willump a révélé un problème complémentaire : « Comment s'assurer que [l'identité] est bien détenue par la bonne personne? Parce que s'il y a un vol de téléphone ou un truc comme ça, quelqu'un pourrait se faire passer pour toi, sauf si tu as justement des vérifications supplémentaires pour terminer cette confirmation. Donc là je parle d'un mot de passe, mais ça peut être une vérification biométrique ou un truc du genre. » (Entrevue P4C). S'il est attendu que les individus gèrent eux-mêmes leur identité, il faudra s'assurer que leur offrir des garde-fous suffisamment robustes et simples pour éviter qu'un tiers ne puisse en prendre le contrôle en cas de faille physique ou numérique.

Ces différents éléments montrent que la réussite d'un IDD ne dépendant pas seulement de sa performance algorithmique ou de son interopérabilité. Elle dépend aussi de son habileté à s'insérer harmonieusement dans la vie quotidienne des gens. Faute de résoudre cette problématique, les projets d'IDDs risquent de rester confinés à des cercles d'utilisateurs restreints et seront incapables de faire évoluer la technologie à plus grande échelle telle qu'elle était prévue.

5.3.2.2 Résistance au changement

Dans toute transformation profonde, le changement impacte inévitablement les humains. L'efficacité d'une transformation dépend de sa résonance avec les usages, les habitudes et les représentations des acteurs concernés. C'est dans cette tension entre l'innovation promise et la réalité vécue que s'enracine la résistance au changement. Étant un phénomène poignant pour certains et enthousiasmant pour d'autres, l'intégration d'une nouvelle technologie peut susciter diverses réactions des personnes impliquées directement et indirectement au changement.

Kennen résume bien cette dynamique lorsqu'il interroge la capacité des individus et des institutions à tolérer une certaine complexité pour accéder à un plus grand contrôle sur leurs données : « La véritable question est : jusqu'à quel point sommes-nous prêts à accepter la complexité pour permettre aux individus de contrôler leurs données? Car même si nous sommes capables de comprendre quelque chose dans un cadre académique ou dans un cadre idéaliste, quand on pense à ce qui compte réellement, les seules choses qui comptent sont celles qui sont adoptées par les marchés. Et pour cela, il faut transformer les comportements, ce qui échappe en partie au pouvoir des régulateurs. » (Entrevue P6E, traduction libre). Cette remarque, en apparence pragmatique, pointe en réalité une frontière invisible entre la conception

et l'usage ainsi qu'entre l'intention technologique et l'appropriation sociale. La question de la maturité des écosystèmes accentue cette inertie. Alors, Kennen rappelle que l'adoption du modèle d'IAS demeure embryonnaire et que son intégration à court terme, notamment dans les petites institutions, reste peu envisageable hors d'une logique de coopération avec le passage suivant :

> « L'adoption est encore à ses débuts, ce qui rend la faisabilité faible pour le moment. Selon Gartner, l'adoption massive des identités numériques est encore dans deux à cinq ans. Ce sera donc beaucoup plus simple plus tard. Lorsque les écosystèmes seront plus matures et que les grands joueurs auront développé des solutions sur lesquelles les plus petites pourront s'appuyer, l'intérêt viendra. Pour l'instant, l'intérêt pour une petite banque locale reste limité, sauf en cas de collaboration avec d'autres banques pour bénéficier de l'interopérabilité. » (Entrevue P6E, traduction libre)

Autrement dit, l'enthousiasme des promoteurs de solutions décentralisées ne suffit pas à faire avancer les choses. Il faut pour cela un environnement favorable, une dynamique d'entraide, voire un alignement d'intérêts interbancaires que l'écosystème peine encore à offrir. Cette prudence stratégique s'accompagne d'un réflexe de préservation des systèmes existants. Comme l'indique Ekko, « lorsqu'un changement d'expérience utilisateur est introduit, le système existant ne doit pas être abandonné, les deux systèmes, [l'ancien et le nouveau], doivent fonctionner en parallèle. » (Entrevue P5E, traduction libre). Il est impératif de préserver le système en place avant d'orienter le changement vers le nouveau système. C'est donc dire que pour mitiger la gestion de changement vers les IDDs, il est nécessaire de conserver les systèmes legacy en place pour transitionner progressivement vers un nouveau modèle. Sans cela, les utilisateurs n'auront pas eu l'occasion de se familiariser avec la technologie en amont et le projet sera voué à l'échec. Au cœur de la résistance au changement se trouve une innovation perturbatrice qui suscite l'inquiétude. À cet effet, Ekko rappelle les propos partagés par les employés de la banque au sujet de la gestion de changement : « Les utilisateurs plus jeunes ou ceux qui possèdent les appareils plus récents s'adapteront plus facilement, mais il ne faut pas négliger la part de la population qui n'est pas en mesure d'utiliser ces nouvelles technologies. » (Entrevue P5E, traduction libre). C'est pourquoi « lors du développement d'une nouvelle application ou d'un nouveau système, l'expérience utilisateur doit rester inchangée autant que possible. » (Entrevue P5E, traduction libre). Ekko intervient à nouveau en soulignant que « lorsqu'il s'agit de l'interface utilisateur, il est difficile de changer les habitudes des utilisateurs. » (Entrevue P5E, traduction libre). En ce sens, « la priorité est d'intervenir dans le backend, tout en préservant l'expérience et les comportements utilisateurs, car tout changement perceptible provoque une forme de rejet. » (Entrevue P5E, traduction libre). La résistance au changement n'est pas une opposition de principe, mais une défense des équilibres cognitifs et émotionnels.

Il faut donc préparer, accompagner et négocier le changement pour le mener à réussite. Toute stratégie d'intégration des IDDs devra s'appuyer sur ces principes et sur une pédagogie du changement patiente et progressive capable de faire émerger la confiance sans brusquer les utilisateurs. L'enjeu ne sera pas simplement de convaincre les utilisateurs que les IDDs et le modèle d'IAS sont meilleurs, mais de leur démontrer qu'il est fait pour eux, dans leurs conditions, à leur rythme.

Codification / Thème	Nombre d'entrevues	Références
Last Mile	2	6
Résistance au changement	2	8

Tableau 10 Codifications et références des Défis des IDDs - Humain

5.3.3 Opportunités des IDDs – Amélioration des processus

Après avoir mis en lumière les nombreux obstacles des IDDs, tant sur le plan technique qu'humain, nous passons maintenant aux opportunités de l'intégration des identifiants décentralisés dans les systèmes bancaires. Pour commencer, nous aborderons les opportunités axées sur l'amélioration des processus, soit le côté plus technique et organisationnel. Parmi les thèmes identifiés, nous y retrouvons la diminution des risques. Elle se distingue nettement avec 11 références dans deux transcriptions comme le bénéfice le plus fréquemment évoqué. Les transformations associées à l'usage d'un portefeuille numérique, qui rassemblent six références dans une transcription, et la simplification, citée trois fois dans une transcription suivront dans l'analyse pour montrer la capacité des IDDs à améliorer les processus. Puis, nous terminerons avec le reste des opportunités. Bien que moins cités, elles méritent une attention particulière pour leur portée stratégique. La gouvernance des données, évoquée dans une transcription, ainsi que la transparence, présente dans deux transcriptions, renvoient à des principes fondamentaux de gestion décentralisée. Les points d'entrée, cités deux fois dans une transcription, mettent en lumière la capacité des IDDs à fluidifier les interactions entre institutions, tandis que la réduction des coûts, mentionnée trois fois dans deux transcriptions, suggère un potentiel de rationalisation à long terme.

5.3.3.1 Diminution des risques

L'un des apports les plus fréquemment avancés en faveur de l'intégration des identifiants décentralisés dans les systèmes bancaires est la possibilité de réduire substantiellement divers risques de l'ordre opérationnel, réputationnel et surtout sécuritaire. À travers les propos recueillis lors de nos entretiens, la diminution des risques apparaît comme un argument stratégique susceptible d'accélérer l'adhésion des parties prenantes au modèle de l'identité auto-souveraine. Ce thème se décline en plusieurs dimensions, allant de la sécurité cryptographique jusqu'à la lutte contre la fraude, en passant par le contrôle des flux de données personnelles.

La réduction des risques liés à la gestion de l'identité constitue l'un des bénéfices clés anticipés par les experts interrogés. En effet, lorsque nous avons demandé quels sont les principaux avantages de l'intégration des IDDs, Kennen répond instinctivement : « L'avantage #1 est la sécurité » (Entrevue P6E, traduction libre). Cette affirmation place la sécurité au centre de la proposition de valeur des identifiants décentralisés. Elle indique clairement que l'intégration d'un modèle d'identité auto-souveraine s'inscrit avant tout dans une logique de maîtrise des vulnérabilités systémiques. La sécurité dans ce contexte ne se limite pas à la confidentialité des données. Elle s'étend à la consolidation d'un environnement de confiance où la réputation numérique devient un attribut vérifiable. Comme l'énonce Kennen : « La sécurité et la réputation » (Entrevue P6E, traduction libre). Il faut comprendre ici que l'identité, une fois sécurisée par des mécanismes cryptographiques robustes, permet aussi d'établir un historique fiable et réutilisable des interactions. La réputation devient alors un levier de stabilité dans les relations interpersonnelles, commerciales et institutionnelles.

Sur un horizon plus immédiat, l'intégration des IDDs promet d'avoir un impact tangible sur la fraude. À ce sujet, Kennen précise que : « Au début, les premiers bénéfices concerneront la réduction de la fraude et l'amélioration de la sécurité. » (Entrevue P6E, traduction libre). La perspective est ici est opérationnelle. Les institutions financières font face à des coûts considérables liés à la fraude identitaire. La traçabilité inhérente aux IDDs, combinée à leur résilience cryptographique, constitue un rempart contre la falsification de documents et la réutilisation illicite d'informations personnelles. Ce renforcement de la sécurité s'appuie notamment sur les capacités matérielles des appareils utilisés par les individus. Ekko met en lumière cette évolution avec les propos suivants :

> « Aujourd'hui la majorité des téléphones sont équipés de systèmes biométriques d'identité. L'identité n'a même pas besoin d'aller sur le cloud. L'idée est de conserver son identité dans

> un périmètre personnel, au sein de son propre appareil. C'est cryptographiquement sécure. C'est un mécanisme à sens unique. Le même nombre d'entrées doit mener au même nombre de sorties. Si tu changes quelque chose, tu ne peux pas regénérer la même réponse. » (Entrevue P5E, traduction libre).

Ce qui est intéressant dans ces propos c'est la localisation des données. En conservant les données sur l'appareil lui-même, protégé par un environnement biométrique sécurisé, et en l'isolant des serveurs, l'exposition aux intrusions est réduite considérablement. Un élément technique vient appuyer cette stratégie, soit le hachage cryptographique. Ekko souligne ce point avec précision : « Grâce au hachage cryptographique, il est impossible de remonter à l'information d'origine. C'est précisément ce niveau de sécurité que permettent les IDDs » (Entrevue P5E, traduction libre). Ce mécanisme garantit donc l'intégrité unidirectionnelle des données. Il devient ainsi pratiquement impossible de reconstituer les informations sensibles à partir de leur empreinte, même en cas d'accès non autorisé. La manière dont les données sont partagées constitue un autre levier de sécurisation. Ekko illustre ce principe à travers un exemple simple : « Si tu dois prouver ton âge pour acheter de l'alcool, seul l'élément nécessaire est transmis. L'identifiant vérifie simplement que vous avez plus de 18 ans, sans révéler d'autres données personnelles. » (Entrevue P5E, traduction libre). Ce cas permet de saisir, à nouveau, l'intérêt des preuves à divulgation sélective, les ZKP, où seules les informations strictement requises sont transmises. Cette approche contribuer à limiter l'accumulation de données inutiles, réduisant par le fait même les risques associés à leur conservation. Ce positionnement est soutenu par une logique de contrôle granulaire de l'information. Ekko résume ainsi : « l'entité vérificatrice n'a pas besoin de tout savoir. Les données ne devraient être accessibles que selon le principe du besoin d'en connaître. » (Entrevue P5E, traduction libre). La philosophie de la donnée exprimée par cet extrait est fondée sur le principe de proportionnalité. C'est donc dire que l'accès n'est plus déterminé par l'appartenance institutionnelle, mais par la finalité de l'opération. En limitant la visibilité des données, les vecteurs potentiels d'abus sont également limités.

Le modèle devient encore plus pertinent lorsqu'il est observé dans une perspective de réseau interbancaire. Ekko donne un exemple frappant : « Un fraudeur actif chez Demacia pourrait facilement tenter de se faire passer par un client légitime chez Noxus, mais si toutes les banques partagent un même réseau d'identités décentralisées, un tel individu serait immédiatement identifié et signalé à l'ensemble du système. » (Entrevue P5E, traduction libre). L'idée véhiculée ici est que la coordination des institutions autour d'un réseau identitaire partagé permettrait une réactivité collective. Un individu signalé par une banque ne pourrait plus dupliquer sa fraude dans une autre, car l'alerte circulerait automatiquement sur

l'ensemble du réseau. Le partage d'information à des fins de conformité va dans le même sens. Ekko le détaille en ces termes :

> « Il serait possible de bloquer leurs comptes. De plus, si une banque comme Demacia a déjà réalisé une procédure KYC à un coût de 30$, une autre banque comme Noxus, n'aurait pas besoin de recommencer l'opération, car les justificatifs pourraient être réutilisés. C'est une solution gagnante-gagnante pour tous. En matière de lutte contre le blanchiment d'argent, le partage d'information sur les entités malveillantes deviendrait plus efficace. La puissance de la blockchain et des IDDs repose sur la mise en réseau, non sur des systèmes isolés. » (Entrevue P5E, traduction libre).

Ce passage met en évidence un avantage économique et réglementaire simultanément. En s'appuyant sur des vérifications KYC déjà effectuées, les institutions réduisent les doublons d'efforts, tout en augmentant leur capacité à détecter des comportements illicites grâce à un flux d'information distribué. Cette efficacité provient d'un postulat fondamental rappelé par Ekko : « Le pouvoir provient du réseau » (Entrevue P5E, traduction libre). Nous comprenons que la robustesse de l'ensemble du réseau repose sur l'interconnexion de ses parties. L'intelligence collective du système ne dépend pas d'un serveur central ou d'un prestataire unique, mais de la contribution coordonnée de tous les acteurs. C'est cette distribution du pouvoir informationnel qui permet d'anticiper les risques plutôt que de les subir. Cette distribution est renforcée par la nature même de la blockchain, comme le rappelle Ekko : « Dans un système centralisé, il n'existe qu'une seule base de données, un seul point de vérité. En revanche, avec la blockchain, chaque nœud détient les mêmes informations, ce qui permet d'en garantir l'intégrité et la disponibilité. La couche fondamentale de stockage est ainsi transformée. » (Entrevue P5E, traduction libre). L'importance de cette architecture réside dans la capacité de chaque nœud à reproduire intégralement l'historique. L'uniformité de la donnée, répartie entre les participants, garantit sa résilience face à la manipulation ou à la corruption. Le passage suivant quant à lui met en lumière une dernière dimension de la gestion des risques, soit l'indépendance vis-à-vis plateformes fermées. Ekko résume cette vision dans les termes suivants :

> « Lors de la création d'une identité, il faut s'assurer qu'elle ne soit pas liée à une seule plateforme ou application. À l'instar de l'évolution d'internet, où nous sommes passés d'une architecture de réseau distribué à un modèle dominé par les plateformes, l'identité doit revenir principes fondamentaux, soit le contrôle total par l'utilisateur, la divulgation minimale, le consentement éclairé et la portabilité entre services et juridictions, y compris à l'international. » (Entrevue P5E, traduction libre).

En somme, les extraits recueillis auprès d'Ekko et Kennen mettent en évidence une série d'arguments convergents en faveur d'un paradigme identitaire fondé sur la sécurité distribuée, la limitation des accès,

la détection proactive des fraudes et la souveraineté informationnelle. Loin d'être un avantage marginal, la diminution des risques s'impose comme une promesse structurante du modèle des IDDs.

5.3.3.2 Simplification & Portefeuille numérique

L'intégration des identifiants décentralisés s'accompagne d'un changement de paradigme dans la façon dont les services numériques sont conçus et consommés. Un passage met en lumière cette dynamique d'ouverture : « Une fois un identifiant décentralisé mis en place, un nouvel espace d'innovation s'ouvre. Par exemple, si une application requiert une vérification d'identité, KYC, il suffit d'appeler une API issue d'un service décentralisé. Cela facilite l'intégration rapide dans les systèmes existants et ouvre la voie à de nombreux cas d'usage. » (Entrevue P5E, traduction libre). Ce que ces propos laissent entrevoir, c'est qu'en mettant en place une infrastructure d'identité décentralisée, un nouveau socle est créé sur lequel des cas d'utilisation multiples pourront émerger. La simplicité réside ici dans la possibilité d'intégrer rapidement des processus d'identification à des systèmes existants par de simples appels d'API, rendant les opérations à la fois plus rapides et moins couteuses.

L'un des premiers domaines transformés par cette approche est celui de l'ouverture de compte. L'avantage principal se trouve dans la réduction drastique du temps requis pour effectuer cette opération. « L'ouverture de compte deviendra entièrement numérique, sans vérification manuelle. Ce qui prenait plusieurs jours pourra être réduit à quelques minutes, grâce à la suppression des interventions humaines. » (Entrevue P5E, traduction libre), explique Ekko. Ce passage indique que les formalités manuelles, souvent lentes et sujettes à des erreurs manuelles, pourront être éliminées au profit de processus numériques fiables et fluides. Le gain est autant en efficacité qu'en expérience utilisateur. Cette nouvelle infrastructure repose en partie sur des initiatives déjà en cours. Ekko évoque les cadres nationaux et provinciaux déjà en place : « Le Canada dispose déjà de son propre cadre de référence en matière d'identité numérique. La Colombie-Britannique possède son portefeuille numérique et Montréal développe également des initiatives locales. Ces identifiants permettront d'associer l'identité aux transactions en vue de faciliter la lutte contre le blanchiment d'argent grâce à une meilleure traçabilité. » (Entrevue P5E, traduction libre). Ce que nous comprenons avec cet exemple, c'est que la mise en œuvre de portefeuilles numériques dans certaines provinces démontre non seulement la faisabilité du concept, mais également son efficacité en matière de traçabilité, notamment dans les efforts de conformité réglementaire.

Ces identifiants seront hébergés dans le portefeuille numérique d'un individu. Pour l'illustrer voici les propos de Ekko : « L'identité numérique pourra être stockées dans un portefeuille numérique, contenant divers certificats officiels émis par le gouvernement. » (Entrevue P5E, traduction libre). Lorsqu'il est mention de certificats officiel, il s'agit de documents comme : permis de conduire, passeport, RAMQ, etc. Ce passage suggère que la simplicité agit sur la dématérialisation des documents physiques en plus de converger les documents dans un même portefeuille numérique décentralisé. L'identité devient dès lors un agrégat d'attestation infalsifiables, accessibles de manière sécurisée à partir d'un seul point. L'impact de cette infrastructure se manifeste de manière concrète dans l'utilisation qu'en feront les utilisateurs. Ekko donne l'exemple d'un processus d'ouverture de compte bancaire : « Lorsqu'un client se rend à la banque pour ouvrir un compte, il pourra simplement présenter son portefeuille numérique. La banque scannera l'identifiant pertinent pour procéder à la vérification, sans aucun formulaire à remplir. Ce processus facilitera l'intégration client à tous les niveaux. » (Entrevue P5E, traduction libre). Cela implique une élimination procédures fastidieuses et redondantes. Le rôle du client devient plus actif, mais allégé, car il présente son portefeuille, l'agent bancaire valide les informations pertinente et l'opération est conclue sans frictions.

Alors, la logique de simplification s'étend également aux démarches administratives, notamment dans les interactions avec les services publics. Ekko évoque un scénario de demande de passeport : « Que ce soit pour une demande de passeport ou pour tout autre service public, les démarches seront simplifiées. Le nombre de visites en succursale diminuera grâce aux mécanismes d'autorisation à distance, par exemple via l'envoi d'une requête sur le téléphone mobile de l'usager, demandant l'accès à un identifiant spécifique comme la RAMQ. Seul le hachage cryptographique de cette carte sera transmis au vérificateur, qui pourra valider l'information auprès des autorités compétentes. » (Entrevue P5E, traduction libre). Ce passage met en évidence une transformation majeure, soit celle du service public comme écosystème interopérable. La réduction du nombre de visites physiques implique que l'usage conserve le contrôle de ses données tout en les rendant accessibles, à distance, aux entités autorisées.

Dans une perspective d'inclusion social et de soutien gouvernemental, le portefeuille numérique devient également un vecteur d'accès simplifié à une application ou aux prestations : « Pour commander un produit, s'inscrire à une application ou recevoir des prestations gouvernementales, il ne sera plus nécessaire de fournir des justificatifs à répétition. Le gouvernement, en tant qu'émetteur des identifiants, pourra valider directement l'éligibilité du citoyen et lui octroyer les bénéfices sans formalités

supplémentaires. » (Entrevue P5E, traduction libre). Cette déclaration montre que le citoyen pourra recevoir automatiquement des droits, car il est déjà validé comme bénéficiaire. Ce principe serait également applicable au niveau bancaire pour des prêts hypothécaires par exemple. La technologie supprime le besoin de réexpliquer, de prouver et de justifier son identité dans le but de réduire les délais et les barrières administratives. La réussite d'un tel modèle repose sur une division claire des rôles institutionnels. Ekko précise que : « Le gouvernement joue le rôle d'émetteur des identifiants, mais il peut déléguer la vérification à divers agréés tels que des banques, des hôpitaux ou des tiers certifiés. Ces entités agissent alors comme vérificateurs pour confirmer l'identité d'un utilisateur selon les normes établies. » (Entrevue P5E, traduction libre). L'analyse de ce passage met en évidence une architecture distribuée, mais gouvernée où les fonctions d'émission, de détention et de vérification sont assurées par des entités différentes. Cette séparation des responsabilités est une source de robustesse. Le gouvernement garde la maîtrise de l'authenticité, tandis que les institutions partenaires assurent l'opérabilité.

Dans l'ensemble, les entretiens révèlent que la simplicité fonctionnelle apportée par les IDDs ne tient pas à un appauvrissement des processus, mais à une meilleure orchestration de leurs composantes. Le portefeuille numérique devient la clé d'un écosystème fluide, où chaque interaction, chaque demande, chaque vérification s'effectue de manière contextualisée, rapide et sécurisée. L'utilisateur gagne en autonomie, les institutions gagnent en efficacité et la société en général bénéficie d'une meilleure traçabilité sans sacrifier les droits fondamentaux à la protection des données. Ce modèle offre donc à travers sa simplicité apparente une sophistication opérationnelle remarquable.

5.3.3.3 Autres opportunités

Au-delà des bénéfices en matière de sécurité et de simplicité, l'intégration des IDDs offre d'autres opportunités substantielles non négligeables. Premièrement, en matière de gouvernance de données, un premier passage amené par Ekko souligne l'opportunité sur ce sujet :

> « Les IDDs s'inscrivent dans un modèle de gouvernance des données fondamentalement différent de celui des systèmes centralisés. Alors que les systèmes traditionnels reposent sur une hiérarchie rigide de gestion des données, les IDDs s'appuient sur une gouvernance plus transparente, alignée sur les principes de l'identité auto-souveraine. Grâce à la blockchain, les données sont répliquées sur plusieurs nœuds, ce qui permet des audits en temps réel. Contrairement aux systèmes centralisés, où les modifications doivent être poussés vers un serveur principal sans réplication immédiate, générant ainsi des erreurs de lecture ou de verrouillage, ces problèmes sont évités avec la décentralisation. » (Entrevue P5E, traduction libre)

Avec ces propos, nous sommes en mesure de voir un changement de paradigme dans la manière de concevoir la gouvernance des données. Le modèle décentralisé abolit les rigidités hiérarchiques des systèmes centralisés et introduit un pilotage transversal fondé sur la transparence, la réplicabilité et la possibilité d'audit en temps réel. Les erreurs liées à la centralisation des écritures, les verrous applicatifs ou les conflits de versions deviennent marginaux dans un tel environnement.

Un autre extrait resouligne l'importance des banques comme précurseurs de la technologie : « Les banques figurent parmi les premières institutions à avoir lancé des projets pilotes utilisant la blockchain. Elles y voient un potentiel unique en matière de transparence, de traçabilité et de fiabilité des données. Lorsqu'il s'agit de disposer d'une source unique de vérité vérifiable, la blockchain représente une solution sans équivalent. » (Entrevue P5E, traduction libre). Ce passage souligne que les banques perçoivent la blockchain comme un levier stratégique de fiabilité, notamment pour établir une source de vérité unique, distribuée et vérifiable. Le recours aux IDDs s'intègre dans cette dynamique en apportant une couche identitaire transparente, compatible avec les exigences du secteur bancaire en matière de contrôle, de conformité et de traçabilité.

La robustesse fonctionnelle de ces identifiants repose sur des principes d'architecture distribuée. Ekko rappelle que : « Les IDDs sont conçus pour être minimalistes et sécurisés. Leur architecture distribuée élimine tout point unique de défaillance, à la différence des systèmes décentralisés. Lorsqu'un identifiant est requis, il est validé par plusieurs sources avant d'être accepté, ce qui renforce la fiabilité du système. À l'image de la blockchain, chaque élément est dupliqué afin d'assurer la résilience du réseau. Ce n'est plus l'organisation qui contrôle l'identité, c'est l'utilisateur. » (Entrevue P5E, traduction libre). À travers cette formulation, nous comprenons que le système d'identité gagne en résilience structurelle, car chaque validation est confirmée par plusieurs nœuds et la perte ou la corruption d'un seul ne suffit plus à compromettre l'intégrité de l'ensemble. Le caractère minimaliste renforce par ailleurs la performance des traitements en limitant les charges inutiles. La gouvernance se fait par design et non par superposition d'outils de contrôle.

Le dernier apport identifié est certainement les coûts. Cet apport est évoqué dans le passage suivant : « Les systèmes centralisés entraînent des coûts élevés de maintenance, car toute l'infrastructure repose sur un point unique. Cela limite leur capacité à évoluer et à s'adapter à une montée en charge, contrairement aux architectures distribuées, qui offrent une scalabilité nettement supérieure. » (Entrevue

P5E, traduction libre). Ce que ces propos mettent en relief, c'est que les infrastructures traditionnelles centralisées nécessitent des investissements lourds pour maintenir la disponibilité, gérer les pics de charge et assurer la conformité. En comparaison, les architectures distribuées permettent une montée en charge fluide, une meilleure gestion de la redondance et une réduction des interventions techniques récurrentes.

Ainsi, les IDDs n'impliquent pas seulement la transformation de la relation entre les banques et les clients, mais ils réorganisent les fondations des systèmes bancaires modernes. Le passage à une infrastructure identitaire distribuée redessine les flux, simplifie la gouvernance, réduit les fragilités techniques, encourage la transparence et favorise une logique d'efficacité pérenne. Cette perspective fait des IDDs un vecteur de modernisation à part entière.

Codification / Thème	Nombre d'entrevues	Références
Diminution des risques	2	11
Gouvernance des données	1	1
Portefeuille numérique	1	6
Réduction des coûts	2	3
Points d'entrée	1	2
Simplification	1	3
Transparence	2	3

Tableau 11 Codifications et références des Opportunités des IDDs - Amélioration des processus

5.3.4 Opportunités des IDDs – Humain

Au-delà de la transformation des processus internes et des infrastructures, l'autre levier à prendre en considération par rapport aux opportunités réside dans la manière que les identifiants décentralisés impactent la relation entre l'utilisateur et son identité numérique. Cette dimension s'incruste directement

dans l'expérience vécue par les utilisateurs. Bien qu'une nouvelle technologie amène des défis, elle amène du même fait des opportunités en matière de confiance, de contrôle personnel et d'interactions fluides avec les institutions.

Deux sous-thèmes principaux ressortent des propos recueillis liés à l'humain : la fiabilité perçue et l'autonomisation. Le premier, présent dans une transcription avec six références, met en lumière l'importance d'un capital réputationnel numérique, traçable et sécurisé, que les individus peuvent mobiliser dans leurs relations avec les institutions. Le second, présent dans deux transcriptions avec cinq références, aborde la manière dont les individus peuvent exercer un contrôle granulaire sur leurs données, en définissant ce qu'ils partagent, à qui et sous quelles conditions. Ces thématiques traduisent une évolution du rôle de l'utilisateur en leur redonnant le plein pouvoir sur leurs données.

5.3.4.1 Fiabilité perçue

La question de confiance est un thème irrévocable lorsqu'il s'agit d'une nouvelle technologie à implémenter. Les systèmes décentralisés promettent d'améliorer les processus tels qu'ils le sont aujourd'hui, mais ce sont des individus qui sont derrière les systèmes. Ainsi, la fiabilité des identifiants décentralisés désigne la confiance qu'ils projettent aux yeux des utilisateurs et des institutions. Lorsqu'un client interagit avec des services financiers, chaque action, validation et relation participe à la construction d'un capital réputationnel. C'est ce que souligne explicitement Kennen en évoquant le rôle fondamental des identités décentralisées dans cette dynamique. « Lorsque je parle de réputation, je fais référence à la capacité d'offrir à ses clients un capital de confiance visible aux yeux des tiers. Chaque transaction vérifiée renforce ce statut. Les banques, qui détiennent les données de transaction, doivent pouvoir les consulter. Ce qui a du sens, c'est que les banques contrôlent, avec le client, qui peut y accéder. C'est précisément ce que permettent les outils de provenance de données comme KERI. » (Entrevue P6E, traduction libre). Le passage met en lumière une faculté essentielle des systèmes comme KERI. KERI permet au client de projeter une image de fiabilité au sein d'un réseau distribué, car comme le mentionne Kennen :

> « La raison que c'est possible, c'est que tu as une preuve cryptographique de l'historique de données et il est possible de savoir à qui payer des redevances. Les banques peuvent donc désormais transformer ces données, de manière vérifiable et éthique, en un flux de redevances pour tous leurs clients. Elles peuvent vendre ces données comme un complément à chaque fois que les données sont vendues, elles peuvent rapporter de l'argent à leurs clients lorsque leurs données sont vendues aux enchères et elles peuvent également apporter des niveaux de sécurité extrêmement élevés par rapport au système existant. » (Entrevue P6E, traduction libre)

Donc, avec cet extrait, nous comprenons qu'un client est en mesure d'avoir un contrôle granulaire sur l'accès à ses propres données. L'utilisateur ne subit plus le traitement de ses données, il en devient acteur. Ce principe de souveraineté partagée, entre un détenteur de l'identité et l'institution, réintroduit un équilibre dans la gestion de la réputation numérique. L'élément différenciateur majeur de cette approche repose sur la vérifiabilité cryptographique de l'historique des données. Dans un environnement où la provenance de l'information est systématiquement prouvée, les interactions deviennent non seulement traçables, mais également profitables pour la banque et le client au moyen de redevances. Ce changement du rapport à la donnée ouvre la voie à des mécanismes de redevance permettant donc à chacun de monétiser, de façon éthique et contractuelle, l'usage secondaire de ses informations personnelles. Ce positionnement confère à l'identité décentralisée une valeur économique directe, qui transforme la relation entre institutions financières et individus, en développant une nouvelle relation d'affaires. En posant les bases de cette économie émergente de la donnée authentifiée, Kennen invite à réfléchir à une redéfinition des flux de valeur entre utilisateurs et institutions. « Je pense que les redevances sur les données seront la plus grande source de revenus dans le futur. Elles reposeront sur des flux de données traçables et digne de confiance. » (Entrevue P6E, traduction libre), indique Kennen. Si les perspectives de valorisation des données sont bien réelles, leur concrétisation à grande échelle nécessitera des déclencheurs structurels. Comme l'indique Kennen, ces marchés de la donnée authentifiée mettront du temps à s'imposer dans l'économie numérique, à moins qu'un événement majeur ne catalyse leur adoption. « Je pense qu'il faudra plus de temps pour que les flux de redevances sur le marché des données authentiques émergent et nous devrons assister à des imprévus. » (Entrevue P6E, traduction libre). Toutefois, ces flux ne reposent plus uniquement sur l'échange de services, mais sur une logique de confiance validé par la technologie elle-même. Le registre distribué devient alors le garant d'un récit transactionnel dont l'intégrité n'a plus besoin d'être arbitrée par un tiers.

Il convient néanmoins de mettre l'emphase sur la dimension humaine de la confiance. Bien que la confiance repose sur le registre distribué, cela ne couvre pas là où la vraie confiance se trouve. Kennen nous rappelle que la confiance n'est pas une abstraction technique comme la TBC, c'est plutôt une construction sociale enracinée dans des siècles de pratiques collectives entre humains : « Les relations humaines sont bâties sur la confiance. Les sociétés humaines sont fondées sur la confiance. Il en est ainsi depuis des milliers d'années et il en sera toujours ainsi. » (Entrevue P6E, traduction libre). Or, l'authenticité des relations sociales ne peut être simulée ni automatisée. Elle nécessite des mécanismes de validation rigoureux certes, mais aussi compréhensibles et acceptables pour les humains. C'est pourquoi la

technologie, aussi avancée soit-elle, ne pourra jamais remplacer l'infrastructure sociale de la confiance tel que le mentionne Kennen : « Les machines ne peuvent pas remplacer la confiance. » (Entrevue P6E, traduction libre). En effet, la technologie peut appuyer, renforcer, documenter, mais jamais substituer la confiance. La crédibilité d'un individu dans un écosystème numérique distribué découlera de la reconnaissance collective de sa fiabilité et non de sa conformité cryptographique.

En somme, la fiabilité perçue constitue l'un des fondements prometteurs des identifiants décentralisés. Elle lie la technologie avec l'humaine au moyen de la confiance et de la légitimité. En permettant à chacun de gérer son identité comme un actif vérifiable et traçable, les IDDs, porteurs de valeur, redéfinissent les conditions de la confiance dans le monde numérique.

5.3.4.2 Autonomisation & Remise du pouvoir aux individus

L'un des principes fondateurs du modèle d'identité décentralisée réside dans la réattribution du contrôle des données aux individus. Cette autonomie repose sur un repositionnement fondamental de l'utilisateur dans l'architecture numérique. L'utilisateur passe du sujet administré à l'acteur souverain de sa propre identité. En effet, l'architecture décentralisée redéfinit la distribution des responsabilités. Ekko affirme un basculement net dans la logique de gouvernance des identités avec les propos suivants : « Il ne s'agit plus d'un contrôle exercé par l'organisation mais bien d'un contrôle exercé par l'utilisateur lui-même. » (Entrevue P5E, traduction libre). Dans les systèmes classiques, les institutions centralisent les autorisations, stockent les attributs et décident des règles de partage. Dans un modèle décentralisé, l'utilisateur détient les clés, au sens propre comme au figuré, et pilote lui-même les accès à ses données. Ekko appuie sur cette déclaration avec les propos qui suivent : « Contrairement aux systèmes traditionnels fondés sur un modèle maître-esclave, où un administrateur détient un accès complet aux données, l'approche décentralisée privilégie une limitation structurelle du contrôle et renforce l'autonomie des utilisateurs sur leurs propres informations. » (Entrevue P5E, traduction libre). Ce passage confirme que les plateformes traditionnelles reposent souvent sur des mécanismes unilatéraux de gestion des droits, où l'utilisateur ne fait qu'accepter ou refuser des conditions préétablies. À l'inverse, le modèle des IDDs introduit une horizontalité technique, dans laquelle aucune entité ne détient seule l'accès aux données et où chaque requête doit être validée explicitement par l'individu concerné.

En ce sens, Kennen introduit une réflexion en distinguant deux courants de pensée qui structurent aujourd'hui les approches d'identité auto-souveraine et du contrôle des données personnelles :

> « [Lorsqu'on parle de redonner aux individus le contrôle sur leurs données], il y a deux grandes écoles de pensée. La première est les preuves de divulgation nulle (ZKP) et la deuxième est les contrats Ricardiens. » (Entrevue P6E, traduction libre)

La première école de pensée, basée sur les Zero-Knowledge Proofs, permet de limiter l'exposition des données via des preuves de divulgation minimale. Ekko introduit les ZKP comme suit : « De nouvelles technologies, comme les ZKP, permettent de vérifier certaines caractéristiques sans révéler l'identité complète d'un individu. » (Entrevue P5E, traduction libre). Le contrôle ne réside pas uniquement dans la détention des identifiants, mais également dans la capacité de l'utilisateur à moduler l'information qu'il souhaite rendre visible. Il est donc possible pour l'utilisateur de prouver certaines caractéristiques qui lui sont propre, comme son âge, sans livrer l'ensemble de son identité. Cette approche granulaire renforce le consentement et l'autonomie, tout en réduisant les risques d'exploitation secondaire des données.

La seconde école de pensée, fondée sur les contrats ricardiens, intègre juridiquement les droits de l'utilisateur à travers des règles exécutables. Kennen l'explique ainsi :

> « Il existe un concept appelé chaîne de confidentialité. Ce que cela veut dire c'est que lorsque tu partages des données, tu exiges de ceux avec qui tu partages tes données qu'ils signent un contrat stipulant qu'ils acceptent de soumettre toute personne avec qui ils partagent tes données aux mêmes contraintes que celles auxquelles tu les soumets. » (Entrevue P6E, traduction libre).

Nous comprenons avec l'extrait qu'il s'agit d'une confiance entre deux entités liées par un contrat, ce qui veut dire que l'aspect légal prend place dans cette école de pensée. Voici un exemple, un exemple donné par Kennen pour illustrer le concept de chaîne de confidentialité :

> « Si tu partages tes données avec Chevron lorsque tu achètes de l'essence, Chevron signe ton contrat ricardien qui stipule que Chevron doit imposer les mêmes restrictions sur tes données à quiconque il souhaite partager tes données. C'est pourquoi cela se nomme une chaîne. » (Entrevue P6E, traduction libre).

Cela signifie que ce mécanisme assure une continuité des protections indépendamment du nombre d'intermédiaires. La confiance agit ici en tant qu'obligation légale, transmissible et paramétrable selon les besoins de l'utilisateur. La confidentialité est respectée, car elle est fondée sur une traçabilité contractuelle.

La dualité entre les ZKP et les contrats Ricardiens révèle que la question du contrôle dépasse les considérations techniques, car elle touche au rôle que la technologie et les droits personnels doivent jouer

dans la protection des identités numériques. Ce nouveau pouvoir décisionnel repose également sur la transparence des échanges. L'utilisateur n'est plus un simple bénéficiaire passif de services numériques, il devient un gestionnaire actif de ses permissions. Ekko le résume ainsi : « Le contrôle revient à l'utilisateur et il sait exactement quelles données sont partagées. » (Entrevue P5E, traduction libre). Ainsi, redonner le pouvoir aux utilisateurs dans un écosystème d'IDDs revêt d'une refonte profonde des relations entre l'humain, la donnée et l'infrastructure. Le contrôle devient paramétrable, visible, traçable et révocable. L'autonomie repose maintenant sur la capacité à manier avec discernement l'identité numérique dans un cadre cryptographique et juridique qui garantit l'effectivité des interactions. Cette perspective ne constitue toutefois pas un état atteignable à court terme dans le contexte bancaire actuel, mais plutôt un horizon conceptuel mettant en tension les logiques institutionnelles existantes avec les potentialités offertes par les identifiants décentralisés. Les entretiens révèlent ainsi un écart significatif entre les promesses théoriques de la gouvernance distribuée et les contraintes organisationnelles, réglementaires et culturelles propres au secteur bancaire. Ce retour du pouvoir à l'utilisateur ouvre la voie à un modèle de gouvernance distribuée centré sur l'individu porteur de nouvelles formes de responsabilité et de souveraineté numérique.

Codification / Thème	Nombre d'entrevues	Références
Fiabilité perçue	1	6
Autonomisation	2	5

Tableau 12 Codifications et références des Opportunités des IDDs - Expérience utilisateur

5.3.5 Opportunités des IDDs – Solutions

Afin de comprendre plus concrètement les opportunités qu'offrent les identifiants décentralisés, nous allons présenter dans cette section les solutions évoquées par nos répondants. Avec une description concrète des solutions par les experts, nous serons en mesure d'identifier, pour chaque solution présentée, les caractéristiques distinctives, les mécanismes de gouvernance associées, ainsi que les bénéfices opérationnels et stratégiques qu'elles peuvent offrir aux institutions financières. Cette analyse s'appuie

sur 30 références issues de deux transcriptions, ce qui témoigne de la richesse des perspectives recueillies pour les solutions abordées. Les solutions KERI, Hyperledger Indy et Corda feront l'objet d'un examen comparatif selon leur conformité aux principes de l'identité auto-souveraine et leur pertinence dans un contexte bancaire.

5.3.5.1 Solution Key Event Receipt Infrastructure

Parmi les solutions évoquées par les répondants, KERI occupe une place centrale dans le discours de Kennen. Selon lui, KERI représente la mise en œuvre la plus cohérente des principes d'identité auto-souveraine. Il affirme que « la façon dont la sécurité fonctionne dans KERI adhère complètement à la promesse d'identité auto-souveraine où l'utilisateur contrôle vraiment son identité. » (Entrevue P6E, traduction libre). Ce passage souligne que l'architecture même de KERI est conçue pour que l'utilisateur conserve une maîtrise directe sur la création, la gestion et la diffusion de ses identifiants, et ce sans intermédiation institutionnelle. Il présente KERI comme étant « un protocole véritablement décentralisé. » (Entrevue P6E, traduction libre), ce qui signifie qu'à ses yeux KERI se différencie des autres solutions blockchain soi-disant décentralisées.

Ainsi, KERI se distingue par sa capacité à générer des historiques de clés vérifiables tel que confirmé par les propos suivants : « KERI fait un excellent travail à créer un identifiant décentralisé et un historique de clés vérifiables. » (Entrevue P6E, traduction libre). La continuité cryptographique d'identité est un élément clé de la solution KERI, car elle est en mesure de perdurer dans le temps à travers d'un fil d'évènements vérifiables. « Tout système qui réclame être sous un modèle d'identité auto-souveraine, mais qui ne te donnes pas d'historique de clés vérifiables manque un morceau critique. », insiste Kennen. À cela, Kennen ajoute : « Parmi les centaines de méthodes IDD existantes, peu atteignent le niveau d'intégration offert par KERI. KERI propose une pile technologique unifiée qui intègre des IDDs, des informations d'identification vérifiables et des conteneurs de données authentiques. » (Entrevue P6E, traduction libre). Cette unification permet de réduire les risques d'incompatibilité tout en garantissant une cohérence systémique entre les différentes composantes de l'identité. Les propos de Kennen montrent ensuite que KERI ne repose pas uniquement sur des garanties cryptographiques. Tel qu'expliqué plus tôt, elle repose également sur des garanties contractuelles au moyen de contrats ricardiens et de chaînes de confidentialité. « Ce type de dispositif n'est pas un dispositif technologique, mais bien un dispositif légal. »

(Entrevue P6E, traduction libre), clarifie Kennen. Grâce à la chaîne de confidentialité, l'utilisateur est en mesure d'obliger contractuellement toute entité qui souhaite obtenir et partager ses informations d'identification vérifiables à ce que chaque diffusion de ses données applique les mêmes restrictions auxquelles l'utilisateur consent. Or, plutôt que d'utiliser la technologie pour faire respecter la vie privée, comme c'est le cas avec les ZKP, Kennen explique que KERI intègre directement ces règles dans les justificatifs eux-mêmes avec les propos suivants :

> « [le fondateur de KERI] a conçu les conteneurs de données de chaîne authentique. Il s'agit du standard de spécification des informations d'identification vérifiables pour que chaque justificatif détenu, il soit possible d'avoir un langage juridique, soit un contrat ricardien, autour de chaque information d'identification et autour de chaque divulgation de cette information d'identification. » (Entrevue P6E, traduction libre).

De plus, Kennen ajoute que dans KERI il existe, tout comme avec les ZKP, « une version de la divulgation sélective dans laquelle il est possible de mettre en place un processus d'aveuglement ou de levée d'aveuglement par attribut ou par justificatif de sorte que dès que quelqu'un accepte tes conditions, tu le débloques et il peut voir les données. » (Entrevue P6E, traduction libre). Avec cette proposition, nous comprenons que KERI est en mesure d'aller au-delà des protocoles ZKP en octroyant les mêmes paramètres et fonctionnalités, mais sous une protection juridique plutôt que technologique. Par ailleurs, il est d'autant plus important de nos jours d'avoir accès à une architecture comme celle-ci selon Kennen en raison des propos suivants : « dans un monde où l'intelligence artificielle réidentifie facilement les gens, nous sommes presque certains qu'il sera illégal de détenir des données qui ne sont pas signées. KERI est un outil qui permet de signer ces données. C'est ce que l'on appelle la provenance des données. » (Entrevue P6E, traduction libre). KERI est donc conçu comme un système préemptif, qui anticipe les régulations futures en apportant une infrastructure de consentement éclairé et robuste par sa nature légale. « Si tu as un contrat stipulant que tu n'utiliseras pas les données de manière abusive, tu es légalement dissuadé de le faire, car si tu en abuses, cet accord peut être invoqué et tu peux être poursuivi en justice. » (Entrevue P6E, traduction libre). Cette robustesse s'étend également à la résilience du système en cas de compromission. Comme le mentionne Kennen :

> « Deux caractéristiques indispensables pour rendre l'identité décentralisée réellement accessible au grand public. La première est la rotation des clés, qui permet de remplacer une clé perdue ou compromise ou d'ajouter de nouveaux appareils sans difficulté. La seconde est la multisignature, qui te permet à toi, un ami, ou quiconque de détenir une copie sécurisée de ta clé. Ainsi, même en cas de perte totale d'accès à tes dispositifs, tu peux demander à ces

> personnes de désactiver l'ancienne clé et d'activer la nouvelle. » (Entrevue P6E, traduction libre).

