REPUBLIQUE DU SENEGAL



Un Peuple-Un But-Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE L'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DE SCIENCES APPLIQUEES ET DE TECHNOLOGIE

DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN DE CYCLE EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER

SPECIALITE : RESEAUX SECURITE ET SYSTEMES DISTRIBUES

THEME : « Sécurité de l'identité en ligne : étude de l'impact des références vérifiables et des identifiants distribués »

Réalisé par :

M Baïlo BALDE

Sous la direction de :

Pr. Chérif DIALLO

Jury :

Président et Examinateur : Pr Maïssa MBAYE

Membre : Dr El Hadji S. Mamour DIOP

Membre : Dr Cheikh M. Bamba DIONE

Encadrant : Pr. Chérif DIALLO

Année Académique 2022/2023

Dédicace

Je dédie ce souvenir à :

- **Ma mère :** Pour son amour, ses sacrifices, ses conseils et son soutien constant. Paix à son âme, que le tout puissant lui pardonne et l'élève parmi les habitants de Firdaws.
- **Mon père :** Pour ses sacrifices, son éducation et son soutien indéfectible. Puisse le miséricordieux faire fructifier ce travail et le récompenser.
- **Mes tantes :** Pour leur soutien incommensurable. Que le Tout-Puissant leur rende au centuple.
- M**es frères et sœurs :** Vous êtes ma force et ma motivation. Merci pour votre soutien indéfectible.
- **Ousmane BALDE (Hamadou) :** Je te remercie sincèrement pour tes précieux conseils et corrections, notamment en orthographe, grammaire et vocabulaire. Ton aide attentive et bienveillante a significativement amélioré la qualité de ce travail. Que Dieu t'ouvre davantage les portes du succès.
- **Yacine Badji :** Ma tante, grand-mère et mère à la fois, merci pour ton amour et tes sacrifices. Que le tout puissant te récompense.
- **Sidya SANE et Amy FALL :** Pour votre grande contribution dans ma vie. Que vos prières et sacrifices soient exaucés.
- **Maman Sane, Mama Boye et toute la famille :** Merci pour votre ouverture et votre soutien.
- **Saliou, Ibrahima Konte et Ngagne :** Pour votre amitié et votre soutien précieux.
- M**oustapha SANE, Ndèye Astou SANE et Bourama Diambang SANE :** Que vos efforts et projets soient couronnés de succès. Merci pour votre aide inestimable.
- **Mes amis de l'USSEIN et de l'UGB :** Pour votre amour et votre solidarité. Que le bonheur vous accompagne tous.
- **Les membres de l'AEECN :** Merci pour l'hébergement et le soutien, particulièrement Hamadou BALDE et Souleymane BALDE.
- **Rokhyatou MAR :** Pour tes encouragements et ton soutien lors de mes recherches. Je te souhaite le meilleur dans ta vie. Que le Tout-Puissant te bénisse et t'accorde ce qui est meilleur pour toi.
- **Dr Bambado BALDE et aux koldois :** Pour leur confiance et leur soutien.
- **Mes amis de Sédhiou :** Pour leur confiance et leur soutien continu, je pourrai oublier votre aide, particulièrement à la P32, Grand DIAO, mon patron MD et Ibrahima SAGNA qu'Allah vous facilite les projets mes très chers.
- **Les frères et sœurs de Village P :** Merci pour votre reconnaissance et votre amitié.
- **Mes colocataires des chambres 121, 122, 124 et 129 P :** Pour votre solidarité et votre considération, particulièrement à ceux de 122. Que Dieu facilite vos projets.
- **Souleymane Sabaly :** mon très chers je te remercie beaucoup mon frère et je prie au tout puissant de t'accorder ce que tu désires.
- **Borom Africa Tech et son équipe :** Franchement vous êtes un des rare vendeurs et réparateurs que je n'ai jamais vu votre honnêteté et ouverture en vers les clients. Je vous remercie beaucoup très chers.

Remerciements

Je remercie le tout puissant, qui m'a donné la force et la patience pour l'accomplissement de ce travail.

Je profite par cette occasion aussi pour remercier ma famille pour leurs bénédictions, leurs prières et leurs conseils pour la réussite de ce travail.

Ce modeste travail m'offre l'occasion d'exprimer nos profondes gratitudes à Pr DIALLO, qui n'a ménagé aucun effort pour la réussite de ce travail pendant toute la durée du choix de sujet jusqu'à la mise en forme du document final. Ses nombreux conseils ne m'ont jamais fait défaut. Je suis très heureux de lui exprimer ici nos respectueuses reconnaissances.

Je remercie l'ensemble des enseignant qui ont eu à intervenir dans le département Informatique, plus particulièrement dans la filière R2SD.

Je tiens à exprimer mes reconnaissances envers les membres du jury pour l'intérêt qu'ils ont porté à ce mémoire en acceptant d'en être examinateurs.

Je remercie aussi l'ensemble des enseignant qui m'ont eu en première cycle dans le département Mathématique Informatique, plus particulièrement à Dr Faye pour ses efforts continues.

Je remercie également tous les étudiants de l'université qui ont toujours été de près et de loin là pour me soutenir, que ce soit étudiant de M1 ou M2.

Enfin, je tiens à remercier tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail.

Merci à tous et à toutes.

Résumé

Dans cette étude, nous avons explorer les Verifiable Credentials et les Decentralized Identifiers, qui sont des technologies innovantes visant à sécuriser d'avantage et rendre l'identité numérique plus privé dans un contexte décentralisé. À cette fin, nous avons réalisés une analyse documentaire approfondis qui nous aide à bâtir un cadre théorique. Pour ce faire, nous exploitons des sources académiques, des normes internationales du W3C et les rapports des organisations spécialisé afin d'analyser les tendances actuelles et d'identifier les avantages et difficultés de l'utilisation de ces technologies.

En outre, nous avons réalisé une analyse de différent cas d'utilisations dans les domaines de l'éducation, de la santé et des services financiers. Dans chaque cas, il a été mise en évidence les fonctions spécifiques de VC et DID pour répondre aux besoins de ces domaines : la vérification des autorisations scolaires et des diplômes, la préservation de la confidentialité des informations de santé sur le patient, et les procédures d'identification de simplifications dans le domaine des services financier. Plateformes vérifiable offrent une haute sécurité, confidentialités et contrôle de l'utilisateur sur les informations et la conformité avec les régulations de la loi.

En plus, nous avons regardés comment ces technologies sont utilisés dans des solutions comme Microsoft Entra. Microsoft Entra utilise les VC et DID pour mieux géré les identités d'entreprise. En offrant des identités vérifiables et une meilleure protection des données, Microsoft Entra montre bien les avantage pratique de ces technologies pour les organisations. Cela aides à la fois à garder les informations en sécurités et à gérer les identités numériques plus facilement.

Il est important de souligné que, malgré les avantages indéniables des technologies d'identités décentralisés, plusieurs défis demeurent. Parmi eux, on trouve des problèmes d'interopérabilités, des coûts de mises en œuvre souvent élevé et un besoin urgent d'accroitre la sensibilisation tant des utilisateurs que des organisations. Afin de favorisé une adoption plus large de ces solutions, nous proposons plusieurs recommandations. Celles-ci inclus l'établissement de norme commune, l'améliorations de l'interopérabilité entre les différentes plateformes et une sensibilisation accrue des parties prenante sur les bénéfices offerts par les identités décentralisées. Par notre recherche, nous espérons ainsi apporter une contribution significative à la compréhension des perspectives et des effets que peuvent avoir les certificats vérifiable (VC) et les identités décentralisées (DID) sur la gestion des identités numérique.

Abstract

In this study, we explore Verifiable Credentials and Decentralized Identifiers, which are innovative technologies aimed at making digital identity more secure and private in a decentralized context. To this end, we conducted an in-depth literature review that helps us build a theoretical framework. To do this, we exploit academic sources, international W3C standards and reports from specialized organizations in order to analyze current trends and identify the advantages and difficulties of using these technologies.

Additionally, we conducted an analysis of different use cases in education, healthcare, and financial services. In each case, specific functions of VC and DID were highlighted to meet the needs of these areas: verification of educational authorizations and diplomas, preservation of confidentiality of patient health information and procedures for identification of simplification in the field of financial services. These verifiable platforms provide high security, privacy and user control over information and compliance with law regulations.

Additionally, we looked at how these technologies are used in solutions like Microsoft Entra. Microsoft Entra uses VC and DID to better manage corporate identities. By providing verifiable identities and better data protection, Microsoft Entra demonstrates the practical benefits of these technologies for organizations. This helps both keep information secure and manage digital identities more easily.

It is important to emphasize that, despite the undeniable advantages of decentralized identity technologies, several challenges remain. These include interoperability issues, often high implementation costs, and an urgent need to increase awareness among both users and organizations. To encourage broader adoption of these solutions, we have proposed several recommendations. These include establishing common standards, improving interoperability between different platforms and increasing stakeholder awareness of the benefits offered by decentralized identities. Through our research, we hope to make a significant contribution to understanding the perspectives and effects that VC certificates and DID can have on the management of digital identities.

Liste des acronymes

AD : Active Directory

ANR : Agence Nationale de la Recherche

API : Application Programming Interface

AVAX : Avalanche (a blockchain platform)

BFT : Byzantine Fault Tolerance

CBOR : Concise Binary Object Representation

CCPA : California Consumer Privacy Act

CIEM : Cloud Infrastructure Entitlement Management

CNIe : Carte Nationale d'Identité électronique (France)

CoT : Chain of Trust

DAG : Directed Acyclic Graph

DeFi : Decentralized Finance

DHT : Distributed Hash Table

DID : Decentralized Identifiers

DIDComm : Decentralized Identity Communication

DLT : Distributed Ledger Technology

DPoS : Delegated Proof of Stake

ECDSA : Elliptic Curve Digital Signature Algorithm

EDPB : European Data Protection Board

eIDAS : Electronic Identification and Trust Services (EU)

EBSI : European Blockchain Services Infrastructure

EOS : EOS.IO (blockchain platform)

EVM : Ethereum Virtual Machine

FCA : Financial Conduct Authority

FIDe : France Identité Numérique

FIDO : Fast Identity Online

FTM : Fantom (blockchain protocol)

HSM : Hardware Security Module

IETF : Internet Engineering Task Force

IPFS : InterPlanetary File System

IoT : Internet of Things

ISO : International Organization for Standardization

JWT : JSON Web Token

JWS : JSON Web Signature

JWK : JSON Web Key

JSON-LD : JavaScript Object Notation for Linked Data

MD5 : Message Digest Algorithm 5

MFA : Multi-Factor Authentication

NIST : National Institute of Standards and Technology

OIDF : OpenID Foundation

PoS : Proof of Stake

PoW : Proof of Work

RBAC : Role-Based Access Control

RPCA : Ripple Protocol Consensus Algorithm

ROI : Return on Investment

saas : Software as a service

SAML : Security Assertion Markup Language

SHA-256 : Secure Hash Algorithm 256-bit

SSI : Self-Sovereign Identity

TPS : Transactions Per Second

VC : Verifiable Credentials

W3C : World Wide Web Consortium

ZKP : Zero-Knowledge Proofs

Glossaire

Ce glossaire présente les principaux termes et concept que nous avons utilisé dans ce travail. Ces vocabulaires sont essentiels pour comprendre les technologies, principes et pratiques qui renforcent la sécurité, la confidentialité et le contrôle des utilisateurs sur leurs données personnelles.

Identité numérique : Ensemble d'informations qui représentent une personne ou entité en ligne, incluant des données personnelles et d'identification.

VC (Verifiable Credentials) : Attestations numérique permettant de prouver des informations sur une entité sans divulguer d'informations sensibles.

DID (Decentralized Identifiers) : Identifiants uniques permettant de créer des identités numériques décentralisées, contrôlées par les utilisateurs.

SSI (Self-Sovereign Identity) : Modèle d'identité décentralisée où l'utilisateur gère et contrôle pleinement ses données personnelles.

Registre distribué (DLT) : Base de doNnées partagées entre plusieurs nœuds d'un réseau, assurant la transparence et la sécurité des enregistrements.

Blockchain : Registre distribué, sécurisé et immuable, permettant de stocker des données de manière transparente et vérifiable.

Cryptographie : Science de la protection des informations par chiffrement, garantissant la confidentialité et l'intégrité des données.

Signature numérique : Méthode de validation cryptographique qui certifie l'intégrité et l'authenticité d'un document.

Consensus : Mécanisme par lequel les participants d'un réseau distribué s'accordent sur l'état des données, essentiel pour la sécurité dans les systèmes décentralisés.