La possibilité de faire tourner une clé ou d'activer des mécanismes de cogestion réduit fortement le risque de perte d'identité numérique. C'est un peu comme les courriels de secours lorsqu'il y a un mot de passe oublié ou bien comme une clé de maison qui être prêtée à un être proche en cas de soucis. Le passage suivant témoigne d'un exemple indiquant qu'il est même possible d'externaliser cette sécurité à des tiers de confiance :

> « KERI résout ce problème de perte de clés. » (Entrevue P6E, traduction libre). Kennen poursuit en donnant un exemple : « Imaginons que nous faisons partie d'un groupe multisignature avec chacun une moitié du poids requis. Aucune opération liée à l'identité ne pourrait être effectuée sans la signature conjointe des deux parties. Ou bien tu peux détenir une clé, je peux en détenir une moitié et un de tes amis une autre. Si tu perds ta clé, tu peux appeler ton ami et moi et dire : J'ai besoin que tu effectues une rotation de mon ancienne clé et que tu actives la nouvelle clé. » (Entrevue P6E, traduction libre).

La perte de clé ne signifie pas la fin de l'identité dans cette proposition contrairement à ce qui est observé dans d'autres systèmes comme Bitcoin où la perte de clés entraîne la perte des cryptomonnaies. Kennen va plus encore en soulignant que KERI offre cette même avenue, mais avec des institutions de confiance que nous connaissons aujourd'hui. « Dans un portefeuille multisignature, l'ajout d'un nouveau signataire passe par une rotation de clés. La multisignature et la rotation de clés se passe en même temps. Si on devait ajouter une troisième chose, ce serait un fournisseur de services de clé de garde comme une banque, c'est-à-dire un des gens qui apportent la confiance à l'économie. Tu leur dis : Je te fais confiance de conserver [ma clé]. » (Entrevue P6E, traduction libre). Cette analogie montre que les banques conserveraient toujours leur statut d'institution de confiance en agissant comme détenteurs de clés secondaires pour leurs clients. « Ce qui est vraiment intéressant avec l'architecture KERI c'est qu'il existe des méthodes encore plus avancées comme la rotation déléguée de clés multisignature où même tu perds tes clés ou que tu te fais pirater, tu restes protégé, car chaque rotation doit être approuvée par un délégué que tu as préalablement désigné comme hautement fiable et compétente. » (Entrevue P6E, traduction libre). Cela répond directement aux problèmes liés à la gestion des clés et, par le fait même, au last mile. Il n'est plus du tout impossible, contrairement à Bitcoin, de récupérer ses clés, et ce à travers plusieurs moyens différents qui assurent plusieurs angles de gestion des clés.

En outre, Kennen recentre la discussion sur la philosophie même de l'identité auto-souveraine lorsque nous avons demandé à savoir si dans KERI, le gouvernement agissait toujours en tant qu'émetteur

d'identité. « Le gouvernement ne fournit pas l'identité. Il l'assure. Ce que je veux dire c'est que c'est toi qui fournis ton identité. Il s'agit ici d'une distinction philosophique importante. C'est de ça qu'il s'agit quand on parle d'identité auto-souveraine. » (Entrevue P6E, traduction libre). Pour mieux comprendre ce que Kennen sous-entend voici un exemple :

> « Ce que tu fais c'est que tu t'adresses au gouvernement et tu lui dis : Voici ma clé ou voici mon identité et signez mon identité. Ils endossent ou affirment ton identité et ce que la banque fait, ils ne sont pas un fournisseur d'identité, c'est un fournisseur de sécurité et de disponibilité [des clés]. Elle est donc ta partenaire en cas de perte, de sorte que si tu perds accès à ton jumeau numérique, soit à ton identité numérique, elle peut t'aider à la récupérer. Ce n'est pas nécessairement une banque. Cela peut être un fournisseur de service technologique. Cela ouvre le marché à n'importe quelle société dont tu estimes qu'elle possède les compétences techniques ou morale, la réputation morale, le caractère et l'intégrité auxquels tu lui fais confiance. » (Entrevue P6E, traduction libre).

Cela règle le problème de dépendance au fournisseur d'identité ainsi qu'à ses problèmes inhérents liés à la sécurité des données. Toutefois, Kennen soutient que les gouvernements conservent un rôle structurant avec le passage qui suit : « Les gouvernements sont nécessaires lorsque tu veux avoir une reconnaissance commune de certains documents d'identité, comme un passeport ou un numéro d'assurance sociale. C'est là que le gouvernement intervient et dit : Toi en tant que telle personne, tu émets ce titre justificatif qui dit que tu as ce statut dans notre système. Ils aident essentiellement à standardiser les attributs de ton identité et là où les banque entrent en jeu c'est lorsqu'elles reconnaissent cette identité et l'autorisent à participer à des transactions. » (Entrevue P6E, traduction libre). Avec cet extrait, nous comprenons que le gouvernement émet toujours des pièces justificatives, mais que les utilisateurs sont les réels émetteurs d'identité. Finalement, tel qu'itéré précédemment, KERI offre une dimension économique dans son modèle via des redevances. En effet, les utilisateurs pourront contrôler leurs données, les monétiser en plus d'emporter avec eux leur réputation, suggérant que la donnée identitaire peut devenir un actif personnel valorisable et attestables de la réputation.

> « La raison que c'est possible, c'est que tu as une preuve cryptographique de l'historique de données et il est possible de savoir à qui payer des redevances. Les banques peuvent donc désormais transformer ces données, de manière vérifiable et éthique, en un flux de redevances pour tous leurs clients. Elles peuvent vendre ces données comme un complément à chaque fois que les données sont vendues, elles peuvent rapporter de l'argent à leurs clients lorsque leurs données sont vendues aux enchères et elles peuvent également apporter des niveaux de sécurité extrêmement élevés par rapport au système existant. » (Entrevue P6E, traduction libre)

Ainsi, KERI émerge comme une solution d'identité auto-souveraine complète, articulant technologie, droit, sécurité et économie dans un cadre intégré et cohérent. KERI répond à la fois aux exigences réglementaires, aux besoins opérationnels et aux aspirations sociales des individus.

Codification / Thème	Nombre d'entrevues	Références
Solutions	2	30

Tableau 13 Codifications et références des Opportunités des IDDs - Solutions

5.3.5.2 Solution Hyperledger & Corda

Du côté d'Ekko, d'autres solutions sont abordées, notamment celles issues de la fondation Hyperledger et Corda. La présentation et l'analyse de ces plateformes permettent de mieux cerner les prérequis technologiques et politiques de l'implémentation d'un modèle d'identité décentralisée. Les plateformes présentées permettent donc d'illustrer les avantages des IDDs au moyen de leurs bienfaits. Nous allons donc commencer par Hyperledger, puis brièvement aborder Corda. Tout d'abord, comme l'explique Ekko dans l'extrait qui suit, Hyperledger est un projet qui regroupe plusieurs sous solutions et objectifs dont Aries, Fabric et Indy :

> « Hyperledger Indy est un registre distribué en mode open-source. L'objectif premier derrière la création de Indy fût les identités décentralisées. Hyperledger Fabric et Aries font également partie de l'écosystème Hyperledger. Indy a spécifiquement été créé pour les identités décentralisées. C'est un projet Hyperledger supporté par la fondation Linux et il supporte les informations d'identification vérifiables. C'est pourquoi Indy est l'un des projets clé dans l'écosystème Hyperledger et un des premiers réseaux auto-souverains. » (Entrevue P5E, traduction libre).

Ces propos soulignent que Hyperledger fait de Indy l'un des rares projets ayant été orientés dès le départ vers la gestion d'identifiants numériques auto-souverains avec une comptabilité native aux IIVs. Cette orientation initiale est importante à souligner, car elle distingue Indy de nombreuses solutions blockchain génériques qui ne sont pas nativement conçues pour gérer les identifiants décentralisés. Pour faire suite à ces propos, le passage suivant indique que la gouvernance ouverte et l'utilisation publique sont au cœur de la philosophie qui soutient cette solution.

> « [Indy] opère en tant que blockchain publique avec permission et sert en tant qu'identité numérique ouverte à quiconque. Elle est basée sur un modèle de gouvernance sans but lucratif et intègre la protection de la vie privée. Ces caractéristiques sont clairement avantageuses. Toute technologie de ce type devrait absolument être open-source, car le monde est en train de progressivement se diriger dans cette direction. Si tu bâtis quelque chose destiné à être interopérable, cela ne doit pas appartenir à quelqu'un. Confier le contrôle complet à une entité propriétaire mène à des coûts significativement plus élevés. À l'inverse, un projet open-source permet à chacun de contribuer. On peut toujours y greffer une couche propriétaire, mais les fondements doivent demeurer open-source. C'est ça l'essentiel. (Entrevue P5E, traduction libre).

Ce modèle assure dès lors une accessibilité universelle par nature open-source, tout en intégrant des protections renforcées à la vie privée. Il répond donc à des exigences techniques et éthiques dans un perspective d'adoption à grande échelle. La question du coût et de l'autonomie technologique devient alors centrale. Une solution fondée sur des composants open-source limite les barrières financières à l'entrée pour les institutions de plus petite taille. Elle favorise l'émergence d'un écosystème participatif et d'un modèle à but non lucratif qui soutent une logique de confiance et d'impartialité. Pour créer un cadre partagé de confiance entre plusieurs acteurs d'un réseau distribué, nous comprenons qu'il suffit de s'éloigner de la dépendance envers un fournisseur unique. Cette approche s'aligne sur les principes fondamentaux de l'identité auto-souveraine. Par ailleurs, l'extrait suivant élargit la perspective en comparant Indy à une autre solution à une autre solution explorée par Ekko :

> « En plus d'Indy et des réseaux souverains, nous avons également utilisé Corda, développé par R3. Conçu principalement pour le secteur bancaire, Corda possède son propre mécanisme de consensus. Néanmoins, ses cas d'utilisation sont limités et la solution reste propriétaire. Comme je l'ai déjà souligné, une solution open-source peut être personnalisée via une surcouche (wrapper), mais un système propriétaire n'est pas viable à grande échelle. Dans un contexte de réseau [distribué], tous les participants doivent pouvoir contribuer et toute le monde ne peut pas se permettre de payer des frais de licence. Confier le pouvoir à un acteur unique nuit à l'écosystème. C'est pourquoi j'insiste qu'une solution doit être open-source et reposer sur un modèle de gouvernance non lucrative. Ce sont là les deux critères lorsqu'on choisit un cadre technologique pour la blockchain. » (Entrevue P5E, traduction libre)

Cette remarque souligne les limites des architectures fermées, notamment leur capacité réduite à évoluer dans des environnements collaboratifs, ouverts et de grande échelle. C'est pour cette raison que Ekko insiste sur le fait d'avoir une dynamique d'ouverture technologique, de partage et de gouvernance non lucrative. Ces exigences définissent une grille de critères sur lesquels baser ses choix, applicable à tout projet visant l'implémentation d'un cadre d'IAS, et ce particulièrement dans le domaine bancaire. Tel

qu'exprimé dans les propos suivants de Ekko, la valeur ajoutée fonctionnelle offerte par Indy consiste à redonner le pouvoir aux utilisateurs :

> « Oui, l'identité auto-souveraine te donne le contrôle sur ce que tu partages. Si quelqu'un souhaite vérifier son identité, le système te laisse choisir quel justificatif fournir parmi plusieurs. Le système est conçu avec des mécanismes de contrôle intégrés. Il s'agit fondamentalement de propriété identitaire. C'est exactement ce que Indy offre, soit le contrôle sur ton identité. » (Entrevue P5E, traduction libre)

Il est donc possible pour un utilisateur, au sein de Indy, d'avoir une capacité de sélection sur ses attributs et justificatifs d'identité en vue de répondre aux besoins de confidentialité et de souveraineté numérique. Cette capacité de sélection confère à l'utilisateur un contrôle granulaire sur ses échanges. Elle permet de construire des interactions numériques basées sur le strict nécessaire, ce qui renforce à la fois la confidentialité des données et leur pertinence contextuelle. Les propos de Ekko montrent ensuite que cette gestion granulaire repose sur une architecture de portefeuille numérique conçue pour protéger la vie privée :

> « Tu peux gérer plusieurs identifiants grâce au mécanisme de portefeuille numérique. Tu peux les contrôler et les préserver. La gestion de l'identité dans ce contexte se concentre sur ce qu'on appelle la gestion d'identité respectueuse de la vie privée. L'architecture de Indy repose sur des identifiants décentralisés, des informations d'identification vérifiables et des interactions P2P. Ce sont tous des composants fondamentaux de la blockchain. Mais l'identité auto-souveraine met l'emphase sur le contrôle de l'individu et la vie privée au-dessus de tout. » (Entrevue P5E, traduction libre)

L'intégration native de ces composants permet une orchestration fluide entre les différentes étapes de vérification, de consentement et de traçabilité. L'utilisateur n'a plus besoin de naviguer entre différentes plateformes ou services pour gérer ses preuves, car tout est regroupé dans un environnement cohérent, accessible et sécurisé. Le rôle du portefeuille numérique sert comme un espace de gestion des identités et comme une interface de confiance entre l'utilisateur et le fournisseur de service.

En somme, l'analyse des propos de Ekko sur Indy et sur Corda met en lumière l'importance de concevoir des solutions alignées avec les valeurs de l'identité auto-souveraine. Les caractéristiques techniques, bien qu'importantes, doivent être accompagnées d'une gouvernance ouverte, une interopérabilité native et une architecture pensée pour l'utilisateur. Ce sont des fondements qui permettront aux identifiants décentralisés de s'imposer comme un levier de transformation durable dans le secteur bancaire. La section

suivante approfondira d'autres aspects de cette transformation à travers l'analyse des perspectives stratégiques liées à la gouvernance, aux usages et aux parties prenantes.

5.3.6 Synthèse de l'analyse des opportunités et défis de l'intégration des IDDs

À l'issue de l'analyse des thèmes structurants liés à l'intégration des identifiants décentralisés dans les systèmes bancaires, nous apercevons que cette transition technologique ne peut être appréhendée uniquement sous l'angle de l'innovation. Elle constitue une transformation systémique touchant à la fois les fondements techniques, les processus organisationnels et les usages humains. Les défis et opportunités recensées, codifiées à partir des entretiens avec les experts Ekko et Kennen, révèlent une tension permanente entre complexité d'intégration, exigence d'interopérabilité, gestion du changement et promesse d'efficience accrue.

Du côté des défis d'implémentation, les constats convergent vers une double contrainte. D'une part, la mise à niveau des infrastructures bancaires exige une refonte profonde des systèmes bancaires traditionnels marquées par la centralisation, la segmentation fonctionnelle et les logiques propriétaires. D'autre part, l'absence de standards universellement reconnus et la fragmentation actuelle des solutions d'IAS compliquent encore davantage les efforts de standardisation et d'adoption. Ce constant est renforcé par l'analyse des défis techniques liés à l'infrastructure d'IAS, ce qui souligne une tension entre les promesses d'une gouvernance distribuée et la réalité des architectures partiellement centralisées. L'exemple de la rotation des clés, des historiques vérifiables ou encore de la résistance aux réidentifications non consenties souligne le degré de maturité encore inégal des technologies disponibles. Dans ce contexte, les affordances des technologies d'IAS restent latentes. Bien que les fonctionnalités existent, elles ne sont pas encore suffisamment matures ou activables par les institutions bancaires. À cela s'ajoute la question du last mile, soit l'adéquation entre les mécanismes cryptographiques proposés et la capacité réelle des utilisateurs à gérer leur identité au quotidien. Le pouvoir théorique accordé à l'utilisateur devient un facteur d'exclusion s'il n'est pas accompagné de mécanismes simples, intuitifs et sécurisés. Ce constat s'inscrit dans une dynamique plus large de résistance au changement, qui témoigne de frictions sociales et organisationnelles induites par toute transformation numérique. L'enjeu ne réside pas seulement dans la technologie, mais dans l'acceptabilité, la progressivité et l'appropriation des nouveaux paradigmes par les utilisateurs et les institutions. Les affordances liées aux IDDs doivent donc être traduites en interactions concrètes, compréhensibles et sécurisantes pour permettre leur activation par tout utilisateur.

Face à ces défis, les opportunités identifiées par les répondants sont néanmoins substantielles. La diminution des risques, qu'ils soient opérationnels, réputationnels ou réglementaires, constitue l'argument le plus fréquemment avancé. Les mécanismes de traçabilité, les preuves cryptographiques, les divulgations minimales et les vérifications distribuées ouvrent la voie à une architecture de confiance fondée sur la résilience et la transparence. Dans la même perspective, les bénéfices liés à la simplification des processus, notamment par le recours aux portefeuilles numériques et à l'authentification décentralisée, amèneraient une fluidification des parcours utilisateurs, une réduction des frictions administratives et une plus grande efficience dans les opérations bancaires courantes. Ces dispositifs technologiques offrent des affordances évidentes pour les institutions, car ils transforment des contraintes en leviers de sécurité, d'agilité et de conformité. Au-delà des gains fonctionnels, les entretiens révèlent une redéfinition plus profonde de la relation entre l'utilisateur et son identité. L'autonomisation des individus et la valorisation de la réputation numérique redonnent à l'utilisateur un pouvoir décisionnel sur ses données, ses interactions et ses engagements. L'identité devient ainsi un actif personnel vérifiable, portable, interopérable et monétisable, inaugurant une économie de la donnée fondée sur des flux contractuellement encadrés. Ces nouvelles affordances identitaires repositionnent l'utilisateur comme agent central de valeur, capable de négocier, conditionner et transférer son capital informationnel et identitaire.

Finalement, l'analyse des solutions concrètes évoquées dans les entretiens, telles que KERI, Hyperledger Indy ou même Corda, montre que le choix d'un cadre technologique ne peut se faire sans considérer la gouvernance, l'ouverture du code, la capacité à protéger la vie privée et l'interopérabilité native. Ces solutions traduisent des visions complémentaires de l'IAS, certaines misant sur la preuve cryptographique, d'autres sur la traçabilité contractuelle. L'affordance d'un système d'IAS ne réside pas seulement dans sa performance cryptographique, mais dans sa capacité à rendre visibles et accessibles ses fonctions clés à ses utilisateurs comme à ses opérateurs. Ainsi, l'intégration des IDDs dans les banques repose sur une condition fondamentale, soit la capacité à concilier la robustesse technologique, la simplicité d'utilisation et la confiance. Tant que cette convergence ne sera pas atteinte, les IDDs resteront confinés à des projets pilotes, sans provoquer la transformation systémique qu'ils promettent. Toutefois, les fondations analysées ici indiquent que cette transition, bien que complexe, est en voie de maturation.

Thème	Sous-thème
Défis - Implémentation	• Complexité d'intégration • Infrastructure d'IAS • Mise en œuvre • Interopérabilité
Défis - Humain	• Last Mile • Résistance au changement
Opportunités - Processus	• Diminution des risques • Simplification • Portefeuille numérique • Gouvernance des données • Réduction des coûts • Point de défaillance unique
Opportunités - Humain	• Fiabilité • Autonomisation
Opportunités - Solutions	• KERI • Hyperledger Indy • Corda

Tableau 14 Synthèse des défis et opportunités de l'intégration des IDDs

5.4 Analyse de la vision stratégique de la haute direction

L'analyse de la vision stratégique de la haute direction constitue la troisième étape du processus d'analyse des résultats. Il s'agit de l'étape qui nous permettra de répondre à notre troisième question de recherche : quelle est la vision stratégique des dirigeants concernant les identifiants décentralisés ? Pour répondre à cette question, nous avons élaboré un guide d'entrevue adapté au profil des personnes interrogées, à savoir les membres de la haute direction. Bien qu'ils appartiennent effectivement au haut de la hiérarchie de l'entreprise, ces individus ne se trouvent pas au sommet de la structure organisationnelle. Leur rôle leur permet d'influencer les choix stratégiques, de prendre part à des procédures décisionnelles cruciales, de développer un point de vue global sur les défis technologiques, tout en restant suffisamment près du terrain pour comprendre les réalités pratiques entourant l'adoption de nouvelles technologies ainsi que les limites actuelles de l'organisation. De plus, nous reconnaissons que les dirigeants participants n'ont pas une connaissance détaillée de la technologie blockchain, en particulier des identifiants décentralisés. Nous avons choisi de centrer notre analyse sur les identifiants décentralisés, en partant du principe que la compréhension stratégique d'une technologie ne dépend pas uniquement d'une expertise technique approfondie, mais aussi de la capacité à envisager ses implications, à évaluer ses opportunités et à prévoir ses répercussions au sein de l'organisation. Par conséquent, nous avons axé les entrevues sur les défis liés à la mise en œuvre, à l'acceptation, à la gouvernance, à la transformation numérique et à l'alignement stratégique plutôt que sur les aspects techniques des IDD. Cette méthode permet d'évaluer non pas les connaissances précises des cadres sur la technologie des identifiants décentralisés, mais plutôt la manière dont ils l'intègrent dans leur réflexion stratégique, leurs décisions et leur perception de l'avenir de l'identité numérique dans le secteur bancaire.

Les réponses recueillies dans cette section offrent donc un aperçu des points de vue et des orientations des décideurs concernant l'adoption, l'harmonisation et la planification stratégique à long terme de nouvelles technologies, telles que les identifiants décentralisés dans le domaine bancaire canadien. Cette analyse met de l'avant les dimensions de gouvernance stratégique, de pilotage de l'adoption technologique et de positionnement stratégique de l'organisation, telles que ressorties de notre codification. L'analyse des thèmes récurrents lors de nos entretiens avec les membres de la haute direction permettra de mettre en lumière les conditions de faisabilité d'un virage identitaire vers les IDDs. Cette analyse sera effectuée en fonction de la posture adoptée par la direction vis-à-vis de la concurrence, des cadres réglementaires, des priorités organisationnelles, des stratégies de transformation numérique et autres. L'identification de cette vision stratégique est importante pour comprendre à la fois les leviers

d'actions possibles et les freins à l'opérationnalisation d'un tel projet, en évaluant le degré de maturité numérique de l'organisation, sa capacité d'alignement interne, ainsi que sa sensibilité au minutage de l'innovation (« early vs late adoption »). Ces facteurs seront décisifs pour évaluer la faisabilité de l'intégration des IDDs dans les structures bancaires actuelles.

5.4.1 Positionnement stratégique

Dans l'optique globale de la haute direction concernant l'implantation d'une nouvelle technologie, comme les identifiants décentralisés, l'analyse de la première dimension, soit le positionnement stratégique, mettra en lumière les mécanismes internes de planification et d'organisation des décisions stratégiques. Cela inclut l'alignement interne, la justification économique des projets, la définition des objectifs de réussite, ainsi que la perspective à long terme de la transition numérique. Nous avons abordé ce sujet en profondeur en examinant plusieurs sous-thèmes. La stratégie à long terme, qui se compose de trois sous-codes distincts, révèle un développement d'approches : « early adoption » a été mentionné deux fois, « late adoption » l'a été également deux fois, tandis que le plan de transformation numérique a été évoqué 20 fois dans deux transcriptions, ce qui témoigne d'un grand intérêt pour une feuille de route structurée dans le temps. Le « business case », mentionné onze fois dans deux transcriptions, témoigne d'une attention particulière accordée à la valeur ajoutée, aux coûts et à la rentabilité des initiatives. Les facteurs clés du succès ont seulement fait l'objet d'une mention unique, suggérant ainsi que les indicateurs de succès pour l'intégration des identifiants décentralisés restent flous ou insuffisamment explorés. 26 références ont été portées à l'alignement stratégique, ce qui la rend la plus évoquée durant nos entretiens. Ces facteurs nous aident à comprendre la manière dont les dirigeants envisagent l'adoption d'une nouvelle technologie tels que les identifiants décentralisés, en mettant en évidence les considérations liées aux scénarios de temps pour l'innovation, à l'alignement interne et à la rentabilité.

5.4.1.1 Plan de transformation numérique et alignement stratégique

Pour commencer, nous avons demandé à nos deux répondants quelle est la vision à long terme sur la transformation numérique à la banque Piltover. Cette question sert de point de départ pour positionner l'organisation dans une perspective de changement à long terme, en fonction de ses priorités et de ses engagements. D'une part, Jayce nous explique que la banque met en place une stratégie axée sur le numérique au cours d'une période de trois ans, comme le mentionne le passage suivant :

> « On fait une vision stratégique sur trois ans dans trois axes qui regroupe l'ensemble des canaux. Le client est servi par trois canaux principaux. Les centres contacts qu'on appelle les équipes de support. Il y a également toute la force conseil, [soit] le réseau des succursales. Et il y a toute l'accessibilité au niveau du numérique, donc toutes les plateformes numériques que ça soit les sites web, les sites transactionnels ou tout ce qui est mobile. L'objectif de ça, c'est de mieux servir le client d'un point de vue omnicanalité et de regrouper l'ensemble des capacités technologiques offertes à un client dans les différents canaux. L'ambition est élevée. Donc c'est ça notre ambition. Peu importe le réseau qu'il utilise, il accès à la même information dans le secteur. On travaille sur une vision numérique, de consolider, de converger l'ensemble des capacités d'affaires et des capacités technologiques pour mieux servir le client. On veut lui donner une expérience unique [ainsi que] simplifier l'empreinte technologique et les efforts en termes des coûts. » (Entrevue P8H).

Les propos de Jayce exhibent une tendance de la banque à se tourner vers une expérience numérique qui rassemble autant les capacités d'affaires que les capacités technologiques. En d'autres mots, il y a un désir de rapprocher l'univers des affaires au monde des TI à la banque, et ce dans l'intérêt des clients. Soucieuse de l'expérience qu'elle offre à ses clients, la banque Piltover s'engage également à réduire son empreinte technologique, ce qui témoigne une importance accordée aux enjeux ESG [37]. Diminuer l'impact environnemental des technologies et des appareils électroniques figure comme étant une priorité aux yeux de la banque dans le but, également, de faire des économies de coûts. La banque conjugue donc ses priorités environnementales, sociales, de gouvernance, d'affaires, technologiques et économiques au sein d'une même vision stratégique. D'autre part, Ezreal nous fait part de son avis sur la question en amenant sa réponse sous un angle complémentaire, comme le montrent ses propos ci-dessous :

> « La vision de la banque c'est surtout de pousser le libre-service. Un autre aspect important aussi [c'est] qu'il y a une volonté d'avoir une seule expérience commune pour le numérique […] peu importe le secteur impliqué. Le but aussi c'est d'aller chercher un 80% de la population, selon les statistiques que j'ai vus. Au niveau de l'adoption numérique, on est encore en bas des cibles qu'on s'est donnés. Donc, c'est de pousser l'adhésion au numérique sur les segments d'âge et de population qui sont visés. » (Entrevue P7H).

Selon l'avis de nos répondants, la vision stratégique numérique consiste à unifier l'expérience des clients sur tous les canaux numériques utilisés. La banque souhaite offrir une expérience numérique commune, mais pour ce faire, elle doit également prioriser l'adoption du numérique chez ses clients. À cet effet, la banque encourage le libre-service auprès de sa clientèle. Dans cette même lignée de pensée, nous avons procédé à une question complémentaire afin de bien comprendre l'objectif du libre-service.

[37] ESG est un acronyme pour Environnement, Social et Gouvernance

> « On veut inciter plus de transactions en libre-service du côté numérique versus un mode plus traditionnel d'aller en succursale pour faire un retrait au guichet ou de commander des chèques. On veut inciter le client à le faire lui-même. » (Entrevue P7H).

Ainsi, avec les propos de Ezreal, nous constatons une volonté de la part de la banque à se dissocier d'anciens modèles pour se tourner vers une clientèle plus autonome et libre d'effectuer ses propres transactions bancaires. Pour faire écho aux autres répondants dans l'analyse des lacunes actuelles, les membres de la haute direction sondés soulignent que la banque accorde une grande importance à l'expérience client. « On a pas mal parlé de la partie MFA, parce c'est quelque chose qui impacte directement les clients où vraiment ça change leur expérience, mais il y a beaucoup de choses qui sont faites autour pour faciliter, mieux protéger le client, éviter le hameçonnage, [etc.] Donc la banque continue d'avancer sur ce genre de chose et cherche à s'améliorer. » (Entrevue P4C) révélait Willump lors de notre entretien avec lui. « La banque est très soucieuse du feedback de ses clients, de son taux de recommandation, etc. Beaucoup de sondages sont envoyés après chaque interaction avec le client pour savoir si ça l'a été à la hauteur de ses attentes et s'il est satisfait. » (Entrevue P7H). La banque cherche à protéger ses clients tout en maintenant une expérience client de qualité. Elle souhaite s'améliorer continuellement en ayant une vision stratégique holistique et c'est justement ce que les dirigeants expriment dans leurs réponses vis-à-vis de la vision stratégique de la banque. « On parle souvent du plan d'évolution sur trois ans, un gros volet en TI, qui nous amène à revoir nos façons de travailler, d'aller chercher des efficiences, diminuer les coûts, mais c'est aussi un dossier qui passe par les décisions d'affaires. On veut simplifier, on veut optimiser la banque. » (Entrevue P7H), atteste Ezreal.

Considérant que la banque est en mode amélioration continue, nous avons poursuivi la discussion sur la mentalité et l'approche de la banque. Les propos de Ezreal confirment que la banque essaie de changer sa mentalité : « On essaie de s'éloigner d'un mode on te vend un produit, mais plutôt on veut être Conseiller pour un projet de vie » (Entrevue P7H). Après avoir entendu ces propos, nous avons ensuite pensé à savoir si cela s'applique également aux informations que la banque possède, car nous estimons que par rapport à la sécurité des données, tel que soulevé dans les lacunes actuelles, la banque pourrait détenir trop d'informations au sujet des clients. La nécessité d'avoir autant d'information sur les clients est donc une question importante pour déterminer si la banque souhaite refléter sa mentalité évolutive dans d'autres domaines. En effet, nous avons donné l'exemple suivant pour mettre en lumière le fait qu'il nous arrive de divulguer plus d'informations qu'il le faut dans une autre sphère que l'univers bancaire. « Lorsque tu souhaites entrer dans un bar et que tu te fais carter par le garde de sécurité, tu présentes une pièce

d'identité, comme ton permis de conduire, pour prouver que tu es majeur. En revanche, sur ton permis de conduire, il y a non seulement ta date de naissance, il y a ton adresse domicile, ton nom, ton prénom, etc. Le garde de sécurité a seulement besoin de savoir si tu es majeur ou pas. Il n'a pas nécessairement besoin de savoir ta date de naissance complète, il doit juste savoir si tu as 18 ans ou plus. » (Exemple présenté lors de nos entretiens). Avec cet exemple, nous cherchions à savoir si la banque appliquerait la même mentalité d'amélioration et évolution en continu, mais au niveau des données et informations de leurs clients. Pour y répondre, Ezreal nous partage un exemple qui fait écho au fait que la banque s'éloigne d'un ancien modèle pour se diriger vers une nouvelle façon de faire :

> « Par exemple, avec la prise de rendez-vous, on n'est plus dans un mode on essaie de te vendre quelque chose. On est dans un mode on veut bien comprendre ce que tu veux pour être sûr de couvrir ton besoin. Il y a une différence à dire je me magazine une hypothèque vers dire j'aimerais ça avoir un chalet pour prendre mes vieux jours. Ce n'est plus la même affaire. On va te faire une stratégie pour tes investissements, pour te rendre jusqu'à la retraite, puis on tombe dans un mode de conseil. Pour que ce conseil soit pertinent et qu'il fonctionne bien, on a besoin de savoir c'est quoi tes projets de vie, tes intérêts, ta situation familiale? As-tu des enfants qui approchent l'école secondaire? Tu veux les envoyer au privé? Il y a toutes sortes de choses comme ça qu'on fait au niveau du CRM. » (Entrevue P7H).

Notre répondant exprime ici que les informations ont un but et renchérit sur ses propos en y ajoutant l'aspect stratégique derrière la gestion des informations client pour maintenir une saine gestion de la relation avec ses clients.

> « D'un point de vue stratégique, la banque a besoin de ces informations-là. Puis, ce n'est pas quelque chose que t'as sur ton permis de conduire ou sur ta facture d'électricité ou quoi que ce soit. C'est sûr que la banque va avoir besoin d'un paquet d'informations où c'est ton nom, ton numéro de téléphone, ton adresse, ton numéro d'assurance sociale, toutes ces [informations-là], mais d'un point de vue stratégique, pour bien savoir ce que sont nos stratégies d'effondrement, des segments de clients qu'on a, est-ce un jeune, un millénium, un nouvel arrivant, une personne à risque, [etc.] On a besoin de ces informations. » (Entrevue P7H).

Nous comprenons, avec ces extraits, que les informations sont utiles pour développer une meilleure relation de confiance avec les clients, de comprendre leurs besoins et en bout de ligne, même si « on est un organisme à but lucratif » (Entrevue P2A) comme le souligne Fiora, elle agit en fonction des besoins de ses clients. Ce n'est pas nécessairement faire du profit en premier et ensuite s'occuper des clients. C'est plutôt l'inverse. Dans ce même ordre d'idées, nous avons posé la question si la banque serait intéressée à redonner plus de pouvoir, de « ownership », à ses clients par rapport à la gestion des données.

> « Oui, je pense que pour avoir un incitatif [à redonner du ownership aux clients], il y a beaucoup de processus en ce moment de gouvernance autour des données, de rétention, des points de vue légal, le nombre d'années qu'on devrait garder la donnée. Est-ce que la banque pourrait être intéressée à un modèle où la seconde que le client décide qu'il est à l'aise, nous donne son accord ou tout ça de façon numérique? Je suis à l'aise avec ça. Puis à tout moment, il y a un request qui est fait de les supprimer, tout est seemless automatisée, tout ça, je pense que oui, la banque pourrait être intéressée. » (Entrevue P7H).

Il y a donc une volonté à redonner la propriété des données aux clients de la banque Piltover selon les commentaires de Ezreal. Nous constatons que l'évolution de la banque n'est pas terminée et qu'elle souhaite s'améliorer en continue non seulement en fonction de l'expérience client, mais aussi en fonction de l'industrie.

5.4.1.2 Précurseurs ou Retardataires

Parallèlement, Jayce ajoute que « au niveau des centres contact, ce n'est pas du numérique, mais on est en accélération par rapport à l'industrie. On est en train de mettre toutes les capacités et aides génératives dans les centres contact. » (Entrevue P8H). Il s'agit ici d'une référence à l'intelligence artificielle et à l'outil technologique Nuance discuté plus tôt où il est possible de reconnaître les « patterns » des voix et identifier plus rapidement les cas de fraude. Les aides génératives, l'IA, fait déjà partie des avancées technologiques que la banque a premièrement considéré lors d'une revue d'un « business case ». Dans cette optique, nous avons demandé à nos participants s'ils considéraient la banque comme étant plutôt une pionnière, « early adopter », ou retardataire, « late adopter ». Il est important d'évaluer le positionnement de la banque par rapport à l'adoption de nouvelles technologies pour mieux orienter nos questions subséquentes. La figure 79 montre cinq positionnements possibles sur l'échelle d'adoption. Les innovateurs, les premiers adeptes, la majorité précoce, la majorité tardive et les retardataires.

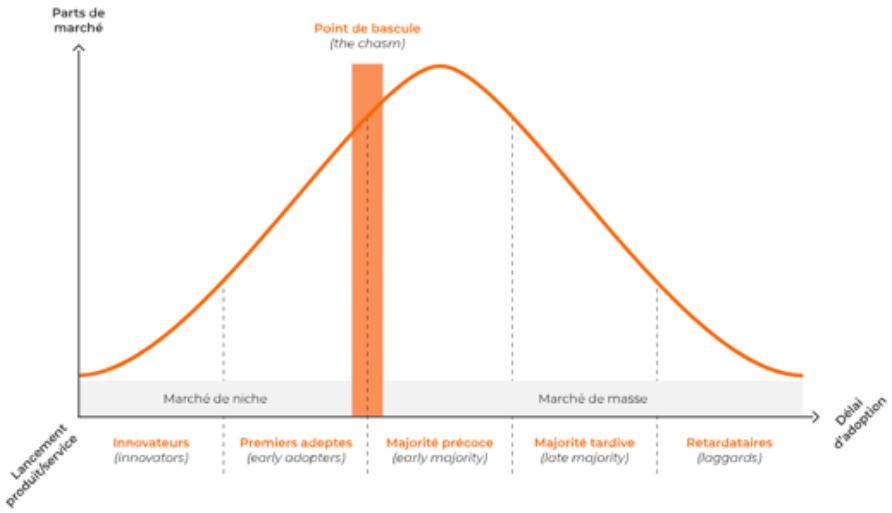


Figure 57 Graphique des vagues d'adoption[38] lors d'un lancement de produit/service (Duchesne, 2021)

« Je te dirais qu'au tout début, quand j'ai commencé, on était hyper les derniers à faire quoi que ce soit. Maintenant, on veut se faire une banque plus moderne, plus technologique, plus cloud. Ça, avant on n'avait pas ça du tout. » (Entrevue P3A), témoigne Teemo. Dans le même ordre d'idées, Ezreal explique que « dans le passé, on était vraiment late adopters. On traînait de la patte en arrière. La modernisation de nos solutions bancaires par Internet, c'est un très bon exemple. On était définitivement en arrière vis-à-vis de la concurrence je dirais dans les dernières années. C'est sûr qu'on n'est pas précurseurs, on n'est pas en avant de la parade sur toutes ces choses-là, je te dirais qu'on se situe plus dans le milieu de la vague » (Entrevue P7H). À l'inverse, Jayce nous suggérait plus tôt que la banque était dans une vague des premiers adeptes lorsqu'il disait « on est en accélération par rapport à l'industrie » (Entrevue P8H). En effet, il nous révèle que la banque essaie de se positionner comme une banque avant-gardiste dans l'extrait suivant « d'un point de vue mes équipes TI, puis de la direction TI, on pousse beaucoup pour être early adopter, à savoir la personnalisation du portefeuille dans le bilan, d'utiliser des FinTechs, d'avoir une meilleure compréhension des agrégations en termes des produits numériques, l'usage d'authentification MFA plus forte que ce qu'on a actuellement. Puis on participe à beaucoup de vigie au Québec et en Amérique du Nord pour voir ce qui se passe dans l'industrie […]. Ce qu'on essaie de faire c'est de mettre les principes de base, puis de respecter notre calendrier, puis nos budgets, puis après ça d'amener des nouvelles technologies émergentes qu'on pourrait avoir. » (Entrevue P8H). Avec ces propos, la banque

[38] Voir Annexe G pour plus d'informations

témoigne d'une ouverture face aux nouvelles technologies, et ce dans un positionnement mitigé auprès des répondants. Tout compte fait, la banque se positionne vraisemblablement dans le milieu précurseur de la vague, soit au point de bascule, puisqu'elle agit sur certains fronts aux devants de l'industrie, notamment avec l'utilisation de l'IA au niveau de la reconnaissance vocale, elle souhaite numériser ses processus pour encourager le libre-service et elle fait de la vigie technologique.

5.4.1.3 Business Case

Après avoir mis la table sur le plan de transformation numérique et l'alignement stratégique, considérons ensuite le « business case ». Ce terme désigne le plan d'affaires ou le dossier de projet pour une nouvelle technologie dans notre contexte. Selon nos deux cadres supérieurs, le « business case » représente un tournant important dans la décision de lancer un nouveau projet ou un outil technologique. Dans cette section, nous examinerons les conditions préalables d'un « business case » et l'élan nécessaire pour le mener à bien. Tout d'abord, revisitons les propos de Jayce sur l'engouement pour la banque: « il y un appétit au niveau de l'organisation, mais faut leur démonter qu'on a la capacité de livrer puis d'amener de la valeur. Puis ça c'est le défi qu'on a comme organisation. » (Entrevue P8H). Pour démontrer qu'il est possible d'amener de la valeur, il est clair que le « business case » doit être robuste. Nous avons donc demandé comment le « business case » doit être bâti pour obtenir un retour favorable des décideurs sur une nouvelle technologie proposée. La réponse suivante explique les conditions gagnantes et les éléments à surveiller lors de l'élaboration d'un « business case » pour une transition technologique :

> « Tout dépend comment ton business case est ficelé. Puis l'appétit aussi du leadership à vouloir aller de l'avant avec une solution comme ça. Il y a plein de projets qui ne vont pas amener les bénéfices jour 1 ou que ça va être amorti sur 5-10 ans. Ça va prendre un bout de temps avant que la banque revienne dans son argent. Il y a des projets aussi qui sont drivés par d'autres business drivers, mais ça dépend de comment ton business case a été fait. La plupart du temps ce qu'ils regardent ce sont les bénéfices attendus ou la réduction des coûts. Après ça, ça va plus dans une optique de : est-ce que la direction est à l'aise avec l'orientation, la stratégie qu'on prend? Est-ce que ça vient répondre à une des grandes stratégies qu'on a pour la banque du futur? Tous ces facteurs ensemble vont peser dans la balance pour savoir est-ce qu'on a un Go ou on n'a pas un Go d'aller de l'avant avec cette initiative là (Entrevue P7H)

Cette réponse indique qu'il n'est pas aussi simple de bâtir un « business case » en raison de facteurs comme l'appétit de l'organisation, du délai sur le retour sur investissement, soit les bénéfices attendus ou les réductions des coûts, l'aisance et la stratégie de la banque. Ezreal insiste en affirmant qu'un processus et un endroit existent où le « business case » est traité avec les propos suivant :

> « Il y a plusieurs tribunes de priorisation, plusieurs comités, jusqu'à ce que l'équipe de direction donne son oui ou non dépendamment de l'ampleur et du montant. Dans le cadre d'une initiative [d'envergure], il y aurait fort probablement trois ou quatre comités avec une décision d'équipe, de direction, avant d'aller de l'avant avec quelque chose de transformationnel. C'est seulement après ça et que ton business case soit monté que la haute direction donne son feu vert. » (Entrevue P7H)

D'un autre côté, Jayce pèse sur l'importance du réalisme en termes de portée et de coûts quand vient le temps de considérer un « business case » et son rendement, ce qui peut expliquer une réticence à donner le feu vert à de gros projets.

> « Faut être réaliste aussi. Souvent on fait des business cases puis quand tu rencontres la haute direction, on te pose la question est-ce qu'on a rencontré [les bénéfices escomptés]? Souvent le coût d'investissement a doublé et les bénéfices ont été très peu rencontrés. Souvent on travaille dans une culture de dire qu'on peut passer un business case d'à peu près une fourchette de $2-3.5M, on prend la fourchette basse et quand on arrive dans des situations où il y a un dépassement qui avait été identifié par nos experts, ça paraît plus mal. À l'interne, il faut aussi revoir cette culture du coût d'investissement et des bénéfices, chose qu'on a fait niveau des centres de contacts. On a diminué tous les nice-to-have qui étaient difficilement évaluable d'un point de vue financier pour aller à l'essentiel. On a accéléré et on a réalisé qu'on est capables de livrer nos engagements. On a découpé l'éléphant beaucoup plus en s'engageant sur des réalités un peu plus terrain. » (Entrevue P8H)

Il y a donc un engagement de la banque à entamer des projets sous un angle réaliste qui peut atteindre ses objectifs initiaux. À partir de l'exemple des centres de contacts, nous observons que la banque Piltover est en mesure de changer sa culture axée sur les coûts pour se concentrer sur la portée des projets et en même temps rencontrer les objectifs atteignables qu'elle s'était posée en phase de planification de projet. Le « business case » dans ce scénario comprend donc autant l'ampleur du projet, son rendement et sa valeur ajoutée à la banque. Après avoir discuté des facteurs clés incitant l'approbation du lancement d'un « business case », nous avons ensuite abordé la question des indicateurs de réussite une fois la technologie implantée ou déployée. En partant de leurs expériences passées, nous avons encouragé nos interlocuteurs à imaginer une situation où un projet serait approuvé et mis en œuvre. Cette projection permet à nos interlocuteurs à réfléchir à ce qui a fonctionné et ce qui caractérise un projet réussi.