Token : Unité numérique représentant une valeur ou un droit, utilisée dans les réseaux décentralisés pour gérer l'accès ou la propriété.

Contrats intelligents : Programmes automatisés exécutant des accords contractuels sur la blockchain sans intervention humaine.

Hachage : Fonction cryptographique produisant une empreinte unique pour une donnée,, utilisée pour assurer l'intégrité.

Portefeuille numérique : Application permettant de stocker et de gérer des identités et attestations numériques sécurisées.

Authenticité : Assurance que les données proviennent de la source réelle et n'ont pas été altérées.

Immuabilité : Caractéristique d'un registre ou système où les données enregistrées ne peuvent pas être modifiées.

Décentralisation : Distribution du contrôle entre plusieurs participants, correspondant à la dépendance à une autorité centrale.

Interopérabilité : Capacité de différents systèmes et plateformes à communiquer et partager des informations de manière cohérente.

Non-répudiation : Garantie qu'une action ou transaction ne peut être niée par l'auteur après réalisation.

Confidentialité : Protection des données contre les accès non autorisés, garantissant que seules les parties autorisées peuvent voir l'information.

Tolérance aux pannes byzantines (BFT) : Capacité d'un système à fonctionner correctement même si certains participants sont défaillants ou malveillants.

Table des matières

Dédicace i
Remerciements ii
Résumé iii
Abstract iv
Liste des acronymes v
Glossaire vii
Table des matières ix
Liste des figures xii
Liste des tableaux xiii
1. Introduction 1
1.1 Contexte et Importance du Projet 2
1.1.1 Présentation générale du problème de la sécurité des identités en ligne 2
1.1.2 Importance des références vérifiables (VC) et des identifiants distribués (DID) dans le paysage actuel de la cybersécurité 3
1.1.3 Objectifs spécifiques du projet 4
1.2 Problématique et Questions de Recherche 4
1.2.1 Définition des problématiques spécifiques à la sécurité des identités numériques 4
1.2.2 Questions de recherche principales 5
1.3 Méthodologie et Approche 5
1.3.1 Description des méthodes de recherche 5
1.3.2 Justification de l'approche méthodologique 7
2. État de l'Art 8
2.1 Cryptographie et Réseaux Décentralisés 8
2.1.1 Fondements de la cryptographie dans les systèmes d'identité numérique 8
2.1.2 Réseaux décentralisés et leur rôle dans les systèmes d'identité numérique 11
2.2 Technologies Associées 14
2.2.2 Registres distribués (Distributed Ledger Technology, ou DLT) 14
2.2.3 Identité auto-souveraine (SSI) 28
2.3 Applications et Cas d'Utilisation 33
2.3.2 Études de cas dans divers secteurs : 33
2.3.3 Analyse des résultats 35
2.4 Conclusion 36
3. Compréhension des Références Vérifiables (VC) et des Identifiants Distribués (DID) .. 37

3.1 Etude des références vérifiables 37
3.1.1 Définition des VC 37
3.1.2 Aperçu de l'écosystème VC 37
3.1.3 Composants des VCs 38
3.1.4 Fonctionnement des VCs 42
3.2 Etude des Identifiants Distribués (DID) 44
3.2.1 Définition des DID 44
3.2.2 Structure d'un DID 45
3.2.3 L'écosystème des Identifiants Distribués 49
3.2.4 Principes de Fonctionnement des DID 52
3.3 Protocoles et Normes des VC et DID 54
3.3.1 Protocoles de Communication et d'Authentification 55
3.3.2 Normes et Standards 55
3.4 Avantages des VC et des DID 56
3.4.1 Amélioration de la sécurité et de la vérifiabilité 56
3.4.2 Réduction des fraudes et des usurpations d'identité 56
3.4.3 Simplification des processus d'authentification et de vérification 56
3.5 Défis Techniques et Réglementaires 57
3.5.1 Défis techniques : 57
3.5.2 Défis réglementaires 57
3.6 Conclusion 58
4. Impact des VC et DID sur la Sécurité et la Vérifiabilité des Identités en Ligne 59
4.1 Problématiques Actuelles de la Sécurité des Identités en Ligne 59
4.1.1 Problèmes courants de sécurité 59
4.1.2 Limitations des systèmes d'identification traditionnels 62
4.2 Améliorations Apportées par les VC 64
4.2.1 Renforcement de la vérifiabilité des informations d'identité 64
4.2.2 Réduction des risques de falsification et d'usurpation 65
4.3 Améliorations Apportées par les DID 66
4.3.1 Autonomie des utilisateurs dans la gestion de leur identité 66
4.3.2 Amélioration de la confidentialité et du contrôle des données personnelles 68
4.4 Études de cas et exemples Pratiques 69
4.4.1 Présentation de cas d'utilisation réels 69
4.4.2 Analyse des résultats et des bénéfices obtenus 72
4.5 Conclusion 73

5. Obstacles à l'adoption des VC et des DID 74
5.1 Obstacles techniques 74
5.1.1 Limitations technologiques et solutions potentielles 74
5.1.2 Problèmes d'interopérabilité entre différentes plateformes et systèmes 77
5.2 Obstacles réglementaires 79
5.2.1 Analyse des obstacles légaux et réglementaires 79
5.2.2 Exigences en matière de conformité et solutions proposées 81
5.3 Obstacles organisationnels et culturels 82
5.3.1 Barrières internes aux organisations 82
5.3.2 Facteurs culturels influençant l'adoption 83
5.4 Conclusion 84
6. Recommandations stratégiques pour l'adoption des VC et des DID 85
6.1 Stratégies de mise en œuvre 85
6.1.1 Étapes clés pour l'implémentation des VC et DID 85
6.1.2 Meilleures pratiques pour une adoption réussie 89
6.2 Pratiques recommandées pour les développeurs 92
6.2.1 Directives pour le développement de solutions VC et DID 92
6.2.2 Outils et Framework recommandés 94
6.3 Considérations pour les décideurs politiques 98
6.3.1 Recommandations pour les régulateurs et les décideurs politiques 98
6.3.2 Politiques favorisant l'adoption des VC et DID 99
6.4 Étude du cas de microsoft entra 102
6.4.1 Présentation de Microsoft Entra 102
6.4.2 Technologies utilisées 112
6.4.3 Analyse de l'intégration des VC et DID dans Microsoft Entra 116
6.4.4 Recommandations spécifiques pour optimiser utilisation de microsoft intra 123
6.5 Conclusion 125
7. Conclusion générale et perspectives 126
7.1 Conclusion 126
7.2 Perspectives 127
Références bibliographique et webographie 128

Liste des figures

Figure 1.1 : Évolution des systèmes de gestion d'identité [1] 1
Figure 2.1 : Système de cryptographie symétrique [1] 9
Figure 2.2 : Système de cryptographie asymétrique [1] 10
Figure 2.3 : Signature numérique associé à la cryptographie asymétrique [1] 11
Figure 2.4 : Exemple d'un réseau décentralisé 12
Figure 2.5 : Triangle de confiance du Self-Sovereign Identity (SSI) 31
Figure 3.1 : Flux d'Informations et Rôles dans un Écosystème des VC [46] 38
Figure 3.2 : Composants de base d'un justificatif vérifiable [54] 39
Figure 3.3 : Exemple de VC attestant que le titulaire est diplômé d'une Licence en science à Acme University [50] 41
Figure 3.4 : Exemple de présentation vérifiable avec divulgation sélective [49] 43
Figure 3.5 : Exemple de DID [57] 45
Figure 3.6 : Composants de l'écosystème des DID [59] 49
Figure 3.7 : Exemple extrait code de DDO [63] 51
Figure 3.8 : Fonctions de résolution DID avec entrées et sorties [59] 53
Figure 3.9 : Illustration des fonctions resolve() et resolveRepresentation() [59] 54
Figure 3.10 : illustration de la positivité des VC et DID [59] 56
Figure 4.1 : Attaques de phishing par mois, mai 2020 - avril 2023 [66] 60
Figure 4.2 : Nombre d'infractions liées au cyber entre 2019 et 2023 [74] 61
Figure 4.3 : pourcentage de réutilisation des mots de passes [75] 62
Figure 4.4 : logo de BCDiploma [79] 70
Figure 4.5 : Logo de Medicalchain [82] 70
Figure 5.1 : illustration avec sidechain [89] 75
Figure 6.1 : Logo de Hyperledger Aries [136] 95
Figure 6.2 : Logo de Sovrin 95
Figure 6.3 : Logo de Veramo [138] 95
Figure 6.4 : Gestion des identités dans un environnement hybride et cloud 103
Figure 6.5 : Architecture Azure AD [175] 104
Figure 6.6 : Diagramme illustrative de l'architecture Vérification d'identité Microsoft Entra [172] 105
Figure 6.7 : exemple de diagramme illustrative du permissions management [171] 106
Figure 6.8 : Cas d'utilisations clés de gestion des autorisations [171] 107
Figure 6.9 : Gouvernance des identités [173] 108
Figure 6.10 : Gouvernance des accès [173] 108
Figure 6.11 : Gouvernance des accès privilégiés [173] 109
Figure 6.12 : illustration des identités humaine et machines [156] 111
Figure 6.13 : Architecture de Microsoft intra [161] 116

Liste des tableaux

Tableau 2.1 : Synthèse des registres distribués 25
Tableau 2.2 : Synthèse des registres distribués (blockchain, DAG, Hashgraph, Holochain) classés en fonction de leur type : avec autorisation (permissioned) et sans autorisation (permissionless), avec des exemples pour chaque cas 25
Tableau 2.3 : Comparaison des registres distribués en fonction des principes clés des registres distribués 26
Tableau 3.1 : Différentes méthodes de DID, le registre utilisé, leurs propriétés, et leurs spécificités 46
Tableau 6.1 : présentation de quelques outils 86
Tableau 6.2 : résumé des différences entre identités humaines et machines 111
Tableau 6.3 : Normes prise en charge par microsoft entra 114
Tableau 6.4 : Types de clé et des algorithmes JWT pris en charge par Microsoft Entra 115

1. Introduction

Dans un monde de plus en plus connecté, la gestion sécurisée des identités en ligne est devenue un défi majeur. Selon la norme ISO/IEC 24760 [77], la gestion des identités est l'ensemble des processus, des technologies et des standards permettant de créer, d'utiliser, de mettre à jour, de suivre et de supprimer une identité numérique. Par ailleurs, elle doit permettre, à travers des identifiants distincts pour chaque entité, d'identifier, d'authentifier, de garantir l'intégrité, de contrôler et de suivre l'usage des informations d'identifications et données personnelles [1].

Une identité numérique est un instantané de l'identité réelle d'une personne, d'une entreprise, d'un appareil, d'une voiture, plus généralement : d'une entité. L'identité réelle englobe toutes les caractéristiques déterminantes d'une entité, ce qui la distingue des autres. Chaque identité numérique ne consiste qu'en un fragment de l'identité et est généralement créée dans un but spécifique dans un contexte spécifique, pour utiliser un service particulier ou pour interagir avec une autre entité. Les différentes identités numériques diffèrent par leur niveau de détail : en ce qui concerne les propriétés fournies (telles que le nom, âge, etc.) l'exactitude de leur description et le degré d'abstraction (par exemple : nom complet vs nom sur la carte d'identité plus nom de naissance, date de naissance/âge précis vs âge de la majorité légale) [5]. Une identité numérique peut être simplement décrite comme un moyen permettant aux personnes de prouver électroniquement qu'elles sont bien celles-là [6]. Nous pouvons donc définir l'identité en ligne comme l'ensemble des informations et des caractéristiques qui représentent une personne ou une entité sur Internet.

Ce projet vise à explorer des technologies émergentes pour renforcer cette sécurité. L'introduction de ce projet de recherche fournit un cadre détaillé pour comprendre les enjeux de la sécurité des identités en ligne, ainsi que l'importance et les objectifs de l'étude sur les références vérifiables (VC) et les identifiants distribués (DID).

Avant l'intégration des DID et des VC dans les technologies, les systèmes de gestions des identités ont connu plusieurs modèles.