> « Souvent on va regarder l'achalandage. On va regarder les gens, les ventes générées, la rétention, le retour, le nombre d'usage qui en font. Ce sont des choses qu'on va aller cibler directement [pour] voir l'appétit du consommateur. » (Entrevue P8H)

Il est intéressant de souligner avec ces propos qu'il s'agit, au-delà des retours sur investissements, de constater l'impact sur les clients directement. Le fait qu'une nouvelle technologie comme les identifiants décentralisés, qui rend le pouvoir sur les données aux clients eux-mêmes, puisse inviter les clients à recourir davantage aux services offerts par la banque s'impose comme élément crucial à considérer pour notre analyse. Inciter les clients à interagir un tant soit plus avec la banque en raison du pouvoir qui leur est remis encourage simultanément la confiance auprès de la banque. Cela pourrait être un facteur favorable à l'adoption des identifiants décentralisés. À l'opposé, nous avons aussi pris le temps d'étudier un exemple négatif d'un « business case » pour mitiger nos attentes avec l'exemple qui suit :

> « Cette année, on voulait mettre des Strong MFA. Finalement, l'enveloppe, il y avait trop de monde qui pouvaient faire des activités, ils ont priorisé les activités d'affaires. Ça l'a été repoussé à l'année prochaine. Donc parfois c'est vraiment d'être à la bonne tribune, d'exercer la bonne influence et d'exposer clairement ton cas. Je ne pense pas que la banque ne serait pas intéressée d'une solution pour se départir de certaines responsabilités. Faut que le sujet soit bien amené et il faut trouver qui est le porteur. » (Entrevue P8H)

Ainsi, les défis liés au « business case » se traduisent par la présence sur les bonnes tribunes de priorisation, avoir la bonne influence et la verbalisation claire des objectifs.

Codification / Thème	Nombre d'entrevues	Références
Early adoption	1	2
Late adoption	2	2
Plan de transformation numérique	2	20
Business case	2	11
Indicateurs de succès	1	1
Alignement stratégique	2	26

Tableau 15 Codification et références du positionnement stratégique

5.4.2 Pilotage interne de l'adoption technologique

Pour aborder l'introduction d'une nouvelle technologie, tels que les identifiants décentralisés, il est impératif d'analyser les aspects internes de la conduite du changement. Cette analyse mettra en évidence les mécanismes pratiques de mise en œuvre, les processus décisionnels et les facteurs clés de transformation au sein de la banque. Ce thème met donc en évidence plusieurs aspects liés à la gestion du changement, aux structures de décision, aux impacts organisationnels anticipés et au rôle du leadership dans le processus d'adoption.

Nous avons examiné ces points sous quatre angles différents. La prise de décision, qui revient 30 fois dans les deux transcriptions, est de loin la catégorie la plus évoquée. Elle révèle une préoccupation centrale quant à la manière dont les décisions technologiques sont prises, justifiées et articulées dans l'écosystème bancaire. La gestion du changement, mentionnée huit fois dans les deux transcriptions, met en lumière la reconnaissance, par les membres de la haute direction, de l'importance d'un accompagnement structuré lors de l'introduction d'une innovation, comme les IDDs. Les implications organisationnelles, qui sont mentionnées cinq fois dans les deux transcriptions, montrent que l'organisation s'interroge sur les effets futurs qu'une telle technologie pourrait entraîner (ex : redéfinition des rôles, réingénierie des processus, impact sur les équipes). Finalement, le leadership, cité sept fois dans les deux transcriptions, correspond à la posture que les cadres supérieurs doivent adopter pour porter le changement, mobiliser les parties prenantes et créer un climat favorable à l'innovation.

L'analyse de ces thèmes codifiés nous aidera à saisir comment la haute direction projette de solidifier l'intégration d'une nouvelle technologie dans la structure de l'entreprise. Cela met en évidence les conflits entre innovation, gestion interne et maturité opérationnelle.

5.4.2.1 Adoption technologique

Bien que le « business case » soit un outil d'aide à la décision utilisé pour évaluer la viabilité et la rentabilité d'un projet avant son lancement, l'adoption technologique fait référence à la mise en œuvre concrète, soit à l'intégration, d'une nouvelle technologie au sein d'une organisation. Cette étape nécessite de nombreux ajustements, tant sur le plan humain que structurel. Elle implique des ressources, modifie les méthodes de travail et exige souvent une révision des procédures actuelles. Dans le contexte des identifiants décentralisés, cette transition revêt une importance particulière, car elle concerne les données personnelles des clients et les systèmes de sécurité en place. L'introduction de cette technologie nécessite

une planification minutieuse, tel qu'exploré dans le thème précédent, et une adaptabilité constante pour faire face aux défis du changement. Il ne s'agit pas seulement de préparer le terrain avant le changement, mais aussi de comprendre les dynamiques en jeu pendant le processus. Cette section s'intéresse aux mécanismes internes de la gestion de changement et aux décisions prises pendant la mise en œuvre. L'adoption technologique est donc envisagée ici comme un processus continu, itératif et profondément ancré dans la réalité opérationnelle. À cet effet, nous analyserons ce qu'il se passe durant un changement, plutôt que ce qu'il se passe avant que le changement soit approuvé. Pour débuter, nous nous sommes penchés sur une première question concernant la phase de préparation au changement approuvé. Jayce s'exprime avec les propos suivants lorsque nous avons demandé comment la banque se prépare au changement :

> « D'un point de vue technologique, c'est très partagé, parce qu'on est dans un environnement bancaire. Donc, au niveau exécutif, il y en a beaucoup qui viennent du domaine bancaire, soit des centres conseil, des succursales, etc. Il y a des VPs[39] qui viennent de l'extérieur qui ont connu plus le numérique. Il y a beaucoup d'adoption et de gestion de changement à travers toute cette orientation numérique. » (Entretien P8H)

L'avis de Jayce révèle qu'à haut niveau, les perspectives des dirigeants sont mitigées en raison de leur profil et leur expérience passée. Lors de la phase de préparation d'un nouveau changement, les exécutifs peuvent avoir des orientations, des opinions et des connaissances différentes, ce qui entraîne une difficulté dès le début et un besoin criant d'arrimage lors d'un changement.

5.4.2.1.1 Prise de décision

Considérant le profil hétérogène des dirigeants, nous avons ensuite demandé à nos deux répondants leur avis par rapport aux raisons d'intégrer une nouvelle technologie d'un point de vue stratégique. Cette interrogation revêt une importance fondamentale, car elle concerne les points clés sur lesquels nous pourrions axer nos efforts de promotion d'un système bancaire utilisant des identifiants décentralisés.

D'une part, Jayce indique, selon lui, qu'il y a plusieurs axes de réponses pour cette question avec l'extrait qui suit :

> « L'écosystème, le marché, la politique, le réglementaire. Ce sont pas mal ces axes-là. On voit le marché numérique, ça va très très vite. On voir que notre achalandage augmente de façon

[39] VP est un acronyme pour Vice-Président.e

> importante, la conversion. On regarde la compétition, où ils sont rendus dans certains services offerts, il y en a qui sont au-devant de nous. Mais faut changer la culture interne de l'organisation bancaire je te dirais dans un premier temps et ensuite se mettre plus dans une perspective entrepreneur. » (Entrevue P8H)

À titre d'exemple, Jayce nous fait part de deux exemples concrets pour mettre en lumière ses propos précédents sur les différents axes observés. Il commence avec l'exemple du déploiement des centres contacts. Cet exemple réfère directement à l'axe du marché, mentionné par Jayce, en tant que raison principale du changement.

> « On avait beaucoup de désuétude par rapport à l'ensemble du marché, énormément. Ça nous a pris quatre ans à nous décider pour différentes raisons légitimes, incompréhension du roadmap, incompréhension des coûts, des efforts, de la gestion de changement… On a donc revu la roadmap, on a renoncé à des requis qu'on souhaitait faire au début, puis on est passé en accélération. On est passé d'un plan de cinq ans à deux ans et on va même devancer le marché. Alors actuellement on a des tribunes avec la vice-présidence des autres organisations bancaires qui nous questionne à savoir comment qu'on est arrivé là et comment qu'on a été capables de rattraper le marché. »

Même si l'intention au départ était poussée par d'autres facteurs que le marché, il y a eu une re-priorisation du même changement pour accélérer le changement, mais en fonction du marché. Ainsi, la banque Piltover a été capable d'observer le marché, s'y comparer et agir différemment à l'interne pour accélérer significativement son changement afin de devancer le marché vis-à-vis duquel elle se jugeait en retard. En outre, Jayce révèle un deuxième exemple, qui concerne cette fois-ci l'écosystème de la banque. Par écosystème, Jayce sous-entend l'ensemble des acteurs, processus, technologies ou environnements qui interagissent et s'influencent mutuellement.

> « Au niveau du numérique, dans le passé, il y avait une incompréhension sur ce que c'était le numérique. Les gens trouvaient ça coûteux, ne voyaient pas les bénéfices court-terme, que ce soit d'un point de vue bénéfices financiers ou bénéfices technologiques et depuis la dernière année, on met des nouvelles capacités en ligne et [les dirigeants] le voient. Là il y a un appétit et cette année on investit de façon importante sur le chantier numérique. » (Entrevue P8H)

D'autre part, la réponse suivante de Ezreal sur la question reste plutôt axée sur les aspects financiers, du risque que la banque subit et de la simplification des processus :

> « Grosse pression sur les coûts. Je te dirais un driver de changement c'est définitivement la diminution des coûts opérationnels. On cherche partout à trouver des façons de diminuer nos

> coûts opérationnels. L'autre des raisons aussi, on est une banque, on n'aime pas le risque. [Si] ça permet aussi de diminuer le risque d'exfiltration de données, de cybercrime, de CRS[40] FATCA[41], de financement du terrorisme ou de l'évasion fiscale, je pense que ça effectivement c'est un gros business driver pour faire ce genre de changement. En termes de simplification aussi de notre footprint applicatif ou d'infrastructures. Si on amène une certaine simplification de nos solutions. » (Entrevue P7H)

En complément, nous avons demandé à quel point est-ce ce que les coûts d'investissement jouent un grand rôle pour donner le feu vert à un projet. Jayce nous a répondu avec les propos suivants en y ajoutant un exemple :

> « Bien c'est crucial je te dirais. Cette année on investit plus de $5M en saine gestion de notre plateforme pour développer le talent à l'interne et de faire de la vigie technologique. Dans le passé, avant que je reprenne le numérique, c'était des coûts d'investissements tous les deux ans. Donc on faisait un Blitz en 2017. En 2018, on réactivait la plateforme mobile, on ne faisait plus rien. Donc, on revenait toujours à la désuétude, on faisait toujours : on investit, on arrête. Puis, les exécutifs, ils disaient, pourquoi faut réinjecter $5M si on le fait depuis deux ans? Bien c'est parce que la technologie a évolué. Le talent a quitté. Donc pour maintenir le talent, faut un budget régulier. J'ai un budget d'un point de vue technologique et maintenance. J'ai un budget évolutif et maintenance, mais plus pour saine gestion de nos plateformes. Si tu veux là-dedans ça va couvrir les pratiques, la formation, les vigies, les rehaussements d'outils, les infrastructures, les grandes tendances. C'est nouveau de cette année. » (Entrevue P8H)

Nous comprenons que le budget joue un rôle crucial avec les propos de Jayce, mais nous avons également prêté attention à la désuétude. Pour qu'il y ait un changement, il faut améliorer quelque chose d'existant. C'est pourquoi la désuétude requiert une attention particulière puisque nous jugeons que les systèmes bancaires traditionnels commencent ou même sont déjà désuets, surtout au niveau de la gestion des identités. Pour mieux comprendre comment la désuétude est adressée stratégiquement, nous avons demandé à Jayce lorsque la désuétude est adressée, est-ce que la banque essaie de rattraper le marché ou d'aller un pas devant, tout comme pour les centres contact.

> « Par rapport au marché, on rattrape. Par rapport à nos comparables, on est aux devants. Pour l'exemple que je te donnais, on n'a pas la rapidité d'une petite organisation. Quand je regarde le Time-to-Market, tout le nombre de mises en production au niveau du numérique dans les petites organisations versus la banque, on a du travail à faire. Quand je regarde d'un point de vue évolution numérique des centres contact, notre fournisseur évolue à tous les six mois [avec] une nouvelle capacité que les clients leur demandent, [tandis] que nous on est encore en train d'adresser la désuétude. On met de l'intelligence artificielle, on est en train

[40] CRS est un acronyme pour Common Reporting Standard

[41] FATCA est un acronyme pour Foreign Account Tax Compliance Act

> d'activer des capacités, mais leur rythme est beaucoup plus rapide. Donc, il faut être capable de se mettre dans une perspective, une vision cinq ans où on souhaite aller, et ça incite quoi comme investissement régulier ou comme coût récurrent. On ne le fait pas assez malheureusement. » (Entrevue P8H)

Il y a donc du parallélisme qui est fait par la banque si nous considérons qu'elle rattrape le marché, mais qu'elle essaie tout de même de devancer ses comparables. Les propos de Jayce suggère qu'il faut se positionner dans le temps avec un plan clair et temporel. Alors, nous avons demandé quels sont les facteurs les plus importants aux yeux de la banque à prioriser au niveau de la stratégie. Est-ce faire du profit? Est-ce l'expérience utilisateur? Est-ce la sécurité? Nous avions déjà évalué cette réponse avec d'autres répondants, mais nous avons recueilli auprès de Jayce que :

> « C'est l'acquisition de clients, la rétention de clients, qui va être un générateur de profits […]. Après ça, tu as les équipes de risque qui nous disent faites attention, vous créez des produits avec un risque de capital élevé. Si le risque de capital est trop élevé et les probabilités de défauts sont trop élevés, alors le produit ne sera pas généré. Le risque est très important. Les gens de risque sont vus comme des freins, mais c'est important pour une organisation de bien faire une saine de gestion de risque. Après ça, si on prenait une perspective cyber, c'est la même chose. Ça va être dans un contexte de sécurité renforcée […]. D'un point de vue expérience client, l'autonomie des utilisateurs, mais à quel coût? Tu peux t'adresser à la population et d'un pont de vue TI, il faut que les systèmes soient open running [pour] mieux servir le client. Donc je te dirais que d'un point de vue stratégique, tu as souvent tous ces grands joueurs : la personne de cyber, de risque, d'audits internes, le conseil d'administration, [etc.] » (Entrevue P8H).

Les grands joueurs qui sont autour de la table lors de la prise de décision vont courir plusieurs domaines du changement. Ils prévoient les aspects financiers, le risque, l'expérience client, etc. Mais qu'en est-il de de leur rôle lors d'un changement? Nous cherchons à savoir le rôle de la haute direction dans la facilitation et la promotion de l'adoption de nouvelles technologies. Voici comment nous répond Ezreal :

> « Je ne pense pas que ce soit la mission de la haute direction. Honnêtement, ça tombe plus aux gestionnaires qui vont être plus dans la livraison et dans le quotidien des activités de ce projet-là. La haute direction, en tant que partie prenante, à mon sens, veut juste être informé des avancements ou s'il y a des bloquants. [Son rôle serait] plus à l'externe par contre, pour faire rayonner la banque versus les autres institutions ou les autres compagnies dans la région. Dans le quotidien de l'initiative, c'est très rare que tu vas voir les exécutifs. » (Entrevue P7H)

Or, la haute direction, bien qu'elle joue un rôle en amont de changement, n'agit pas nécessairement sur le terrain ou durant le changement. Elle délègue habituellement cette tâche à la classe de gestionnaires de projet, qui servent de relais opérationnels à la stratégie établie en amont. Ces responsables sont

chargés de la réalisation pratique des projets et doivent jongler avec les limites techniques, humaines et temporelles. Les responsables ont pour mission de convertir les directives générales en tâches spécifiques, en veillant à ce que les groupes concernés restent sur la bonne voie. La haute direction demeure néanmoins active grâce aux réunions de contrôle, aux comités de gestion et aux examens de projets. Elle agit principalement en cas de prises de décision ou lorsqu'un ajustement stratégique est nécessaire. Cette délégation de responsabilités offre une certaine souplesse dans la mise en œuvre, mais elle peut aussi entraîner un éloignement entre la vision stratégique et les réalités opérationnelles. Il arrive que les gestionnaires se retrouvent à arbitrer seuls des décisions importantes sans toujours avoir accès à l'intention stratégique sous-jacente. Cette dynamique souligne l'importance d'une gestion efficace et d'un leadership solide. Elle révèle également qu'adopter une technologie comme les identifiants décentralisés nécessite une cohérence étroite entre la vision, le pilotage et l'exécution.

5.4.2.1.2 Gestion du changement et Leadership

L'aspect humain de la gestion du changement comporte une dimension essentielle dans l'adoption d'une nouvelle technologie. Au-delà des procédures et des outils, ce sont les individus qui doivent s'adapter et modifier leurs pratiques, parfois en remettant en question des habitudes bien ancrées. Le changement peut susciter des réactions variées, allant de l'enthousiasme à la résistance passive, en passant par la crainte de l'inconnu. La composante humaine des initiatives technologiques est trop souvent négligée, alors qu'elle joue un rôle fondamental dans leur adoption. Pourtant, la réussite de l'adoption dépend largement de la capacité à rallier les équipes, à prendre en compte leurs préoccupations et à offrir un accompagnement adapté. Cela exige une communication ouverte et honnête, une formation continue et un échange constant entre les parties prenantes. La haute direction doit faire preuve d'écoute, de pédagogie et de souplesse pour faciliter cette transition. Il est possible que le changement soit perçu comme une perte de contrôle ou une menace pour les compétences acquises. Il est donc impératif de mettre en évidence les avantages tangibles du changement, tout en valorisant les connaissances existantes. L'aspect humain ne devrait pas être considéré comme un obstacle, mais plutôt comme un levier, car lorsque bien géré, il se transforme en un moteur de transformation durable.

Nous aborderons donc la question de la gestion du changement auprès de la haute direction, qui se trouve à la tête du leadership de l'organisation. Pour ce faire, nous avons demandé les points irritants ou les facteurs de résistance qui reviennent le plus souvent au niveau de la gestion de changement pour les nouvelles technologies. Jayce nous mentionne :

> « Je dirais la peur d'avoir peur. Si je te dis ça va être un changement important, le rehaussement des centres contact, jusqu'à une date X, ça va super bien, on va être là. Le message est important d'une part. De deux, il ne faut pas s'improviser. Dans le sens qu'à la banque, on croit au développement des gens, mais des technologies de pointe, […] souvent on va prendre des gens qui ont lu ou qui n'ont pas vraiment de spécialité, qui ont fait quelques lectures et se disent spécialistes. Ça devient difficile quand le porteur de ballon ne maîtrise pas le sujet. [Enfin], trop souvent, il y en a que ça fait très très longtemps qu'ils sont là, ils ont des craintes en partant [et] ça nous empêche de mettre les nouvelles technologies. » (Entrevue P8H)

Ezreal soutient les derniers propos de Jayce en soulignant que

> « C'est sûr que n'importe quoi qui touche la force conseil c'est toujours compliqué à faire vivre le changement. Il y a des personnes que ça fait longtemps qui sont là et dès qu'on leur demande de changer quelque chose de leur routine, c'est compliqué. » (Entrevue P7H)

Nous avons ensuite terminé la discussion sur la gestion de changement en se tournant vers une optique futuriste optimiste. En effet, nous avons demandé aux répondants s'il était de leur avis que la banque puisse un jour collaborer avec d'autres banques pour former un réseau interbancaire à grande échelle. À la suite de cette question, nos répondants ont communément répondu la même chose :

> « Je pense qu'il y aura toujours de la collaboration et de l'entraide entre les différentes institutions financières. C'est la preuve avec les histoires de tarifs et Trump. Je pense que tout le monde est capable de se rallier dans un objectif commun, même si ce sont des concurrents. Si jamais un sujet comme [les IDDs], est game changer au niveau de la gestion des identités, la façon qu'on partage l'information et que chacun devient propriétaire de sa donnée et de l'utilisation qu'il en fait… Est-ce que les banques pourraient se mettre tous ensemble pour faire ces changements-là, apprendre et être capable de partager ? Je pense que oui. » (Entrevue P7H)

> « Il y a déjà certaines tribunes où est ce qu'on est avec les autres institutions financières, l'open banking. Il y aurait une ouverture de contribuer et de partager un modèle similaire avec d'autres institutions […] La banque est ouverte à partager son savoir avec d'autres institutions financières. » (Entrevue P8H)

Toutefois, tel que précédemment soulevé par Jayce, si le porteur de ballon du changement n'est pas à la hauteur, les chances de succès sont minces. Nous avons donc demandé ce qu'il fallait pour qu'une collaboration interbancaire blockchain fonctionne.

> « Je pense que ça prend un porteur de ballon. Je vais te donner un exemple. Quand on parlait d'authentification et de Strong MFA, actuellement on utilise Okta pour authentifier les gens, [et] on vient proposer une solution blockchain, il faut qu'il y ait sur la table des gens qui

> génèrent des ventes pour qu'ils soient à la table de livraison. Ils sont tellement distants parfois qu'ils peuvent être le porteur de ballon, mais ce n'est peut-être pas le bon porteur de ballon. Il y a donc une incompréhension du côté affaires et si je ne maîtrise pas le sujet, et il y en a beaucoup, l'appétit va être moindre. On est encore très axé sur le P&L[42], notre performance individuelle. Donc, il y a une perspective de culture aussi. Si on veut converger tous les secteurs banque vers une technologie blockchain, il faudrait que les gens se mettent la main à la pâte sur une solution unique et non pas les partager comme on le fait actuellement » (Entrevue P8H)

Ces propos nous semblent très intéressants. Jayce soulignait la tendance de la banque à se rapprocher du modèle de banque ouverte, ce qui montre qu'elle est prête à collaborer. En revanche, Jayce met en garde la collaboration interbanque contre l'illusion du simple partage. Les banques doivent travailler ensemble, plutôt que de rester dans une dynamique de partage. Il est crucial de comprendre cette nuance : partager des données ou des méthodes ne suffit pas pour construire un écosystème d'innovation durable. Il est essentiel d'avoir une gestion collaborative, une planification concertée et une détermination partagée pour établir des normes. Sinon, chaque organisation agira de manière isolée, répètera les mêmes efforts et ralentira la progression globale du secteur. Le rôle de porteur de ballon évoqué par Jayce renvoie à la nécessité d'un leadership clair, assumé et orienté vers l'action. Une banque qui accepte ce rôle devient un catalyseur du changement, non seulement pour elle-même, mais pour toute l'industrie. Toutefois, cela exige une prise de risque mesurée, une vision commune ainsi qu'un engagement fort de la part de la haute direction.

5.4.2.2 Implications organisationnelles

Pour conclure le thème pilotage interne de l'adoption technologique, nous allons analyser les implications organisationnelles. Par implications organisationnelles, nous entendons ce à quoi la banque réfléchit pour la banque de demain. Nous avons donc demandé à nos deux répondants comment la banque se prépare aux futurs besoins de ses clients et systèmes.

D'un côté, Ezreal nous explique comment la banque pense à demain avec l'extrait suivant :

> « Oui, la banque est en constante évolution. Quand tu regardes de plus en plus, il y a des modèles d'affaires où des banques en lignes se servent d'intermédiaires. On expose des API d'affaires à l'externe pour pouvoir faire d'autres types de modèles d'affaires. La banque fait des acquisitions de FinTech. La banque est en constante évolution pour s'assurer qu'on

[42] P&L est un acronyme pour profit and loss

> réponde aux besoins du clients. Ça se voit quand il y a des fusions de succursales, il y a de moins en moins de place où tu peux aller, le retrait des livrets, [etc.] » (Entrevue P7H)

D'un autre côté, le passage suivant de Jayce témoigne une approche plus orientée directement vers le client :

> « Il y a beaucoup de canaux, la voix du client, on écoute nos clients. Bien souvent, c'est pour des plaintes, mais il y a quand même des canaux qui sont ouverts pour les clients pour partager leurs expériences. On fait des focus groups. On va faire aussi des rapports Finalta qui se spécialisent dans l'industrie mondiale, sur le numérique, qui font des recommandations basées sur l'expérience para rapport au benchmark de l'industrie. » (Entrevue P8H).

Les réponses obtenues montrent que la haute direction a une meilleure compréhension des transformations à venir, en fonction des stratégies déployées pour ses clients. Les répondants soulignent la nécessité d'anticiper les besoins technologiques futurs, en prenant en considération l'évolution des modèles d'affaires et la prise de conscience de la réalité de leurs clients. Nous comprenons donc qu'intégrer une nouvelle technologie ne se limite pas à sa mise en place, mais implique un cadre organisationnel pour répondre aux besoins futurs des clients.

Codification / Thème	Nombre d'entrevues	Références
Adoption technologique	1	2
Gestion du changement	2	8
Prise de décision	2	30
Implications organisationnelles	2	5
Leadership	2	7

Tableau 16 Codification et références du pilotage interne de l'adoption technologique

5.4.3 Environnement de gouvernance stratégique

L'environnement de gouvernance stratégique constitue la troisième et dernière dimension analysée dans le cadre de la vision stratégique de la haute direction quant à l'adoption des identifiants décentralisés. Ce thème englobe les facteurs externes et institutionnels qui influencent la prise de décision à l'échelle stratégique, notamment en ce qui concerne l'orientation concurrentielle, les pratiques de gouvernance, l'aspect réglementaire et la gestion de la réputation. La concurrence, mentionnée à cinq reprises dans deux transcriptions, constitue un facteur de stimulation stratégique pouvant inciter à accélérer ou à ralentir l'adoption selon la posture compétitive choisie. La gouvernance, évoquée neuf fois dans deux transcriptions, se réfère aux mécanismes de prises de décision et de surveillance internes qui régissent la faculté de l'organisation à lancer, à superviser et à évaluer des initiatives innovantes. Le facteur réglementaire, mentionné deux reprises depuis deux transcriptions, désigne l'ensemble des normes légales, réglementaires et de conformité qui encadrent les opérations bancaires et l'usage des données personnelles. Enfin, la réputation, évoquée une seule fois dans une transcription, fait référence à l'image publique de l'institution.

5.4.3.1 Concurrence

La concurrence est un facteur clé dans les décisions stratégiques en matière d'innovation technologique. Dans le secteur bancaire, l'analyse des mouvements du marché et des actions d'autres institutions influence la position adoptée à l'égard de nouvelles technologies. Selon les informations obtenues, la haute direction reste vigilante quant aux développements récents, mais adopte une approche mesurée vis-à-vis d'un environnement encore en développement. La logique de positionnement ou de différenciation face aux concurrents revêt une importance significative dans l'élaboration de la stratégie d'adoption des technologies. Ainsi, voici comment nos répondants ont répondu au moment de discuter de la concurrence :

> « La banque se compare beaucoup à la banque Zaun[43]. Il y a certaines places, ça va être le benchmark de savoir où est ce que [Zaun] se situe sur certaines choses. Déjà juste de dire où est ce que [Zaun] se situe vis-à-vis de nous, ça montre qu'on n'est pas en avance, [mais] on suit de proche » (Entrevue P7H)

[43] Le nom de la banque citée a été anonymisée tout comme la banque Piltover

> « Tout le monde est capable de se rallier dans un objectif commun, même si ce sont des concurrents. » (Entrevue P7H)

> « On regarde la compétition, ce qu'ils sont rendus dans certains services offerts, il y en a qui sont au-devant de nous. Mais faut changer la culture interne de l'organisation bancaire, je te dirais dans un dans un premier temps, puis se mettre plus dans une perspective entrepreneur. » (Entrevue P8H)

> « Il y a déjà des certains certaines tribunes où est ce que les institutions financières se parlent, tantôt je te parlais de l'Open banking, bien on est avec les autres banques, il y aurait une ouverture de contribuer puis de partager un modèle similaire avec d'autres institutions financières. » (Entrevue P8H)

> « On participe à beaucoup de vigie au Québec et en Amérique du Nord pour ce, pour voir qu'est ce qui se passe dans l'industrie. » (Entrevue P8H)

En somme, certains propos ci-dessus ont déjà été traités plus tôt, mais il convenait de réitérer la position de la banque par rapport à la concurrence. La banque Piltover observe les mouvements du marché et évalue ses prochaines actions stratégiques en conséquence. Elle étudie, avec une vigie technologique, l'industrie, elle se compare à ses concurrents directs et elle collabore avec ses concurrents pour faire avancer l'industrie au moyen de modèle de banque ouverte.

5.4.3.2 Gouvernance

Le thème de la gouvernance concerne les mécanismes qui régissent les décisions technologiques, les responsabilités décisionnelles et la gestion des risques. Les membres de la haute direction évoquent des structures de gouvernance formelles, mais aussi des dynamiques plus informelles influençant la prise de position sur les IDDs par exemple. Cette gouvernance se manifeste par un équilibre entre innovation et orientation stratégique. Elle encadre les initiatives en veillant à leur cohérence avec la stratégie globale de l'organisation.

Lorsque nous analysions le « business case » et la prise de décision, nous avons soulevé les défis liés à l'adoption technologique. À ce moment, nous nous concentrions sur la perspective de la banque qui était plutôt axée sur les résultats attendus. Ici, nous soulignons dans l'extrait suivant la gouvernance derrière le « business case » et la prise de décision :

> « Tout dépend comment ton business case est ficelé […]. La plupart du temps ce qu'ils regardent ce sont les bénéfices attendus ou la réduction des coûts. Après ça, ça va plus dans

> une optique de : est-ce que la direction est à l'aise avec l'orientation, la stratégie qu'on prend? Est-ce que ça vient répondre à une des grandes stratégies qu'on a pour la banque du futur? Tous ces facteurs ensemble vont peser dans la balance pour savoir est-ce qu'on a un Go ou on n'a pas un Go d'aller de l'avant avec cette initiative là (Entrevue P7H)

La haute direction oriente le changement selon sa stratégie globale, en alignant les priorités d'innovation avec les priorités organisationnelles. Elle évalue quels investissements méritent d'être poursuivis, en fonction des retombées attendues sur le long terme. Dans cette optique, le « business case » devient un outil de cadrage et de légitimation des décisions futures. Il ne suffit pas d'évaluer la rentabilité d'un projet, il faut également en examiner la cohérence par rapport aux orientations stratégiques. La gouvernance de ces décisions repose sur des mécanismes structurés de validation, incluant des comités, des responsables du projet et des critères d'acceptabilité organisationnelle. Cependant, l'avis des répondants stipulent que ces mécanismes peuvent parfois entraver l'innovation en imposant des étapes fastidieuses, autant pour le porteur de projet que pour les décideurs, et une pression accrue pour démontrer de la valeur ajoutée. La prise de décision devient alors un subtil équilibre entre prudence institutionnelle et volonté d'innover. Les cadres supérieurs doivent donc peser les risques technologiques, les éventualités réglementaires et les désirs des consommateurs. L'évaluation des avantages des identifiants décentralisés s'avèrera complexe s'il n'y pas de porteur de ballon qui maîtrise le sujet et s'il n'y a pas une entité qui gouverne le changement que les IDDs apporteront aux banques. Ce constant renforce l'idée que la gouvernance stratégique n'est pas simplement un filtre décisionnel, mais un espace de négociation entre la vision, la faisabilité et la temporalité.

5.4.3.3 Réglementaire

Le paysage réglementaire joue un rôle important dans l'élaboration de la stratégie liée à l'identité numérique. Dans le domaine bancaire, où les données sont particulièrement réglementées, tout changement touchant des informations confidentielles doit se plier à des règles internes et externes rigoureuses. Bien que le cadre réglementaire ne figure pas dans la portée de notre évaluation finale, il demeure important de soulever les témoignages à son sujet, puisqu'il est perçu à la fois comme une contrainte et un garde-fou indispensable. Voici les deux passages recueillis lors de nos entretiens avec les membres de la haute direction.

D'une part, Ezreal nous partage qu'il y a des règles gouvernementales en place pour donner le droit aux clients bancaires de soumettre une demande de destruction des données :

> « Ce sont toutes des règles gouvernementales. Le gouvernement a quand même un gros rôle à jouer sur ce que la banque fait. À tout moment, tu peux demander à ce que tes données soient écrasées, détruites et tout ça, puis avoir confirmation que ça a été fait. Ce sont les nouvelles lois de renseignements personnels » (Entrevue P7H)

D'autre part, nous souhaitons revenir sur les propos énoncés par Jayce alors que nous traitions des principales raisons d'intégrer une nouvelle technologie d'un point de vue stratégique. À ce moment, Jayce évoquait plusieurs raisons dont l'aspect réglementaire, puis nous avons discuté du modèle de BO[44]. Par conséquent, Jayce constate qu'il y a des défis en lien avec les réglementations et la participation au modèle de BO en donnant un exemple :

> « On a des gens qui participent à [l'Open Banking] au Canada. Même que la personne que je te parle, c'est elle qui réside et qui préside un peu les rencontres au niveau canadien pour mettre en place l'Open Banking, le défi qu'on a, c'est le gouvernement fédéral qui est en attente. Avec le départ de Justin Trudeau, ça l'a retardé un peu les GO, il n'y a pas d'appétit gouvernemental. Le réglementaire là-dedans fait on n'a pas le désir de le faire. C'est juste que nous, pour avoir le GO, faut avoir une compréhension réglementaire, puis il faut que le fédéral investisse. » (Entrevue P8H)

Avec cet extrait, nous comprenons qu'il est difficile d'aller de l'avant avec un projet d'envergure si le gouvernement n'est pas au fait. Les changements gouvernementaux affectent les réglementations, qui elles affectent les banques aussi. Ce que Jayce indique en parlant de l'appétit gouvernemental reflète la dépendance des banques face au gouvernement. Nous prendrons ce point en considération lors de notre discussion des résultats, mais nous le prendrons avec un grain de sel, puisque tel que mentionné plus tôt il ne fait pas partie de notre portée finale. Nous souhaitons souligner que l'aspect réglementaire, bien qu'essentiel, n'a pas suffisamment été étudié au Canada par rapport aux identifiants décentralisés. Il serait donc encore plus difficile pour nous de juger de son impact et des répercussions si nous n'avons pas de cas concret qui a su perdurer dans le temps et faire ses preuves dans l'écosystème bancaire canadien.

5.4.3.4 Réputation

La réputation de l'organisation, bien qu'elle soit abordée plus discrètement, émerge comme un enjeu inévitable dans les propos d'un répondant. L'introduction de nouvelles technologies d'identification peut avoir un impact considérable sur la perception publique de la banque en matière de sécurité, de transparence et d'innovation. Cette préoccupation quant à la perception extérieure peut inciter la haute

[44] BO est un acronyme pour banque ouverte ou open banking

direction à opter pour une stratégie plus conservatrice, en rejetant les projets susceptibles de miner la fidélité de la clientèle. La réputation agit ainsi comme un filtre dans l'évaluation des risques liés à l'innovation. Or, nous citons Jayce lorsqu'il s'exprimait sur les équipes de risques qui freinent les projets.

> « Les équipes de retail souvent parlent aux gens de risque qui sont vus comme des freins. Mais c'est important pour une organisation de bien faire, une saine gestion de notre risque. C'est ce qui nous permet de garder notre réputation après ça. » (Entrevue P8H)

En d'autres termes, bien que les équipes de gestion des risques soient parfois perçues comme des obstacles à l'innovation, elles agissent en réalité en faveur de la réputation de la banque. Elles veillent à protéger l'image de la banque en évitant tout geste susceptible de compromettre la confiance des clients ou des régulateurs. Leur mission est d'anticiper les impacts d'une innovation technologique sur la perception du public et de gérer les risques liés à la réputation. Cette retenue, quoique restrictive, est perçue comme fondamentale pour préserver la réputation de l'organisation. Les équipes de gestion des risques participent donc indirectement à la gouvernance stratégique en imposant un cadre de vigilance et de responsabilité.

5.4.4 Synthèse de l'analyse de la vision stratégique de la haute direction

L'analyse de la vision stratégique de la haute direction révèle une posture nuancée à l'égard de l'adoption d'une nouvelle technologie, comme les identifiants décentralisés, marquée par un équilibre entre volonté d'innovation, prudence institutionnelle et alignement avec les réalités internes. Trois dimensions principales structurent cette vision : le positionnement stratégique, le pilotage interne de l'adoption technologique et l'environnement de gouvernance stratégique.

Tout d'abord, le positionnement stratégique met en lumière une réflexion croissante pour de nouvelles technologies dans la stratégie à court, moyen et long terme, les plans de transformation numérique, notamment à travers un alignement stratégique, les justifications économiques, au moyen d'un « business case », et les indicateurs de succès d'adoption. Toutefois, certaines affordances clés restent partiellement développées. Par exemple, l'affordance de projection éthique organisationnelle, c'est-à-dire la capacité d'évaluer l'impact de futures technologies ayant l'intérêt de remettre aux clients la pleine propriété de leurs données, demeure limitée. De même, l'affordance de cohérence entre la vision stratégique et les projets numériques n'est pas toujours claire, créant des tensions dans la priorisation des initiatives.

Ensuite, le pilotage interne de l'adoption technologique reflète un ensemble de pratiques de de responsabilités centrées sur la mise en œuvre concrète des innovations. La prise de décision, la gestion du changement, le leadership et les implications organisationnelles constituent les piliers de cette dimension. Nous observons ici une affordance d'ancrage décisionnel, qui permet aux dirigeants de se référer à des processus établis pour guider l'innovation. Cependant, les lacunes en matière d'affordance d'appropriation collective, soit la faible mobilisation des équipes autour des nouveaux outils et d'affordance d'agilité organisationnelle, soit la rigidité des processus décisionnels, freinent l'élan d'innovation.

Enfin, l'environnement de gouvernance stratégique joue un rôle de filtre externe et institutionnel. Les facteurs concurrentiels, réglementaires, de gouvernance interne et de réputation influencent fortement la perception des risques et des opportunités liés aux identifiants décentralisés. La haute direction semble dotée d'une affordance de veille stratégique, lui permettant d'observer l'évolution de l'industrie, du marché et des normes. Néanmoins, l'affordance d'indépendance est un obstacle pour la banque considérant sa dépendance envers les réglementations et le gouvernement avant d'agir à grande échelle.

En somme, la vision stratégique analysée témoigne d'une maturité en développement. Si les fondations sont présentes, c'est-à-dire la sensibilité aux risques et enjeux, l'alignement stratégique, la volonté de transformation, plusieurs affordances critiques devront être renforcées pour permettre à la banque de passer d'une posture exploratoire à une stratégie d'adoption maîtrisée et proactive des identifiants décentralisés. De plus, il importe également de souligner que certaines dimensions inter-organisationnelles liées à la gouvernance d'un réseau blockchain supportant une solution d'identité décentralisée n'ont pas été pleinement approfondies dans l'analyse. Bien que ces enjeux aient été abordés de manière exploratoire lors des entretiens avec la haute direction, notamment en lien avec la collaboration interbancaire et les conditions de déploiement d'un réseau partagé, les propos recueillis sont demeurés limités, en partie en raison d'une familiarité inégale des participants avec la technologie blockchain. Ces éléments constituent ainsi des pistes d'analyses pertinentes pour des recherches ultérieures.

Codification / Thème	Nombre d'entrevues	Références
Concurrence	2	5
Gouvernance	2	9
Réglementaire	2	2
Réputation	1	1

Tableau 17 Codification et références de l'environnement de gouvernance stratégique

Thème	Sous-thème
Positionnement	• Transformation numérique • Alignement stratégique • Business Case
Pilotage interne d'adoption	• Adoption technologique • Prise de décision • Gestion du changement • Leadership • Implications organisationnelles
Gouvernance	• Concurrence • Gouvernance • Réglementaire • Réputation

Tableau 18 Synthèse de la vision stratégique de la haute direction

5.5 Synthèse globale de l'analyse des résultats

Ce chapitre a permis de mettre en lumière, à partir des données empiriques recueillies, les principales lacunes des processus actuels de gestion de l'identité numérique, les défis et opportunités associés à l'intégration des identifiants décentralisés, ainsi que la vision stratégique de la haute direction. La synthèse qui suit propose une lecture transversale de ces résultats à la lumière du cadre conceptuel présenté au chapitre 3.

Dans un premier temps, l'analyse des pratiques actuelles de gestion de l'identité numérique met en évidence des lacunes structurelles récurrentes au sein des systèmes bancaires traditionnels. Les résultats empiriques révèlent une fragmentation des processus, une redondance des vérifications d'identité, une dépendance marquée aux systèmes centralisés et une lourdeur opérationnelle. Ces constats empiriques rejoignent les limites théoriques associés aux modèles d'identité centralisés et fédérés présentés dans la revue de littérature et confirment la pertinence d'interroger les capacités de transformation des processus de gestion de l'identité et des accès dans un contexte bancaire fortement réglementé.

Dans un deuxième temps, les analyses issues des entretiens avec les experts blockchain et les employés techniques permettent de dégager les principaux défis et opportunités liés à l'intégration des identifiants décentralisés. Les résultats soulignent que les affordances associées aux IDD, notamment le contrôle accru des données par l'utilisateur, la réduction de la duplication des vérifications, l'amélioration de la portabilité des identités et le potentiel de simplification des processus KYC, sont perçues comme porteuses de valeur. Toutefois, ces opportunités sont contrebalancées par des enjeux significatifs liés à la maturité technologique, à la conformité réglementaire, aux coûts d'intégration, à la formation des employés et à l'acceptabilité organisationnelle. Cette tension entre potentiel de transformation et contraintes opérationnelles illustre pleinement la logique des affordances mobilisée dans le cadre conceptuel, où les technologies n'imposent pas des usages déterminés, mais ouvrent des possibilités conditionnelles à leur contexte d'implantation.

Dans un troisième temps, l'analyse de la vision stratégique de la haute direction met en lumière une posture à la fois prudente et exploratoire. Les dirigeants reconnaissent l'intérêt stratégique des identifiants décentralisés et leur alignement potentiel avec les objectifs de sécurité, d'expérience client et d'innovation à long terme. Néanmoins, les résultats montrent que l'adoption de telles solutions demeure conditionnée à des facteurs organisationnels, réglementaires et inter-organisationnels, notamment en ce

qui concerne la gouvernance, la collaboration entre institutions et la viabilité d'un déploiement à l'échelle d'un réseau interbancaire. Cette vision stratégique confirme que l'intégration des IDD ne peut être envisagé comme une simple substitution technologique, mais bien comme un projet de transformation sociotechnique nécessitant une réingénierie progressive des processus existants.

Pris dans leur ensemble, les résultats de ce chapitre mettent en évidence une dynamique de transformation marquée par un décalage entre les limites des pratiques actuelles et les possibilités offertes par les identifiants décentralisés. Cette dynamique s'inscrit directement dans le cadre conceptuel articulant les affordances de Gibson et le modèle proposé par Kuperberg, en montrant comment les IDD peuvent reconfigurer les relations entre utilisateurs, institutions et infrastructures technologiques, tout en demeurant contraintes par des enjeux de gouvernance, de conformité et d'acceptation. Ces constats empiriques constituent ainsi une base solide pour approfondir, au chapitre suivant, la discussion théorique et interprétative des résultats, en mettant en perspective les implications organisationnelles, stratégiques et conceptuelles de l'intégration des identifiants décentralisés dans le secteur bancaire canadien.

CHAPITRE 6
DISCUSSION DES RÉSULTATS

Le présent chapitre constitue une étape charnière de cette étude, puisqu'il vise à déployer une analyse approfondie et critique des résultats empiriques obtenus dans le cadre de notre recherche sur l'intégration des identifiants décentralisés au sein d'une banque canadienne. Il s'agira non seulement de dépasser la simple restitution des constats, mais surtout de s'engager dans une interprétation de ces données, en les examinant à la lumière du cadre théorique mobilisé tout au long de cette investigation. Plus précisément, nous explorerons comment les affordances sociotechniques de la technologie blockchain, telles que décrites par Kuperberg (2020) et influencées par les travaux fondateurs de Gibson (1977), nous aident à appréhender le potentiel transformateur des IDDs pour les processus de gestion de l'identité numérique et des données clients.

Cette démarche analytique nous permet de mettre en perspective les opportunités et les défis complexes inhérents à l'adoption de ces nouvelles technologies, en soulignant leurs implications pour les pratiques bancaires existantes et en identifiant les conditions nécessaires à une mise en œuvre réussie. Afin d'orienter la compréhension de cette discussion, le chapitre s'articule autour de plusieurs axes principaux. Dans un premier temps, nous reviendrons brièvement sur les résultats obtenus lors de la collecte de données via nos entretiens semi-dirigés. Dans un deuxième temps, nous procéderons à une discussion critique des résultats, en mettant en évidence leur convergence ou divergence avec les constats de la littérature scientifique. Dans un troisième temps, nous proposerons une explication des similarités et des écarts identifiés, en examinant les facteurs contextuels, organisationnels ou technologiques qui peuvent rendre compte de ces observations. Dans un quatrième temps, nous procéderons à une interprétation globale des résultats en formulant des recommandations théoriques et pratiques en lien avec l'évolution des pratiques de gestion de l'identité numérique dans une banque canadienne. Dans un dernier temps, nous conclurons ce chapitre en récapitulant les principaux enseignements tirés de l'analyse et en soulignant leur contribution à l'avancement des connaissances sur l'adoption des IDDs dans le secteur financier canadien.

6.1 Retour sur les principaux résultats

L'objectif de cette recherche était d'explorer de manière critique comment l'intégration des identifiants décentralisés pourrait transformer la gestion de l'identité numérique dans une banque canadienne, en s'appuyant sur une étude de cas unique approfondie ainsi que sur des entretiens avec des employés et membres de la haute direction de la banque étudiée en plus de deux experts de la technologie blockchain appliquée à l'identité. Pour structurer cette exploration, trois sous-questions ont été formulées : 1) quelles sont les lacunes du processus actuel de gestion de l'identité et des données clients? ; 2) quels sont les défis et opportunités liés à l'intégration des identifiants décentralisés? ; 3) quelle est la vision stratégique de la haute direction face à cette innovation technologique? L'analyse des résultats a permis d'atteindre les objectifs spécifiques de l'étude, à savoir : établir un diagnostic des inefficacités du processus actuel, analyser les leviers et les obstacles liés à l'adoption des IDDs et comprendre comment ces innovations pourraient s'inscrire dans une stratégie bancaire de de transformation numérique. Notre analyse s'est appuyée sur le concept d'affordances, permettant l'interprétation les possibilités d'action créées ou limitées par les architectures traditionnelles et les nouvelles solutions décentralisés. Dans une logique de continuité analytique, la discussion s'organise selon une progression qui reprend la structure des sous-questions de recherche tout en les replaçant dans une lecture transversale. Elle part d'un diagnostic des lacunes structurelles des systèmes actuels, examine ensuite les dynamiques de transformation induites par les identifiants décentralisés à travers leurs affordances sociotechniques, pour enfin aborder les implications stratégiques et organisationnelles de leur intégration dans le contexte bancaire étudié. Cette progression vise à maintenir une cohérence analytique entre les objectifs de recherche, le cadre conceptuel et les résultats empiriques analysés.