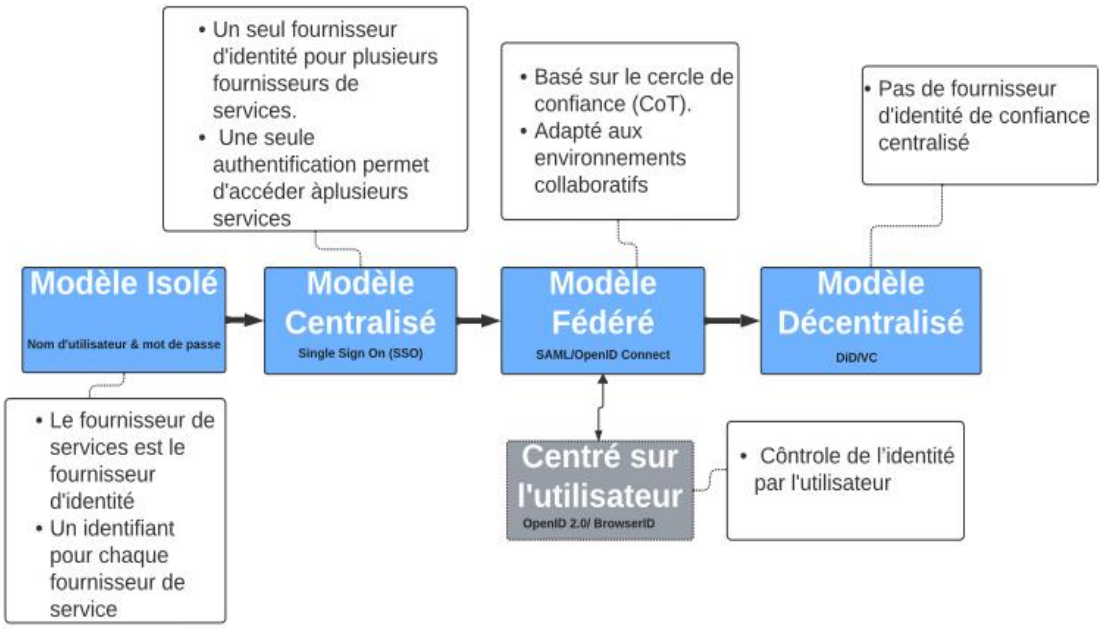


Figure 1.1 : Évolution des systèmes de gestion d'identité [1]

- **Le modèle de gestion isolée**

Egalement appelé gestion de l'identité de l'utilisateur le fournisseur de service ou le fournisseur d'identité est totalement responsable de la gestion des identifiants et des informations de ses utilisateurs. Donc, chaque service ou fournisseur avec lequel l'utilisateur interagit lui donne son propre identifiant. Par conséquent, un utilisateur doit gérer des identifiants séparés pour chaque service, dont il est un utilisateur. Par conséquent, le nombre d'identités à gérer de l'utilisateur est multiplié d'une manière significative.

- **Le modèle de gestion centralisée**

Le modèle de gestion centralisée des identités est une méthode de gestion des identités des utilisateurs dans laquelle une entité est responsable de la gestion des identifiants des utilisateurs. Ces identifiants uniques sont créés pour les utilisateurs eux-mêmes, qui seront utilisés pour accéder à différents services. Cette approche vise à simplifier et à sécuriser le processus d'authentification en centralisant la gestion des identités, ce qui peut faciliter la gestion des accès aux services et renforcer la sécurité des données.

- **Le modèle de gestion fédérée**

Le modèle de gestion fédérée vise à simplifier l'accès aux services en regroupant plusieurs fournisseurs de services au sein d'une fédération et en permettant aux utilisateurs d'utiliser un seul ensemble d'identifiants pour accéder à l'ensemble des services offerts, tout en maintenant une certaine gestion des identités multiples.

- **Le modèle décentralisé**

Le modèle de gestion décentralisée des identités est une approche où la responsabilité de la gestion des identifiants des utilisateurs est répartie entre plusieurs entités plutôt que centralisée. Dans ce modèle, chaque fournisseur de services est responsable de la création et de la gestion des identifiants de ses propres utilisateurs. Contrairement au modèle centralisé, où une seule entité fournit des identifiants pour tous les services, le modèle décentralisé permet une plus grande autonomie et flexibilité pour chaque fournisseur de services. Cela peut être réalisé via des protocoles d'authentification distribués tels que OAuth ou OpenID Connect, où les utilisateurs peuvent utiliser les identifiants délivrés par une entité pour accéder à plusieurs services sans que ces derniers partagent nécessairement des données d'identification.

1.1 Contexte et Importance du Projet

Pour bien comprendre l'importance de ce projet, il est essentiel de situer le contexte global dans lequel il s'inscrit. La prolifération des cyberattaques et des vols d'identité a mis en lumière les limites des méthodes traditionnelles d'authentification. Dans ce cadre, les références vérifiables et les identifiants distribués se présentent comme des solutions prometteuses.

1.1.1 Présentation générale du problème de la sécurité des identités en ligne

La sécurité des identités en ligne est devenue un enjeu crucial dans notre société de plus en plus numérisée. Avec l'augmentation des transactions et des interactions sur internet, la protection des informations personnelles et des identités numériques est essentielle pour prévenir les fraudes, les vols d'identité et les violations de données. Les méthodes traditionnelles d'authentification, telles que les mots de passe et les questions de sécurité, se

révèlent souvent insuffisantes face à la sophistication croissante des cyberattaques. Cette situation nécessite le développement de solutions plus robustes et innovantes pour garantir la sécurité et la confidentialité des identités numériques.

Dans ce contexte, l'identité auto-souveraine (Self-Sovereign Identity, SSI) émerge comme une solution révolutionnaire. Le SSI est un nouveau modèle de système de gestion des identités numériques qui donne aux utilisateurs le pouvoir et la possibilité de définir eux-mêmes leurs propres identités numériques et d'assurer le contrôle de leurs données personnelles sans dépendre de fournisseurs de services centralisés. Dans [2], un SSI est défini comme un concept d'identité, dans lequel l'individu est libre de revendiquer sa propre identité sans partie de confiance centralisée. Les systèmes d'identités auto-souveraine tentent de répondre aux préoccupations en matière de confidentialité et de protection de données soulevées par les précédents systèmes de gestion des identités.

Les utilisateurs peuvent gérer leurs informations d'identité via des technologies décentralisées, réduisant ainsi les risques associés aux points de défaillance uniques et aux violations de données centralisées. En offrant aux utilisateurs un contrôle total sur leurs données, le SSI améliore la confidentialité et la sécurité tout en facilitant des processus d'authentification plus robustes.

Les technologies du SSI, telles que les DID et les VC, permettent de créer des écosystèmes où la vérification de l'identité peut être effectuée de manière sécurisée et privée. Les DID permettent de créer des identités numériques décentralisées, tandis que les VC permettent la vérification de ces identités sans exposer de données sensibles. Ensemble, ces technologies offrent une solution complète pour la gestion sécurisée des identités numériques, répondant aux besoins actuels de sécurité et de confidentialité dans un paysage numérique de plus en plus menacé par les cyberattaques.

1.1.2 Importance des références vérifiables (VC) et des identifiants distribués (DID) dans le paysage actuel de la cybersécurité

Dans le contexte actuel de cybersécurité, marqué par le développement de l'internet et la multiplication des cyberattaques, les VC et les DID ont un rôle très important à jouer.

Les identifiants décentralisés (DID) sont un nouveau type d'identifiant destiné à un système d'identité auto-souverain, c'est-à-dire entièrement sous le contrôle d'une entité et ne dépendant pas d'un registre centralisé ou d'une autorité de certification [4].

Un DID est une URL qui fait référence à une entité pour les interactions de confiance [3].

Les DID sont des identifiants uniques et persistants qui permettent de représenter des entités numériques (comme des personnes, des organisations ou des objets) dans un environnement décentralisé.

Les empreintes des documents sources seraient enregistrées sous la forme d'assertions vérifiables, prouvant l'intégrité du document source (y compris sa date d'émission précisément enregistrée). Un vérificateur disposant des autorisations requises pour satisfaire au contrôle d'accès serait en mesure de s'assurer que les documents présentés par une personne sont exacts et valides [7].

Ainsi, les assertions vérifiables sont utilisées pour associer une identité à une clé publique dans un système décentralisé, là où les certificats numériques signés d'une autorité de certification sont employés dans un système centralisé [7].

Les VC sont des déclarations numériques qui permettent de prouver des informations spécifiques concernant une entité. Elles sont utilisées pour attester de la véracité de certaines données.

Les VC et les DID représentent des technologies émergentes offrant des promesses significatives pour l'amélioration de la sécurité des identités en ligne. Les VC permettent de créer des attestations numériques sécurisées et vérifiables, réduisant ainsi les risques de falsification et de fraude. Les DID, quant à eux, permettent aux utilisateurs de posséder et de contrôler leurs propres identités numériques de manière décentralisée, sans dépendre d'autorités centrales. Ensemble, ces technologies offrent une nouvelle approche de l'authentification et de la gestion des identités, favorisant une meilleure sécurité, une plus grande confidentialité et une réduction de la dépendance aux intermédiaires de confiance traditionnels.

1.1.3 Objectifs spécifiques du projet

Ce projet de recherche vise à explorer en profondeur les références vérifiables et les identifiants distribués pour évaluer leur potentiel à améliorer la sécurité des identités en ligne. Les objectifs spécifiques incluent :

- **Comprendre les principes des VC et des DID**

Nous analyserons leur fonctionnement, leurs avantages et les défis techniques et réglementaires associés.

- **Évaluer l'impact sur la sécurité et la vérifiabilité**

Dans cette partie, nous examinerons comment ces technologies peuvent renforcer l'authentification et la sécurité des identités en ligne.

- **Identifier les obstacles à l'adoption**

Ici nous tenterons de déterminer les obstacles à la mise en œuvre et à l'acceptation généralisée de ces technologies.

- **Formuler des recommandations stratégiques**

Et enfin nous essayerons de proposer des stratégies pour faciliter l'adoption des VC et des DID, en utilisant le produit Entra de Microsoft comme cadre de référence.

1.2 Problématique et Questions de Recherche

1.2.1 Définition des problématiques spécifiques à la sécurité des identités numériques

La sécurité des identités numériques pose plusieurs défis majeurs, tels que la vulnérabilité aux cyberattaques, la difficulté de vérification de l'authenticité des identités et la gestion centralisée des données personnelles. Ces problématiques sont exacerbées par la fragmentation des systèmes de gestion des identités et le manque de normes de sécurité

unifiées. Le besoin de solutions qui offrent une sécurité renforcée, tout en étant facilement adoptables et interopérables, est donc primordial.

1.2.2 Questions de recherche principales

Les questions de recherche de ce projet sont formulées pour aborder les principaux défis et opportunités liés à l'utilisation des VC et des DID :

- ***Comment les références vérifiables et les identifiants distribués peuvent-ils améliorer la vérifiabilité et la sécurité des identités numériques ?***
- ***Quels sont les principaux avantages et défis techniques des VC et des DID pour la gestion des identités en ligne ?***
- ***Quels sont les obstacles à l'adoption des VC et des DID par les utilisateurs et les organisations ?***
- ***Quelles recommandations stratégiques peuvent être proposées pour encourager l'adoption de ces technologies ?***

Ces questions guideront l'étude et permettront de fournir des réponses détaillées sur l'efficacité et la viabilité des VC et des DID en tant que solutions innovantes pour la gestion sécurisée des identités numériques.

1.3 Méthodologie et Approche

Une méthodologie de recherche est cruciale pour pouvoir structurer le travail de manière cohérente et rigoureuse. Dans cette partie, nous allons montrer comment nous allons procéder pour répondre aux besoins de recherche et d'atteindre les objectifs spécifiques du projet.

1.3.1 Description des méthodes de recherche

Pour mener à bien cette étude, nous allons utiliser deux méthodes de recherches à savoir : des analyses documentaires et des analyses de cas d'utilisations.

- **Analyse documentaire**

Une analyse documentaire riche et approfondie permet de comprendre l'état de l'art, les théories existantes et les cadres conceptuels autour des VC et DID. Les différentes étapes que nous avons suivies lors de cette étude sont :

- ✓ **Sélection de sources**

Tout d'abord nous avons choisi des sources de recherches à savoir google scholar [9], ArXiv [8], et des sites web et blogs que nous avons jugés intéressants.

- ✓ **Recherche de littérature**

Ensuite nous avons effectué une collecte d'articles académiques, des livres, des rapports d'organisations et des normes (W3C).

- ✓ **Analyse des contenus**

Par la suite nous avons exploité les documents pour extraire des informations clés sur les VC, les DID ainsi que la gestion des identités en ligne.

- ✓ **Synthèse des informations**

Après avoir extrait les informations pertinentes, nous les avons organisés pour construire un cadre théorique c'est-à-dire identifier les tendances, les avantages, les inconvénients et les défis des différentes approches des gestions des identités.