Premièrement, l'analyse a mis en lumière plusieurs lacunes structurelles, notamment liées à la gouvernance centralisée des données, à la complexité des processus d'authentification, à l'inefficacité des systèmes de gestion de données et de la relation client, ainsi qu'à la difficulté d'adapter les infrastructures existantes aux exigences croissantes en matière de sécurité, de transparence et d'expérience utilisateur. Ces lacunes sont renforcées par des enjeux de confiance, de redondance informationnelle et de gestion de la conformité, ce qui alourdit les processus opérationnels et affaiblit la relation client.

Deuxièmement, la recherche a révélé que les identifiants décentralisés, conceptualisés comme affordances nouvelles dans le cadre théorique, ouvrent des dynamiques de changement profondes. Ces dynamiques se traduisent par la réduction des risques opérationnels, l'amélioration la granularité de

l'authentification, la traçabilité vérifiable, la portabilité et l'interopérabilité des identités numériques, ainsi que l'autonomisation des utilisateurs dans la gestion de leurs données. Des solutions concrètes comme KERI, Hyperledger Indy et Sovrin ont été analysées pour leur capacité à générer ces dynamiques de transformation, tant au niveau technique qu'organisationnel. Toutefois, l'intégration de ces dynamiques est confrontée des défis considérables, notamment en ce qui concerne la complexité d'implémentation dans les systèmes bancaires traditionnels, la nécessité d'une interopérabilité inter-organisationnelle, le manque de standards techniques consolidés, ainsi que les obstacles liés à l'acceptabilité sociale et à la gouvernance distribuée.

Troisièmement, du point de vue stratégique, les résultats montrent que l'intégration des IDDs est perçue par les membres de la haute direction comme une opportunité d'innovation, de sécurisation et de compétition. Cependant, cette vision est confrontée à plusieurs freins : la résistance au changement, la gestion du last mile technologique, l'absence de standardisation réglementaire, le développement d'un business case robuste et le manque de maturité des infrastructures. L'adhésion des directions stratégiques à ce paradigme repose donc sur leur capacité à s'approprier les affordances offertes par les IDDs et à les inscrire dans un modèle de gouvernance technologique partagé.

Finalement, les résultats mettent en évidence une tension constante entre la structure rigide du système actuel et les dynamiques d'innovation portées par les identifiants décentralisés, ouvrant ainsi la voie à une réflexion sur les conditions d'une transformation durable et soutenable dans le secteur bancaire. Dans la section suivante, nous confronterons ces résultats aux acquis de la littérature existante afin d'évaluer leur portée théorique et d'en préciser l'apport à l'état de l'art.

6.2 Confrontation des résultats avec la littérature

Après avoir présenté les principaux résultats empiriques de notre étude, il importe désormais de les confronter aux acquis de la littérature mobilisée dans notre cadre théorique. Cette démarche vise à situer nos observations dans le champ de recherche existant, en examinant si elles confirment, complètent ou contredisent les connaissances établies sur la gestion de l'identité numérique, les identifiants décentralisés et les systèmes de gestion de la relation client en contexte bancaire. En procédant à ce dialogue analytique entre les informations recueillies sur le terrain et les connaissances théoriques, nous

serons en mesure de préciser la position de nos résultats par rapport à l'état de l'art et ainsi générer une interprétation et des recommandations. C'est précisément que la figure 80 illustre, soit la confrontation de nos résultats avec l'état de l'art pour finalement produire des recommandations.

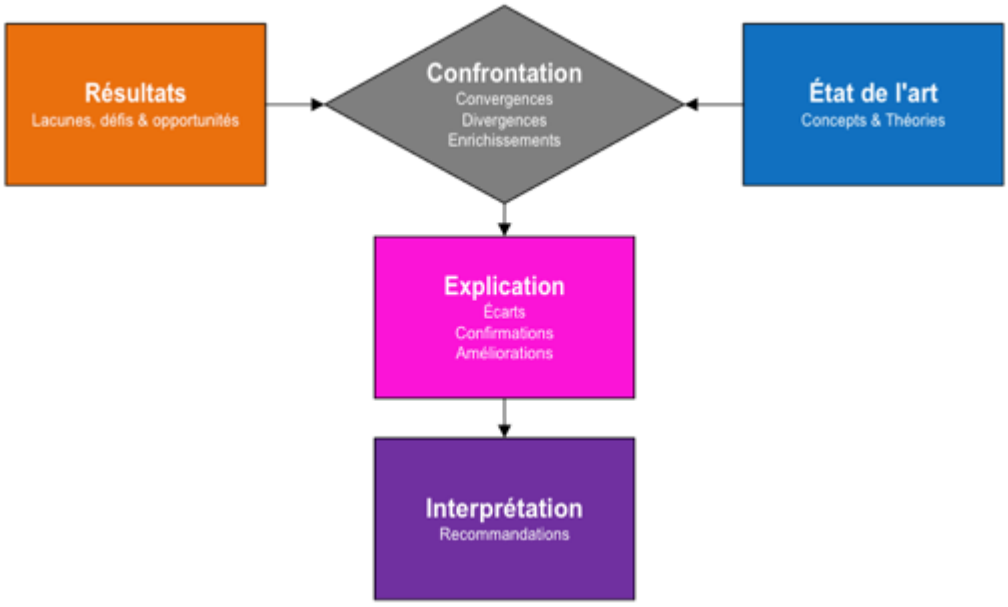


Figure 58 Illustration de la confrontation de la littérature avec les résultats et leur produit (création propre)

6.2.1 Confrontation des lacunes actuelles des processus avec l'état de l'art

Afin de mieux situer nos constats empiriques dans le champ de la recherche existante, cette première sous-section analyse la manière dont les lacunes observées dans la pratique concernant la gouvernance des données, la sécurité, l'organisation interne et l'expérience client viennent confirmer ou nuancer les critiques formulées dans la littérature sur les limites des processus bancaires traditionnels. En confrontant les résultats du terrain et les acquis théoriques, nous pouvons évaluer le degré de validité externe de nos observations.

6.2.1.1 Confrontation : Gouvernance de données

La gouvernance de l'identité et des flux de données constitue un enjeu fondamental dans la littérature sur la gestion des identités numériques. Nous examinerons ici dans quelle mesure la fragmentation, l'absence d'interopérabilité et la centralisation identifiées dans notre étude confirment ou prolongent les analyses précédentes.

Tout d'abord, la problématique de la tokenisation des données, identifiée comme un levier de sécurisation des données dans la littérature, se heurte en pratique à d'importants défis opérationnels. Nos résultats montrent que même si les données sont tokenisées, il demeure toujours des risques de fraude et de personnification d'identité considérant la totalité des données disponibles sur un individu sur internet, ce qui vient enrichir les analyses de Stapleton et Poore (2011).

En ce qui concerne les systèmes MDM, notre étude sur le terrain met en évidence des tensions concrètes entre l'objectif de centralisation des données et la réalité de leur gouvernance quotidienne. Parallèlement, la gestion des données à travers SAP CRM montre également des limites sur la véridicité des données affichées. Or, les entretiens révèlent un manque profond d'interopérabilité en temps réel de ces systèmes en raison de la fragmentation des processus et l'orchestration d'échange des données clients dans la pratique bancaire. Nos résultats viennent ici enrichir la littérature concernant MDM et SAP CRM dont ceux de Haneem et al. (2021) et Costin et Cojocaru (2017) respectivement. Pour ce qui est du processus KYC, notre analyse révèle une convergence forte avec les défis théoriques déjà relevés par plusieurs auteurs dont Mamun et al. (2020) ainsi que Parra Moyano et Ross (2023). Les répondants ont largement souligné la lourdeur, la redondance, l'inefficacité du processus et le fait qu'il n'est même pas certain de savoir si le client identifié est réellement lui. Cela confirme à nouveau l'absence d'interopérabilité des données et accentue la complexité et la lenteur du processus d'identification des clients.

De façon générale sur la question des risques de fraude, nos résultats corroborent les analyses théoriques existantes et confirment que la fraude demeure un enjeu transversal directement lié aux failles de gouvernance de l'identité numérique et des données clients. Du côté du stockage de données, notre étude valide les inquiétudes exprimées par Morris et Truskowski (2003) sur la fiabilité des infrastructures centralisées. Les participants interrogés ont souligné que les banques, en conservant les données d'identité selon un modèle d'identité centralisé et fédéré, peinent à garantir une disponibilité, une résilience et une traçabilité robuste et adaptées aux besoins contemporains opérationnels.

Ainsi, l'analyse croisée entre nos résultats empiriques et les contributions de la littérature souligne à la fois une convergence importante sur les faiblesses du modèle actuel et des processus KYC, mais aussi un enrichissement significatif en ce qui concerne les défis terrain liés à la tokenisation et aux systèmes MDM et SAP CRM. Ces constats permettent de mieux comprendre la réalité organisationnelle et la pratique des processus et systèmes utilisés au sein de la banque étudiée.

6.2.1.2 Confrontation : Sécurité

Les vulnérabilités en matière d'authentification et de protection contre les menaces émergentes ont été largement documentées dans les travaux scientifiques. Cette section évalue comment les insuffisances de sécurité observées dans nos résultats empiriques s'inscrivent ou dévient par rapport aux problématiques de sécurité soulevées dans la littérature.

Tout d'abord, sur la question de la simplicité et de l'efficacité au prix de la sécurité, nos résultats confirment les observations de Haneem et al. (2021) qui soulignaient que la centralisation des données d'identité facilite les processus. En revanche, elle laisse place à des vulnérabilités. Nos entretiens révèlent que la quête d'efficacité et simplicité opérationnelle continue de primer dans les choix technologiques au détriment de la robustesse des mécanismes de protection. La centralisation des flux de données dans les systèmes de la banque, bien qu'elle facilite l'accès et la maintenance pour les employés, expose en contrepartie l'ensemble du réseau bancaire à des risques systémiques importants. Cette convergence et cet enrichissement entre la littérature et la pratique indique que le trilemme entre fonctionnalité, efficacité et sécurité reste profondément ancré dans les décisions stratégiques.

En ce qui concerne l'authentification client, nos résultats apportent un enrichissement notable par rapport aux analyses existantes, notamment celles d'Ometov et al. (2018) et de Lal et al. (2024). Si la littérature souligne déjà les faiblesses des méthodes classiques d'authentification (mots de passes, SMS, etc.) face aux cyberattaques, nos entretiens mettent en lumière deux facteurs aggravants spécifiques au contexte actuel. D'une part, la priorité stratégique donnée à l'expérience client freine l'amélioration des méthodes d'authentification, car la banque hésite à introduire des procédures différentes, qu'elles soient plus simples ou complexes, de crainte à rendre les parcours clients moins intuitifs et fluides qu'ils ne le sont déjà. D'autre part, l'essor de l'intelligence artificielle pose de nouveaux défis que la littérature commence seulement à documenter. Nos participants ont exprimé leur inquiétude face à la capacité croissante des technologies de Deepfakes à répliquer la voix, le visage et même les comportements biométriques des utilisateurs, rendant les processus d'authentification beaucoup plus vulnérables qu'anticipé. Cet enrichissement empirique suggère que les menaces actuelles ne se limitent plus aux failles des systèmes existants, mais s'étendent aux nouvelles capacités de falsification rendues possibles par l'IA générative, ce que les modèles théoriques classiques n'avaient pas encore pleinement intégré.

En somme, la confrontation entre nos résultats et la littérature révèle une double tendance. D'un côté, nos résultats confirment les tensions structurelles entre efficacité, expérience client et sécurité bancaire. D'un autre, elles enrichissent l'état de l'art en montrant que l'évolution rapide des technologies adverses, comme l'intelligence artificielle, impose désormais un renouvellement des cadres théoriques d'analyse de la sécurité identitaire. Cette lecture invite à repenser les standards d'authentification non seulement sous l'angle de la robustesse cryptographique, soit leur capacité à résister aux intrusions, mais aussi en intégrant leur capacité à contrer les menaces plus subtiles et insidieuses, comme les manipulations comportementales (voix, visage, etc.)..

6.2.2 Confrontation des défis et opportunités des IDDs avec l'état de l'art

Au-delà des limites du modèle bancaire actuel, cette sous-section vise à confronter les défis et opportunités identifiées lors de nos entretiens autour de l'intégration des IDDs aux perspectives développées dans la littérature sur l'identité numérique décentralisée. Ce dialogue critique permettra de mieux situer les apports spécifiques de notre étude à l'état de l'art.

6.2.2.1 Confrontation : Défis des IDDs

Ici, nous confrontons les défis d'implémentation et d'adoption des identifiants décentralisés identifiés dans notre étude sur le terrain aux constats théoriques mobilisés dans la littérature scientifique. En examinant ces problématiques telles que la complexité technique, les enjeux d'interopérabilité, la résistance organisationnelle et les difficultés d'acceptabilité sociale, nous évaluerons dans quelle mesure les obstacles rencontrés sur le terrain confirment, nuancent ou complètent les analyses théoriques existantes sur les freins à la transformation identitaire en contexte bancaire.

Tout d'abord, notre analyse confirme fortement la complexité technique associée à l'intégration des IDDs dans les systèmes bancaires existants. Cette convergence émerge, car, comme le mettent en évidence Dib et Toumi (2020), les structures existantes, hautement hiérarchisées, s'avèrent peu propices à intégrer des schémas décentralisés d'identité, qui exigent une refonte majeure des architectures et des processus opérationnels. À cela s'ajoute la question de scalabilité. Les résultats empiriques corroborent les inquiétudes de la littérature concernant la capacité limitée des blockchains actuelles à supporter un grand volume d'identifiants et de transactions sans dégrader leur performance.

Dans le même ordre d'idées, les défis liés à l'interopérabilité inter-organisationnelle ressortent également avec force. Dans nos résultats ainsi que dans les écrits comme dans Dib et Toumi (2020), nous constatons que l'absence de normes uniformes constitue un obstacle majeur pour les diverses organisations qui tentent de reconnaître et d'utiliser en douceur les identités développées dans des environnements hétérogènes. La convergence est ici totale sur l'idée que sans cadre d'interopérabilité robuste, l'impact des IDDs restera fragmenté et limité. En revanche, notre étude vient enrichir la littérature sur certains aspects moins abordés. L'enjeu du last mile, c'est-à-dire la difficulté de lier de manière fiable une identité physique à une identité numérique auto-souveraine, est explicitement ressorti des entretiens, alors qu'il est peu traité par la littérature. Nos résultats montrent que cette phase initiale de preuve d'identité reste critique et constitue un maillon faible dans la chaîne de confiance, nécessitant des protocoles renforcés et une vigilance accrue au moment de la création des identifiants.

Par ailleurs, l'aspect organisationnel représente un autre enrichissement. Alors que Dib et Toumi (2020) concentrent leur analyse sur les contraintes techniques et réglementaires, nos résultats mettent en lumière une résistance interne forte au changement au sein de la banque étudiée. La crainte de déstabiliser des processus existants, les inquiétudes liées à l'expérience client et la culture de prudence de la banque freinent l'adoption des IDDs indépendamment de la faisabilité technologique. Ce décalage souligne l'importance des facteurs humains et culturels dans toute transition vers une gouvernance décentralisée de l'identité. Enfin, concernant l'acceptabilité sociale, nos constats viennent confirmer les observations de la littérature, soit la méfiance des utilisateurs face à un modèle d'identité auto-souveraine est un frein important. Les entretiens ont révélé que la compréhension des mécanismes des IDDs reste faible auprès du grand public et que nous sommes mêmes plusieurs années en avance, ce qui complexifie l'adoption à grande échelle.

Ainsi, la confrontation entre nos résultats empiriques et l'état de l'art révèle une forte convergence sur les défis techniques fondamentaux, mais enrichit l'analyse existante en introduisant une lecture plus complète des contraintes humaines et organisationnelles qui conditionnent la réussite de l'intégration des identifiants décentralisés dans le secteur bancaire.

6.2.2.2 Confrontation : Opportunités des IDDs

Après l'analyse des défis, cette partie confronte les opportunités de transformation, récoltées lors de nos entretiens, offertes par l'intégration des identifiants décentralisés aux perspectives théoriques

développées sur l'innovation en gestion de l'identité numérique. Nous discuterons de la capacité des IDDs à améliorer la sécurité, à renforcer la portabilité et la souveraineté des identités, à fluidifier les parcours d'authentification et à repositionner l'utilisateur au centre des processus d'identification bancaire, en comparant ces dynamiques d'innovation à celle proposées dans l'état de l'art.

Tout d'abord, la diminution des risques, de l'ordre opérationnel, réputationnel et sécuritaire, observée dans nos résultats rejoint directement les constats de Bharadwaj et al. (2023) et Ahmed et al. (2023), qui soulignent que le contrôle direct des flux d'identité offert par les IDDs réduit significativement les vulnérabilités aux fraudes et aux usurpations d'identité. Cette convergence renforce la pertinence stratégique d'une migration vers des modèles d'identité décentralisés à la banque. De même, la simplification des processus d'identification par l'orchestration fluide des composants et la suppression des lourdeurs administratives est corroborée par Sim et al. (2019), qui décrivent comment les systèmes basés sur la blockchain permettent de rationaliser les vérifications KYC et les procédures d'authentification. Nos résultats confirment pleinement que la fluidité obtenue grâce aux IDDs représente un levier concert pour améliorer l'expérience client tout en réduisant les délais opérationnels internes.

Par ailleurs, l'opportunité liée aux portefeuilles numériques contenant les informations d'identification vérifiable fait écho aux travaux de Dixit et al. (2022), qui mettent en avant l'importance de telles solutions pour faciliter des interactions sécurisées et contextuelles. Nos données de terrain soulignent que la capacité de l'utilisateur à regrouper, gérer et présenter informations d'identification vérifiables via un portefeuille unique constitue un facteur décisif d'adhésion aux nouveaux modèles identitaires. En matière de gouvernance de données, notre analyse converge également avec Ahmed et al. (2023), qui insistent sur la nécessité de basculer vers une gouvernance distribuée alignée sur les principes de l'identité auto-souveraine. Les répondants ont exprimé l'importance de ne plus dépendre exclusivement des banques ou des fournisseurs comme gardiens uniques de l'identité, mais plutôt d'instaurer un modèle où la confiance est partagée entre plusieurs parties prenantes. Concernant la transparence et la traçabilité, nos résultats s'alignent avec les constats de la littérature dont celle de Bharadwaj et al. (2023), qui démontrent que la réplication décentralisée des données facilite les audits en temps réel et renforce la confiance de tous les acteurs du réseau.

Parallèlement, nos résultats révèlent aussi des enrichissements par rapport à la littérature existante. La fiabilité construite autour d'un capital réputationnel numérique traçable enrichit l'état de l'art. Si

Bharadwaj et al. (2023) évoquent la fiabilité cryptographique offertes par les IDDs, nos résultats vont plus loin en montrant que la capacité à constituer une réputation numérique portable sur le long terme devient un levier d'attractivité et de fidélisation client. Les thèmes d'autonomisation et de la remise du pouvoir aux individus trouvent une confirmation forte dans la littérature, notamment chez Ahmed et al. (2023) et Dixit et al. (2022). Nos entretiens confirment que la capacité pour les utilisateurs de contrôle eux-mêmes l'accès à leurs données, de décider des informations divulguées et de gérer leur identité de manière granulaire représente une transformation majeure par rapport aux systèmes d'identité bancaires traditionnels.

En somme, la confrontation entre nos résultats et l'état de l'art témoigne d'une forte cohérence théorique entre les opportunités perçues par les experts et celles théorisées dans la littérature scientifique. Toutefois, elle permet également de souligner des dimensions d'enrichissement importantes sur l'émergence d'un capital réputationnel numérique, ce qui contribue à affiner la compréhension stratégique des bénéfices que les IDDs peuvent apporter au secteur bancaire.

6.2.3 Confrontation des solutions d'identifiants décentralisés avec l'état de l'art

Pour compléter cette confrontation théorique, cette dernière sous-section évalue dans quelle mesure les solution analysées, KERI, Indy et Sovrin, répondent aux critères de robustesse, de décentralisation, d'interopérabilité et d'éthique attendus dans les modèles conceptuels de gestion décentralisée de l'identité.

6.3 Explication des écarts et des confirmations

Nous allons maintenant expliquer les points de convergence, de divergence et d'enrichissement identifiés précédemment entre nos résultats empiriques et la littérature scientifique mobilisée. Cette analyse vise à comprendre les mécanismes sous-jacents qui expliquent pourquoi certaines dynamiques théoriques sont confirmées par notre étude de cas, pourquoi d'autres s'en écartent et en quoi notre recherche vient enrichir l'état de l'art existant.

Tout d'abord, les nombreux constats de convergence entre la littérature et les résultats de terrain s'expliquent en grande partie par le fait que les limites des systèmes bancaires traditionnels, notamment

en matière de gouvernance de données, de sécurité, d'architecture centralisée et de lourdeur procédurale, sont bien documentées depuis plusieurs années dans la recherche académique. La lourdeur procédurale observée dans les architectures existantes apparaît toutefois moins comme une conséquence directe de leur caractère centralisé que comme le produit de choix institutionnels, réglementaires et organisationnels, lesquels conditionnent la manière dont les technologies sont mises en œuvre et exploitées. Cette distinction permet également de comprendre pourquoi plusieurs initiatives décentralisées à grande échelle ont rencontré des difficultés majeures, malgré leurs promesses techniques, soulignant que la transformation des architectures d'identité demeure avant tout un enjeu sociotechnique et institutionnel. Les critiques récurrentes concernant la fragmentation des processus d'identité, le manque d'interopérabilité des systèmes (CRM, MDM, KYC), les vulnérabilités des mécanismes d'authentification ou encore la rigidité organisationnelle des banques face à l'innovation ont ainsi été pleinement confirmées par les observations menées au sein de l'institution bancaire étudiée. Cela suggère une certaine robustesse théorique du cadre existant et indique que les dysfonctionnements soulevés dans la littérature sont bien présents et persistants dans la réalité opérationnelle des institutions bancaires. De plus, les résultats empiriques confirment d'autres constats établis dans la littérature, notamment en ce qui concerne les enjeux de gouvernance des données, de sécurité et d'interopérabilité associés aux identifiants décentralisés.

Toutefois, notre étude terrain permet également d'enrichir la littérature à plusieurs niveaux. Cette valeur ajoutée découle essentiellement de la perspective empirique mobilisée. Alors que la plupart des articles scientifiques analysent les IDDs dans une approche conceptuelle, technique ou spéculative, notre recherche s'ancre dans une étude de cas réelle, au sein d'une banque canadienne en activité, avec ses contraintes spécifiques, ses arbitrages, ses logiques d'acteurs et ses réalités organisationnelles. C'est dans cet ancrage pratique que réside la principale source d'enrichissement. Par exemple, la question de la tokenisation, souvent présentée dans la littérature comme un mécanisme sécuritaire efficace, peut se révéler en pratique vulnérable lorsque les données sont partiellement tokenisées ou mal encadrées, ce qui expose les promesses des identifiants décentralisés en termes de contrôle utilisateur, elle traite peu des défis du last mile. Les résultats étendent également les travaux de littérature en mettant en évidence la centralité du facteur organisationnel et stratégique dans les conditions réelles d'adoption. Si ces dimensions sont maîtrisées, elles peuvent constituer un levier de transformation. À l'inverse, leur négligence expose les institutions à un risque de fragmentation accrue des systèmes, de perte de crédibilité auprès des clients et de retard stratégique face aux acteurs plus agiles de l'écosystème financier.

En outre, les résultats de terrain révèlent des dimensions organisationnelles et culturelles souvent sous-estimées dans les travaux académiques. L'inertie stratégique, la peur de perdre le contrôle des processus en place, le manque de maturité des infrastructures internes ou encore l'incompréhension généralisée des principes de souveraineté numérique par les utilisateurs, apparaissent comme des freins puissants que la littérature technique ne parvient pas toujours à intégrer pleinement. Ces résistances ne sont pas forcément visibles dans les modèles abstraits de décentralisation, mais elles émergent fortement dans les récits des employés de la banque.

Enfin, il convient de souligner qu'aucune divergence majeure n'a été observée entre nos résultats et la littérature mobilisée. En revanche, les écarts constatés se traduisent surtout par une complexification des dynamiques identifiées ou par leur contextualisation dans un environnement spécifique, ce qui constitue en soi un enrichissement significatif du champ.

En somme, l'intégration des identifiants décentralisés dans le secteur bancaire ne peut être pleinement comprise sans tenir compte des conditions concrètes de mise en œuvre. Ce que notre recherche met en évidence, c'est que les dimensions humaines, politiques, organisationnelles et contextuelles viennent colorer, nuancer et parfois détourner les trajectoires d'innovation théoriquement attendues. C'est à cette interface entre théorie et terrain que notre étude contribue de manière substantielle.

6.4 Interprétation globale et recommandations

À la lumière des résultats obtenus et de leur confrontation à l'état de l'art, il est désormais possible de formuler une interprétation intégrée visant à répondre directement à notre question de recherche principale : Comment la gestion de l'identité numérique dans le secteur bancaire canadien peut-elle être transformée par l'intégration d'identifiants décentralisés dans son système de gestion de la relation client ?

Pour y parvenir, nous avons articulé notre investigation autour de trois sous-questions de recherche, chacune ayant permis d'éclairer un aspect important de cette transformation. Cette structure a permis d'aborder la problématique sous plusieurs angles complémentaires, en partant d'un diagnostic des pratiques actuelles pour ensuite analyser les impacts potentiels de l'intégration des IDDs et finalement prendre en compte la vision stratégique portée par les acteurs décisionnels. Pour savoir comment la gestion de l'identité peut être transformée, nous devions absolument commencer par l'étude de l'état des lieux sur le terrain, soit dans une vraie banque canadienne.

6.4.1 Réponse à l'objectif #1 – Identifier les lacunes des systèmes actuels

Le premier objectif visait à identifier les lacunes structurelles, techniques et humaines des systèmes actuels de gestion de l'identité numérique dans une banque canadienne. L'étude de cas menée au sein de la banque Piltover a mis en lumière un ensemble de lacunes critiques affectant la qualité, la sécurité, et l'efficacité des processus identitaires et de gestion des données. Parmi celles-ci se trouvent la centralisation excessive des données clients, la fragmentation entre les systèmes SAP CRM, MDM et KYC, les erreurs manuelles liés aux indexations, ainsi que les redondances dans les vérifications d'identité. En parallèle, l'étude a révélé que les pratiques actuelles d'authentification (mots de passe, MFA par SMS, reconnaissance vocale) demeurent vulnérables aux attaques par ingénierie sociale ou par intelligence artificielle, ce qui crée un écart entre les exigences de sécurité contemporaines et les solutions en place. Ces constats soulignent également l'influence des contraintes organisationnelles (budgets limités, culture de prudence, expérience client) qui freinent les tentatives de modernisation. En somme, cette analyse des pratiques en place montre que le modèle de gestion de l'identité actuel, bien qu'opérationnel, repose sur des bases techniques rigides et une gouvernance asymétrique, où l'utilisateur n'a qu'un pouvoir limité sur ses données. Ces lacunes renforcent la pertinence d'explorer des solutions plus décentralisées et dynamiques, telles que les identifiants décentralisées et l'identité auto-souveraine.

6.4.2 Réponse à l'objectif #2 – Évaluer les défis et opportunités liés à l'intégration des IDDs

Le deuxième objectif visait à évaluer les conditions techniques et organisationnelles permettant ou freinant l'intégration des identifiants décentralisés à la banque étudiée et dans le secteur bancaire. À cet égard, les résultats ont confirmé plusieurs défis importants. Sur le plan technique, la complexité d'implémentation dans des infrastructures bancaires traditionnelles centralisées, le manque de standards interopérables et la dépendance à des fournisseurs d'identité externes rendent l'adoption difficile à grande échelle. Sur le plan organisationnel, les résistances humaines, la faible compréhension des principes de souveraineté numérique, ainsi que l'absence d'une stratégie cohérente de transformation identitaire apparaissent comme des obstacles importants. Néanmoins, l'étude a aussi mis en évidence de multiples opportunités dont l'amélioration de la traçabilité, la preuve réputationnelle, la réduction des risques de fraude, l'interopérabilité des identifiants entre institutions, l'autonomisation des utilisateurs dans la gestion de leurs données, la nouvelle source de profits avec les redevances et la capacité à renforcer la confiance client. Ces bénéfices ne sont toutefois pas garantis sans une approche progressive, interopérable et centrée sur l'utilisateur, ce que les entretiens ont clairement fait ressortir. Il en découle une conclusion claire, soit la promesse des IDDs ne pourra se matérialiser que si elle est accompagnée

d'un cadre structuré et piloté à la fois par l'expertise technique et une vision organisationnelle cohérente avec le changement.

6.4.3 Réponse à l'objectif #3 – Comprendre la vision stratégique de la haute direction

Le troisième objectif visait à comprendre la posture stratégique de la haute direction face aux identifiants décentralisés. Les résultats montrent une ouverture conditionnelle qui implique que la haute direction ne rejette pas les IDDs, mais qu'elle n'envisage leur adoption que dans la mesure où ils s'intègrent harmonieusement à la stratégie numérique de la banque sans compromettre la qualité de l'expérience client ni la conformité réglementaire. Les leviers déterminants de cette décision de transformation numérique sont la capacité de livraison de valeur, la clarté du modèle d'affaires (business case), l'alignement avec les exigences de protection des données et la démonstration de bénéfices tangibles (financier, expérience client, achalandage, etc.). L'étude souligne également la posture de la banque dans la mesure où sa culture organisationnelle fait prévaloir la prudence, mais où l'innovation est envisageable tant qu'elle respecte certains seuils de rentabilité, de stabilité et de transparence. Cela confirme que la transformation de l'identité devra être orchestrée avec le soutien explicite de la haute direction, en tenant compte des dynamiques de pouvoir, de gouvernance et de gestion du risque.

6.4.4 Réponse à l'objectif transversal – Comparer les processus traditionnels et décentralisés

Le dernier objectif de cette recherche visait à établir une comparaison entre les processus actuels de gestion de l'identité et les modèles décentralisés proposés par les IDDs. Cette comparaison, fondée à la fois sur des observations empiriques et des apports théoriques, montre une rupture significative. D'un côté, les processus traditionnels sont marqués par des logiques de centralisation, des contrôles manuels, des interactions redondantes et un faible contrôle accordé aux utilisateurs. De l'autre, les IDDs reposent sur des principes d'interopérabilité, de preuve cryptographique, de divulgation sélective, de remise de contrôle aux utilisateurs, d'automatisation, de transparence et de protection renforcée de la vie privée. La bascule vers un modèle basé sur les IDDs permettrait de simplifier l'expérience utilisateur, de renforcer la confiance grâce à des mécanismes transparents et de garantir la vérification d'identité.

Au-delà des considérations technologiques, les résultats de cette recherche mettent en évidence que la portée stratégique des identifiants décentralisés ne peut être pleinement appréhendée à l'échelle d'une seule institution. Bien que l'analyse se concentre sur une banque canadienne, les bénéfices associés aux IDDs reposent intrinsèquement sur une logique inter-organisationnelle, impliquant des mécanismes de

coordination, de gouvernance partagée et de confiance mutuelle entre les institutions financières. L'absence actuelle de cadres formels de collaboration interbancaire constitue ainsi un frein stratégique majeur, non pas en raison d'un manque de maturité technologique nécessairement, mais en raison des enjeux de synchronisation des priorités, des responsabilités et des modèles de gouvernance. Cette dimension, bien que volontairement peu développée dans le cadre de cette étude de cas, représente un levier stratégique déterminant pour toute mise à l'échelle future des identifiants décentralisés dans l'écosystème bancaire canadien.

6.5 Recommandations

Les recommandations formulées dans ce chapitre se concentrent volontairement sur des choix technologiques structurants, non pas en raison d'une sous-estimation des enjeux organisationnels, mais parce que le terrain empirique met en évidence que ces dimensions conditionnent en amont toute capacité de transformation stratégique. Elles doivent ainsi être comprises comme des prérequis techniques à une évolution plus large des modèles de gouvernance et de coordination inter-organisationnelle. Ainsi, afin de jeter les bases d'un système d'identité numérique plus robuste, interopérable et centré sur l'utilisateur, il est recommandé d'initier une démarche structurée de proposition de transformation numérique. Cette démarche devrait débuter par la création d'un comité de priorisation stratégique rassemblant des représentants des directions technologiques, réglementaires, opérationnelles, de gestion des risques, de cybersécurité, des lignes d'affaires et de l'expérience client, chargé de définir un premier cas d'usage à fort impact, tel que la simplification du processus d'ouverture de compte ou la réutilisation d'une identité vérifiée entre services internes. Ce comité aurait également la responsabilité de superviser le business case fondé sur une estimation de coûts, des bénéfices attendus en matière d'efficacité opérationnelle, de réduction des frictions clients et de gains en matière de conformité, ainsi que sur une évaluation rigoureuse des risques liés à la transformation du modèle d'identité actuel.

Pour démarrer cette transformation, un projet pilote devra être mis en place. La phase pilote devrait s'appuyer sur un périmètre restreint, contrôlé et testable, afin d'expérimenter les mécanismes d'émission, de détention et de vérification de justificatifs dans un environnement sécurisé, tout en permettant d'évaluer les implications techniques, humaines et organisationnelles. Il s'agira également d'identifier les ajustements requis pour assurer l'intégration fluide aux systèmes d'information existants sans compromettre la stabilité opérationnelle. De plus, il sera impératif d'envisager l'évolution de cette

initiative à l'échelle nationale pour maximiser les bénéfices d'interopérabilité entre les banques canadiennes. En effet, les bénéfices des identifiants décentralisés ne peuvent être pleinement réalisés qu'à travers l'existence d'un réseau interbancaire. Il est donc recommandé que cette transformation soit d'une part menée par l'Association des Banquiers Canadiens (ABC)[45] et d'autre part pensée dès le départ dans une perspective de mutualisation sectorielle, impliquant des démarches concertées entre les institutions financières afin de bâtir un socle commun d'interopérabilité, de reconnaissance mutuelle des identifiants et de gouvernance partagée. Une telle approche ne vise pas uniquement la modernisation technologique interne des institutions, mais l'émergence d'un espace identitaire canadien intégré, capable de soutenir des parcours clients fluides, sécurisés et transversaux à l'ensemble des services financiers canadiens.

Les recommandations suivantes proposent deux trajectoires technologiques qui peuvent être envisagées selon le degré de maturité organisationnelle, la stratégie d'innovation et la capacité d'alignement avec l'écosystème bancaire canadien.

6.5.1 Recommandation #1 – Hyperledger Indy

Parmi les trajectoires technologiques possibles pour soutenir une transformation identitaire vers un modèle décentralisé, Hyperledger Indy se présente comme une solution structurée, conforme aux standards ouverts du W3C et capable de répondre aux exigences réglementaires du secteur financier. À cet effet, il convient de se rappeler que Hyperledger est une blockchain publique open-source avec permission. Or, le réseau interbancaire canadien pourrait s'approprier du réseau en contribuant à faire développer la plateforme et ainsi jouir de pleinement de la blockchain publique permissionnée. Cependant, son adoption suppose une transition graduelle vers des logiques d'infrastructure distribuée, ce qui constitue un changement profond pour des institutions qui, à ce jour, ne disposent pas de tels mécanismes techniques en production. Ainsi, la réussite d'une telle trajectoire repose sur une capacité à bâtir, de manière itérative, un socle d'infrastructure partagé, aligné avec les besoins des banques canadiennes et piloté dans une perspective de gouvernance interbancaire.

[45] L'Association des Banquiers Canadiens représente les grandes banques canadiennes et défend leur intérêts auprès des autorités et du public

Tout d'abord, l'un des leviers essentiels à activer serait le contrôle sécurisé de l'infrastructure initiale par le recours à des environnements en mode « sandbox »[46]. Cette étape permettrait aux institutions participantes de s'initier aux concepts d'Indy, de preuves vérifiables et registre distribué sans assumer d'emblée la charge d'un nœud en production. L'objectif n'est pas de construire dès le départ un réseau pleinement opérationnel, mais d'accumuler un savoir-faire technique et organisationnel sur l'émission, la présentation et la validation des informations d'identification vérifiables fondées sur des identifiants Indy. À mesure que la compréhension des flux se consolide, les institutions pourront progressivement envisager la mise en place de leurs propres composants (nœuds validateurs), avec un niveau d'autonomie croissant et en parallèle des systèmes d'identification classiques pour continuer d'offrir une expérience transparente aux yeux des utilisateurs. Cette cohabitation temporaire permettra d'observer les conditions d'intégration aux architectures existantes tout en posant les bases d'une infrastructure distribuée souveraine. L'analyse des résultats a mis en évidence l'importance de ce passage progressif, notamment en raison des contraintes humaines et systémiques. L'objectif ici est de minimiser les coûts de transformation, les ruptures opérationnelles et l'impact sur l'expérience en vue de préparer l'environnement technologique à accueillir des flux d'identité décentralisées.

Au de-là des constats directement issus des données empiriques, l'analyse met en lumière une condition structurante de faisabilité à l'échelle sectorielle. Sur le plan interbancaire, la constitution d'un réseau de ce calibre fondé sur Indy nécessitera un engagement clair en matière de gouvernance partagée, et ce de l'ensemble des participants au réseau. Pour ce faire, une entité comme l'ABC pourrait mener le bal et orienter l'adoption du registre décentralisé commun, des standards sur le cycle de vie des identifiants sur lequel toutes les banques du réseau sont en accord, une structure des informations d'identification, un alignement avec les réglementations et des modalités de participation à la chaîne. Dans ce contexte, les institutions financières canadiennes gagneraient à initier la création d'un groupe de travail formel et collaboratif, pas juste dans le partage, mais dans la contribution, afin de structurer les bases d'un écosystème de confiance. L'objectif est de permettre, à terme, la reconnaissance interinstitutionnelle d'identités émises de manière décentralisée en vue d'offrir une véritable fluidité des parcours clients et réaliser les bénéfices attendus en matière de sécurité, d'agilité et d'expérience utilisateur. Cette proposition ne découle pas directement des propos des répondants, mais constitue une extrapolation

[46] Sandbox réfère à des environnements de test

analytique visant à mettre en évidence les conditions institutionnelles minimales nécessaires à un déploiement interbancaire cohérent.

En résumé, la trajectoire Hyperledger Indy constitue une option robuste, mais exigeante, qui demande un investissement initial en développement de compétences, en expérimentation technique et en coordination interbancaire. Elle est particulièrement adaptée à des institutions souhaitant bâtir, de manière structurée, les fondations d'un réseau canadien d'identité auto-souveraine, dans un cadre technologique et normatif bien établi, mais dont l'appropriation reste encore à construire.

6.5.2 Recommandation #2 – Solution KERI

La seconde trajectoire possible repose sur l'adoption graduelle du protocole « Key Event Receipt Infrastructure » perçu par l'un de nos experts interrogés comme la forme la plus aboutie de mise en œuvre des principes de l'identité auto-souveraine. Contrairement à des solutions qui adaptent des structures existantes à des logiques décentralisées, KERI propose une refonte complète du modèle identitaire à partir de mécanismes d'auto-certification, de journalisation cryptographique et de contrôle contractuel natif. Cette approche, fondée sur des identifiants auto-certifiants et une chaîne d'évènements vérifiables, offre à l'utilisateur une maîtrise intégrale sur la création, la délégation, la rotation et la diffusion de ses identifiants sans dépendre d'un registre ni d'un tiers de confiance institutionnel comme une banque. Cependant, intégrer KERI à un environnement bancaire demande une reconfiguration conceptuelle de la gouvernance identitaire, ainsi qu'un effort important de traduction juridique, technologique et organisationnelle. Le protocole suppose en effet une redistribution radicale du contrôle vers l'utilisateur, appuyée sur des garanties cryptographiques, mais aussi contractuelles, comme l'utilisation de conteneurs de données authentiques intégrant des contrats ricardiens. Ces éléments permettent non seulement de tracer les divulgations, mais aussi d'encadrer juridiquement chaque interaction, en imposant des obligations continues aux parties réceptrices des données.

L'adoption de KERI ne peut donc pas être envisagée comme un simple projet technologique. Elle exige une phase d'exploration appliquée, ancrée dans des cas d'usages ciblés à faible risque réglementaire, tels que des preuves d'identité temporaires à usage unique, la délégation de droits d'accès ou encore la vérification contractuelle de conditions d'accès à des produits et services. Ces expérimentations doivent permettre de tester les capacités de KERI à intégrer les contraintes réglementaires existantes (révocabilité, auditabilité, gestion des consentements, etc.) dans une approche proactive. Sur le plan organisationnel, cette

trajectoire suppose aussi la mobilisation de compétences nouvelles. Or, il est recommandé d'initier toute démarche KERI avec des consultants experts, de la recherche approfondie ou même avec des universités et étudiants spécialisés. Cela permettra de former des équipes polyvalentes pouvant expérimenter la solution KERI dans les meilleures conditions possibles. L'adoption de KERI, ne requérant pas d'infrastructure blockchain publique ni de registre partagé, présente l'avantage de contourner certaines limites techniques observées dans les projets actuels de type Hyperledger. En outre, elle offre l'opportunité de créer un nouveau flux de revenus grâce aux redevances de données. Avec le principe de redevances, un utilisateur peut contractuellement faire confiance à l'entité qui détient son information de vendre ses données et ainsi gagner un pourcentage sur les profits engendrés par la vente de ses données.

En somme, la trajectoire de KERI doit être envisagée comme une démarche exploratoire encadrée et destinée aux institutions souhaitant se positionner en amont sur les modèles de gouvernance identitaire de demain. Elle nécessite une capacité à articuler enjeux cryptographiques, exigences contractuelles et contraintes réglementaires dans un cadre encore peu exploré, mais porteur d'un haut potentiel de transformation systémique positif pour les utilisateurs. Si les conditions de maturité technologique et juridique sont réunies, cette approche pourrait permettre de dépasser les limitations structurelles actuelles en offrant une infrastructure d'identité véritablement distribuée, auto-certifiée et juridiquement traçable.

6.5.3 Synthèse des recommandations

Les deux trajectoires proposées s'inscrivent dans une volonté commune de moderniser la gestion de l'identité numérique dans le secteur bancaire canadien en rupture avec les logiques de centralisation actuelles. Elles diffèrent toutefois fondamentalement quant à leur architecture, leur maturité technologique, les conditions de leur mise en œuvre et le degré de transformation qu'elles impliquent. Le choix entre ces deux options de doit pas être envisagée comme une décision purement technologique, mais comme un positionnement stratégique quant au rôle que chaque institution souhaite jouer dans la transformation de l'identité numérique bancaire. Tandis qu'Indy permet de structurer un réseau interbancaire distribué à court et moyen terme, KERI quant à lui ouvre la voie à un modèle radicalement nouveau qui pallie aux défis de solutions blockchains plus répandues comme Indy, mais est encore très peu connue et n'as pas fait ses preuves. Le degré de maturité interne, la capacité à collaborer au sein d'un réseau interbancaire, la tolérance au risque et l'ambition d'innovation sont autant de facteurs à considérer dans l'arbitrage entre ces trajectoires. Quelle que soit l'option retenue, une gouvernance partagée, une

feuille de route itérative et un alignement interbancaire seront des conditions incontournables pour garantir le succès d'une telle réingénierie.

6.6 Limites de la recherche

Comme toute recherche qualitative, cette étude comporte un certain nombre de limites qui doivent être prises en compte dans l'interprétation des résultats et dans l'appréciation de leur portée.

La première limite concerne la portée exploratoire et contextuelle de l'étude. Le choix d'une étude de cas unique, centrée sur une seule institution bancaire canadienne, permet une analyse approfondie et contextualisée, mais cela limite la possibilité de généraliser les résultats à d'autres banques. Bien que certains constats puissent trouver un écho dans d'autres banques ou secteurs d'activité, il serait abusif d'en extrapoler des conclusions universelles sans précautions méthodologiques supplémentaires. Cette limitation est inhérente à la nature inductive et qualitative de l'enquête, qui vise davantage à comprendre en profonde les dynamiques locales qu'à produire des lois générales.

Une deuxième limite tient à la sélection des répondants et le fait que le chercheur principal soit un employé de la banque étudiée. Les employés analystes interrogés sont tous des collègues du chercheur principal, ce qui peut avoir introduit un biais de proximité ou de désirabilité sociale dans les réponses. De même, les membres de la haute direction consultés occupent des postes hiérarchiquement supérieurs au chercheur. Cette situation a pu influencer la posture réflexive du chercheur au moment des entretiens de l'interprétation des données. Bien que des efforts aient été faits pour atténuer ce biais, notamment par une triangulation rigoureuse des sources et une grille d'analyse structurée, ils ne peuvent être totalement écartés.