- **Analyse de cas d'utilisation**

L'analyse de cas d'utilisation a pour but de comprendre l'application concrète des VC et des DID dans différents contextes et domaines d'usage. Cette méthode permet d'identifier comment ces technologies sont intégrées dans des systèmes existants, de mesurer leurs impacts et de tirer des leçons sur leurs bénéfices et limitations. Les étapes clés observées lors de cette analyse sont les suivantes :

- ✓ **Identification des cas d'utilisation**

Nous avons d'abord sélectionné des cas d'utilisation pertinents en nous concentrant sur les secteurs de l'éducation, de la santé, et des services financiers. Ces domaines offrent des exemples variés et concrets de l'implémentation des identités numériques décentralisées, avec des enjeux importants en matière de sécurité et de protection de la vie privée.

- ✓ **Définition des objectifs et exigences**

Pour chaque cas d'utilisation, nous avons défini les objectifs spécifiques, comme la vérification sécurisée de l'identité, la protection des données sensibles, et l'amélioration de l'expérience utilisateur. Nous avons également identifié les exigences techniques et réglementaires à respecter, en particulier la conformité aux normes de sécurité (ex : RGPD) et l'interopérabilité entre systèmes.

- ✓ **Collecte de données sur les solutions existantes**

Nous avons ensuite étudié les solutions concrètes mises en œuvre par certaines organisations ou entreprises dans chaque domaine. Par exemple :

- Dans l'éducation, nous avons analysé des projets comme BCDiploma, qui utilise les VC pour émettre des diplômes vérifiables.
- Dans la santé, nous avons examiné des initiatives comme Medicalchain, qui permet aux patients de gérer leurs données médicales de manière décentralisée.
- Dans les services financiers, nous avons exploré des projets de KYC (Know Your Customer) décentralisés pour simplifier et sécuriser l'identification des clients.

- ✓ **Évaluation des avantages et des limites**

Chaque cas d'utilisation a été évalué en fonction de ses avantages, notamment la sécurité, la décentralisation et le contrôle utilisateur, mais aussi de ses limitations. Nous avons analysé les obstacles rencontrés, tels que les défis d'interopérabilité, les coûts de mise en œuvre et les résistances à l'adoption.

- ✓ **Synthèse des leçons apprises**

Enfin, nous avons synthétisé les enseignements de chaque cas pour identifier des tendances communes et des recommandations pour l'avenir. Cela nous a permis de mieux comprendre

les conditions nécessaires pour une adoption réussie des VC et DID et d'envisager des améliorations pour maximiser leur impact dans différents contextes.

1.3.2 Justification de l'approche méthodologique

La justification de l'approche méthodologique est essentielle pour démontrer la pertinence et l'efficacité des méthodes choisies, afin de garantir que les objectifs de recherche soient atteints de manière exhaustive et rigoureuse.

- ✓ **Analyse documentaire**

L'analyse documentaire nous a permis d'avoir une base théorique solide, d'identifier les travaux antérieurs et d'établir le contexte scientifique et technologique du projet. Elle est essentielle pour la compréhension des concepts clés, les tendances et les normes en matière de gestion des identités numériques.

- ✓ **Analyse de cas d'utilisation**

Une brève analyse de cas d'utilisation est un aspect essentiel pour comprendre comment les technologies étudiées, telles que les Verifiable Credentials et les Decentralized Identifiers, sont appliquées dans des contextes réels. Elle nous a permis de visualiser concrètement l'impact de ces technologies sur les utilisateurs, les processus et les systèmes, tout en mettant en évidence leurs avantages, défis et opportunités.

En résumé, cette approche méthodologique intégrée combinant analyse documentaire et analyse de cas d'utilisation permet de traiter de manière exhaustive et rigoureuse les questions de recherche, tout en offrant des insights théoriques et pratiques précieux pour l'adoption des technologies de VC et DID.

2. État de l'Art

L'état de l'art dans le domaine de la cryptographie et des réseaux décentralisés est en constante évolution, avec de nouvelles technologies et concepts émergents pour répondre aux besoins croissants de sécurité et d'intégrité des systèmes d'identité numérique.

2.1 Cryptographie et Réseaux Décentralisés

La cryptographie et les réseaux décentralisés jouent un rôle crucial dans la sécurisation et la gestion des identités numériques modernes.

2.1.1 Fondements de la cryptographie dans les systèmes d'identité numérique

Les fondements de la cryptographie sont essentiels pour garantir la sécurité et l'intégrité des systèmes d'identité numérique, en permettant de protéger les données personnelles et les transactions numériques contre les menaces de piratage et d'usurpation d'identité.

- ✓ **Définition de la cryptographie**

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle nous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire. [10]

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses [12].

La cryptographie est une discipline du domaine de la sécurité de l'information et des communications qui permet à travers des primitives mathématiques de fournir un ensemble de services de sécurité telles que la confidentialité, l'intégrité, l'authenticité et la non répudiation [11].

En analysant les trois définitions, on peut formuler la définition suivante de la cryptographie :

La cryptographie est une filière interdisciplinaire qui utilise les mathématiques, l'informatique et parfois la physique pour sécuriser et protéger les données sensibles. Elle permet le chiffrement et le déchiffrement des informations, assurant ainsi la confidentialité, l'intégrité, l'authenticité et la non répudiation lors de leur stockage et de leur transmission à travers des réseaux non sécurisés comme Internet.

- ✓ **Quelques concepts clés et techniques de la cryptographie**

La cryptographie englobe plusieurs concepts et techniques essentiels qui sont utilisés pour sécuriser les communications et les données numériques. Voici quelques-uns des principaux concepts clés et techniques en cryptographie :

- ✓ **Confidentialité**

La confidentialité est le principe de protéger les données sensibles contre les tiers non autorisés. L'objectif est de prévenir que des personnes ou des organisations non autorisées ne puissent accéder, lire, modifier, copier ou utiliser les données protégées. La confidentialité garantit que les données ne sont pas lues, modifiées ou utilisées par des tiers non autorisés.

- ✓ **Authenticité**

L'authenticité garantit que les données sont véritables et ont été envoyées par l'expéditeur réel. Cela signifie que les données ne peuvent pas être falsifiées, altérées ou volées pour prétendre être envoyées par une autre personne ou organisation. L'authenticité vérifie l'identité de l'émetteur et garantit que les données ne sont pas modifiées en cours de transmission.

- ✓ **Intégrité**

L'intégrité garantit que les données ne sont pas altérées ou modifiées non autorisées. Cela signifie que les données sont intactes et non modifiées pendant leur stockage ou leur transmission. L'intégrité empêche tout changement accidentel ou intentionnel des données sans autorisation.