Une troisième limite est à propos de l'évolution récente de l'écosystème technologique analysé, en particulier Sovrin. L'arrêt du registre principal du projet Sovrin fût le 31 mars 2025 (Curran, 2025). Cette évolution souligne la fragilité des initiatives open source fondées sur des structures de gouvernance bénévoles ou sous-financées. Néanmoins, cette interruption ne remet pas en question la pertinence des résultats obtenus dans le cadre de cette étude. En effet, Sovrin n'est qu'une implémentation parmi d'autres principes de l'identité auto-souveraine. Les modèles techniques, protocolaires et conceptuels que Sovrin incarne peuvent tout aussi bien être répliqués ou adaptés au sein d'un réseau interbancaire national

ou sectoriel. Il importe donc de distinguer l'architecture conceptuelle du projet Sovrin, qui reste valide, de sa gouvernance opérationnelle, qui a montré ses limites.

Une dernière limite est l'aspect réglementaire et juridique des identifiants décentralisés. Bien que la recherche ait intégré une réflexion sur les enjeux de conformité, le cadre réglementaire et juridique entourant les IDDs et la technologie blockchain en général demeure en plein évolution tant au Canada qu'à l'international. Les interprétations légales de concepts tels que l'auto-certification, la preuve cryptographique ou encore la portabilité des identifiants ne font pas encore l'objet d'un consensus réglementaire. Par conséquent, les projections avancées dans cette étude quant à l'alignement des IDDs avec les exigences de conformité doivent être prises avec précaution. L'absence d'encadrement législatif spécifique, conjugué à la rapidité des innovations technologiques, constitue une incertitude majeure quant à la transposabilité à court et moyen terme des modèles explorés.

Ces limites ne remettent pas en question les réalisations, mais plutôt, elles soulignent que ces dernières devraient être interprétées en fonction du contexte méthodologique, organisationnel et temporel. Elles ouvrent également des pistes pour de futures recherches visant à tester, affiner ou étendre les conclusions ici présentées.

6.7 Contributions de la recherche à la science

Cette recherche apporte plusieurs contributions originales à la littérature scientifique sur la gestion de l'identité numérique et les technologies décentralisées. Trois apports principaux méritent d'être soulignés tant en raison de leur originalité que de leur potentiel structurant pour les travaux futurs.

Premièrement, cette étude constitue, à notre connaissance, la première analyse empirique approfondie des conditions d'intégration des identifiants décentralisés dans une banque canadienne. Alors que la littérature sur l'identité auto-souveraine demeure majoritairement théorique, cette recherche s'ancre dans un terrain réel et contextualisé. En effet, en mobilisant notre approche qualitative appliquée au cas d'une banque canadienne spécifique, nous avons pu mettre en relation un cas réel avec l'expertise blockchain réelle et concrète. Cette contribution est d'autant plus précieuse que le secteur bancaire virgule bien que souvent cité comme candidat naturel à l'adoption des identifiants décentralisés, reste peu documenté dans les travaux empiriques à ce sujet. En ce sens, notre étude comble un vide en fournissant une lecture nuancée des perceptions, résistance, levier et conditions de succès propres à une organisation

confrontée au défi de l'identité distribuée. Elle offre également un premier cadre méthodologique transférable, permettant à d'autres banques de reproduire cette démarche afin d'identifier leurs propres lacunes, d'évaluer la vision stratégique et de nourrir leur réflexion en matière de transformation numérique fondée sur l'identité décentralisée.

Deuxièmement, l'étude offre une analyse comparative des trajectoires technologiques possibles pour l'intégration des IDDs, illustrée à travers les cas d'Hyperledger Indy et de KERI. Plutôt que de trancher entre deux solutions concurrentes, la recherche met en lumière les conditions spécifiques de mise en œuvre, les niveaux d'engagement requis, les compétences nécessaires, les défis à surmonter, les opportunités offertes, et ce dans le cadre appliqué d'une banque canadienne. Cette mise en tension conceptuelle permet de proposer un outil d'aide à la décision pour les institutions bancaires en fonction de leur maturité technologique, de leur capacité à collaborer dans un cadre interbancaire et de leur volonté stratégique d'innover. Avec cette démarche, la recherche enrichit la littérature en proposant des approches décisionnelles orientées vers des solutions jusqu'ici plus théoriques.

Troisièmement, la recherche identifie et formalise les conditions nécessaires à l'émergence d'un réseau interbancaire canadien de gestion décentralisée de l'identité en tant que socle partagé d'interopérabilité, de reconnaissance mutuelle entre institutions et de gouvernance distribuée. Cette contribution dépasse l'analyse intra-organisationnelle pour aborder la question du passage à l'échelle nationale en soulignant que les bénéfices structurels de l'identité décentralisée ne peuvent être pleinement réalisés que dans un cadre de coopération interbancaire. Elle met ainsi en évidence la nécessité de standardiser le cycle de vie des identifiants, d'établir une gouvernance interinstitutionnelle robuste et de penser l'identité comme un bien infrastructurel collectif. Cette perspective systémique est essentielle à toute démarche sérieuse d'implémentation des IDDs à l'échelle nationale.

En conclusion, cette recherche continue à faire évoluer le débat sur l'identité numérique en proposant un ancrage empirique solide, un cadre d'analyse original, une typologie d'options stratégiques claires et une vision d'un écosystème de transformation identitaire canadien. Elle ouvre ainsi la voie à des travaux futurs plus poussés dans le champ des technologies décentralisées.

CHAPITRE 7

CONCLUSION

7.1 Résumé de la recherche et principaux résultats

Cette recherche avait pour objectif d'analyser la transformation potentielle de la gestion de l'identité numérique dans le secteur bancaire canadien à travers l'intégration des identifiants décentralisés. Elle s'inscrivait dans une approche qualitative et inductive, fondée sur une étude de cas unique menée au sein d'une grande banque canadienne. Trois sous-objectifs guidaient cette recherche : 1) identifier les lacunes actuelles de la gestion de l'identité et des données clients ; 2) évaluer les défis et opportunités de l'intégration des IDDs et 3) comprendre la vision stratégique de la haute direction face à cette innovation.

L'analyse des résultats a d'abord mis en évidence une série de lacunes persistantes dans les modèles traditionnels et rejoignent les critiques bien établies dans la littérature, notamment en ce qui concerne la centralisation des données, les mécanismes d'authentification et la faible efficacité des processus. Puis, la recherche a permis de documenter les freins techniques, organisationnels, humains et réglementaires qui limitent actuellement l'adoption des IDDs. Toutefois, plusieurs opportunités stratégiques se dégagent comme la possibilité de repositionner l'utilisateur au centre des interactions, de renforcer la sécurité des flux de données d'identité, de réduire les coûts liés aux vérifications manuelles et d'instaurer une traçabilité renforcée. Enfin, l'étude révèle une ambivalence dans la vision stratégique de la haute direction. Alors que les bénéfices potentiels des IDDs sont globalement reconnus, leur intégration reste conditionnée à la capacité de l'organisation à construire un business case, une feuille de route claire, à démontrer la valeur ajoutée d'une transformation numérique de ce calibre et à fédérer un écosystème d'acteurs majeurs autour d'un projet commun. Le besoin d'un réseau interbancaire canadien d'identité décentralisée a été largement confirmé comme condition pour éviter un déploiement isolé et inefficace.

En conclusion, cette recherche confirme l'intérêt stratégique que représente l'identité décentralisée pour le secteur bancaire tout en soulignant l'ampleur du travail requis pour adapter les infrastructures, les mentalités et les gouvernances à ce nouveau paradigme. Ce travail de recherche confirme que l'identité décentralisée ne constitue ni une solution clé en main ni un basculement technologique immédiat pour les institutions bancaires. Elle doit plutôt être comprise comme un horizon de transformation sociotechnique, qui met en tension les architectures existantes, les cadres réglementaires, les pratiques

organisationnelles et les rapports de pouvoir institutionnels. Les multiples dimensions explorées tout au long de cette recherche ne relèvent donc pas d'une dispersion analytique, mais traduisent la nécessité d'appréhender un objet fondamentalement transversal, dont les effets dépassent largement le seul champ technologique. En ce sens, l'intérêt stratégique des identifiants décentralisés réside moins dans leur capacité à remplacer les systèmes actuels que dans leur potentiel à reconfigurer progressivement les modalités de confiance, de gouvernance et de coordination inter-organisationnelle qui structurent aujourd'hui la gestion de l'identité numérique dans le secteur bancaire. L'analyse menée invite toutefois à nuancer les discours normatifs entourant l'identité souveraine numérique. Si les identifiants décentralisés ouvrent des possibilités nouvelles en matière de contrôle, de transparence et d'autonomie, les choix réellement laissés au client demeurent fortement encadrés par les architectures institutionnelles, les cadres réglementaires et les modèles de gouvernance propres au secteur bancaire. L'identité souveraine apparaît ainsi moins comme un transfert immédiat de pouvoir vers l'individu que comme un déplacement progressif des équilibres existants, dans lequel les institutions conservent un rôle central de médiation, de validation et de normalisation. Cette tension constitue l'un des apports critiques majeurs de la recherche, en mettant en lumière l'écart persistant entre les promesses théoriques de souveraineté numérique et les conditions concrètes de leur mise en œuvre dans des environnements organisationnels fortement régulés.

7.2 Pistes pour les recherches futures

À la lumière des constats issus de cette recherche exploratoire, plusieurs pistes de recherche peuvent être envisagées afin de prolonger et consolider les résultats obtenus. Ces pistes visent à valider la portée des résultats dans des contextes élargis et à inclure des perspectives actuellement peu représentées. Ainsi, deux pistes se dégagent pour approfondir l'étude des conditions de mise en œuvre et de réception des identifiants décentralisés dans les banques : une recherche comparative entre institutions et une évaluation de l'acceptabilité sociale auprès des clients bancaires.

Premièrement, des études comparatives entre plusieurs institutions bancaires canadiennes permettraient de dépasser les limites d'un design fondé sur une étude de cas unique. La présente recherche s'est déroulée au sein d'une banque précise, avec ses propres contraintes technologiques, sa culture interne, son rapport à l'innovation et son niveau de maturité numérique. Bien que cette approche ait offert une immersion approfondie et nuancée, elle limite nécessairement la portée généralisable des résultats. Or, il est probable que les perceptions, résistances et leviers d'adoption des identifiants décentralisés varient

considérablement d'une institution à l'autre en fonction de leur taille, de leur mission, de leur niveau d'intégration technologique ou encore de leur orientation stratégique. Une étude comparative multi-banques permettrait donc de dresser une typologie des environnements favorables ou défavorables à l'émergence de modèles d'identité décentralisée dans le secteur bancaire. Elle pourrait également favoriser l'identification de points de convergence entre institutions en vue de développer des cadres communs d'adoption, de promouvoir une gouvernance collaborative de l'identité numérique et de poser les bases d'une interopérabilité canadienne soutenue par une vision partagée de l'innovation. Dans cette optique, le cadre d'analyse proposé dans la présente étude peut constituer un point de départ pertinent pour orienter de futures recherches comparatives et faciliter la reproduction de la démarche au sein d'autres banques. Chaque institution pourrait ainsi mener sa propre étude en s'appuyant sur ce cadre et les résultats obtenus pourraient ensuite être compilés par l'Association des Banquiers Canadiens par exemple afin de cartographier collectivement les positionnements, les défis et les priorités du secteur à l'échelle nationale.

Deuxièmement, une évaluation quantitative de l'acceptabilité des identifiants décentralisés auprès des clients bancaires canadiens s'impose comme un complément essentiel aux résultats obtenus. Le présent projet de recherche s'est concentré sur la perspective organisationnelle, en mobilisant les points de vue des employés, des membres de la haute direction et d'experts technologiques. Toutefois, les identifiants décentralisés bouleversent le paradigme traditionnel de gestion de l'identité en redonnant à l'utilisateur un pouvoir décisionnel central dans l'émission, la gestion et la diffusion de ses informations d'identification vérifiables. Cela suppose non seulement une compréhension accrue des mécanismes de souveraineté numérique, mais aussi un changement de posture et de responsabilité pour l'utilisateur. En effet, une enquête quantitative à large échelle permettrait d'estimer le degré de connaissance, de confiance et d'intérêt des clients pour les IDDs, ainsi que leur niveau d'aisance à adopter de nouvelles pratiques liées à l'identité numérique. Elle pourrait explorer des dimensions comme la sensibilité à la confidentialité des données personnelles, l'ouverture à des portefeuilles numériques, la perception de la sécurité offerte par la blockchain ou encore les préférences en matière de gestion du consentement. Ce type de recherche fournirait des données concrètes pour anticiper les besoins d'éducation numérique, de design d'interfaces utilisateurs et de développement de parcours clients adaptés. Elle permettrait également de vérifier si l'acceptabilité sociale constitue un levier ou un frein dans l'éventuelle adoption à grande échelle des IDDs par les banques.

En conclusion, la combinaison d'études comparatives interbancaires et d'une évaluation de l'acceptabilité par les utilisateurs représente une voie de recherche cohérente, structurante et nécessaire pour accompagner le secteur bancaire dans sa transition vers des modèles de gestion de l'identité plus ouverts, distribués et résilients. Ces travaux fourniraient une base empirique multidimensionnelle pour penser une transformation systémique, ancrée dans la réalité des institutions et des attentes des clients.

ANNEXE A

LETTRE DE RECRUTEMENT

LETTRE DE RECRUTEMENT

Bonjour,

Mon nom est Luis Alberto Pastor Rodriguez, étudiant à la maîtrise en technologies de l'information à l'Université du Québec à Montréal. Dans le cadre de ma maîtrise, j'entreprends un projet de recherche dédié à l'étude sur les possibilités d'intégration de la technologie blockchain dans la gestion de l'identité numérique des clients.

J'aimerais donc vous inviter à participer à un entretien semi-dirigé d'une durée approximative de 45 minutes où vous serez amenés à partager votre expertise et votre expérience pour m'aider à comprendre comment l'intégration de la blockchain et la réingénierie des processus qui en découle pourrait transformer les processus actuels de gestion de l'identité. L'entretien prendra forme d'un échange ouvert et consensuel qui pourrait être programmé à votre convenance.

Si vous désirez contribuer à cette recherche en prenant part à une entrevue, veuillez au préalable lire et signer le formulaire de consentement ci-joint. Toute question pourra être posée au chercheur avant de confirmer votre participation. Une fois votre participation confirmée, les détails pour l'organisation de l'entretien vous seront partagés.

En vous remerciant de l'attention que vous accordez à ma recherche, je vous prie de croire en mes salutations distinguées.

Chercheur principal : Luis Alberto Pastor Rodriguez,
Étudiant à la maitrise
Département de Management et technologies
Université du Québec à Montréal
(+1) 514 826 3249
pastor-rodriguez.luis-alberto@courrier.uqam.ca

Directeur de recherche : Régis Barondeau, Ph.D., Professeur
Département de Management et technologies
Université du Québec à Montréal
(+1) 514 987 3000, # 6416
barondeau.regis@uqam.ca

ANNEXE B

FORMULAIRE DE CONSENTEMENT

UQÀM

FORMULAIRE DE CONSENTEMENT

Titre du projet de recherche

LES IDENTIFIANTS DÉCENTRALISÉS AU SERVICE DE LA PROTECTION DE L'IDENTITÉ NUMÉRIQUE - LE CAS D'UNE BANQUE CANADIENNE

Étudiant-chercheur

Luis Alberto Pastor Rodriguez, étudiant Maîtrise en Technologies de l'information à l'UQÀM
(+1) 514 826 3249 / pastor-rodriguez.luis-alberto@courrier.uqam.ca

Direction de recherche

Régis Barondeau, Ph.D., Professeur à l'UQÀM, Département de Management et technologies
(+1) 514 987 3000, #6416 / barondeau.regis@uqam.ca

Préambule

Nous vous invitons à participer à un projet de recherche qui implique un entretien semi-dirigé d'une durée de 45 mins à une heure. Avant d'accepter de participer à ce projet de recherche, veuillez prendre le temps de comprendre et de considérer attentivement les renseignements qui suivent.

Ce formulaire de consentement vous explique le but de cette étude, les procédures, les avantages, les risques et inconvénients, de même que les personnes avec qui communiquer au besoin.

Le présent formulaire de consentement peut contenir des mots que vous ne comprenez pas. Vous pouvez nous poser toutes les questions que vous jugez nécessaires.

Description du projet et de ses objectifs

L'objectif est de comprendre comment les identifiants décentralisés issus de la blockchain peuvent influencer les opérations bancaires en lien avec la gestion de l'identité des clients. Pour ce faire, nous souhaitons identifier les défis et opportunités d'incorporer cette technologie dans le quotidien d'une banque. Vous et une dizaine d'autres personnes avez été ciblés pour cette étude en raison de l'expertise que vous détenez dans votre domaine, ce qui contribuera grandement à répondre à nos questions de recherche.

Nature et durée de votre participation

Afin de comprendre davantage les opportunités et les défis associés aux technologies blockchain, spécifiquement les identifiants décentralisés dans l'industrie bancaire, il vous sera demandé de participer à une entrevue individuelle de 45 minutes sur Microsoft TEAMS ou dans un lieu neutre. Avant la rencontre, un document de deux pages (Voir Annexe) vous sera partagé afin que vous puissiez vous familiariser avec le sujet de l'étude, soit les identifiants décentralisés.

Dans le cadre de ce projet, nous recueillerons les données suivantes sur vous :

- Le contenu des discussions durant l'entrevue (transcription & notes manuscrites)
- Durant les entrevues individuelles, le chercheur vous demandera la permission d'enregistrer vos conversations avec lui. Vous avez le droit de refuser. Si vous acceptez, vous serez toujours libre par la suite de demander au chercheur d'éteindre l'enregistrement temporairement ou pour le reste de la séance.
- Il se peut que le chercheur demande à avoir une copie de documents que vous utilisez ou produisez dans le cadre de votre travail. Vous avez le choix d'accepter ou de refuser.

Avantages liés à la participation

En participant à cette étude, vous influencerez les chercheurs, mais surtout votre industrie afin d'agrandir la compréhension des enjeux reliés à l'impact de l'adoption de telles technologies dans l'industrie bancaire.

Risques liés à la participation

Au meilleur de notre connaissance, votre participation ne comporte aucun risque sérieux. Si un risque vient à notre connaissance, vous en serez averti aussitôt. Vous pouvez vous retirer de l'étude à tout moment.

Confidentialité

La confidentialité de l'information recueillie au cours de l'étude sera respectée. Tous les participants ont le droit d'obtenir tous les documents publics concernant cette étude. Toutes les données recueillies lors de l'étude seront gardées dans un endroit sécuritaire.

Les données brutes (notes écrites, enregistrements audio, commentaires, ou copies d'artefacts), recueillies lors des entrevues seront accessibles seulement aux membres de l'équipe de recherche. Ni votre employeur ni vos superviseurs n'auront accès à ces données brutes.

L'accès aux observations encodées sera restreint à l'équipe de recherche ainsi qu'aux vérificateurs des comités d'éthique de l'UQAM, mais une petite proportion pourra être publiée de façon sélective pour illustrer certains phénomènes. Dans ces cas précis, les données seront codifiées, au moyen de codes secrets pour éviter toute identification directe, et épurées, pour préserver l'identité des sujets directement ou indirectement (ex : en supprimant les noms de lieux ou de personnes cités par un sujet). Si une citation ne peut pas être correctement anonymisée, elle ne sera pas publiée (ex : si les détails donnés sont si précis qu'il ne peut y avoir de doute sur l'identité du sujet).

Les résumés sous forme de synthèses, de cas, de schémas, de figures, de tableaux ou de diagrammes, seront distribués à l'extérieur de l'équipe de recherche. Afin de préserver votre anonymat, votre nom n'apparaîtra nulle part dans ces résumés. Les données brutes et les observations codifiées seront détruites deux ans après la rédaction de la dernière publication scientifique reliée à ce projet.

Bien que l'étudiant tentera de préserver l'anonymat, les participants pourraient se reconnaître entre eux en raison du nombre restreint d'employés spécialisés.

Utilisation secondaire des données

Acceptez-vous que les données de recherche soient utilisées pour réaliser d'autres projets de recherche dans le même domaine ?
Ces projets de recherche seront évalués et approuvés par un Comité d'éthique de la recherche de l'UQAM avant leur réalisation. Les données de recherche seront conservées de façon sécuritaire. Afin de préserver votre identité et la confidentialité des données de recherche, vous ne serez identifié que par un numéro de code.
Acceptez-vous que les données de recherche soient utilisées dans le futur par d'autres chercheurs à ces conditions ?
□ Oui □ Non

Participation volontaire et retrait

Votre participation est entièrement libre et volontaire. Vous pouvez refuser d'y participer ou vous retirer en tout temps sans devoir justifier votre décision. Si vous décidez de vous retirer de l'étude, vous n'avez qu'à aviser Luis Alberto Pastor Rodriguez verbalement; toutes les données vous concernant seront détruites.

Indemnité compensatoire

Aucune indemnité compensatoire n'est prévue.

Des questions sur le projet?

Pour toute question additionnelle sur le projet et sur votre participation, vous pouvez communiquer avec les responsables du projet : Régis Barondeau, (+1) 514 987 3000, #6416 barondeau.regis@uqam.ca et Luis Alberto Pastor Rodriguez, (+1) 514 826 3249, pastor-rodriguez.luis-alberto@courrier.uqam.ca.

Des questions sur vos droits ? Le Comité d'éthique de la recherche pour les projets étudiants impliquant des êtres humains (CERPÉ) a approuvé le projet de recherche auquel vous allez participer. Pour des informations concernant les responsabilités de l'équipe de recherche au plan de l'éthique de la recherche avec des êtres humains ou pour formuler une plainte, vous pouvez contacter la coordination du [*insérer et conserver les coordonnées du CERPÉ plurifacultaire (cerpe-pluri@uqam.ca) ou du CERPÉ FSH (cerpe.fsh@uqam.ca*].

Pour toute autre question concernant vos droits en tant que personne participante à ce projet de recherche ou pour formuler une plainte, vous pouvez communiquer avec le bureau de la protectrice universitaire de l'UQAM protectriceuniversitaire@uqam.ca; 514-987-3151.

Remerciements

Nous vous remercions pour votre participation à ce projet de recherche.

Consentement

Je déclare avoir lu et compris le présent projet, la nature et l'ampleur de ma participation, ainsi que les risques et les inconvénients auxquels je m'expose tels que présentés dans le présent formulaire. J'ai eu l'occasion de poser toutes les questions concernant les différents aspects de l'étude et de recevoir des réponses à ma satisfaction.

Je, soussigné(e), accepte volontairement de participer à cette étude. Je peux me retirer en tout temps sans préjudice d'aucune sorte. Je certifie qu'on m'a laissé le temps voulu pour prendre ma décision.

Une copie signée de ce formulaire d'information et de consentement doit m'être remise.

_____

Prénom Nom

_____

Signature

_____

Date

Engagement du chercheur

Je, soussigné(e) certifie

(a) avoir expliqué au signataire les termes du présent formulaire; (b) avoir répondu aux questions qu'il m'a posées à cet égard;

(c) lui avoir clairement indiqué qu'il reste, à tout moment, libre de mettre un terme à sa participation au projet de recherche décrit ci-dessus;

(d) que je lui remettrai une copie signée et datée du présent formulaire.

_____

Prénom Nom

_____

Signature

_____

Date

Annexe

Sujet : Les Identifiants Décentralisés au Service de la Protection de l'Identité Numérique dans une Banque Canadienne

Introduction

La numérisation croissante de notre économie, accélérée par des événements tels que la pandémie de COVID-19, a profondément transformé les attentes et les pratiques dans le secteur bancaire. Les banques doivent maintenant s'adapter à des technologies émergentes comme la blockchain pour rester compétitives et répondre aux exigences croissantes en matière de sécurité et de gestion de l'identité numérique.

Les identifiants décentralisés (IDD), associés aux concepts d'identité auto-souveraine (IAS) et d'informations d'identification vérifiables (IIV), offrent une approche novatrice pour gérer les identités numériques de manière sécurisée et autonome. Ces technologies permettent aux utilisateurs de reprendre le contrôle sur leurs données personnelles, tout en améliorant l'efficacité et la transparence des processus bancaires.

Pourquoi cette étude ?

Dans les systèmes bancaires traditionnels, les processus de gestion de l'identité (par exemple, le KYC ou "Know Your Customer") sont souvent lourds, coûteux et vulnérables aux fraudes. La blockchain, en tant que technologie décentralisée et sécurisée, propose une alternative prometteuse. Elle permet de réduire les duplications d'efforts, de protéger les données personnelles et d'améliorer l'efficacité des processus.

Cette étude explore comment l'intégration des identifiants décentralisés dans une banque canadienne peut transformer la gestion de l'identité numérique. Elle vise à comprendre les bénéfices et défis de cette transition, tout en tenant compte des implications pratiques pour les employés et les clients.

Principaux concepts

- Blockchain : Un registre numérique distribué et sécurisé qui enregistre des transactions de manière transparente et immuable. Chaque transaction est ajoutée dans un bloc lié au précédent, formant une chaîne inviolable. Cette structure garantit que les données ne peuvent pas être modifiées sans l'accord du réseau
- Cryptographie : Ensemble de techniques permettant de protéger des informations en les rendant accessibles uniquement aux parties autorisées. Elle garantit la confidentialité, l'intégrité et l'authenticité des données.
- Identifiants numériques : Informations uniques associées à une personne ou à une entité, utilisées pour l'authentification et l'identification dans des systèmes numériques. Ces identifiants peuvent inclure des numéros, des codes ou des adresses électroniques.
- Identifiants Décentralisés (IDD) : Des identifiants numériques contrôlés par les utilisateurs et enregistrés sur un réseau blockchain.
- Identité Auto-Souveraine (IAS) : Un modèle où les utilisateurs possèdent et contrôlent leurs données personnelles.
- Informations d'Identification Vérifiables (IIV) : Preuves numériques permettant de valider une identité ou un attribut sans révéler d'informations sensibles.
- Zero-Knowledge Proof : Protocole cryptographique permettant de prouver qu'une déclaration est vraie sans révéler les informations sous-jacentes. Il assure la validation d'une donnée tout en préservant la confidentialité.

Objectifs de l'étude

L'étude cherche à répondre à la question suivante :

Comment les identifiants décentralisés peuvent-ils transformer la gestion de l'identité numérique dans une banque canadienne ?

Elle s'appuiera sur des entretiens avec des employés, des membres de la direction et des experts en blockchain pour explorer les thèmes suivants :

1. Identifier les faiblesses des systèmes actuels de gestion de l'identité.
2. Comprendre les défis et opportunités liés à l'intégration des IDD.
3. Évaluer la vision stratégique de la haute direction à ce sujet.

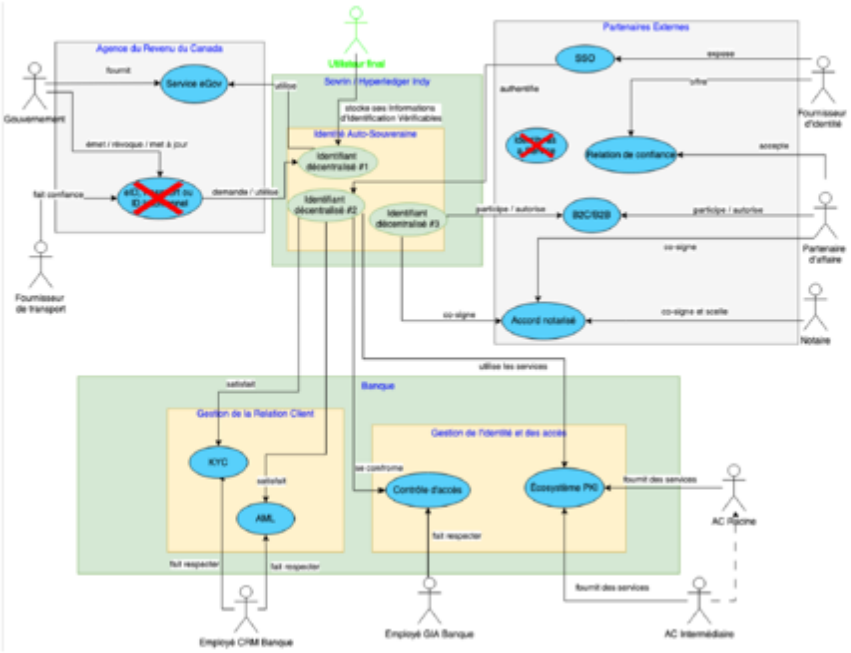


Figure d'un réseau blockchain dans une banque (Inspiré du modèle de Kuperberg 2020)

La figure ci-dessus illustre une proposition de système de gestion des identités numériques décentralisées basé sur des identifiants décentralisés. Il montre comment ces technologies remplacent les systèmes d'identification traditionnels et centralisés en donnant aux utilisateurs le contrôle direct sur leurs données personnelles tout en assurant une interaction sécurisée avec les banques, les services gouvernementaux et d'autres partenaires externes.

Problèmes résolus par le modèle

1. **Centralisation des données**: Les informations personnelles des utilisateurs ne sont plus stockées dans des bases de données centralisées, réduisant ainsi les risques de fuite.
2. **Autonomie des utilisateurs**: Les utilisateurs reprennent le contrôle sur leurs informations, décidant quelles données partager et à quel moment.
3. **Interopérabilité entre les systèmes**: Les identifiants décentralisés et les plateformes comme Sovrin permettent des interactions fluides entre différents systèmes (gouvernement, banque, partenaires externes).
4. **Sécurité renforcée**: Les technologies comme la cryptographie et le Zero-Knowledge Proof garantissent que les données sensibles restent confidentielles.

Fonctionnement général du modèle

- L'utilisateur utilise ses identifiants décentralisés pour interagir avec des services (banque, gouvernement, etc.).
- Ces interactions sont sécurisées via une blockchain et des plateformes comme Sovrin, qui stockent uniquement des informations vérifiables et non les données personnelles complètes.
- Les processus bancaires traditionnels, comme le KYC, sont automatisés et simplifiés grâce à cette approche.

Pourquoi votre participation est importante ?

Votre contribution permettra de recueillir des perspectives variées sur les implications concrètes de ces technologies. Ces informations aideront à formuler des recommandations pratiques pour améliorer les systèmes actuels et anticiper les futurs besoins du secteur bancaire.

Merci de prendre le temps de participer à cette recherche. Ensemble, nous pouvons contribuer à façonner un avenir plus sécurisé et efficace pour la gestion de l'identité numérique.

ANNEXE C

GUIDE D'ENTREVUE - EMPLOYÉ.E.S DE LA GIAC

Introduction

Bonjour, je vous remercie d'avoir accepté de participer à cette entrevue. Avant de commencer, permettez-moi de vous rappeler que toutes vos réponses resteront confidentielles et vous avez le droit de vous retirer du projet en tout temps. Vos réponses seront analysées pour les fins du projet de recherche. Avec votre permission, j'aimerais également enregistrer cet entretien pour m'assurer de toutes vos réponses soient capturées avec précision. L'objectif de cet entretien est de comprendre vos expériences et perceptions concernant la gestion de l'identité numérique des clients et l'utilisation potentielle de la technologie.

Questions Principales

1. Pouvez-vous nous dire et expliquer votre rôle à la banque?

Lacunes du processus actuel

2. Pouvez-vous décrire le processus actuel de création et de vérification d'une identité d'un client dans votre institution?
3. Quels sont les principaux défis, risques et menaces que vous rencontrez dans ce processus?
4. Quels outils technologiques utilisez-vous pour gérer les identités numériques?
5. Quelles sont les limites de ces outils?

Intégration des identifiants décentralisés dans les processus actuels et réingénierie des processus

6. Pour la prochaine partie, j'aimerais vous référez vers le document qui vous a été partagé en amont de l'entretien. Aviez-vous des questions ou des incompréhensions sur le document avant de continuer avec le reste des questions?
7. En observant le modèle présenté, la banque nécessiterait une réingénierie des processus actuels pour pouvoir intégrer les identifiants décentralisés. D'un point de vue réingénierie des processus,

quels avantages potentiels à long terme voyez-vous de l'intégration des IDD par rapport aux méthodes actuelles?

8. Quels défis anticipez-vous de l'intégration des IDD dans le processus de GIA?
9. Pensez-vous que l'intégration d'identifiants décentralisés pourrait aider à mieux répondre aux exigences de sécurité ? Pourquoi ou pourquoi pas?
10. Comment percevez-vous l'acceptation des clients, des employés et de la banque en général vis-à-vis les identifiants décentralisés?
11. Quels types de formation et de sensibilisation seraient nécessaires pour faciliter cette transition?

Conclusion

- Avez-vous d'autres points à ajouter ou des commentaires sur les sujets abordés?
- Si je trouve de nouvelles informations et que j'aimerais vous poser des questions complémentaires, est-ce que ce serait possible de vous contacter?
- Est-ce que vous pouvez me recommander d'autres collègues qui pourraient avoir un point de vue pertinent pour la recherche?
- Je vous remercie sincèrement pour votre temps et votre participation.

ANNEXE D

GUIDE D'ENTREVUE - EMPLOYÉ.E.S DU CRM

Introduction

Bonjour, je vous remercie d'avoir accepté de participer à cette entrevue. Avant de commencer, permettez-moi de vous rappeler que toutes vos réponses resteront confidentielles et vous avez le droit de vous retirer du projet en tout temps. Vos réponses seront analysées pour les fins du projet de recherche. Avec votre permission, j'aimerais également enregistrer cet entretien pour m'assurer de toutes vos réponses soient capturées avec précision. L'objectif de cet entretien est de comprendre vos expériences et perceptions concernant la gestion de l'identité numérique des clients et l'utilisation potentielle de la technologie blockchain.

Questions Principales

Lacunes du processus actuel

1. Pouvez-vous décrire comment le CRM est utilisé dans le processus de relation avec les clients
2. Comment les informations d'identité des clients sont-elles vérifiées, sécurisées et mises à jour dans le CRM?
3. Pouvez-vous décrire le processus KYC à la banque et le rôle du CRM dans ce processus s'il y a lieu?
4. Quels sont les principaux défis, risques et menaces que vous rencontrez dans le CRM concernant les données des clients? Par exemple, lorsqu'un agent doit vérifier l'identité d'un client.
5. Comment les données clients sont-elles partagées entre les différents services et processus?

Intégration des identifiants décentralisés dans les processus actuels et réingénierie des processus

6. Pour la prochaine partie, j'aimerais vous référez vers le document qui vous a été partagé en amont de l'entretien. Aviez-vous des questions ou des incompréhensions sur le document avant de continuer avec le reste des questions?
7. En observant le modèle présenté, la banque nécessiterait une réingénierie des processus actuels pour pouvoir intégrer les identifiants décentralisés. D'un point de vue réingénierie des processus,

quels avantages potentiels à long terme voyez-vous de l'intégration des IDD par rapport aux méthodes actuelles?

8. Quels défis anticipez-vous de l'intégration des IDD à la banque pour le CRM?
9. Pensez-vous que l'intégration d'identifiants décentralisés pourrait aider à mieux répondre aux exigences de sécurité ? Pourquoi ou pourquoi pas?
10. Comment percevez-vous l'acceptation des clients, des employés et de la banque en général vis-à-vis les identifiants décentralisés?
11. Quels types de formation et de sensibilisation seraient nécessaires pour faciliter cette transition?

Conclusion

- Avez-vous d'autres points à ajouter ou des commentaires sur les sujets abordés?
- Si je trouve de nouvelles informations et que j'aimerais vous poser des questions complémentaires, est-ce que ce serait possible de vous contacter?
- Est-ce que vous pouvez me recommander d'autres collègues qui pourraient avoir un point de vue pertinent pour la recherche?
- Je vous remercie sincèrement pour votre temps et votre participation.

ANNEXE E

GUIDE D'ENTREVUE - HAUTE DIRECTION

Introduction

Bonjour, je vous remercie d'avoir accepté de participer à cette entrevue. Avant de commencer, permettez-moi de vous rappeler que toutes vos réponses resteront confidentielles et vous avez le droit de vous retirer du projet en tout temps. Vos réponses seront analysées pour les fins du projet de recherche. Avec votre permission, j'aimerais également enregistrer cet entretien pour m'assurer de toutes vos réponses soient capturées avec précision. L'objectif de cet entretien est de comprendre vos expériences et perceptions concernant la gestion de l'identité numérique des clients et l'utilisation potentielle de la technologie blockchain.

Questions Principales

Fonctionnement du processus actuel

1. Quelle est la vision à long terme sur la transformation numérique de la banque?
2. Comment percevez-vous l'adoption des identifiants décentralisés à la banque et dans le reste du secteur bancaire canadien?
3. Quelles seraient les principales raisons pour leur intégration d'un point de vue stratégique?
4. En quoi l'intégration des IDD correspond-elle à la vision à long terme de la banque en matière de transformation numérique?
5. Sachant que pour que cette solution technologique soit optimale, l'ensemble du secteur bancaire canadien doit être impliqué afin de former un réseau interbancaire connecté sur la blockchain. Quels sont, selon vous, les avantages concurrentiels que l'intégration des IDD pourrait apporter à la banque en étant avant-gardiste par rapport aux concurrents?
6. Quels défis ou résistances anticipez-vous de la part des employés, des clients et du reste de la banque dans l'adoption des IDD?
7. Comment la banque envisage-t-elle de gérer les changements organisationnels nécessaires à l'intégration des IDD?

8. Quels rôle la sécurité et la confidentialité des données jouent-elles dans votre décision d'intégrer les IDD?
9. Comment envisagez-vous l'évolution des besoins des clients en matière de gestion de l'identité numérique et en quoi les IDD pourraient répondre à ces besoins?
10. Quels seraient les principaux indicateurs de succès pour l'intégration des IDD dans la gestion de l'identité numérique?
11. Quel est le rôle de la direction dans la facilitation et la promotion de l'adoption de nouvelles technologies ?

Conclusion

- Avez-vous d'autres points à ajouter ou des commentaires sur les sujets abordés?
- Si je trouve de nouvelles informations et que j'aimerais vous poser des questions complémentaires, est-ce que ce serait possible de vous contacter?
- Est-ce que vous pouvez me recommander d'autres collègues qui pourraient avoir un point de vue pertinent pour la recherche?

Je vous remercie sincèrement pour votre temps et votre participation

ANNEXE F

GUIDE D'ENTREVUE - EXPERT.E.S BLOCKCHAIN

Introduction

Bonjour, je vous remercie d'avoir accepté de participer à cette entrevue. Avant de commencer, permettez-moi de vous rappeler que toutes vos réponses resteront confidentielles et vous avez le droit de vous retirer du projet en tout temps. Vos réponses seront analysées pour les fins du projet de recherche. Avec votre permission, j'aimerais également enregistrer cet entretien pour m'assurer de toutes vos réponses soient capturées avec précision. L'objectif de cet entretien est de comprendre vos expériences et perceptions concernant la gestion de l'identité numérique des clients et l'utilisation potentielle de la technologie blockchain.

Questions Principales

Fonctionnement du processus actuel

1. Quelle est votre expertise blockchain?
2. Selon vous, quelles sont les principales limitations des systèmes actuels en GIA dans les banques?
3. Quelles opportunités technologiques voyez-vous dans l'intégration des IDD dans les processus bancaires par rapport aux systèmes centralisés actuels?
4. Quels sont les principaux défis techniques auxquels les banques feront face en intégrant les IDD dans leurs systèmes actuels?
5. Comment les IDD peuvent-ils transformer les processus bancaires de gestion de l'identité numérique à long terme?
6. Quelles seraient les principales résistances de la part des institutions bancaires vis-à-vis de l'adoption des IDD?
7. Dans quelle mesure les IDD peuvent-ils contribuer à renforcer la sécurité des données et à améliorer la confiance des clients?

8. Quels outils ou solutions complémentaires aux IDD seraient nécessaires pour que leur intégration se fasse de manière optimale dans les banques?
9. Quels coûts supplémentaires les banques devraient-elles prévoir pour mettre en œuvre les IDD à long terme?
10. En quoi l'intégration des IDD pourrait-elle améliorer l'expérience client?
11. Comment voyez-vous l'évolution des TBC et des IDD dans les 5 à 10 prochaines années en termes de réingénierie des processus?
12. Pouvez-vous nous expliquer les principes de base des IDD, IAS, IIV et Hyperledger (Indy ou autre)?
13. Comment percevez-vous le modèle Hyperledger Sovrin dans les infrastructures bancaires actuelles au Canada?
14. Quels obstacles ou opportunités spécifiques voyez-vous concernant son implémentation pratique sur le terrain?
15. Quelles stratégies de sensibilisation et de formation recommanderiez-vous pour faciliter l'adoption des IDD par les banques?

Conclusion

- Avez-vous d'autres points à ajouter ou des commentaires sur les sujets abordés?
- Si je trouve de nouvelles informations et que j'aimerais vous poser des questions complémentaires, est-ce que ce serait possible de vous contacter?
- Est-ce que vous pouvez me recommander d'autres collègues qui pourraient avoir un point de vue pertinent pour la recherche?
- Je vous remercie sincèrement pour votre temps et votre participation.

ANNEXE G

COMPLÉMENTS À LA REVUE DE LITTÉRATURE

Stockage de données

Le stockage des données regroupe l'ensemble des mécanismes permettant de conserver, d'organiser et de sécuriser les informations sensibles des utilisateurs, telles que leurs identifiants, leurs mots de passe et leurs attributs d'identifiant. Dans le secteur bancaire, où la protection des données personnelles est cruciale notamment en raison des différentes lois et réglementations, le choix de la technologie et des stratégies de stockage de données impacte directement la sécurité des données et la confiance des clients. L'évolution des technologies de stockage s'inscrit dans une trajectoire historique marquée par plusieurs ruptures techniques, depuis les cartes perforées utilisées dans les premiers systèmes informatiques jusqu'à l'introduction des disques durs en 1956 (Clark, 2021). Toutefois, « l'apport des disques durs en eux-mêmes ne sont pas suffisants, car ils ne peuvent fournir l'ensemble des requis nécessaires pour les entreprises » (Morris et Truskowski, 2003, p. 207). Les banques, étant des institutions de grande envergure, nécessitent un système d'information pouvant gérer les données efficacement surtout en cas de risques après désastres[47]. Avec le temps, dans le domaine des technologies de l'information, les DRs sont devenus des exigences qui ont impacté le choix et l'usage des solutions technologiques concernant le stockage des données (Morris et Truskowski, 2003, p. 208). Plusieurs techniques ont émergé, mais « la fiabilité des systèmes de stockage de données ne répondait pas aux exigences en matière de disponibilité des données » (Morris et Truskowski, 2003, p. 208). C'est ainsi que, dans les années 90, l'émergence de la technologie à faible coût dénommée LAN[48] a été significativement impactante dans les modèles de stockage de données, car elle permettait désormais aux ordinateurs des institutions d'être interconnectées localement favorisant une meilleure gestion des données (Morris et Truskowski, 2003, p. 208). Parallèlement, au début des années 90, le concept d'entreposage de données reposait en trois phases de transformation de données en information : l'acquisition de données, la gestion des données et la livraison des données (Sammon *et al.*, 2012, p. 8) (Sammon *et al.*, 2012, p. 8). Il était généralement admis que son objectif principal était d'améliorer la disponibilité de l'information à l'échelle de l'entreprise pour faciliter la prise de décision (Sammon *et al.*, 2012, p. 8). Durant cette période, l'entreposage de données a été perçu comme une solution aux problèmes de qualité et d'intégration de données, auxquels

[47] Risques après désastres réfère au terme anglophone « Disaster Risk » avec l'acrnonyme DR

[48] LAN est un acronyme pour Local Area Network

les systèmes d'information de gestion traditionnels ne parvenaient pas à répondre de manière efficace (Sammon *et al.*, 2012, p. 8). Aujourd'hui, « l'objectif est d'améliorer significativement le coût d'appropriation, la fiabilité et la facilité d'utilisation des systèmes de stockage de données pour devenir plus auto-configurable, auto-suffisant et capable de se protéger soi-même (Morris et Truskowski, 2003, p. 212-213).

Somme toute, le défi consiste à trouver l'équilibre entre sécurité, performance et accessibilité tout en minimisant les risques d'exposition aux cyberattaques et aux violations de données. Les banques traditionnelles utilisent des bases de données centralisées, souvent basées sur des infrastructures propriétaires ou des systèmes ERP bancaires tels que SAP et Oracle. Ces bases de données contiennent les données d'identité, les données transactionnelles et les données de profil client et le processus qui les gouverne se nomme la gestion des données maîtresses[49].

Gestion des données maîtresses (MDM)

La définition de la gestion des données maîtresses prend plusieurs formes, mais c'est un système centralisé combinant processus métier et technologies pour assurer l'identification, la synchronisation et la gestion cohérente des données clés à travers l'entreprise et ses systèmes (Sammon *et al.*, 2012, p. 6). Elle vise à garantir une version unique et fiable de l'information, améliorant ainsi la qualité et l'intégrité des données critiques d'une organisation, l'efficacité opérationnelle et la gestion stratégique de l'information (Sammon *et al.*, 2012, p. 6). Elle permet une meilleure intégration entre divers systèmes tel que les ERP et le CRM pour le partage et la rationalisation des données (Sammon *et al.*, 2012, p. 6). Ces données maîtresses, inclut les informations relatives aux clients, aux produits, aux fournisseurs et aux employés qui sont essentiels pour le bon fonctionnement des processus métiers. Lors de son apparition au milieu des années 1990, elle a suscité une attention similaire aux entrepôts de données et progiciels de gestion intégrées (Haneem *et al.*, 2017a, p. 3-4). L'importance de MDM réside dans sa capacité à réduire les silos de données en consolidant les informations issues de plusieurs systèmes et en évitant les incohérences et doublons (Haneem *et al.*, 2017b, p. 4).

[49] L'acronyme MDM sera utilisé pour référer à la gestion des données maîtresses

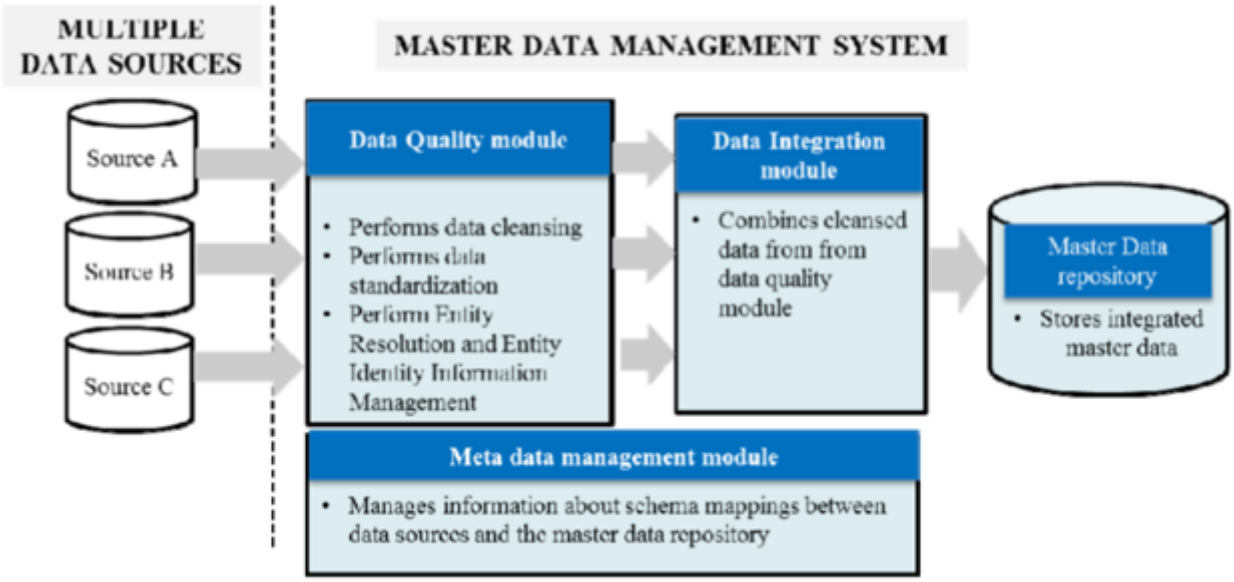


Figure 59 Modules du système MDM (Haneem et al., 2017b, p. 4)

En observant la figure 1, sur la gauche, nous pouvons constater que les données proviennent de plusieurs sources. Dans le cas d'une banque, les données des clients peuvent provenir de sources comme les succursales utilisant un CRM, où les clients se présentent pour créer un compte, l'application mobile de la banque, le site internet, etc. Le premier traitement effectué dans le cadre de MDM est réalisé par le module de qualité des données. Son rôle est de garantir l'exactitude et la standardisation des informations en appliquant plusieurs processus clés (Haneem *et al.*, 2017b, p. 4). Il commence par effectuer un nettoyage des données en supprimant les erreurs, les doublons et les incohérences. Ensuite, il applique une standardisation qui permet d'homogénéiser les formats, par exemple en unifiant les dates, les noms ou les types à utiliser dans les bases de données. Une fois les données nettoyées et standardisées, elle passent dans le module d'intégration des données (Haneem *et al.*, 2017b, p. 4). Celui-ci regroupe et fusionne les informations venant du module précédent afin de produite une version unique et consolidée des données maîtres (Haneem *et al.*, 2017b, p. 4). Ce travail d'harmonisation est essentiel pour éviter que la même personne, entreprise ou produit soit référencé sous plusieurs identités et que les utilisateurs et systèmes puissent exploiter une source fiable et homogène. En parallèle, le module de gestion des métadonnées assure la traçabilité et la structuration des données. Il documente les schémas et les relations entre les différentes sources et le référentiel maître (Haneem *et al.*, 2017b, p. 4). À l'issue du processus, les données consolidées sont stockées dans le référentiel des données maîtres, qui constitue la source unique et centralisée des informations validées et intégrées (Haneem *et al.*, 2017b, p. 4). Ce

référentiel assure que les données restent accessibles aux différents systèmes et utilisateurs de l'entreprise, tout en permettant leur mise à jour et leur synchronisation. Ainsi, ce schéma met en évidence l'importance d'un système gouvernant les données d'entreprise. En partant de sources hétérogènes et parfois incohérentes, MDM applique des processus de nettoyage, de standardisation et d'intégration aboutissant à un référentiel centralisé et fiable.

Interface de programmation d'application (API) & Open API

Dans les SBT, les interfaces de programmation d'application jouent un rôle fondamental dans la modernisation des services et l'interopérabilité des services. Une API désigne une interface logicielle exposée par un composant ou une application, permettant à d'autres composants, internes ou externes, d'accéder ses fonctionnalités de manière standardisée (Lamothe *et al.*, 2022, p. 1). Historiquement, le concept d'API émerge dès 1968 dans le cadre du développement d'interfaces graphiques interactives à distance, avant d'être consolidé dans les années 1970 autour du principe d'encapsulation ou de masquage de l'information, tel que proposé par Parnas (Lamothe *et al.*, 2022, p. 3). Dans le cadre bancaire, ce principe d'interface standardisé permet d'assurer la cohérence entre différents services, de contrôler l'accès aux ressources sensibles et d'orchestrer l'intégration de multiples systèmes hétérogènes. Par exemple, une API de requête de données permet à l'outil SAP CRM d'aller chercher les informations depuis les données stockées dans MDM afin de pouvoir les afficher dans l'interface visuel de SAP CRM nommé Fiori.

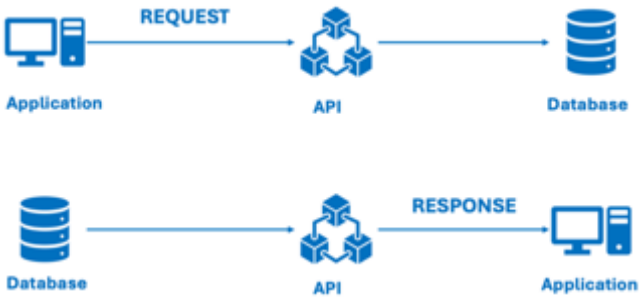


Figure 60 Fonctionnement des API (Molaro, 2024, p. 20)

Une API réfère donc à un ensemble de règles, de protocoles et d'outils permettant à différents logiciels de communiquer entre eux. À l'inverse d'une interface utilisateur, où l'interaction repose sur les actions humaines, l'API fonctionne en arrière-plan comme un intermédiaire logique entre des modules logiciels, tels que SAP CRM et MDM, transmettant les données de manière structurée sans intervention manuelle (Molaro, 2024, p. 19). Son rôle favorise ainsi l'interopérabilité des systèmes, la réduction du temps de

développement, la transparence du code et l'intégration fluide de composants distribués au sein d'architectures complexes (Molaro, 2024, p. 20). Les API peuvent être catégorisées selon leur degré d'ouverture : 1) les API privées, utilisées exclusivement au sein même d'une organisation, 2) les API partenaires, partagées sous conditions contractuelles avec des entités sélectionnées, et 3) les API publiques, dont les modalités d'accès varient selon les cas (Molaro, 2024, p. 20). Parmi ces dernières, les Open APIs occupent une place particulière dans le secteur bancaire. Elles sont caractérisées par une ouverture complète de leur description, documentation et utilisation, permettant à tout développeur autorisé d'interagir avec les systèmes sous-jacents sans restriction ni conditions (Molaro, 2024, p. 21). Cette forme d'ouverture technique est au cœur du paradigme des systèmes bancaires ouverts [50], notamment impulsé par la directive européenne Payment Service Directive 2, qui oblige les banques à exposer certaines fonctionnalités, comme l'accès aux données de compte ou la vérification de compte, à des prestataires tiers certifiés, appelés « Third-Party Providers » (Molaro, 2024, p. 21-22).

L'Open API devient ainsi un vecteur stratégique dans l'évolution des services bancaires, en facilitant l'émergence de nouveaux modèles d'affaires fondés sur la désintermédiation, la personnalisation des services financiers et la transparence de l'écosystème. Elle permet, entre autres aux fintechs de proposer des applications agrégatives de comptes, des outils de gestion budgétaire, des simulateurs de crédit ou des services de paiement instantané, en s'appuyant directement sur les infrastructures bancaires existantes.

SAP

D'une part, fondée en 1972, Systems Application & Productions (SAP) est une entreprise allemande détenant une multitude d'applications dont SAP NetWeaver (Cristea *et al.*, 2010, p.1). SAP propose une gamme de modules et de plateformes connus pour optimiser divers aspects des opérations d'entreprise et bancaires. SAP NetWeaver est une plateforme technologique qui sert de fondation pour l'intégration et l'exécution des applications d'entreprise (Hirsch, 2007, p. 2). Introduit au début des années 2000, il a révolutionné la manière dont les entreprises gèrent leurs processus en offrant un environnement unifié et interopérable basé sur des standards ouverts tel que XML[51] et web services (Cao *et al.*, 2010, p. 1). Grâce

[50] Les systèmes bancaires ouverts font référence au concept Open Banking

[51] XML est un acronyme pour eXtensible Markup Language

à cette plateforme, SAP a pu évoluer au-delà de ses systèmes ERP[52] traditionnels pour proposer une infrastructure flexible et extensible qui permet une meilleure intégration des systèmes internes et externes. NetWeaver repose sur une SOA[53] et « offre deux protocoles de communication pour connecter les systèmes SAP ABAP avec les systèmes externes : Simple Object Access Protocol (SOAP) et Remote Function Call (RFC) » (Cao *et al.*, 2010, p. 457). Parmi ces systèmes, nous y retrouvons les modules et composantes SAP PI, SAP BW, SAP BASIS (SAP, 2015, p. 24-26), SAP CRM et SAP MDM. Pour les fins de notre revue de littérature, nous allons nous concentrer sur SAP CRM et SAP PI, car ce sont les principaux modules pertinents pour la gestion de la relation client et de l'échange d'informations entre systèmes.

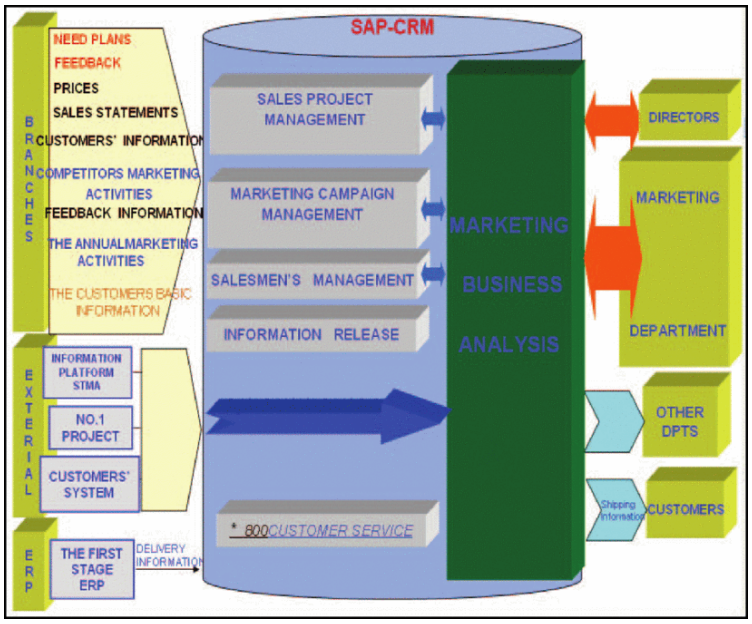


Figure 61 Fonctions de base de SAP CRM (Yi Wu et Fengping Wu, 2011, p. 3)

La figure des fonctions de base de SAP CRM met en évidence les différentes interactions et flux d'informations qui circulent entre les départements internes et les sources externes. SAP CRM sert ici de noyau central qui regroupe et traite les données clients, les stratégies marketing et les analyses commerciales pour optimiser la relation client et améliorer la performance globale de l'entreprise. La figure montre plusieurs éléments interconnectés. D'un côté, les succursales sont le point d'entrée des

[52] ERP est un acronyme pour Entreprise Resource Planning, soit un progiciel de gestion intégré

[53] SOA est un acronyme pour architecture orientée services

clients. Les clients se présentent en succursales pour quelconque activité en lien avec leurs besoins. Dans les SBT, les clients ont besoin d'aller en succursale pour ouvrir un compte, retirer de l'argent, renouveler une hypothèque, etc. Avec le flux de données entrant vers SAP CRM, plusieurs modules fonctionnels gèrent différents aspects du CRM. La gestion du compte et profil client se fait au sein de SAP CRM et celui-ci offre également des interfaces « user friendly » tel que Fiori.

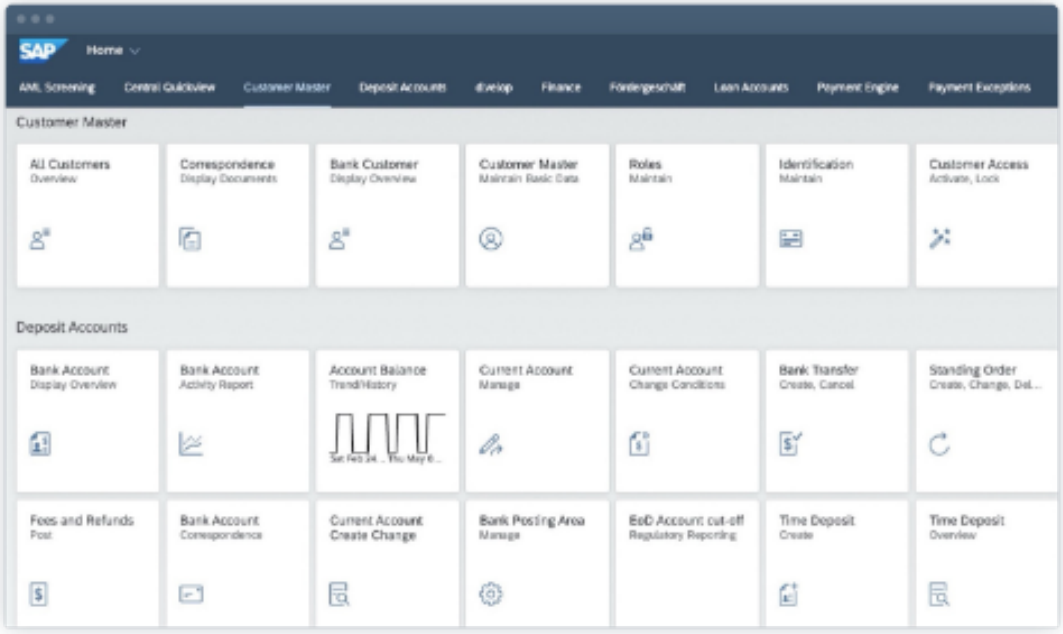


Figure 62 Interface Fiori (SAP, 2025)

« SAP Fiori est le système de conception primé pour tous les produits SAP […] pour créer des applications de gestion avec une expérience utilisateur exceptionnelle » (SAP Fiori, 2025). Les bénéfices d'une interface « user friendly » se traduit par une expérience unifiée de tous les systèmes, une meilleure définition des rôles des utilisateurs, plus de simplicité et une rapidité accrue (Costin et Cojocaru, 2017, p. 2-4). Les tuiles rendent les applications internes plus faciles à naviguer, ce qui réduit l'effort et le nombre de clics pour arriver à une certaine page dans le profil d'un client.

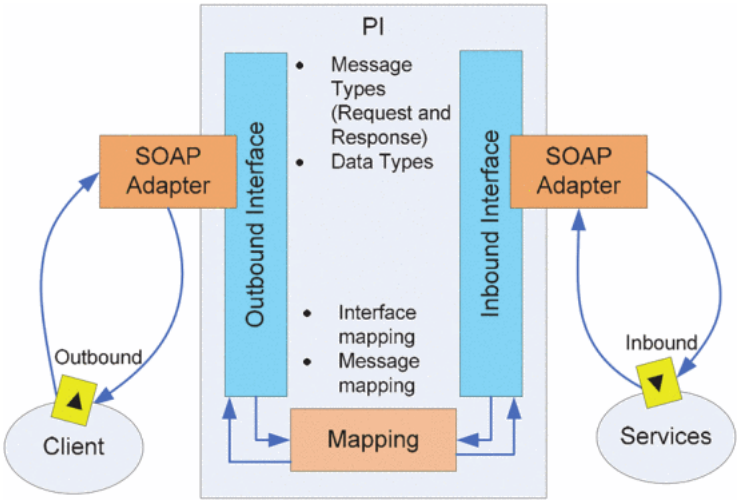


Figure 63 Communication des services web via PI (Cao et al., 2010, p. 458)

Dans les SBT, le module SAP CRM est la solution dédiée à la gestion des relations clients, mais SAP PI (Process Intégration), également connu sous le nom de SAP PO (Process Orchestration), est une plateforme d'intégration qui facilite la communication entre différentes applications, qu'elles soient internes à SAP ou externes. La figure 6 illustre le fonctionnement de SAP PI au moment où le client, soit l'émetteur, envoie une requête à un service en passant par plusieurs étapes de transformation et d'adoption gérées par SAP PI (Cao *et al.*, 2010, p. 458). La requête, ou message, passe d'abord par un adaptateur SOAP. Cet adaptateur convertit le format du message en un standard compréhensible par SAP PI pour faciliter l'intégration avec divers systèmes. Après être entré dans SAP PI, le message subit une transformation dans la phase de « mapping » (Cao *et al.*, 2010, p. 458). Cette étape permet d'adapter le message aux exigences du service récepteur. Deux types de transformation sont réalisés ici : le mapping d'interface, qui établit la correspondance entre les structures de données du système émetteur et du système récepteur, et le mapping de message, qui modifie le contenu du message en fonction des besoins du service cible. Une fois le mapping terminé, le message est redirigé vers l'interface entrante, où il est préparé pour être envoyé au service final. À ce stade, il est ensuite transféré vers un second adaptateur SOAP, cette fois du côté du service récepteur qui effectue une dernière conversion pour rendre le message exploitable par l'application cible (Cao *et al.*, 2010, p. 458). Ce service reçoit les données transformées et peut traiter la requête en conséquence. Ce schéma met en évidence l'important de SAP PI, car grâce à ses capacités de transformation et de routage des messages, il facilite l'échange de données entre des applications hétérogènes en assurant l'uniformité et l'interopérabilité des formats et protocoles utilisés.

L'interconnexion entre SAP CRM et les autres départements, via SAP PI, est identifiée dans la figure des fonctions de base de SAP CRM avec les flèches à double sens et uniques vers la droite. Les données issues du CRM sont utilisées par la direction, le département marketing et d'autres services internes. Enfin, la figure des fonctions de base de SAP illustre la relation directe entre SAP CRM et les clients finaux. Tel que mentionné plus tôt, MDM est le système qui gouverne les données clients. Grâce à des processus comme SAP PI et autres, il est possible pour SAP CRM d'obtenir accès aux informations clients depuis SAP MDM. Les banques peuvent répondre aux demandes et besoins des clients, traiter leurs préoccupations, et renforcer leur engagement au moyen de SAP CRM.

Salesforce

D'autre part, Salesforce, sorti en 1999, est un autre acteur majeur dans le marché du CRM en raison de leur détention de plus de 21% des parts de marché en 2023 (Grljević *et al.*, 2025, p. 2). En plus d'être les meneurs en termes de logiciel infonuagique, Salesforce est « reconnu pour ses capacités complètes de gestion et d'organisation des données clients, des processus de vente et des interactions avec les clients » (Shu *et al.*, 2025, p. 12). Selon Salesforce, une amélioration de 30% est ressentie sur les plans de rapidité de prise de décision, collaboration, revenus de vente, productivité de vente, satisfaction client et croissance d'influence (Salesforce, 2023, p. 8). L'essor du cloud computing a profondément transformé la gestion des données en entreprise. Traditionnellement, les systèmes CRM étaient hébergés sur des serveurs locaux nécessitant une maintenance une maintenance coûteuse et des investissements matériels importants. Salesforce a bouleversé ce modèle en proposant une solution entièrement basée sur le cloud (Koli *et al.*, 2023, p. 1), permettant aux entreprises d'accéder à leurs données en temps réel, sans avoir à se soucier des contraintes d'infrastructure. La collaboration avec les modèles de cloud computing a également permis à Salesforce de proposer différentes options de déploiement, notamment le cloud public, privé, hybride et communautaire (Koli *et al.*, 2023, p. 2). Chacun de ces modèles offre des avantages

spécifiques en fonction des exigences des entreprises en matière de sécurité, de flexibilité et de performance. De plus, Salesforce repose sur trois modèles de service cloud : SaaS[54], PaaS[55] et IaaS[56].

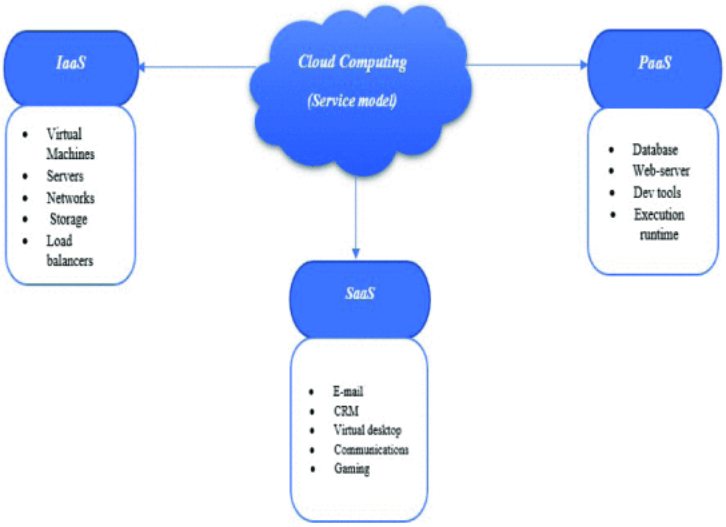


Figure 64 Modèle de service pour salesforce.com (Koli et al., 2023, p. 2)

« Le modèle SaaS permet aux entreprises d'héberger leurs logiciels sur une plateforme distante, accessible aux utilisateurs via divers dispositifs tels que les navigateurs web. […] Le modèle PaaS, quant à lui, prend en charge le cycle de vie du logiciel et offre une plateforme de développement permettant aussi bien l'exécution d'applications terminées que celles encore en cours de création. […] Enfin, le modèle IaaS met à disposition des ressources informatiques telles que la puissance de calcul, le stockage de données et l'organisation. Ce modèle repose sur la fourniture à la demande de ces ressources, allant des systèmes d'exploitation aux serveurs et aux capacités de stockage, via des connexions basées sur le protocole IP » (Koli *et al.*, 2023, p. 2-3).

[54] SaaS est un acronyme pour Software as a service

[55] PaaS est un acronyme pour Platform as a service

[56] IaaS est un acronyme pour Infrastructure as a service

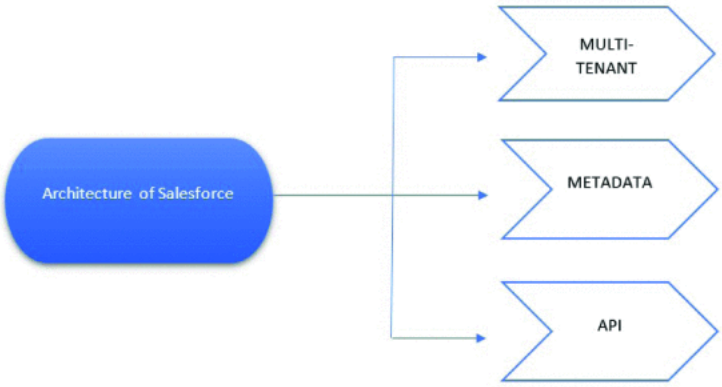


Figure 65 Architecture de salesforce.com (Koli et al., 2023, p. 3)

La figure 8 représente l'architecture de Salesforce en mettant en évidence ses trois composants fondamentaux : Multi-Tenant, Metadata et API[57]. L'architecture de Salesforce repose sur un modèle multi-locataire, ce qui signifie que plusieurs entreprises ou utilisateurs partagent la même infrastructure logicielle tout en ayant leur données strictement isolées et sécurisées (Koli *et al.*, 2023, p. 3). Ce modèle permet une mise à jour centralisée et automatique des fonctionnalités sans perturber les différentes instances des utilisateurs. Le deuxième élément de cette architecture est le système basé sur les métadonnées. Les métadonnées représentent les informations de base utilisées par des champs, codes, configurations, logiques et compositions des pages (Koli *et al.*, 2023, p. 3). Parmi les métadonnées, nous pouvons y retrouver plusieurs objets : Compte, Contacts, Opportunités, Campagnes, Rapports et idées (Manchar et Chouhan, 2017, p. 2). L'architecture de Salesforce repose sur une API robuste qui permet aux développeurs d'intégrer facilement la plateforme avec d'autres applications et services (Koli *et al.*, 2023, p. 3). Ainsi, cette architecture permet à Salesforce d'être une solution flexible et évolutive pour la gestion de la relation client.

Vagues d'adoption au changement

L'adoption d'une innovation technologique au sein d'un organisation suit rarement un mouvement homogène. Elle s'inscrit plutôt dans un processus graduel et différencié, où les acteurs ne réagissent pas tous au même rythme ni selon les mêmes motivations. Cette dynamique est décrite par le modèle des vagues d'adoption, qui identifie cinq catégories distinctes d'adopteurs, chacune jouant un rôle spécifique

[57] API est un acronyme pour Application Programming Interface

dans la diffusion d'une innovation (Duchesne, 2021). La compréhension de ces profils est importante pour analyser le potentiel de diffusion d'un technologie émergente.

Premièrement, il y a les innovateurs (Duchesne, 2021). Ce sont généralement des individus ou des entités sensibles à la nouveauté technologiques dotés « d'une soif de nouveauté » (Duchesne, 2021). Leur motivation première réside dans le désir d'explorer le potentiel d'une technologie avant même que son utilité soit démontrée ou simplement via une vigie technologique (Duchesne, 2021). Leur profil est souvent marqué par une tolérance élevée au risque et une capacité à s'adapter rapidement à des environnements instables ou encore en construction. Bien que minoritaires, les innovateurs sont essentiels, car ils amorcent la mise en mouvement d'une technologie, souvent dans des contextes de laboratoire, de preuve de concept ou de bac à sable réglementaire.

Deuxièmement, il y a les premiers adeptes (Duchesne, 2021). Ce sont ceux qui jouent un rôle pivot dans le processus d'adoption. Contrairement aux innovateurs, ils ne se contentent pas de tester la nouveauté, mais cherchent à évaluer comment celle-ci peut s'intégrer de manière concrète à leurs pratiques professionnelles pour « répondre à des besoins non satisfaits » (Duchesne, 2021).. Ils agissent comme des traducteurs entre la technologie et les usages, en identifiant des cas d'usage pertinents, en formulant des retours d'expérience structurés et en jouant parfois le rôle d'influenceur auprès de leurs pairs. Leur soutien conditionne souvent le passage à une adoption plus large, car ils apportent les premières preuves de la valeur ajoutée de l'innovation.

Troisièmement, il y a la majorité précoce (Duchesne, 2021). Celle-ci représente la technologie une population plus pragmatique. Ces adopteurs ne sont pas hostiles à l'innovation, mais exigent des garanties tangibles avant de modifier leurs pratiques (Duchesne, 2021). Leur décision peut se reposer sur des critères de durabilité, de fiabilité et d'alignement stratégique (Duchesne, 2021). Ils attendent que les premiers retours d'expérience soient consolidés et que des standards soient établis. C'est généralement à ce stade que l'innovation commence à se diffuser à plus grande échelle, mais cette diffusion dépend d'un écosystème suffisamment structuré, d'un encadrement clair et d'une intégration fluide avec les systèmes existants.

Quatrièmement, il y a la majorité tardive (Duchesne, 2021). Cette vague d'adopteur adopte la technologie davantage par nécessité que par choix (Duchesne, 2021). Elle ne s'engage que lorsque l'innovation est devenue un standard ou lorsqu'il n'existe plus d'alternatives viables. Cette population est souvent

contrainte par des pressions sociales externes (Duchesne, 2021), tels que les contraintes réglementaires, les transformations sectorielles ou encore les décisions stratégiques. Son intégration est généralement plus coûteuse, car elle suppose de lever des résistances culturelles, de compenser des retards en formation ou en infrastructure et de répondre à une exigence accrue en termes d'accompagnement au changement.

Finalement, il y a les retardataires (Duchesne, 2021). Ce groupe se distingue par une forte inertie au changement et une préférence marquée pour les systèmes éprouvés. Leur défiance peut s'appuyer sur des considérations rationnelles (ex : coûts d'adoption, dépendances techniques, etc.), mais aussi sur des dynamiques culturelles. Leur adhésion è l'innovation est rarement spontanée, car elle intervient sous la contrainte (Duchesne, 2021), voire par obligation, souvent dans un contexte de rattrapage ou de transformation imposée.

Les vagues d'adoption technologique se répartissent en cinq segments distincts qui traduisent les attitudes variables des individus et des organisations face à l'innovation. Les innovateurs et les premiers adeptes sont les premiers à s'engager, motivés par l'expérimentation et l'opportunité stratégique, alors que la majorité précoce attend des preuves tangibles avant de suivre. La majorité tardive adopte surtout par nécessité, sous l'effet de normes et standards, tandis que les retardataires résistent jusqu'à ce que le changement devienne inévitable.

Chiffrement symétrique

Le chiffrement symétrique se divise en deux grandes catégories : le chiffrement par flot et le chiffrement par blocs. Le chiffrement par flot chiffre les données bit par bit ou caractère par caractère, tandis que le chiffrement par blocs traite des segments entiers de texte clair en une seule opération (Simmons, 1979, p. 4-5). Bien que les chiffrements par flot aient été populaires pour leur rapidité, les chiffrements par blocs, comme l'algorithme DES[58], ont progressivement gagné en adoption en raison de leur résistance accrue aux attaques basées sur l'analyse statistique des fréquences (Simmons, 1979, p. 6 & p. 14). Les méthodes de chiffrement tel que DES et Triple DES ont été introduit respectivement en 1971 et 1998 (Ratnadewi *et al.*, 2018, p. 2).

[58] 3DES est un acronyme pour Data Encryption Standard

Le DES est un chiffrement à clé symétrique par blocs, où les données sont traitées par blocs de 64 bits avec une clé de 56 bits (Ratnadewi *et al.*, 2018, p. 2). Il fonctionne en appliquant une série d'opérations complexes en 16 tours, incluant des substitutions et des permutations (Ratnadewi *et al.*, 2018, p. 2). Chaque tour de chiffrement repose sur une clé dérivée de la clé principale via un processus de permutation et de décalage (Ratnadewi *et al.*, 2018, p. 2-3). L'algorithme suit une structure de réseau de Feistel[59], ce qui permet de rendre le chiffrement et le déchiffrement similaires en inversant simplement l'ordre des sous-clés (Ratnadewi *et al.*, 2018, p. 3). Les étapes principales de l'algorithme incluent la conversion du texte clair en binaire, la permutation initiale, la génération de sous-clés, la diffusion des bits via des boîtes de substitution (S-Box), la permutation et la permutation inverse pour obtenir le texte chiffré (Ratnadewi *et al.*, 2018, p. 3-4).

Figure 66 Diagramme du processus de chiffrement par bloc (DES) (Ratnadewi et al., 2018, p. 3)

Le 3DES, ou Triple DES, est une amélioration du DES qui applique trois itérations successives de l'algorithme pour renforcer la sécurité. Il utilise trois clés distinctes de 56 bits, augmentant ainsi la taille de la clé à 168 bits (Ratnadewi *et al.*, 2018, p. 4). L'algorithme peut être configuré selon trois modes : 3K3DES, soit trois clés différentes, 2K3DES, soit deux clés où la première clé est utilisée comme la troisième, et une version plus faible où une seule clé est répétée trois fois (Ratnadewi *et al.*, 2018, p. 5). L'étude

[59] Horst Feistel a développé les méthodes de chiffrement DES

comparative des performances entre DES et 3DES montre que le 3DES est plus sécurisé, mais plus lent que le DES en raison de ses trois cycles de chiffrement (Ratnadewi *et al.*, 2018, p. 6).

Cependant, un problème inhérent aux chiffrements symétriques réside dans leur dépendance à une clé secrète partagée, nécessitant des mécanismes sophistiqués de distribution des clés. Une clé symétrique est en effet utilisée à la fois pour chiffrer et déchiffrer les données, ce qui implique qu'elle doit être connue des deux parties. Cette exigence soulève des enjeux logistiques importants liés à la distribution sécurisée de cette clé, souvent appelée problème de « mise en accord de clé » (ANSSI, 2020, p. 53). De plus, il convient de souligner un autre risque important dans la gestion des clés symétriques concernant l'usage inapproprié d'une même clé pour plusieurs fonctions cryptographiques pour, par exemple, assurer à la fois la confidentialité et l'intégrité des données. Une telle réutilisation fragilise la sécurité globale du système. C'est pourquoi les règles de bonne pratique recommandent de ne jamais utiliser une même clé pour plusieurs usages (ANSSI, 2020, p. 35). Lorsque plusieurs mécanismes cryptographiques sont utilisés conjointement, il est important de générer des clés différenciées à partir d'une clé maîtresse à l'aide de mécanismes de diversification conformes (ANSSI, 2020, p. 35). En outre, l'utilisation de clés communes, partagées par de nombreux utilisateurs au sein d'un même système, est vivement déconseillé. Une telle architecture engendre un point de défaillance unique, car la compromission d'une seule clé compromettrait la totalité des échanges du réseau (ANSSI, 2020, p. 35). À l'inverse, l'approche consistant à dériver localement des clés à usage unique depuis une clé maîtresse, sans jamais exposer cette dernière, est recommandée, à condition que le mécanisme de dérivation respecte les critères de sécurité du référentiel (ANSSI, 2020, p. 35).

Tel qu'exploré avec le DES et le 3DES, l'un des principes fondamentaux du chiffrement traditionnel repose sur la notion de substitution et de permutation. Les systèmes de chiffrement classiques, tels que le chiffre de César ou la méthode de Vigenére, illustrent comment la simple substitution de caractères selon un schéma fixe peut être facilement cassée par des techniques d'analyse fréquentielles (Simmons, 1979, p. 3-5). Pour remédier à ces faiblesses, des systèmes plus complexes ont été développés, notamment les chiffrements et les transformations linéaires, comme celles proposées par Hill, qui combinent plusieurs lettres dans un processus de chiffrement simultané afin d'augmenter l'entropie du texte chiffré (Simmons, 1979, p. 3-6). Le passage aux systèmes informatiques a nécessité l'adoption de nouveaux mécanismes de protection, notamment l'intégration de registres à décalage à rétroaction linéaire, qui permettent de générer des séquences pseudo-aléatoires pour masquer les données en clair (Simmons, 1979, p. 1 & p.12).

Néanmoins, ces méthodes ne sont pas exemptes de vulnérabilités, puisque les séquences générées peuvent parfois être prévisibles si leur structure mathématique est bien comprise par un attaquant (Simmons, 1979, p. 12). Une attaque contre un algorithme de chiffrement par bloc consiste à exploiter ses propriétés internes afin d'en compromettre la sécurité. L'objectif peut être de retrouver la clé de chiffrement ou, plus simplement, de démontrer que l'algorithme ne se comporte pas comme une transformation totalement aléatoire (ANSSI, 2020, p. 11). Pour y parvenir, un attaquant peut utiliser différentes stratégies, comme l'analyse de textes chiffrés avec ou sans accès aux messages en clair correspondants, l'envoi de requêtes pour obtenir le chiffrement de données spécifiques, ou encore la possibilité de soumettre des chiffrés au déchiffrement (ANSSI, 2020, p. 11). L'efficacité d'une attaque repose sur plusieurs facteurs, notamment le coût computationnel, qui correspond au nombre d'opérations nécessaires pour la mener à bien, l'accès aux données chiffrées ou en clair, dont le volume influence directement la viabilité de l'attaque, ainsi que les besoins en mémoire, indispensables pour stocker des informations intermédiaires ou effectuer des calculs préalables (ANSSI, 2020, p. 11-12). Une attaque contre un algorithme de chiffrement par flot, quant à elle, vise à exploiter les caractéristiques de son fonctionnement pour compromettre la confidentialité des données. Contrairement aux mécanismes de chiffrement par bloc, ces algorithmes ne garantissent généralement pas l'intégrité des messages, ce qui signifie qu'un attaquant peut tenter d'altérer les données transmises sans être détecté (ANSSI, 2020, p. 15). Toutefois, lorsqu'un chiffrement par flot est connu sans mécanisme de rétroaction, le déchiffrement d'un message altéré ne fournit pas d'informations supplémentaires exploitables pour affaiblir la sécurité du système (ANSSI, 2020, p. 15). L'analyse de la robustesse d'un tel algorithme repose donc principalement sur l'hypothèse que l'adversaire peut observer le flot de sortie produit par l'algorithme et tenter d'en déduire des motifs exploitables (ANSSI, 2020, p. 15).

Chiffrement asymétrique

En réponse aux défis posés par le chiffrement symétrique, le chiffrement asymétrique a émergé comme une alternative viable. Simmons (1979) souligne que les systèmes asymétriques permettent de résoudre des situations impossibles à traiter avec la cryptographie symétrique, comme la communication sécurisée entre deux parties sans échange au préalable de clé ou l'authentification de messages dont le contenu est public (Simmons, 1979, p. 18). Contrairement aux systèmes traditionnels, les schémas asymétriques, introduits notamment par Diffie et Hellman en 1976, reposent sur l'utilisation de paires de clés, l'une publique et l'autre privée, rendant inutile la nécessité d'un échange secret préalable (Simmons, 1979, p. 15). Au sein des systèmes asymétriques, la gestion des clés se fait au moyen de la gestion des bi-clés,

composées d'une clé publique et d'une clé privée, et présente des avantages notables, mais soulève également des exigences spécifiques (ANSSI, 2020, p. 54). Dans ces systèmes, la clé privée n'est jamais partagée, ce qui élimine le problème de distribution de clé. Chaque entité détient une clé privée secrète et diffuse librement sa clé publique. Cela rend la gestion des clés intrinsèquement plus scalable et mieux adaptée aux architectures à grande échelle. Toutefois, l'usage d'une bi-clé unique pour plusieurs fonctions, comme le chiffrement et la signature, est également à proscrire, car il expose à des attaques croisées entre les différents usages (ANSSI, 2020, p. 36). Il est donc impératif d'affecter une bi-clé à une clé unique et de générer une nouvelle bi-clé pour chaque type d'opération cryptographique. Un point particulièrement sensible dans la gestion des clés asymétriques concerne les clés racine, souvent utilisées dans les infrastructures à clé publique (PKI). Ces clés doivent être générées, stockées et utilisées dans des conditions de sécurité renforcées, car leur compromission mettrait en danger l'ensemble de la hiérarchie de confiance qu'elles soutiennent (ANSSI, 2020, p. 54). L'utilisation de mécanismes cryptographiques conformes au référentiel est donc essentielle pour toutes ces opérations critiques.

L'avancée des systèmes asymétriques a permis le développement de nouveaux mécanismes d'authentification, sécurisant non seulement la confidentialité des messages, mais aussi leur intégrité et leur origine. Parmi les systèmes les plus connus, RSA utilise la factorisation de grands nombres premiers, tandis que l'échange de clé de Diffie-Hellman exploite le problème du logarithme discret pour établir une clé secrète partagée entre deux parties sans qu'un tiers puisse l'intercepter (ANSSI, 2020, p. 21). Les schémas basés sur la factorisation de grands nombres premiers et ceux utilisant le problème du sac à dos exploitent la complexité computationnelle de certaines opérations pour assurer une sécurité accrue (Simmons, 1979, p. 16). Le problème du sac à dos consiste à déterminer si un ensemble donné de poids peut être combiné de manière à atteindre une somme cible spécifique (Simmons, 1979, p. 16). Ce problème est fondamentalement difficile à résoudre lorsque le nombre d'éléments augmente, car il nécessite d'examiner de nombreuses combinaisons possibles pour trouver la solution optimale. Le chiffrement asymétrique repose donc sur des problèmes mathématiques complexes et difficiles à inverser en l'absence de clé privée (ANSSI, 2020, p. 47). L'intérêt principal de ces méthodes réside dans leur capacité à assurer la confidentialité des échanges même sans clé préalablement partagée entre les parties communicantes. Un autre domaine clé du chiffrement asymétrique est la signature numérique, qui permet d'assurer l'intégrité et l'authenticité d'un message sans nécessité de secret partagé (ANSSI, 2020, p. 49). Contrairement au chiffrement, qui protège la confidentialité, la signature numérique assure que le

message provient bien de l'émetteur déclaré et qu'il n'a pas été altéré (ANSSI, 2020, p. 27). Elle repose sur l'utilisation de la clé privée pour signer un message et de la clé publique pour vérifier cette signature.

En résumé, le chiffrement asymétrique permet une communication sécurisée sans partage de secret au préalable et offre des garanties supplémentaires en matière d'authentification. Sa gestion repose sur la séparation des rôles entre la clé publique et la clé privée, mais exige l'existence d'un cadre de confiance de la vérification des clés publiques, ce qui donne toute son importance aux infrastructures à clé publique. Il s'agit donc d'un modèle puissant, mais qui nécessite une gestion rigoureuse des identités et des autorisations pour assurer une sécurité cryptographique complète.

Chiffrement symétrique versus asymétrique

En pratique, il est recommandé d'utiliser des systèmes hybrides combinant les avantages des deux approches : une clé de session aléatoire est générée et utilisée pour chiffrer les données avec un algorithme symétrique, tel que DES, tandis que cette clé de session est elle-même chiffrée avec un algorithme asymétrique avant d'être transmise (ANSSI, 2020, p. 26). La gestion des clés est un élément central de la cryptographie, puisqu'elle assure la confidentialité et l'intégrité des communications. En cryptographie symétrique, la sécurisation des clés secrètes est un défi majeur, notamment en raison des risques d'interception lors de leur distribution. Des architectures de gestion des clés ont été développées pour pallier ces difficultés, notamment en utilisant des protocoles de renouvellement et de dérivation des clés afin de minimiser les impacts d'une compromission (ANSSI, 2020, p. 34). En cryptographie asymétrique, la problématique se concentre sur la certification des clés publiques, qui doit être réalisée par des autorités de confiance appelées autorités de certification afin de garantir que chaque clé publique appartient bien à son propriétaire légitime (ANSSI, 2020, p. 36). L'infrastructure de gestion des clés publiques est ainsi un élément important pour l'utilisation sécurisé de la cryptographie asymétrique.

<table>
<tr><th colspan="2">Service</th><th>Cryptographie symétrique</th><th>Cryptographie asymétrique</th></tr>
<tr><td colspan="2" rowspan="2">Confidentialité</td><td rowspan="2">Chiffrement conventionnel par bloc (A.1.1.1)
ou par flot (A.1.1.2)</td><td>Chiffrement à clé publique (A.2.1)</td></tr>
<tr><td>Échange de clé (A.2.3)</td></tr>
<tr><td colspan="2">Intégrité</td><td rowspan="2">Code d'authentification de message (A.1.3)</td><td rowspan="3">Signature numérique (A.2.2)</td></tr>
<tr><td rowspan="2">Authentification</td><td>de données</td></tr>
<tr><td>d'entités</td><td>Défi-réponse (A.1.4)</td></tr>
<tr><td colspan="2">Non-répudiation</td><td>Aucune primitive</td></tr>
</table>

Tableau 19 Primitives cryptographiques offrant un service donné (ANSSI, 2020, p. 38)

Le tableau ci-dessus présente une synthèse qui compare les services de sécurité assurés respectivement par la cryptographie symétrique et la cryptographie asymétrique. Ces services incluent la confidentialité, l'intégrité, l'authentification, à la fois des données et des entités, ainsi que la non-répudiation. Pour chaque service, le tableau indique les mécanismes cryptographiques associés selon le type de cryptographie employé. En ce qui concerne la confidentialité, la cryptographie symétrique utilise soit un chiffrement par bloc soit un chiffrement par flot (ANSSI, 2020, p. 38). Ces deux techniques reposent sur une clé secrète partagée entre les parties. À l'inverse, la cryptographie asymétrique assure la confidentialité à l'aide d'un chiffrement à clé publique, ce qui permet de chiffrer des données sans avoir à partager un secret au préalable. Elle permet également l'établissement d'un secret partagé via des protocoles d'échange de clés, comme Diffie-Hellman (ANSSI, 2020, p. 38). Pour assurer l'intégrité des données, la cryptographie symétrique repose sur l'utilisation de codes d'authentification de message, plus connu sous le nom de MAC[60] (ANSSI, 2020, p. 44). Ces codes permettent de vérifier que les données n'ont pas été altérées pendant la transmission. Dans les systèmes asymétriques, l'intégrité est assurée par la signature numérique, qui permet également de vérifier l'origine du message. En matière d'authentification, la cryptographie symétrique distingue deux cas : l'authentification des données, assurée par les codes d'authentification de message, et l'authentification des entités, souvent mise en œuvre via un mécanise de défi-réponse. Ce dernier consiste à prouver l'identité d'un utilisateur ou d'un système sans révéler la clé secrète. En cryptographie asymétrique, l'authentification des entités et des messages est intégrée dans l'usage des signatures numériques, qui reposent sur l'utilisation d'une paire de clés, publique et privée, pour prouver l'identité du signataire. Enfin, au niveau de la non-répudiation, c'est « un service visant à

[60] MAC est un acronyme pour Message authentication code

éviter qu'une entité puisse nier avoir effectué une certaine action. Le principal mécanisme de non-répudiation est la signature à clé publique, une signature sur un message devant en général rester valide, même si le signataire change ensuite d'avis » (ANSSI, 2020, p. 38). La cryptographie symétrique ne possède aucune primitive permettant de garantir ce service, car une même clé est partagée par toutes les parties. Il est donc impossible de prouver qu'un message provient d'un utilisateur spécifique. En revanche, la cryptographie asymétrique, via les signatures numériques, offre une solution robuste à cette problématique, en permettant de prouver qu'un message a bien été signé par une entité donnée et qu'elle ne peut en nier l'origine. Ce tableau illustre donc clairement les complémentarités entre cryptographie symétrique et asymétrique, chacun apportant des garanties spécifiques pour les différents aspects de la sécurité des échanges d'information.

Tokenisation

La tokenisation est une technique de protection des données sensibles qui consiste à remplacer un élément confidentiel, comme un numéro de carte bancaire, par un substitut sans valeur exploitable hors de son système d'origine (Mogull, 2010, p. 5). Cette méthode, qui prend de plus en plus d'importance dans les SBT, répond aux exigences strictes des standards du « Payment Card Industry » publiés dans la version de 2008 du « Data Security Standard », notamment en ce qui concerne le stockage, la transmission et le traitement du PAN[61] (Stapleton et Poore, 2011, p. 91). « Un PAN est composé de 4 éléments : 1) l'identifiant du secteur principal (MII), 2) le numéro d'identification de l'émetteur (IIN), 3) un numéro de compte (AN) et 4) un chiffre de contrôle basé sur la formule Luhn » (Stapleton et Poore, 2011, p. 92). En substituant les PAN par des jetons, ou « tokens », au plus tôt dans le flux transactionnel, les banques peuvent réduire leur exposition aux risques de fuite de données.

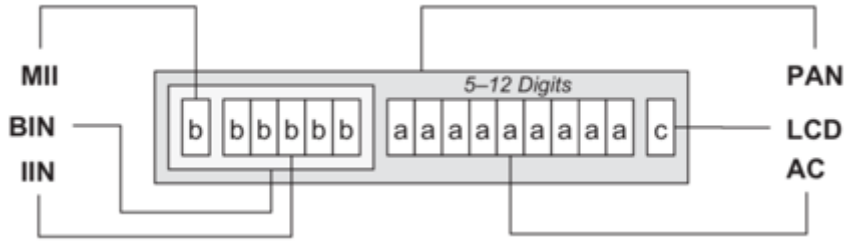


Figure 67 Présentation du PAN (Stapleton et Poore, 2011, p. 92)

[61] PAN est un acronyme pour Primary Account Number

Contrairement au chiffrement, le token ne contient aucune information calculable ou dérivable à partir de la donnée du PAN qu'il remplace, ce qui en fait une mesure de sécurité robuste contre les attaques par rétro-ingénierie (Mogull, 2010, p. 21). Toutefois, pour garantir cette sécurité, il est important que le processus de génération des tokens ne produit jamais deux fois le même token (Mattsson, 2010, p. 1) pour deux PAN distincts. Dans sa forme la plus élémentaire, le modèle de base de la tokenisation repose sur une architecture centralisée constituée de trois composants principaux : une application cliente, comme un système de point de vente ou un service bancaire, un serveur de tokenisation et une base de données sécurisée des tokens (Mogull, 2010, p. 9). Lorsqu'un PAN est reçu par une application, il est immédiatement transmis au serveur de tokenisation, qui vérifie d'abord si un token correspondant à cette valeur a déjà été généré (Mogull, 2010, p. 9). Si tel est le cas, le serveur retourne le token existant, sinon, il génère un nouveau token, enregistre la correspondance dans la base de données des tokens, puis retourne le token à l'application appelante (Mogull, 2010, p. 9). La base de correspondance, centrale dans ce modèle, contient les paires PAN-token et constitue ainsi le cœur de la sécurité du système. Le serveur de tokenisation joue donc un double rôle : d'une part, il assure la logique de transformation entre données sensibles (PAN) et tokens, d'autre part, il applique des règles de sécurité (Mogull, 2010, p. 9).

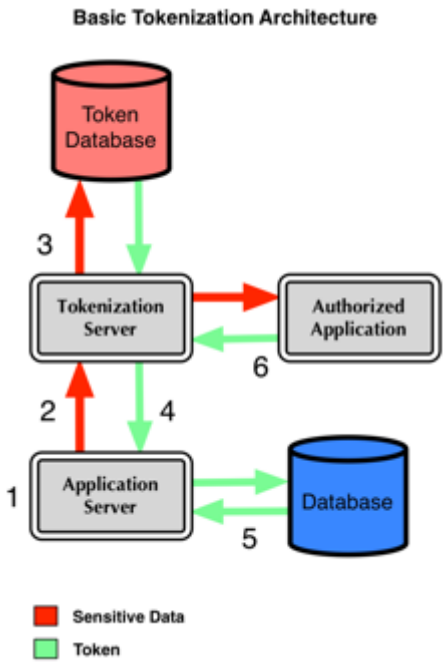


Figure 68 Architecture de base de la tokenisation (Mogull, 2010, p. 9)

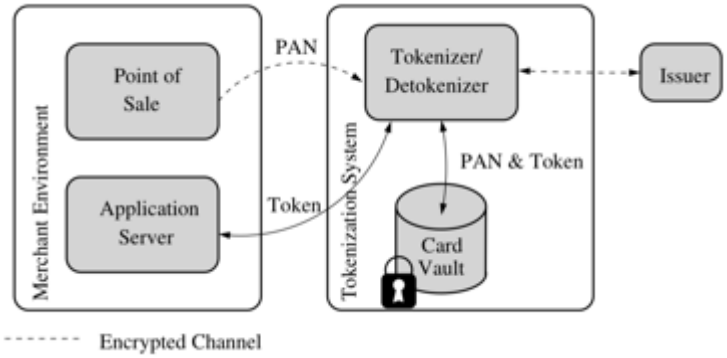


Figure 69 Architecture des systèmes de tokenisation (Díaz-Santiago et al., 2016, p. 3)

Sur le plan cryptographique, les mécanismes de tokenisation peuvent reposer sur diverses méthodes : séquence incrémentale, générateur de nombres pseudo-aléatoires (PRNG), fonctions de hachage et de masquage ou encore les schémas de chiffrement symétrique ou asymétrique (Stapleton et Poore, 2011, p. 93-97). La tokenisation joue un rôle important dans la minimisation du risque en limitant le nombre de points vulnérables dans l'infrastructure bancaire. En ne stockant que les tokens dans les bases de données applicatives et en centralisant les PAN dans un système cloisonné, les institutions financières réduisent drastiquement leur surface d'attaque. De plus, une tokenisation bien conçue facilite la gestion du cycle de vie des données, notamment dans les environnements de test, où l'accès à des données réalistes sans révéler d'informations sensibles est souvent requis (Mattsson, 2010, p. 3).

Cependant, l'implémentation de la tokenisation pose aussi un ensemble de défis organisationnels et opérationnels. Elle nécessite une gestion rigoureuse des clés cryptographiques, des protocoles d'échange sécurisés et une infrastructure résiliente apte à supporter des volumes de transactions important (Stapleton et Poore, 2011, p. 97). Dans les solutions dépendant d'un fournisseur externe, les enjeux de latence, disponibilité, transparence et de contrôle du risque deviennent critiques (Mattsson, 2010, p. 4). Dans ce contexte, la tokenisation interne est privilégiée pour des raisons de gouvernance, de responsabilité juridique et de contrôle opérationnel (Mattsson, 2010, p. 4-5).

Enfin, plusieurs études insistent sur l'importance de coupler la tokenisation avec d'autres techniques de protection des données, telle que le chiffrement et l'anonymisation, pour renforcer la sécurité globale du système et assurer la conformité avec les normes internationales de gestion des risques (Mattsson, 2010, p. 3 ; Stapleton et Poore, 2011, p. 91). La combinaison de ces méthodes, lorsqu'elle est mise en œuvre

selon des standards rigoureux de gestion des clés et d'auditabilité, constitue un socle de protection contre la fraude, le vol de données et les atteintes à la vie privée dans les environnements bancaires.

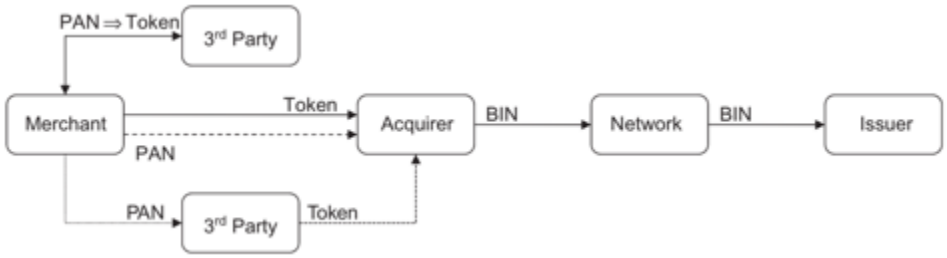


Figure 70 Flux de tokenisation (Stapleton et Poore, 2011, p. 95)

Authentification monofactorielle

Parmi les méthodes d'authentification les plus anciennes et répandues, celle fondée sur le mot de passe constitue le paradigme dominant depuis les débuts de l'informatique bancaire. Elle repose sur la possession d'un secret partagé, une chaîne de caractères connus de l'utilisateur et du système, qui est utilisé pour établir l'identité de l'usager (Sandhu et Samarati, 1996, p. 1). Cette approche, bien que rudimentaire, a été massivement adoptée en raison de sa simplicité d'implémentation, de son faible coût et de sa compatibilité avec la quasi-totalité des infrastructures informatiques existantes (Sandhu et Samarati, 1996, p. 1). Cependant, cette technique souffre de nombreuses faiblesses structurelles, car les mots de passe peuvent être devinés, interceptés, partagés, ou tout simplement oubliés (Sandhu et Samarati, 1996, p. 1). Les politiques de gestion des mots de passe, forçant les utilisateurs à les changer fréquemment, à choisir des combinaisons complexe ou à ne pas les réutiliser, finissent souvent par crée une charge cognitive excessive, contre-productive du point de vue de la sécurité (Sandhu et Samarati, 1996, p. 1).

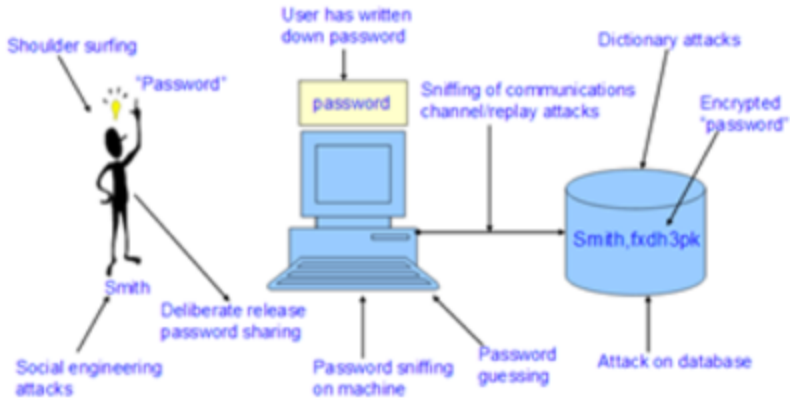


Figure 71 Vulnérabilités dans l'authentification par mot de passe (Farik et al., 2024, p. 2)

Ces constats sont corroborés par Lal et al., qui soulignent que la force d'un mot de passe dépend principalement de sa longueur, de sa cardinalité (diversité des caractères utilisés) et de son entropie, c'est-à-dire la quantité d'information qu'il contient d'un point de vue probabiliste (Lal *et al.*, 2024, p. 2). Un mot de passe de huit caractères, même avec une grande cardinalité, peut être craqué en quelques secondes par un superordinateur. De surcroît, l'humain étant le maillon faible, les attaques par ingénierie sociale, l'observation ou encore l'hameçonnage contournent aisément les barrières purement techniques. Face à ces limites, plusieurs recommandations sont formulées : promouvoir des mots de passe de 12 caractères ou plus avec une cardinalité élevée, limiter le nombre de tentatives, interdire les mots du dictionnaire et éduquer les utilisateurs à reconnaître les tentatives de fraudes (Farik *et al.*, 2024, p. 3). L'usage de mots de passe graphiques ou de mécanismes d'entrée plus intuitifs est également évoqué comme piste d'innovation pour réduire la charge mémorielle sans sacrifier la sécurité (Farik *et al.*, 2024, p. 3).

Authentification double facteur (2FA)

Face aux limites structurelles de l'authentification monofactorielle, les SBT ont progressivement adopté des approches fondées sur la combinaison de plusieurs facteurs indépendants, conduisant à l'émergence des schémas à deux facteurs, puis multi-facteurs. Cette évolution s'inscrit dans un souci croissant de renforcer la sécurité des interactions numériques, tout en maintenant un équilibre acceptable entre ergonomie, coût et robustesse cryptographique.

D'une part, une alternative plus robuste à l'authentification par mot de passe seul est l'utilisation de cartes à puces, un dispositif physique contenant un élément cryptographique unique (Farik *et al.*, 2024, p. 3).

Dans ce schéma, l'authentification porte non pas sur l'utilisateur en tant que tel, mais sur le jeton qu'il possède. Chaque carte contient une clé secrète inviolable, utilisée pour répondre à un défi cryptographique envoyé par le système. Cette méthode est plus difficile à compromettre, à condition que la clé privée ne quitte jamais la carte et que les tentatives de lecture physique soient neutralisées par des mécanismes de destruction automatique (Sandhu et Samarati, 1996, p. 1).

D'autre part, l'authentification à deux facteurs repose sur l'idée que la probabilité d'accès non autorisé diminue considérablement si l'usurpateur doit simultanément compromettre des classes distinctes d'éléments d'authentification : 1) quelque chose que l'utilisateur connaît (ex : code PIN) et 2) quelque chose qu'il possède (ex : carte à puce) (Ometov *et al.*, 2018, p. 2). Cette combinaison s'observe notamment dans les guichets automatiques bancaire, où l'insertion d'une carte bancaire (possession) doit être accompagnée d'un code PIN (connaissance) (Ometov *et al.*, 2018, p. 3). L'ajout du second facteur vise à mitiger les vulnérabilités spécifiques à chaque type d'élément. Par exemple, alors qu'un mot de passe peut être deviné ou volé par ingénierie sociale, une carte physique peut être perdue ou copiée. La combinaison des deux rend une compromission simultanée statistiquement plus rare (Ometov *et al.*, 2018, p. 3).

Authentification multifactorielle (MFA)

En vue d'améliorer les méthodes d'authentification, les chercheurs et institutions ont favorisé le recours à de schémas multi-facteurs. L'authentification multifactorielle est une stratégie de sécurité qui exige l'utilisation de plus de deux facteurs d'authentification distincts pour vérifier l'identité d'un utilisateur. Ces facteurs incluent un élément de connaissance (mot de passe), un élément de possession (téléphone, clé de sécurité) et un élément biométrique (empreinte digitale, reconnaissance faciale) (Sim *et al.*, 2019, p. 1). Contrairement à l'authentification simple par mot de passe, l'utilisation de la MFA réduit considérablement les risques liés aux attaques basés sur le vol d'identifiants en raison de l'accès plus complexe aux comptes même si un criminel vole un mot de passe. Cette stratégie vise non seulement à prévenir les intrusions, mais aussi à établir une preuve plus robuste et non transférable de l'identité de l'utilisateur. L'intérêt du MFA réside dans sa résilience accrue face à l'usurpation d'identité. En combinant plusieurs dimensions, le système multiplie les barrières d'entrée et complexifie les tentatives d'accès frauduleux. Néanmois, le coût d'implémentation, la nécessité de capteurs spécifiques (lecteurs biométriques, caméras, etc.) et les problèmes d'acceptabilité sociale, notamment en matière de vie privée, freinent encore une adoption généralisée dans les SBT.

Figure 72 Caractéristiques de la biométrie (Syed Idrus et al., 2013, p. 9)

Par ailleurs, les méthodes biométriques reposent sur l'analyse des caractéristiques physiologiques ou comportementales propres à chaque individu, telles que les empreintes digitales, l'iris ou la voix (Syed Idrus *et al.*, 2013, p. 8). Ce type de méthode réfère donc à ce qu'un utilisateur est, soit une composante clé du MFA, et présente un avantage en sa non-répudiation, puisque la biométrie ne peut être oubliée, perdue ou partagée comme le serait un mot de passe ou une carte physique (Syed Idrus *et al.*, 2013, p. 9). Sur le plan technique, les performances des systèmes biométriques sont mesurées en fonction de deux indicateurs : le taux de fausses acceptations[62] et le taux de faux rejets[63] (Ometov *et al.*, 2018, p. 4). L'idéal est d'atteindre un équilibre entre ces deux extrêmes, souvent représenté par le taux d'erreurs équivalent[64], c'est-à-dire le « point où FAR et FRR sont égaux » (Ometov *et al.*, 2018, p. 12). Or, dans des environnements à fort enjeu de sécurité comme le secteur bancaire, une trop grande tolérance aux faux positifs peut avoir de grosses conséquences. À l'inverse, une exigence trop stricte entraîne des frustrations légitimes pour les utilisateurs, nuisant à l'expérience utilisateur qui joue un grand rôle dans les décisions de la haute direction.

[62] Le taux de fausses acceptations sera référé en tant qu'acronyme FAR

[63] Le taux de faux rejets sera référé en tant qu'acronyme FFR

[64] Le taux d'erreurs équivalent sera référé en tant qu'acronyme EER

Figure 73 Principaux défis opérationnels du MFA (Ometov et al., 2018, p. 9)

Ometov et al. (2018) identifient six grandes catégories de contraintes qui, interconnectées, conditionnent la viabilité, l'adoption et la performance des systèmes MFA. Le premier défi concerne l'usage, c'est-à-dire la capacité d'un système MFA à s'adapter aux besoins et aux limitations de l'utilisateur final pour répondre aux perspectives d'efficience, d'efficacité et de préférence utilisateur (Ometov *et al.*, 2018, p. 8). Dans le contexte bancaire, où les populations clientes sont hétérogènes, il est impératif de garantir que les mécanismes d'authentification soient à la fois efficaces, intuitifs et inclusifs. Le second enjeu porte sur l'intégration technologique. L'implémentation de solutions MFA requiert une harmonisation interopérable des logiciels hétérogènes, une dépendance auprès des fournisseurs ainsi qu'un enjeu de confiance et de fiabilité des solutions qui ne sont pas « open-source » (Ometov *et al.*, 2018, p. 10). Ces défis sont d'autant plus plus complexes dans les SBT fréquemment caractérisés par une interopérabilité limitée. Sur le plan de la gestion de la vie privée et de la sécurité, des enjeux liés à la captation, au traitement, à la conservation de données sensibles, au « spoofing », à l'interception des communications et à l'ingénierie sociale sont soulevés (Ometov *et al.*, 2018, p. 10-11). Puis, à cela s'ajoute la question de la robustesse, comprise comme la résistance du système face aux perturbations environnementales et aux imprécisions techniques (Ometov *et al.*, 2018, p. 11). Or, un système dont la robustesse est faible peut générer une multiplication des échecs d'authentification ou des rejets d'utilisateurs légitimes (FAR & FRR), ce qui fragilise la confiance dans la technologie déployée (Ometov *et al.*, 2018, p. 11-12).

En somme, l'authentification 2FA/MFA ne constitue pas une panacée, mais un cadre adaptatif dans lequel le niveau de sécurité peut être modulé en fonction du risque associé à l'action effectuée (transaction, accès à des données sensibles, etc.). Dans le contexte bancaire, son intégration efficace suppose une

orchestration dynamique des facteurs disponibles, appuyée par une analyse contextuelle (localisation, appareil utilisé, comportement habituel), ouvrant la voie à une authentification dite continue.

Protocole d'authentification dans les SBT

Après avoir exposé les différentes méthodes d'authentification utilisés dans les systèmes bancaires traditionnels, il importe maintenant d'exposer les protocoles qui sous-tendent techniquement ces méthodes dans les environnements bancaire numériques. Ces protocoles s'érigent comme étant l'infrastructure invisible par laquelle les systèmes valident l'identité des utilisateurs et des machines en encadrant la transmission sécurisée des informations d'authentification. Les sous-sections qui suivent présentent trois protocoles de la chronologie des standards et protocoles couramment utilisés dans les SBT : SAML, FIDO et Kerberos.

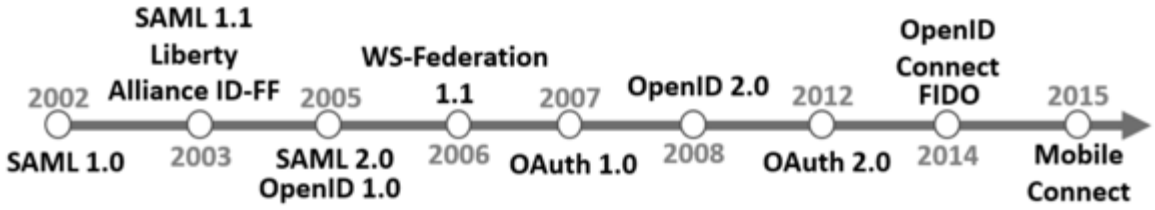


Figure 74 Chronologie des standards d'identification et authentification (Kiourtis et al., 2023, p. 38)

Protocole Security Assertion Markus Language (SAML)

Dans les SBT, le recours à des standards d'identification fédérée s'est imposé comme une solution pour gérer l'authentification sécurisée des clients et des employés à travers des domaines organisationnels multiples. Le protocole SAML constitue l'un des piliers de cette fédération d'identité, en que standard ouvert basé sur XML conçu pour faciliter l'échange sécurisé d'informations d'authentification et d'autorisation entre un fournisseur d'identité et un fournisseur de service (Kiourtis *et al.*, 2023, p. 38). Le fonctionnement de SAML repose sur un modèle tripartite, structuré autour de trois rôles fondamentaux : le principal, souvent un utilisateur final, le fournisseur d'identité et le fournisseur de service (Kiourtis *et al.*, 2023, p. 38). Lorsqu'un utilisateur tente d'accéder à un service, le fournisseur de service délègue l'authentification au fournisseur d'identité, qui, une fois la vérification effectuée, renvoie une assertion SAML signée numériquement contenant des informations sur l'identité de l'utilisateur et les droits associés (Kiourtis *et al.*, 2023, p. 38). Cette assertion agit comme une preuve d'identité portable, compréhensible par différents systèmes, et permet ainsi d'établir une décision d'accès fondée sur une

identité reconnue et vérifiée par une autorité de confiance. L'architecture de SAML repose sur quatre éléments clés : les assertions, les protocoles, les liaisons et les profils (Kiourtis *et al.*, 2023, p. 38).

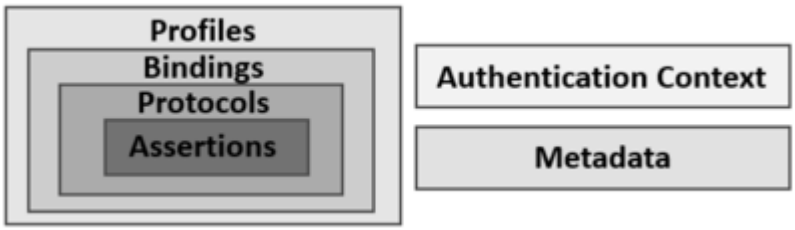


Figure 75 Concepts SAML de base (Kiourtis et al., 2023, p. 38)

Les assertions sont des déclarations XML structurées contenant des informations sur le sujet, telles que l'authentification, les attributs ou les autorisations (Maler et Hughes, 2005, p. 8-10). Les protocoles définissent la manière dont les assertions sont demandées et échangées (Maler et Hughes, 2005, p. 8-10). Les liaisons spécifient les mécanismes de transport des messages, tandis que les profils permettent d'adapter SAML à des cas d'usage spécifiques, par exemple l'authentification Web unique (SSO) dans un contexte bancaire (Maler et Hughes, 2005, p. 8-10). De plus, deux autres concepts SAML sont importants, soit les métadonnées et le contexte d'authentification. Le contexte d'authentification est « utilisé dans une déclaration d'authentification globale que quelqu'un a fourni pendant l'authentification, tandis que les métadonnées spécifient les moyens de diffuser les relatifs à la configuration entre les parties SAML » (Kiourtis *et al.*, 2023, p. 38-39).

En somme, SAML offre aux institutions bancaires un standard mature, extensible et interopérable pour la gestion fédérée des identités, répondant aux exigences croissantes en matière de sécurité, de conformité et d'ouverture des services. Son adoption dans les SBT illustre la transition progressive vers des architectures orientées services, dans lesquelles la confiance est assurée non plus uniquement au niveau local, mais à travers un réseau de partenaires fiables certifiés. Toutefois, SAML présente certaines limitations, notamment en termes de complexité d'implémentation et de performances, ce qui a conduit à l'adoption de solutions plus légères et flexibles comme OpenID Connect.

Protocole Fast IDentity Online (FIDO)

Les institutions financières adoptent massivement la MFA pour se conformer aux normes de cybersécurité et protéger les informations sensibles. Parmi les méthodes les plus courantes, on retrouve l'envoi de codes

à usages unique par SMS ou courriel, les applications d'authentification comme Google Authenticator et Microsoft Authenticator, ainsi que les clés de sécurité physiques utilisant le standard FIDO. Dans une perspective de durabilité des services informatiques et de réponse aux faiblesses structurelles des méthodes d'authentification classiques, le standard FIDO[65], créé en 2013 par un consortium d'acteurs majeurs de l'industrie tels que PayPal, Lenovo et NokNok Labs, propose une alternative fondée sur les clés asymétriques qui permet « d'authentifier en continu les utilisateurs avec une authentification implicite basée sur le contexte de l'utilisateur et une authentification multimodale » (Kim *et al.*, 2018, p. 3).

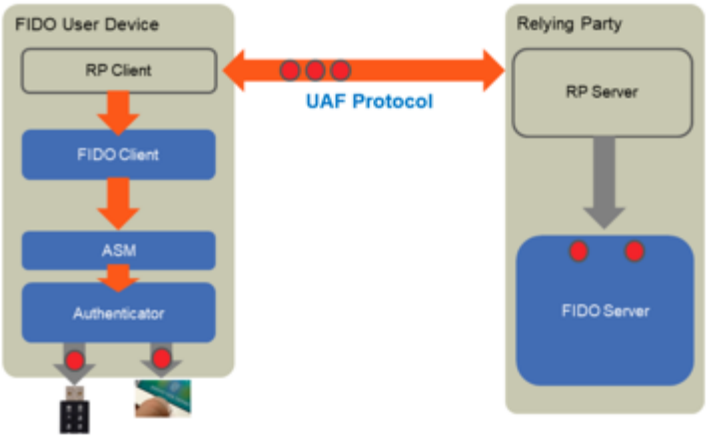


Figure 76 Architecture FIDO de haut niveau (Kim et al., 2018, p. 3)

Le protocole FIDO repose sur une architecture à plusieurs couches, distinguant le FIDO Client, souvent une application mobile ou un navigateur, le FIDO Server et l'authentificateur, matériel ou logiciel (Kim *et al.*, 2018, p. 3). L'architecture fonctionnelle du protocole UAF[66] repose, quant à elle, sur l'interaction entre deux entités distinctes : le dispositif de l'utilisateur (FIDO User Device) et la partie de confiance distante Relaying Party) (Kim *et al.*, 2018, p. 3). Du côté de l'utilisateur, le processus d'authentification débute par une demande d'accès émise par l'application ou le navigateur, appelée RP Client (Kim *et al.*, 2018, p. 3). Cette requête est relayée au FIOD Client, qui orchestre les messages du protocole UAF (Kim *et al.*, 2018, p. 3). Le FIDO Client transmet les instructions à un module intermédiaire, le Authenticator Specific Module, responsable de l'interface avec le dispositif d'authentification proprement dit l'authentificateur (Kim *et al.*, 2018, p. 3). Une fois l'identité de l'utilisateur confirmée localement, l'authentificateur génère une signature numérique à l'aide d'une clé privée conservée de manière sécurisée au sein du terminal (Kim *et*

[65] FIDO est un acronyme pour Fast IDentity Online

[66] UAF est un acronyme pour Universal Authentication Framework

al., 2018, p. 3). La réponse signée est ensuite transmise via le protocole UAF au serveur du fournisseur de service (RP Service), puis au FIDO Server, qui dispose de la clé publique associée (Kim *et al.*, 2018, p. 3). Si la signature est valide, l'authentification est confirmée et l'accès est autorisé (Kim *et al.*, 2018, p. 3).

Protocole Kerberos

Kerberos est un protocole d'authentification centralisé qui repose sur un chiffrement symétrique (El-Emam *et al.*, 2009, p. 1). Développée initialement au Massachusetts Institute of Technology dans le cadre du projet Athena, Kerberos a évolué à travers différentes versions, la plus utilisée étant la version 5 (El-Emam *et al.*, 2009, p. 1). Son architecture repose sur un tiers de confiance centralisé, le « Key Distribution Center », qui regroupe deux entités principales : le serveur d'authentification et le serveur de tickets (El-Emam *et al.*, 2009, p. 2). Le protocole Kerberos vise à permettre à un client de prouver son identité à plusieurs serveurs d'application au sein d'un même domaine, sans avoir à transmettre son mot de passe à chaque fois. Il s'appuie pour cela sur l'émission de tickets de session chiffrés à durée de vie limitée, obtenues en plusieurs étapes. Lors d'une première phase, le client soumet une requête d'authentification au serveur d'authentification afin d'obtenir un ticket de service auprès du serveur de tickets (El-Emam *et al.*, 2009, p. 2). Le serveur répond par un « ticket-granting ticket » et un composant chiffré contenant une clé de session partagée entre le client et le serveur de tickets (El-Emam *et al.*, 2009, p. 2). Dans une seconde phase, ce ticket est présenté au serveur de tickets avec un authentificateur temporaire afin de recevoir un ticket de service destiné au serveur applicatif (El-Emam *et al.*, 2009, p. 1=2). Enfin, dans la troisième phase, le client présente ce ticket au serveur de destination pour accéder au service, accompagné d'un second authentificateur chiffré à l'aide de la clé de session échangée précédemment (El-Emam *et al.*, 2009, p. 2).

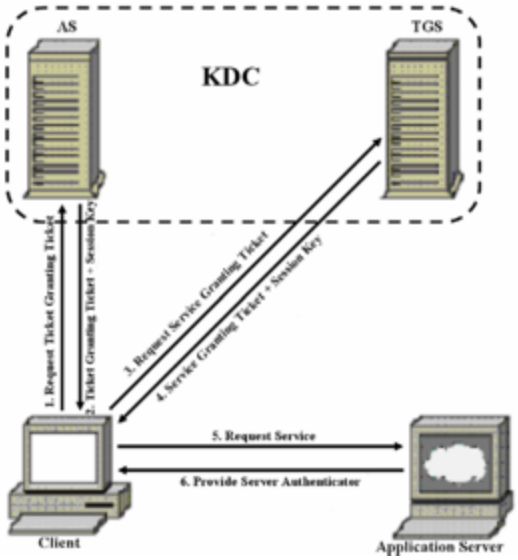


Figure 77 Vue d'ensemble des actions Kerberos (El-Emam et al., 2009, p. 2)

Contrôle d'accès discrétionnaire (DAC)

Le modèle DAC, introduit dès la fin des années 1960 par Larson et formalisé par la suite par Graham, Denning et le trio Harrison-Ruzzo-Ullman, repose (Kashmar *et al.*, 2020, p. 3) sur la capacité d'un utilisateur à déléguer ses droits d'accès à d'autres entités, en fonction de la propriété ou de la responsabilité d'une ressource (Sandhu et Samarati, 1996, p. 1). Dans ce modèle, le propriétaire d'un objet, typiquement un fichier ou une ressource, définit librement les droits d'accès qu'il accorde à d'autres utilisateurs (Kashmar *et al.*, 2020, p. 3). Ces droits sont généralement représentés sous forme de matrices de contrôle d'accès (ACM), de listes de contrôle d'accès (ACL) ou de liste de capacités (CL) (Kashmar *et al.*, 2020, p. 3). DAC offre ainsi une grande flexibilité dans l'attribution des permissions, ce qui peut se révéler pertinent dans les environnements bancaires où certains rôles nécessitent une délégation ponctuelle ou temporaire de droits. Toutefois, cette souplesse s'accompagne d'importants défis en matière de sécurité, notamment une difficulté à garantir la cohérence des permissions et une vulnérabilité accrue aux chevaux de Troie ou à la propagation incontrôlée des privilèges (Kashmar *et al.*, 2020, p. 3). Le modèle DAC souffre en effet de ce que l'on appelle le « safety problem », c'est-à-dire l'incapacité à garantir formellement qu'un droit d'accès ne sera pas acquis ou propagé de manière non autorisée dans le système (Ausanka-Crues, 2006, p. 3). Ce problème découle de l'absence de contraintes sur la copie d'informations d'un objet à un autre (Ausanka-Crues, 2006, p. 3), rendant difficile la mise en œuvre de politiques de sécurité rigoureuses dans environnements critiques comme les banques.

Contrôle d'accès obligatoire (MAC)

Le modèle MAC a été développé pour imposer un contrôle plus rigide et hiérarchisé. Dans ce cadre, les droits d'accès ne sont pas définis par les utilisateurs, mais par une autorité centrale, selon des politiques de sécurité préétablies (Kashmar *et al.*, 2020, p. 3-4). Chaque sujet et chaque objet est associé à un niveau hiérarchique de sécurité (ex : non classifié, confidentiel, secret et top secret) et les règles d'accès sont régies par des étiquettes de sensibilité (Kashmar *et al.*, 2020, p. 3). Le système d'exploitation, ou un noyau de sécurité dédié, applique alors ces règles pour éviter toute fuite ou corruption de données entre niveaux de sécurité hétérogènes. Dans les SBT, le modèle MAC est particulièrement pertinent pour gérer les flux d'information et les attaques contre leurs systèmes (Kashmar *et al.*, 2020, p. 4). Toutefois, son implantation demeure lourde, car elle exige classification rigoureuse des données et des utilisateurs, une réécriture potentielle des applications pour respecter les contraintes de sécurité, ainsi qu'un effort considérable pour maintenir la cohérence des étiquettes de sensibilité dans le temps (Kashmar *et al.*, 2020, p. 3-4). En effet, bien que le modèle MAC soit considéré plus robuste dans des contextes à haute exigence de confidentialité, comme les environnements militaires ou bancaires exposés à des menaces persistantes, il repose sur un ensemble de composants dits de confiance qui doivent être placés en dehors du modèle de contrôle d'accès lui-même, ce qui pose des problèmes importants en termes de vérification et de résilience (Ausanka-Crues, 2006, p. 2). De surcroît, les propriétés de tranquillité forte ou faible, qui régissent la modification des niveaux de classification, peuvent compromettre la flexibilité du système (Ausanka-Crues, 2006, p. 2). L'application du principe du niveau d'eau élevée tend à surclasser inutilement les objets nouvellement créés, réduisant ainsi l'interopérabilité entre les systèmes et affectant la productivité (Ausanka-Crues, 2006, p. 2).

Contrôle d'accès basé sur les rôles (RBAC)

Enfin, le contrôle d'accès basé sur les rôles s'est imposé comme le modèle privilégié dans les SBT. Dans cette approche, les permissions sont attribuées à des rôles organisationnels (ex : conseiller financier, analyste de crédit, auditeur interne, etc.) et les utilisateurs héritent des droits associés au rôle qui leur est assigné (Chapin *et al.*, 2008, p. 13). Ce découpage favorise une administration centralisée, cohérente et évolutive des droits d'accès, ainsi que facilite les politiques de contrôle d'accès (Kashmar *et al.*, 2020, p. 4). Plusieurs variantes du modèle RBAC existent, telles que le RBAC0 plat, RBAC1 hiérarchique, RBAC2 construit avec des contraintes ou encore RBAC3 symétrique, chacune offrant des niveaux de sophistication croissants dans la gestion des permissions et des héritages de rôles (Kashmar *et al.*, 2020, p. 4). En outre, RBAC représente une avancée notable par rapport à DAC et MAC, en ce qu'il intègre de manière native les

principes de séparation des tâches et du moindre privilège, tout en permettant une administration centralisée des droits et des rôles (Ausanka-Crues, 2006, p. 3-4). Sa granularité transactionnelle, qui permet de définir non seulement les objets accessibles, mais aussi les modes d'accès autorisés, en fait un outil efficace pour assurer l'intégrité des opérations dans les grandes organisations (Ausanka-Crues, 2006, p. 3-4), y compris les intuitions financières. Toutefois, le modèle RBAC présente certaines limites au niveau notamment des environnements hautement dynamiques comme les systèmes bancaires (Kashmar *et al.*, 2020, p. 4). Il est souvent critiqué pour la complexité de son initialisation, la définition d'une structure de rôles cohérente, et pour son manque de réactivité face à des contextes où les permissions doivent être modulées en fonction d'attributs dynamiques tels que l'heure, la localisation ou le comportement de l'utilisateur (Kashmar *et al.*, 2020, p. 4).

OAuth & OAuth 2.0

La nécessité de permettre à des applications tierces d'accéder à certaines ressources des utilisateurs sans compromettre leurs identifiants a conduit à l'adoption de protocoles d'autorisation sécurisés et modulaires. Le protocole OAuth, et plus particulièrement sa version 2.0, s'est imposé comme un standard délégué d'autorisation, conçu pour fournir un mécanise sûr permettant à un utilisateur d'accorder un accès limité à ses ressources protégées, sans divulguer son mot de passe à l'application demandeuse (Kiourtis *et al.*, 2023, p. 39). Cette approche est devenue importante dans les environnements bancaires, notamment dans le cadre de « l'open banking », où les utilisateurs souhaitent partager leurs données financières avec des fintechs, agrégateurs ou services analytiques. OAuth 2.0 fonctionne en attribuant un jeton d'accès à une application tierce autorisée, lui permettant d'accéder à une ressource spécifique au nom de l'utilisateur, pour une durée et un périmètre d'actions définis (Kiourtis *et al.*, 2023, p. 39). Le protocole repose sur une architecture REST API et utilise le format JSON[67] pour octroyer l'accès aux ressources (Kiourtis *et al.*, 2023, p. 39).

[67] JSON est un acronyme pour JavaScript Object Notation

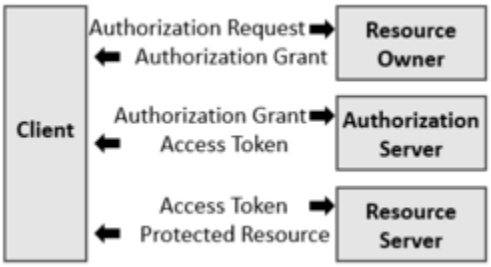


Figure 78: Flux haut niveau de OAuth 2.0 (Kiourtis et al., 2023, p. 39)

Cependant, malgré sa standardisation, OAuth 2.0 présente des limitations importantes en matière d'interopérabilité (Oh et Kim, 2019, p. 1). Le protocole laisse plusieurs composants clés partiellement ou entièrement indéfinis, tel que la structure du jeton, les capacités du serveur d'autorisation ou les paramètres des « endpoints », ce qui entraîne des implémentations divergentes selon les organisations (Oh et Kim, 2019, p. 2). Dans un environnement bancaire interconnecté, cette fragmentation complique l'accès transversal aux ressources réparties entre plusieurs institutions ou domaines de sécurité distincts. Pour remédier à ces obstacles, un cadre appelé « Interoperable OAuth 2.0 Framework », qui introduit une couche d'autorisation virtualisée en amont des serveurs existants, standardise les capacités d'autorisation entre domaines (Oh et Kim, 2019, p. 1). Cette couche fournit un ensemble d'interfaces communes et permet l'émission d'un « Interoperable Access Token », qui possède une portée globale à travers plusieurs domaines de confiance (Oh et Kim, 2019, p. 1). Le principe est de permettre à un client, après avoir authentifié plusieurs propriétaires de ressources dans des domaines distincts, d'accéder à leurs données au moyen d'un seul jeton unifié (Oh et Kim, 2019, p. 4).

Bien qu'OAuth 2.0 ne constitue pas en soi un protocole d'authentification, il s'intègre aisément avec d'autres standards comme OpenID Connect pour permettre une double fonction d'identification et d'autorisation

Authentification unique (SSO)

La multiplication des applications internes, des services numériques client et des interfaces partenaires crée un besoin de rationalisation des mécanismes d'authentification. Le SSO répond à ce besoin en permettant à un utilisateur de s'authentifier une seule fois pour accéder ensuite à plusieurs applications, services ou domaines sans devoir ressaisir ses identifiants à chaque étape (Bazaz et Khalique, 2016, p. 18). Avant l'introduction du SSO, les utilisateurs devaient, et doivent toujours s'il n'est pas disponible,

mémorise une multitude d'identifiants et de mots de passe pour accéder à des services. Cette mémorisation augmente les risques liés à la réutilisation des mots de passe ou à leur simplification excessive, un comportement courant, mais hautement vulnérable aux attaques par devinette ou par hameçonnage (Bazaz et Khalique, 2016, p. 18). Avec le SSO, les utilisateurs n'ont plus à gérer cette complexité, car une seule source d'authentification suffit pour ouvrir l'accès à l'ensemble des ressources auxquelles ils sont autorisés, y compris celles réparties sur plusieurs domaines ou organisations partenaires (Bazaz et Khalique, 2016, p. 18).

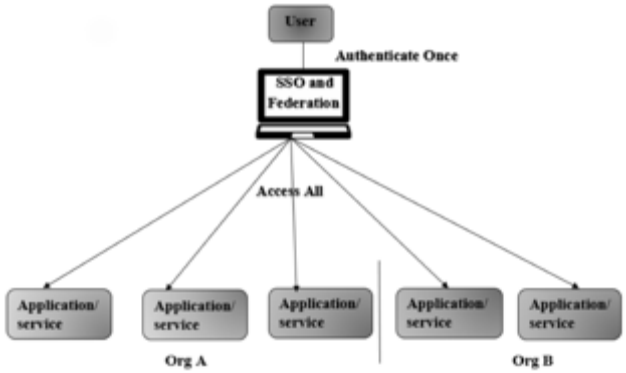


Figure 79 Vue d'ensemble du SSO (Bazaz et Khalique, 2016, p. 18)

L'architecture SSO peut prendre plusieurs formes : 1) la mise en cache sécurisée des informations d'identification côté client, 2) la mise en cache sécurisée des informations d'identification côté serveur, 3) la connexion unique avec un seul jeu d'identifiants, 4) le SSO basé sur les PKI[68] et 5) le SSO basé sur la tokenisation (Bazaz et Khalique, 2016, p. 19). Si la première forme favorise la performance locale, elle est plus vulnérable aux risques de compromission sur des postes non sécurisés (Bazaz et Khalique, 2016, p. 19). À l'inverse, la centralisation des « credentials » côté serveur permet une gouvernance renforcée et une meilleure résilience, au prix d'une dépendance accrue au point d'authentification unique (Bazaz et Khalique, 2016, p. 19). La troisième forme d'architecture est « mieux adaptée pour les environnements homogènes où le tout est géré au sein du réseau complet » (Bazaz et Khalique, 2016, p. 19). Les autres architectures sont, quant à elles, plus adaptées aux environnements bancaires hautement sécurisés. D'une part, le modèle PKI repose sur l'émission de certificats numériques signés par une autorité de certification, qui permet à l'utilisateur de prouver son identité à l'aide d'une signature électronique (Bazaz et Khalique, 2016, p. 19). Lors de chaque demande d'accès, l'utilisateur joint à sa requête son certificat public et signe

[68] PKI est un acronyme pour infrastructure à clé publique

celle-ci avec sa clé privée, le serveur vérifie ensuite la validité de cette signature auprès de l'autorité de certification (Bazaz et Khalique, 2016, p. 19). Le modèle par jeton, quant à lui, repose sur la remise d'un token temporaire après une authentification initiale réussie, que l'utilisateur peut ensuite présenter pour accéder à différents services affiliés, comme dans le cas du protocole Kerberos (Bazaz et Khalique, 2016, p. 19).

En somme, l'usage du SSO soulève des bénéfices, mais aussi des risques. Il est noté que parmi les bénéfices se trouve : l'augmentation de la productivité des usagers, une administration plus simple, une meilleure collaboration entreprise-entreprise et une meilleure sécurité (Bazaz et Khalique, 2016, p. 22). Inversement, il demeure des risques au niveau de la scalabilité, du fait qu'un individu mal intentionné puisse se connecter à l'appareil d'un utilisateur ou un logiciel malveillant, du point de défaillance unique (Bazaz et Khalique, 2016, p. 22). C'est pour cette raison que qu'il est recommandé de combiner le SSO avec une MFA afin de renforcer la preuve d'identité et de limiter l'impacter d'un de session ou de mot de passe (Bazaz et Khalique, 2016, p. 23).

OpenID

En complément de SAML, OpenID Connect (OIDC) est un système open-source et une extension du protocole OAuth 2.0 qui introduit une couche d'authentification permettant de vérifier l'identité des utilisateurs. Le protocole OpenID, en tant que standard d'authentification fédérée, est promu par la fondation à but non lucratif OpenID Foundation, qui permet aux utilisateurs de s'authentifier auprès de services tiers en utilisant un fournisseur d'identité OpenID de confiance (Kiourtis *et al.*, 2023, p. 40). Cette approche évite aux utilisateurs de devoir créer et gérer un compte distinct pour chaque service, car ils peuvent, par exemple, utiliser un compte Google ou une autre entité fédérée conforme à OpenID pour accéder à des portails bancaires partenaires (Kiourtis *et al.*, 2023, p. 40).

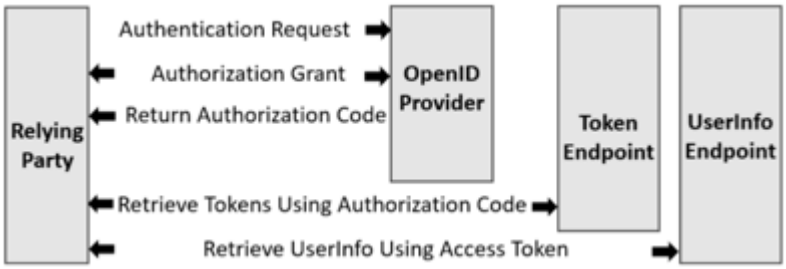


Figure 80 Flux d'autorisation OpenID à haut niveau (Kiourtis et al., 2023, p. 39)

Le modèle OpenID Connect (OIDC) a été développé comme extension d'OAuth 2.0, combinant les fonctionnalités d'authentification d'OpenID avec les capacités d'autorisation d'OAuth (Kiourtis *et al.*, 2023, p. 41). OIDC permet ainsi à une application de vérifier l'identité d'un utilisateur à l'aide d'un serveur d'autorisation tout en ayant la possibilité d'obtenir des informations de profil basiques sur ce dernier de manière sécurisée (Kiourtis *et al.*, 2023, p. 41). Contrairement à OAuth 2.0, qui ne gère que la délégation d'accès aux ressources, OIDC intègre un token d'identification, généralement au format JWT[69], singé numériquement, contenant les affirmations relatives à l'identité de l'utilisateur (Kiourtis *et al.*, 2023, p. 41). OIDC repose donc sur trois rôles fondamentaux : le fournisseur d'identité OpenID, l'entité validatrice ou le RP[70], et l'utilisateur final, dont l'identité est à valider (Kiourtis *et al.*, 2023, p. 41). L'utilisateur interagit avec l'entité validatrice (ex : application bancaire), qui redirige vers le fournisseur d'identité OpenID (Kiourtis *et al.*, 2023, p. 41). Ce dernier authentifie l'utilisateur, puis renvoie au client un token d'identification, un token d'accès et éventuellement un « refresh token » si la session est maintenue (Kiourtis *et al.*, 2023, p. 41). Le token d'identification contient les informations essentielles à propos de l'utilisateur, telles que son identifiant unique, l'émetteur du token, le moment de l'émission et d'autres attributs optionnels comme le nom ou l'adresse électronique (Kiourtis *et al.*, 2023, p. 41).

En somme, OpenID Connect s'affirme comme un protocole de référence pour l'authentification fédérée dans les SBT. Il permet aux banques de déléguer l'authentification à des fournisseurs tiers de confiance tout en maintenant un bon niveau de sécurité, de contrôle et de conformité réglementaire.

[69] JWT est un acronyme pour JavaScript Object Notation Web Token

[70] RP est un acronyme pour relaying party

ANNEXE H

Documents et certifications

Groupe en éthique de la recherche

Piloter l'éthique de la recherche humaine

EPTC 2: FER 2022

Certificat de réussite

Ce document certifie que

Luis Alberto Pastor Rodriguez

a complété avec succès la Formation en éthique de la recherche basée sur l'Énoncé de politiques des trois Conseils : Éthique de la recherche avec des êtres humains (EPTC 2: FER 2022)

Numero de certificat 0000954770

10 septembre, 2023

UQÀM | Comités d'éthique de la recherche avec des êtres humains

No. de certificat : 2025-7297
Date : 2024-12-03

CERTIFICAT D'APPROBATION ÉTHIQUE

Le Comité d'éthique de la recherche pour les projets étudiants impliquant des êtres humains (CERPE plurifacultaire) a examiné le projet de recherche suivant et le juge conforme aux pratiques habituelles ainsi qu'aux normes établies par la *Politique No 54 sur l'éthique de la recherche avec des êtres humains*(2020) de l'UQAM.

- Titre du projet : LES IDENTIFIANTS DÉCENTRALISÉS AU SERVICE DE LA PROTECTION DE L'IDENTITÉ NUMÉRIQUE - LE CAS D'UNE BANQUE CANADIENNE
- Nom de l'étudiant : Luis-Alberto Pastor-Rodriguez
- Programme d'études : **Maîtrise ès sciences (technologies de l'information - mémoire)**
- Direction(s) de recherche : Régis Barondeau

Modalités d'application

Toute modification au protocole de recherche en cours de même que tout événement ou renseignement pouvant affecter l'intégrité de la recherche doivent être communiqués rapidement au comité.

La suspension ou la cessation du protocole, temporaire ou définitive, doit être communiquée au comité dans les meilleurs délais.

Le présent certificat est valide pour une durée d'un an à partir de la date d'émission. Au terme de ce délai, un rapport d'avancement de projet doit être soumis au comité, en guise de rapport final si le projet est réalisé en moins d'un an, et en guise de rapport annuel pour le projet se poursuivant sur plus d'une année au plus tard un mois avant la date d'échéance (**2025-12-03**) de votre certificat. Dans ce dernier cas, le rapport annuel permettra au comité de se prononcer sur le renouvellement du certificat d'approbation éthique.

Raoul Graf, M.A., Ph.D.
Professeur titulaire, Département de marketing
Président du CERPÉ plurifacultaire

BIBLIOGRAPHIE

Abdelgalil, L. et Mejri, M. (2023). HealthBlock: a framework for a collaborative sharing of electronic health records based on blockchain. *Future Internet*, *15*(3), 87. https://doi.org/10.3390/fi15030087

Adams, B. (2023, 28 mars). *How banking works, types of banks, and how to choose the best bank for you*. Investopedia. https://www.investopedia.com/terms/b/bank.asp

Ahmed, K. A. M., Saraya, S. F., Wanis, J. F. et Ali-Eldin, A. M. T. (2023). A blockchain self-sovereign identity for open banking secured by the customer's banking cards. *Future Internet*, *15*(6), 208. https://doi.org/10.3390/fi15060208

Ahmed, Md. R., Islam, A. K. M. M., Shatabda, S. et Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey. *IEEE Access*, *10*, 113436-113481. https://doi.org/10.1109/ACCESS.2022.3216643

Aiello, W., Lodha, S. et Ostrovsky, R. (1998). Fast digital identity revocation: extended abstract. Dans H. Krawczyk (dir.), *Advances in Cryptology — CRYPTO '98* (vol. 1462, p. 137-152). Springer Berlin Heidelberg. https://doi.org/10.1007/BFb0055725

Akram, M. et Sen, A. (2022). A case study evaluation of blockchain for digital identity verification and management in BFSI using zero-knowledge proof. Dans *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (p. 1295-1299). IEEE. https://doi.org/10.1109/DASA54658.2022.9765121

Alamsyah, A., Kusuma, G. N. W. et Ramadhani, D. P. (2024). A review on decentralized finance ecosystems. *Future Internet*, *16*(3), 76. https://doi.org/10.3390/fi16030076

Alanzi, H. et Alkhatib, M. (2022). Towards improving privacy and security of identity management systems using blockchain technology: a systematic review. *Applied Sciences*, *12*(23), 12415. https://doi.org/10.3390/app122312415

Allen, C. (2016, 26 avril). *The path to self-sovereign identity*. Life With Alacrity. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Alolayan, R. M. et Al-Kaabi, A. M. (2020). CRM and mobile applications:an overview of mobile CRM adoption. *Information and Knowledge Management*. https://doi.org/10.7176/IKM/10-2-06

ANSSI. (2020, 1er janvier). *Mécanismes cryptographiques | ANSSI*. https://cyber.gouv.fr/publications/mecanismes-cryptographiques

Ausanka-Crues, R. (2006). *Methods for access control: advances and limitations*.

Bai, P. et Bisht, C. (2022, 9 août). *Decentralized identity management: prerequisiteof Web3 identity model*. https://doi.org/10.36227/techrxiv.20424633.v1

Barondeau, R., McNeil, S. et Pastor Rodriguez, L. A. MNBC et stablecoins: analyse comparative des cas d'usage et leçons apprises. CAHIER DE RECHERCHE DE LA CHAIRE FINTECH AMF – FINANCE MONTRÉAL. https://chairefintech.uqam.ca/wp-content/uploads/2024/01/Cahierrecherche_Barondeau_5ADP.pdf décembre 2023.

Batubara, F. R., Ubacht, J. et Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. Dans *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (p. 1-9). ACM. https://doi.org/10.1145/3209281.3209317

Bazarhanova, A. (2020). *Managing change in a dominant infrastructure for digital identification*. https://research.aalto.fi/en/publications/managing-change-in-a-dominant-infrastructure-for-digital-identifi

Bazaz, T. et Khalique, A. (2016). A review on single sign on enabling technologies and protocols. *International Journal of Computer Applications*, *151*(11), 18-25. https://doi.org/10.5120/ijca2016911938

Beduschi, A. (2019). Digital identity: contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2), 205395171985509. https://doi.org/10.1177/2053951719855091

Bellagarda, J. et Abu-Mahfouz, A. M. (2022). Connect2NFT: a web-based, blockchain enabled NFT application with the aim of reducing fraud and ensuring authenticated social, non-human verified digital identity. *Mathematics*, *10*(21), 3934. https://doi.org/10.3390/math10213934

Bharadwaj, S., Aeron, P., Singla, A., Gupta, N., Jain, A. et Sharma, D. (2023). *Decentralized identity management using blockchain: cube framework for secure usage of IS resources*, *31*(2), 1-24. https://doi.org/10.4018/JGIM.315283

Binduf, A., Alamoudi, H. O., Balahmar, H., Alshamrani, S., Al-Omar, H. et Nagy, N. (2018). Active directory and related aspects of security (p. 4474-4479). 2018 21st Saudi Computer Society National Computer Conference (NCC), IEEE. https://doi.org/10.1109/NCG.2018.8593188

BitFury Group. (2015, 13 septembre). *Proof of stake versus proof of work whitepaper*. https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

Boi, B., De Santis, M. et Esposito, C. (2024). Enhancing security in user-centered authentication using KERI. Dans *2024 32nd Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)* (p. 161-166). https://doi.org/10.1109/PDP62718.2024.00030

Boysen, A. (2021). Decentralized, self-sovereign, consortium: the future of digital identity in canada. *Frontiers in Blockchain*, *4*, 624258. https://doi.org/10.3389/fbloc.2021.624258

Braun, V. et Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brunner, C., Gallersdörfer, U., Knirsch, F., Engel, D. et Matthes, F. (2020). DID and VC:untangling decentralized identifiers and verifiable credentials for the web of trust. Dans *2020 the 3rd*

International Conference on Blockchain Technology and Applications (p. 61-66). ACM. https://doi.org/10.1145/3446983.3446992

Bulinge, F. (2010). Renseignement militaire : une approche épistémologique. *Revue internationale d'intelligence économique*, *Vol 2*(2), 209-232.

Bulinge, F. (2014). Chapitre 4. Épistémologie du renseignement . Cairn.info. Dans *Maîtriser l'information stratégique* (p. 79-101). De Boeck Supérieur. https://www.cairn.info/maitriser-l-information-strategique--9782804189143-p-79.htm

Buterin, V. (2014). *Ethereum whitepaper: a next generation smart contract & decentralized application platform*.

C3L Security. (2019, 10 juin). Balancing functionality, usability and security in design. https://blog.c3l-security.com/2019/06/balancing-functionality-usability-and.html

Campbell, M. (2023). The road to decentralized identity: the techniques, promises, and challenges of tomorrow's digital identity. *Computer*, *56*(6), 96-100. https://doi.org/10.1109/MC.2023.3263020

Canadian Business. (2001, 19 février). *CRM: although it defies definition, customer relationship management has become critical to an organization's success and even survival*. https://www.proquest.com/abicomplete/docview/221361664/fulltext/8AC487CF549446A7PQ/1?accountid=14719&sourcetype=Magazines

Cao, Z., Jandhyala, R. et Koduvayur, S. (2010). Performance evaluation for SOAP and RFC in SAP netweaver platform (p. 457-464). 2010 IEEE International Conference on Web Services (ICWS), IEEE. https://doi.org/10.1109/ICWS.2010.114

Catalini, C. et Gans, J. S. (2016). *Some simple economics of the blockchain*.

Chan, W., Gai, K., Yu, J. et Zhu, L. (2025). Blockchain-assisted self-sovereign identities on education: a survey. *Blockchains*, *3*(1), 3. https://doi.org/10.3390/blockchains3010003

Chapin, P. C., Skalka, C. et Wang, X. S. (2008). Authorization in trust management: features and foundations. *ACM Computing Surveys*, *40*(3), 1-48. https://doi.org/10.1145/1380584.1380587

Choudhari, S., Das, S. K. et Parasher, S. (2021). Interoperable blockchain solution for digital identity management (p. 1-6). 2021 6th International Conference for Convergence in Technology (I2CT), IEEE. https://doi.org/10.1109/I2CT51068.2021.9418220

Clark, R. (2021, 14 octobre). Evolution of data storage. *Platinum Data Recovery*. https://platinumdatarecovery.com/blog/data-storage-evolution

Cloutier, L. M. (2024a). *1. Cadres d'échantillonnages 2. Instruments de recueil des données (questionnaires, guides d'entrevues, prétests)*.

Cloutier, L. M. (2024b). *Méthodologies de recherche et perspectives théoriques*.

Cloutier, M. (2024c). *Conception d'une recherche qualitative*.

Costin, B. V. et Cojocaru, D. (2017). Integration of metrology applications in the calibration reservoir suites using SAP fiori, portal and cloud. A study case (p. 297-302). 2017 21st International Conference on System Theory, Control and Computing (ICSTCC), IEEE. https://doi.org/10.1109/ICSTCC.2017.8107050

Cristea, A. D., Prostean, O., Muschalik, T. et Tirian, O. (2010). The advantages of using SAP NetWeaver platform to implement a multidisciplinary project (p. 383-386). IEEE International Joint Conference on Computational Cybernetics and Technical Informatics (ICCC-CONTI 2010). IEEE 8th International Conference on Computational Cybernetics and 9th International Conference on Technical Informatics, IEEE. https://doi.org/10.1109/ICCCYB.2010.5491245

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. et Kalyanaraman, V. (2016). *BlockChain technology: beyond bitcoin*, (2).

Curran, S. (2025, 8 février). Sovrin foundation MainNet ledger shutdown likely on or before march 31, 2025. *Sovrin*. https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025/

Damiani, E., De Capitani diVimercati, S. et Samarati, P. (2003). Managing multiple and dependable identities. *IEEE Internet Computing*, *7*(6), 29-37. https://doi.org/10.1109/MIC.2003.1250581

De Filippi, P. (2018). *Blockchain et cryptomonnaies* (vol. 3e éd.). Presses Universitaires de France. https://stm.cairn.info/blockchain-et-cryptomonnaies--9782715424135?lang=fr

Denzin, N. K. et Lincoln, Y. S. (2011). *The Sage handbook of qualitative research* (4th ed). Sage. https://books.google.ca/books?hl=en&lr=&id=AIRpMHgBYqIC&oi=fnd&pg=PP1&dq=Denzin,+N.+K.,+%26+Lincoln,+Y.+S.+(2011).+The+SAGE+Handbook+of+Qualitative+Research.+Sage.&ots=kqANAJeBjc&sig=i7WGXMIOSRmqGAsO_7LZ8gUIuHc#v=onepage&q=Denzin%2C%20N.%20K.%2C%20%26%20Lincoln%2C%20Y.%20S.%20(2011).%20The%20SAGE%20Handbook%20of%20Qualitative%20Research.%20Sage.&f=false

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, *19*(5), 92-95. https://doi.org/10.1109/MCSE.2017.3421554

Dib, O. et Toumi, K. (2020). Decentralized identity systems: architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing*, *4*(5), 19-40. https://doi.org/10.33166/AETiC.2020.05.002

DiCicco-Bloom, B. et Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Dieye, M., Valiorgue, P., Gelas, J.-P., Diallo, E.-H., Ghodous, P., Biennier, F. et Peyrol, É. (2023). A self-sovereign identity based on zero-knowledge proof and blockchain. *IEEE Access*, *11*, 49445-49455. https://doi.org/10.1109/ACCESS.2023.3268768

Diffie, W. et Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638

Dixit, A., Smith-Creasey, M. et Rajarajan, M. (2022). A decentralized IIoT identity framework based on self-sovereign identity using blockchain. Dans *2022 IEEE 47th Conference on Local Computer Networks (LCN)* (p. 335-338). IEEE. https://doi.org/10.1109/LCN53696.2022.9843700

Doğan, Ö. et Karacan, H. (2023). A blockchain-based E-commerce reputation system built with verifiable credentials. *IEEE Access*, *11*, 47080-47097. https://doi.org/10.1109/ACCESS.2023.3274707

Duchesne, A. (2021, 23 août). *Early adopters | les 13% de clients qui feront votre succès*. https://systemproject.fr/ § Conseil Marketing. https://systemproject.fr/early-adopters/

Eisenhardt, K. M. (1989). *Building Theories from Case Study Research*.

El-Emam, E., Koutb, M., Kelash, H. et Farag Allah, O. (2009). An optimized kerberos authentication protocol (p. 508-513). Systems (ICCES), IEEE. https://doi.org/10.1109/ICCES.2009.5383213

Falk, B. H., Tsoukalas, G. et Zhang, N. (2022, 1er décembre). *Economics of NFTs: the value of creator royalties*. arXiv. https://doi.org/10.48550/arXiv.2212.00292

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T. et Zuffo, M. K. (2020). Self-sovereign identity for IoT environments: a perspective. Dans *2020 Global Internet of Things Summit (GIoTS)* (p. 1-6). IEEE. https://doi.org/10.1109/GIOTS49054.2020.9119664

Feher, K. (2021). Digital identity and the online self: footprint strategies – an exploratory and comparative research study. *Journal of Information Science*, *47*(2), 192-205. https://doi.org/10.1177/0165551519879702

Fenergo. (2023, 10 janvier). *KYC compliance for banks: addressing the cost*. https://resources.fenergo.com/blogs/kyc-compliance-for-banks-addressing-the-cost

Fereday, J. et Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80-92. https://doi.org/10.1177/160940690600500107

Ferrer-Estévez, M. et Chalmeta, R. (2023). Sustainable customer relationship management. *Marketing Intelligence & Planning*, *41*(2), 244-262. https://doi.org/10.1108/MIP-06-2022-0266

Feulner, S., Sedlmeir, J., Schlatt, V. et Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*, *32*(3), 1759-1777. https://doi.org/10.1007/s12525-022-00573-9

Fu, J., Qiao, S., Huang, Y., Si, X., Li, B. et Yuan, C. (2020). A study on the optimization of blockchain hashing algorithm based on PRCA. *Security and Communication Networks*, *2020*, 1-12. https://doi.org/10.1155/2020/8876317

Gaudet, S. et Robert, D. (2018). *Choisir un projet de recherche qualitative*.

Gautam. (2020). Decentralized banking system on EthereumBlockchain. *International Journal for Modern Trends in Science and Technology*, *6*(12), 113-116. https://doi.org/10.46501/IJMTST061222

Gibson, J. J. (1977). *"The theory of affordances," in perceiving, acting, and knowing. Towards an ecological psychology.* Hoboken, NJ: John Wiley & Sons Inc.

Grenier, S., Barrette, G., Houle, L. et Labrie, S. (2021). *Sortir plus fort de la pandémie en misant sur l'analytique RH*, *46*(3), 76-80.

Grljević, O., Marić, M. et Božić, R. (2025). Exploring mobile application user experience through topic modeling. *Sustainability*, *17*(3), 1109. https://doi.org/10.3390/su17031109

Groth, J. (2011). Efficient zero-knowledge proofs. Dans A. Nitaj et D. Pointcheval (dir.), *Progress in Cryptology – AFRICACRYPT 2011* (vol. 6737, p. 379-379). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21969-6_24

Gupta, A. et Gupta, S. (2018). *Blockchain technology: application in indian banking sector*, *19*(2), 75-84.

Haneem, F., Ali, R., Kama, N. et Basri, S. (2017a). Descriptive analysis and text analysis in systematic literature review: a review of master data management (p. 1-6). 2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE. https://doi.org/10.1109/ICRIIS.2017.8002473

Haneem, F., Ali, R., Kama, N. et Basri, S. (2017b). Resolving data duplication, inaccuracy and inconsistency issues using master data management (p. 1-6). 2017 5th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE. https://doi.org/10.1109/ICRIIS.2017.8002453

Harrell, D. T., Usman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J., Oliveira, E. de, Bautista, J. R., Meyer, E. T. et Khurshid, A. (2022). Technical design and development of a self-sovereign identity management platform for patient-centric healthcare using blockchain technology. *Blockchain in Healthcare Today*. https://doi.org/10.30953/bhty.v5.196

Heakal, R. (2023, 25 juillet). *What central banks do*. Investopedia. https://www.investopedia.com/articles/03/050703.asp

Hendrickson, L. (2025, 28 mars). Your guide to self-sovereign identity (SSI). *Identity*. https://www.identity.com/self-sovereign-identity/

Hirsch, R. (2007). Experience report: use of SAP NetWeaver technology to realize SOA-based BPM tasks (p. 303-308). IEEE International Conference on Service-Oriented Computing and Applications (SOCA '07), IEEE. https://doi.org/10.1109/SOCA.2007.18

Jackson, G. H. et Taiuru, K. (2023). Mechanisms for digital transformation in the education and healthcare sectors utilizing decentralized self-sovereign identity. *International Journal of Network Security & Its Applications*, *15*(2), 1-21. https://doi.org/10.5121/ijnsa.2023.15201

Jøsang, A. et Pope, S. (2005). *User centric identity management*.

Kaneriya, J. et Patel, H. (2020). A comparative survey on blockchain based self sovereign identity system. Dans *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (p. 1150-1155). https://doi.org/10.1109/ICISS49785.2020.9315899

Kardiner, A. (1969). *L'individu dans sa société: essai d'anthropologie psychanalytique* (T. Prigent, trad.). Gallimard.

Kashmar, N., Adda, M. et Atieh, M. (2020). From access control models to access control metamodels: a survey. Dans K. Arai et R. Bhatia (dir.), *Advances in Information and Communication* (vol. 70, p. 892-911). Springer International Publishing. https://doi.org/10.1007/978-3-030-12385-7_61

Kathrin, O. N. et Riedel, J. (2021). *Know-your-customer (KYC) requirements for initial coin offerings*, *63*(5), 551-567. https://doi.org/10.1007/s12599-020-00677-6

Katz, J. et Lindell, Y. (2007). *Introduction to modern cryptography*.

Kayani, U. et Hasan, F. (2024). *Unveiling cryptocurrency impact on financial markets and traditional banking systems: lessons for sustainable blockchain and interdisciplinary collaborations*, *17*(2), 58. https://doi.org/10.3390/jrfm17020058

Kayrouz, P. (2021). *Central bank digital currencies and the future of money*. PwC. https://www.pwc.com/m1/en/media-centre/2021/documents/central-bank-digital-currencies-and-the-future-of-money-part1.pdf

Keller, B. (2024). *Designing a self-sovereign identity system with KERI*. https://sonar.ch/global/documents/329884

Khanna, P. et Haldar, A. (2023). Will adoption of blockchain technology be challenging: evidence from Indian banking industry. *Qualitative Research in Financial Markets*, *15*(2), 361-384. https://doi.org/10.1108/QRFM-01-2022-0003

Kim, S.-H., Choi, D., Kim, S.-H., Cho, S. et Lim, K.-S. (2018). Context-aware multimodal FIDO authenticator for sustainable IT services. *Sustainability*, *10*(5), 1656. https://doi.org/10.3390/su10051656

Kiourtis, A., Giannetsos, T., Menesidou, S., Mavrogiorgou, A., Symvoulidis, C., Graziani, A., Kleftakis, S., Mavrogiorgos, K., Zafeiropoulos, N., Gkolias, C. et Kyriazis, D. (2023). Identity management standards: a literature review. *Computers and Informatics*, *3*(1), 35-46.

Koli, S., Singh, R., Rana, P., Aggarwal, A. et Dumka, A. (2023). Salesforce technology: a complete CRM solution on the cloud (p. 1-5). 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON), IEEE. https://doi.org/10.1109/DELCON57910.2023.10127497

Kour, M. (2023). Blockchain technology changing landscape of banking industry. Dans *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (p. 1212-1216). IEEE. https://doi.org/10.1109/ICAAIC56838.2023.10140854

Kovács, G. et Spens, K. M. (2005). Abductive reasoning in logistics research. *International Journal of Physical Distribution & Logistics Management*, *35*(2), 132-144. https://doi.org/10.1108/09600030510590318

Kulkarni, V. et Singh, A. P. (2019). Sustainable KYC through blockchain technology in global banks. *Annals of Dunarea de Jos University of Galati. Fascicle I. Economics and Applied Informatics*, *25*(2), 34-38. https://doi.org/10.35219/eai1584040929

Kumar, D. M. et Anand, P. (2020). *A blockchain based approach for an efficient secure KYC process with data sovereignty*, *9*(01).

Kumar, P. V. et Raghavendra, Dr. (2022). Blockchain technology adoption in banking and financial sector: a literature review. *Towards Excellence*, 765-781. https://doi.org/10.37867/TE140464

Kuperberg, M. (2020). Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, *67*(4), 1008-1027. https://doi.org/10.1109/TEM.2019.2926471

Lal, N. A., Prasad, S. et Farik, M. (2024). A review of authentication methods. *ResearchGate*. https://www.researchgate.net/publication/311514269_A_Review_Of_Authentication_Methods

Lamothe, M., Guéhéneuc, Y.-G. et Shang, W. (2022). A systematic review of API evolution literature. *ACM Computing Surveys*, *54*(8), 1-36. https://doi.org/10.1145/3470133

Lau, L. (dir.). (2005). *Managing business with SAP: planning implementation and evaluation*. IGI Global. https://doi.org/10.4018/978-1-59140-378-4

Longhurst, R. (2003). Semi-structured interviews and focus groups. *Key methods in geography*, *3*(2), 143-156.

Luís, J., Santos, J., Dias, T. et Correia, M. (2024). *Comunicação: real estate documentation authentication with blockchain and self-sovereign identity*.

Mafike, S. S. et Mawela, T. (2022). Blockchain design and implementation techniques, considerations and challenges in the banking sector: a systematic literature review. *Acta Informatica Pragensia*, *11*(3), 396-422. https://doi.org/10.18267/j.aip.200

Maler, E. et Hughes, J. (2005, 12 septembre). *Security assertion markup language (SAML) V2.0 technical overview*. https://groups.oasis-open.org/higherlogic/ws/public/document?document_id=14361

Malhotra, D., Saini, P. et Singh, A. K. (2022). How blockchain can automate KYC: systematic review. *Wireless Personal Communications*, *122*(2), 1987-2021. https://doi.org/10.1007/s11277-021-08977-0

Mamun, A. A., Al Mamun, A., Hasan, S. R., Hasan, S. R., Bhuiyan, M. S., Bhuiyan, M. S., Kaiser, M. S., Kaiser, M. S., Abu Yousuf, M. et Yousuf, M. A. (2020). Secure and transparent KYC for banking system using IPFS and blockchain technology. Dans *2020 IEEE Region 10 Symposium (TENSYMP)* (p. 348-351). IEEE. https://doi.org/10.1109/TENSYMP50017.2020.9230987

Manchar, A. et Chouhan, A. (2017). Salesforce CRM: a new way of managing customer relationship in cloud environment (p. 1-4). 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE. https://doi.org/10.1109/ICECCT.2017.8117887

Martínez-Mesa, J., González-Chica, D. A., Duquia, R. P., Bonamigo, R. R. et Bastos, J. L. (2016). Sampling: how to select participants in my research study? *Anais Brasileiros de Dermatologia*, *91*(3), 326-330. https://doi.org/10.1590/abd1806-4841.20165254

Martino, P. (2019). Blockchain technology: challenges and opportunities for banks. *International Journal of Financial Innovation in Banking*, *2*(4), 314. https://doi.org/10.1504/IJFIB.2019.104535

Mattsson, U. T. (2010). A new scalable approach to data tokenization. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1627284

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P. et Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*, 1-1. https://doi.org/10.1109/COMST.2025.3543197

Mogull, R. (2010, 21 septembre). *Understanding and selecting a tokenization solution*. Securosis. https://securosis.com/research/papers/understanding-and-selecting-a-tokenization-solution/

Mohite, R., Mulani, M., Basve, S., Bansal, S. et Raskar, Dr. P. (2023). Decentralized payment system by using blockchain. *International Journal of Advanced Research in Science, Communication and Technology*, 54-57. https://doi.org/10.48175/IJARSCT-9318

Molaro, M. (2024). *Analysis of the open API services in europe*. https://www.politesi.polimi.it/handle/10589/222900

Morris, R. J. T. et Truskowski, B. J. (2003). The evolution of storage systems. *IBM Systems Journal*, *42*(2), 205-217. https://doi.org/10.1147/sj.422.0205

Moyano, J. P., Thoroddsen, T. et Ross, O. (2019). Optimised and dynamic KYC system based on blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, *1*(1), 85. https://doi.org/10.1504/IJBC.2019.101854

Myronov, O. (2024). Effectiveness of cryptocurrencies as a means of international payments: analysis of cost, speed, and transaction security. *Actual Problems of Economics*, *1*(272), 96-104. https://doi.org/10.32752/1993-6788-2024-1-272-96-104

Nahar, P. et Dhaka, V. P. (2014). *A review : benefits and critical factors of customer relationship management*. ResearchGate. https://www.researchgate.net/publication/318700789_A_Review_Benefits_and_Critical_Factors_of_Customer_Relationship_Management

Nakamoto, S. (2008). *Bitcoin: a peer-to-peer electronic cash system*.

Narayanan, A. et Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, *60*(12), 36-45. https://doi.org/10.1145/3132259

Newton, F. J., Haregu, T. N., Newton, J. D., Donovan, R., Mahal, A., Mackenzie-Stewart, R., Ewing, M. T., Bauman, A., Manera, K. E. et Smith, B. J. (2023). Effects of customer relationship management (CRM) strategies and socio-cognitive constructs on the physical activity of individuals with arthritis over time. *PLOS ONE*, *18*(10), e0292692. https://doi.org/10.1371/journal.pone.0292692

Ngai, E. W. T. (2005). Customer relationship management research (1992-2002): an academic literature review and classification. *Marketing Intelligence & Planning*, *23*(6), 582-605. https://doi.org/10.1108/02634500510624147

N'Goala, G., Pez-Pérard, V. et Prim-Allaz, I. (dir.). (2019). *Augmented customer strategy: CRM in the digital age* (1re éd.). Wiley. https://doi.org/10.1002/9781119618324

Noone, C., Brophy, T., Dribusch, D., Schumann, J., Martin, A., Spremo, B., Mora, O. et Aran, S. (2024, 29 mai). *Digital identity – corporates and institutions*. https://corporates.db.com/publications/White-papers-guides/digital-identity?language_id=1

Oh, S.-R. et Kim, Y.-G. (2019). Interoperable OAuth 2.0 framework. Dans *2019 International Conference on Platform Technology and Service (PlatCon)* (p. 1-5). IEEE. https://doi.org/10.1109/PlatCon.2019.8668962

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. et Koucheryavy, Y. (2018). Multi-factor authentication: a survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

OneLogin. (s. d.). *IDaaS: identity as a service | OneLogin*. Récupéré le 18 mai 2024 de https://www.onelogin.com/learn/idaas

Opiah, A. (2024, 13 juin). *Privado ID to tackle global demand for decentralized digital identity software on its own | Biometric Update*. https://www.biometricupdate.com/202406/privado-id-to-tackle-global-demand-for-decentralized-digital-identity-software-on-its-own

Parate, S., Josyula, H. P. et Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*. https://doi.org/10.56726/IRJMETS44476

Paré, G. (2004). Investigating information systems with positivist case study research. *Communications of the Association for Information Systems*, *13*.

Parra Moyano, J. et Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411-423. https://doi.org/10.1007/s12599-017-0504-2

Parry, G. et Ellul, J. (2024, 16 avril). *NFTs and self-sovereign identity: opportunities and challenges*. https://doi.org/10.36227/techrxiv.171328049.93969442/v1

Patil, C., Jain, S., Khare, R. A. et Lahire, S. (2024). Age verification using zero-knowledge proof. Dans *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (p. 1-9). https://doi.org/10.1109/ICBDS61829.2024.10837396

Patton, M. Q. (2002). *Qualitative research & evaluation methods*. sage.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: integrating theory and practice*. SAGE Publications. https://books.google.ca/books?hl=en&lr=&id=ovAkBQAAQBAJ&oi=fnd&pg=PP1&dq=Patton,+M.+Q.+(2015).+Qualitative+Research+%26+Evaluation+Methods:+Integrating+Theory+and+Practice+(4th+ed.).&ots=ZSXX7ozIG3&sig=iTvjZcwuqJP9ZbAmex3_IzyANaE#v=onepage&q=ethic&f=false

Peters, G. W. et Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money.

Dans P. Tasca, T. Aste, L. Pelizzon et N. Perony (dir.), *Banking Beyond Banks and Money* (p. 239-278). Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_13

Phiri, J. et Agbinya, J. I. (2006). Modelling and information fusion in digital identity management systems. Dans *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)* (p. 181-181). IEEE. https://doi.org/10.1109/ICNICONSMCL.2006.152

Podgorelec, B., Alber, L. et Zefferer, T. (2022). What is a (digital) identity wallet? A systematic literature review (p. 809-818). 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), IEEE. https://doi.org/10.1109/COMPSAC54236.2022.00131

Polygon. (2023, 2 novembre). *Why HSBC is building a decentralized identity solution with polygon ID*. https://polygon.technology/blog/why-hsbc-is-building-a-decentralized-identity-solution-with-polygon-id

Popek, G. J. et Kline, C. S. (1979). Encryption and secure computer networks. *ACM Computing Surveys*, *11*(4), 331-356. https://doi.org/10.1145/356789.356794

Pourtois, J.-P., Desmet, H. et Lahaye, W. (2006). Chapitre 8. Postures et démarches épistémiques en recherche. Dans *La méthodologie qualitative* (p. 169-200). Armand Colin. https://doi.org/10.3917/arco.paill.2006.01.0169

Raipurkar, A. R., Bobde, S., Tripahi, A. et Sahu, M. (2023). Digital identity system using blockchain-based self sovereign identity & zero knowledge proof. Dans *2023 OITS International Conference on Information Technology (OCIT)* (p. 611-616). https://doi.org/10.1109/OCIT59427.2023.10430981

Ramamoorthi, K., Stamenova, V., Liu, R. H. et Bhattacharyya, O. (2024). The implementation of federated digital identifiers in health care: rapid review. *Journal of Medical Internet Research*, *26*, e45751. https://doi.org/10.2196/45751

Rana, R., Zaeem, R. N. et Barber, K. S. (2019). An assessment of blockchain identity solutions: minimizing risk and liability of authentication. Dans *IEEE/WIC/ACM International Conference on Web Intelligence* (p. 26-33). ACM. https://doi.org/10.1145/3350546.3352497

Ratnadewi, Adhie, R. P., Hutama, Y., Saleh Ahmar, A. et Setiawan, M. I. (2018). Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). *Journal of Physics: Conference Series*, *954*, 012009. https://doi.org/10.1088/1742-6596/954/1/012009

Ratnawat, N., Pandey, S., Paradkar, R. et Banerjee, S. (2022). Optimizing the KYC process using a blockchain based approach. *ITM Web of Conferences*, *44*, 03039. https://doi.org/10.1051/itmconf/20224403039

Rees, M. (2024, 9 février). Identity and access management in financial services. *Expert Insights*. https://expertinsights.com/insights/best-practices-for-identity-and-access-management-in-financial-services/

Renaud, D. (2024, 7 septembre). Dossier: fraudes envers les aînés | des « proies faciles » de plus en plus ciblées (2 articles). *La Presse*, Actualités. https://www.lapresse.ca/actualites/fraudes-envers-les-aines/des-proies-faciles-de-plus-en-plus-ciblees/2024-09-07/c-est-un-crime-degueulasse.php

Resnik, D. B. (2020, 23 décembre). *What is ethics in research and why is it important?* National Institute of Environmental Health Sciences. https://www.niehs.nih.gov/research/resources/bioethics/whatis

Rjoub, H., Adebayo, T. S. et Kirikkaleli, D. (2023). *Blockchain technology-based FinTech banking sector involvement using adaptive neuro-fuzzy-based K-nearest neighbors algorithm*, *9*(1), 65. https://doi.org/10.1186/s40854-023-00469-3

Rodriguez, D. M. et Johnson, S. (2019). *Unlocking the power of azure AD best practices for enterprise identity control*.

Salesforce. The beginner's guide to CRM. 2023.

Samal, A. et Pradhan, B. B. (2019). A review on identity safety using block chain. *International Journal of Psychosocial Rehabilitation*, *23*(6), 31-36. https://doi.org/10.37200/IJPR/V23I6/PR190732

Sammon, D., Nagle ,Tadhg et and Carlsson, S. (2012). Making sense of the master data management (MDM) concept: old wine in new bottles or new wine in old bottles? *Journal of Decision Systems*, *21*(3), 245-258. https://doi.org/10.1080/12460125.2012.735583

Sandhu, R. et Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys*, *28*(1), 241-243. https://doi.org/10.1145/234313.234412

SAP. (2015). *Master guide SAP for banking*.

SAP Fiori. (2025). *SAP fiori | expérience utilisateur et applications*. https://www.sap.com/france/products/technology-platform/fiori.html

Satybaldy, A., Ferdous, Md. S. et Nowostawski, M. (2024). A taxonomy of challenges for self-sovereign identity systems. *IEEE Access*, *12*, 16151-16177. https://doi.org/10.1109/ACCESS.2024.3357940

Savoie-Zajc, L. (2009). *L'entrevue semi-dirigée*.

Schäffner, M. (2019). *Analysis and evaluation of blockchain-based self-sovereign identity systems*.

Schwandt, T. A. (2000). *Three epistemological stances for qualitative inquiry: interpretivism, hermeneutics, and social constructivism. In N. K. Denzin & Y. S. Lincoln (eds.), handbook of qualitative research (2nd ed., pp. 189–213).* (2nd ed). Sage.

Sedlmeir, J., Lautenschlager, J., Fridgen, G. et Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), 1779-1794. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Smethurst, R., Rieger, A. et Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Sharma, A., Vyas, M., Bansal, D. et Sharma, G. (2023). A study of blockchain based solution for KYC verification. *Journal of Analysis and Computations*, *17*(1), 17-23. https://doi.org/10.30696/JAC.XVII.1.2023.17-23

Shu, Z., Llorens-Marin, M., Carrasco, R. A. et Romero, M. S. (2025). Customer electronic word of mouth management strategies based on computing with words: the case of spanish luxury hotel reviews on TripAdvisor. *Electronics*, *14*(2), 325. https://doi.org/10.3390/electronics14020325

Sim, W. L., Chua, H. N. et Tahir, M. (2019). Blockchain for identity management: the implications to personal data protection (p. 30-35). 2019 IEEE Conference on Application, Information and Network Security (AINS), IEEE. https://doi.org/10.1109/AINS47559.2019.8968708

Simmons, G. J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys*, *11*(4), 305-330. https://doi.org/10.1145/356789.356793

Singhal, R., Sangeeta, Dolly, Sharma, S., Garg, M. et Bhateja, R. (2024). *Banking digitalisation: an analysis of literature using bibliometric analysis*, *28*(2). https://www.proquest.com/abicomplete/docview/2907667401/abstract/1F8C2B37989745CBPQ/1

Sirvent, T. (2022). La cryptographie, socle de la souveraineté numérique. *Revue Défense Nationale*, *855*(10), 59-66. https://doi.org/10.3917/rdna.855.0059

Smith, S. M. (2021, 11 octobre). *Key event receipt infrastructure (KERI)*. arXiv. https://doi.org/10.48550/arXiv.1907.02143

Sousa, P. R., Resende, J. S., Martins, R. et Antunes, L. (2022). *The case for blockchain in IoT identity management*, *35*(6), 1477-1505. https://doi.org/10.1108/JEIM-07-2018-0148

Sreenath, G., Sridhar, G. T., Sannabhadti, A. A., S J, R. M. et Kounte, M. R. (2024). Blockchain based digital identity solution (p. 387-391). 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), IEEE. https://doi.org/10.1109/IDCIoT59759.2024.10467241

Stapleton, J. et Poore, R. S. (2011). Tokenization and other methods of security for cardholder data. *Information Security Journal: A Global Perspective*, *20*(2), 91-99. https://doi.org/10.1080/19393555.2011.560923

Syed Idrus, S. Z., Cherrier, E., Rosenberger, C. et Schwartzmann, J.-J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, *7*(5), 95-107.

Tan, K. L., Chi, C.-H. et Lam, K.-Y. (2023). Survey on Digital Sovereignty and Identity: From Digitization to Digitalization. *ACM Computing Surveys*, *56*(3), 1-36. https://doi.org/10.1145/3616400

Theyse, M. (2024, 6 mars). Scalability, decentralization & security — what trilemma? *Verus Coin*. https://medium.com/veruscoin/scalability-decentralization-security-what-trilemma-8d2d6869924d

Tobin, A., Reed, D., Windley, F. P. J. et Foundation, S. (2017). *The inevitable rise of self-sovereign identity*.

Travers, M. (2001). *Qualitative research through case studies*. SAGE. https://us.sagepub.com/en-us/nam/qualitative-research-through-case-studies/book210591#preview

Vasuki, M. et Rajashree, M. (2023). The impact of blockchain on digital identity management. *International Journal for Research in Applied Science and Engineering Technology*, *11*(7), 290-294. https://doi.org/10.22214/ijraset.2023.54616

Vries, H. de et Stjernlöf, L. S. (2023). *Okta administration up and running: drive operational excellence with IAM solutions for on-premises and cloud apps* (1re éd.). Packt Publishing Limited.

Wailgum, T. (2017). *CRM definition and solutions*. https://www.proquest.com/abicomplete/docview/1889290676/abstract/43D935649A684258PQ/1

Wardhana, I. P. S. P., Dantes, G. R. et Aryanto, K. Y. E. (2020). Analysis of digital identity transactions with Ethereum blockchain ethereum in a case study of credit applications in banking. *Journal of Physics: Conference Series*, *1516*(1), 012020. https://doi.org/10.1088/1742-6596/1516/1/012020

Werth, J., Berenjestanaki, M., Barzegar, H., El Ioini, N. et Pahl, C. (2023). A review of blockchain platforms based on the scalability, security and decentralization trilemma: Dans *Proceedings of the 25th International Conference on Enterprise Information Systems* (p. 146-155). SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0011837200003467

Wust, K. et Gervais, A. (2018). Do you need a blockchain? Dans *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (p. 45-54). IEEE. https://doi.org/10.1109/CVCBT.2018.00011

Yin, R. K. (2009). *Case study research: design and methods* (vol. 5). sage. https://books.google.ca/books?hl=en&lr=&id=FzawIAdilHkC&oi=fnd&pg=PR1&dq=Yin,+R.+K.+(2014).+Case+Study+Research:+Design+and+Methods+(5th+ed.).+Sage+Publications.&ots=l-_R4fhU0v&sig=velW6_Pggqo6E7vzHpl39U5i5Lc#v=onepage&q&f=false

Zheng, G., Gao, L., Huang, L. et Guan, J. (2021). Decentralized Application (DApp). Dans G. Zheng, L. Gao, L. Huang et J. Guan, *Ethereum Smart Contract Development in Solidity* (p. 253-280). Springer Singapore. https://doi.org/10.1007/978-981-15-6218-1_9

Zheng, Z., Xie, S., Dai, H., Chen, X. et Wang, H. (2017). An overview of blockchain technology: architecture, consensus, and future trends. Dans *2017 IEEE International Congress on Big Data (BigData Congress)* (p. 557-564). https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J. et Imran, M. (2020). An overview on smart contracts: challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491. https://doi.org/10.1016/j.future.2019.12.019