- ✓ **Cryptographie symétrique**

Aussi appelé chiffrement symétrique ou encore chiffrement à clé secrète, est une technique qui utilise des algorithmes cryptographiques pour chiffrer ou déchiffrer des messages. Cette méthode repose sur le partage d'une même clé entre deux entités engagées dans une communication. La clé en question est utilisée pour le cryptage et le décryptage des messages.

Les algorithmes symétriques les plus connus sont dans l'ordre chronologique de définition, le DES (Data Encryption Standard), le 3DES (prononcé « Triple DES »), et l'AES (Advanced Encryption Standard). [14]

La figure suivante montre un peu plus en détails sur le fonctionne le chiffrement symétrique.

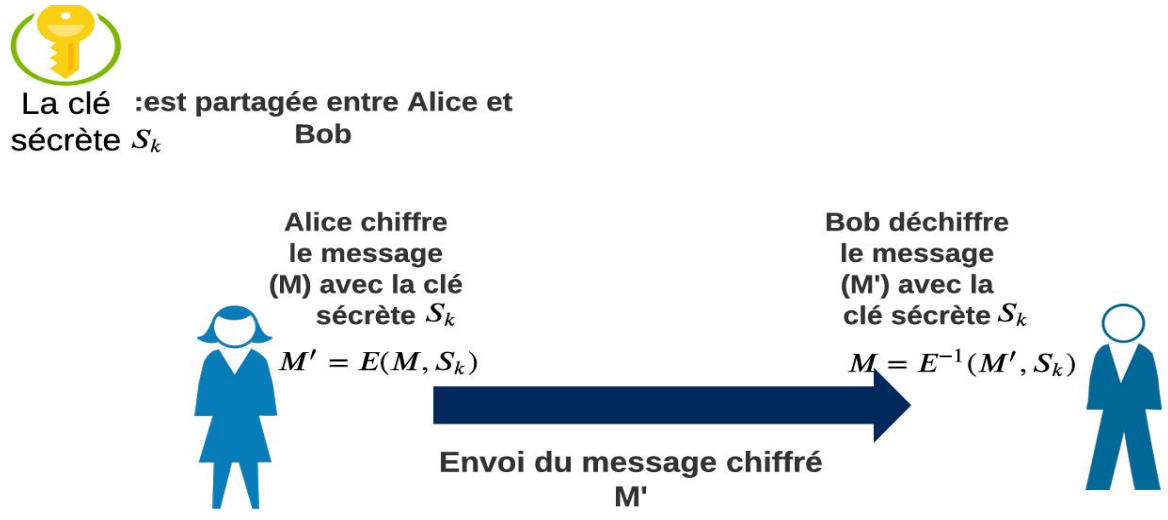


Figure 2.1 : Système de cryptographie symétrique [1]

Avec :

$\boldsymbol{E}$: la fonction de chiffrement

$\boldsymbol{E^{-1}}$: la fonction de déchiffrement

✓ **Cryptographie asymétrique**

Le chiffrement asymétrique ou à clé publique est une technique cryptographique dans laquelle les entités concernées utilisent des clés de chiffrement différentes. Chacune des entités crée sa propre paire de clé de chiffrement, qui se compose d'une clé privée et d'une clé publique. Les interlocuteurs disposant de la clé publique peuvent envoyer des données cryptées au propriétaire de la clé privée, vérifier leur signature numérique ou les authentifier. La clé privée peut ensuite être utilisée pour décrypter les données cryptées à partir de la clé publique. Quelques algorithmes utilisés dans la cryptographie asymétrique : RSA (Rivest-Shamir-Adleman) et ECDSA (Elliptic Curve Digital Signature Algorithm) sont deux algorithmes de cryptographie asymétrique utilisés pour la signature numérique et l'authentification.

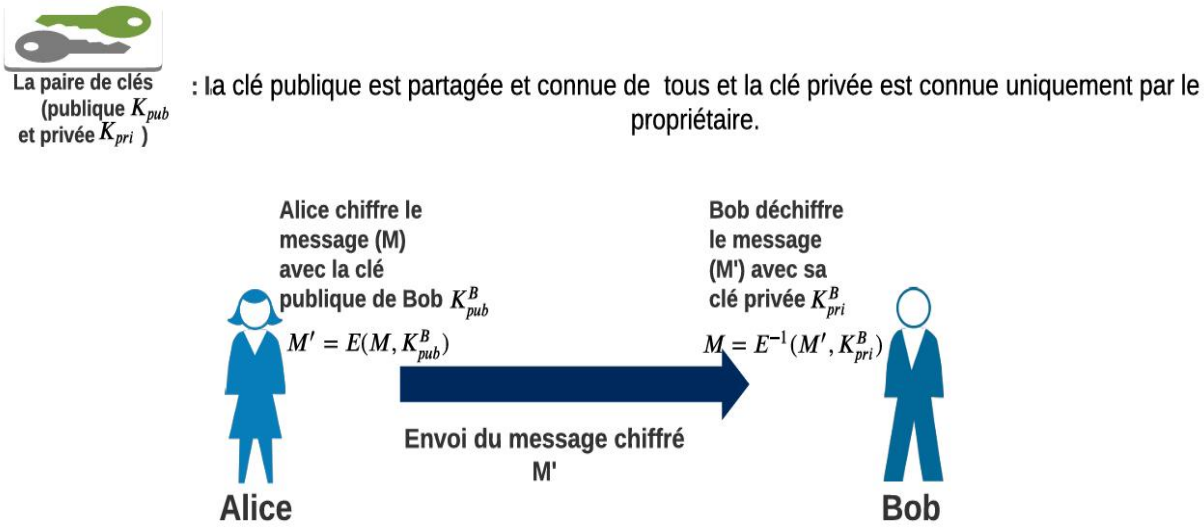


Figure 2.2 : Système de cryptographie asymétrique [1]

Avec :

E : la fonction de chiffrement

E^{-1} : la fonction de déchiffrement

✓ **Fonctions de hachage**

Une fonction de hachage est un algorithme à sens unique qui prend en entrée une donnée de taille arbitraire et fournit en sortie une donnée de longueur fixe appelée hache ou empreinte. La taille d'une valeur de hache varie en fonction de l'algorithme. À titre d'exemple, les algorithmes MD5, SHA-1, SHA-256 ont des tailles d'empreintes respectives de 128, 160, 256 bits. [15]

La fonction de hachage est une fonction à sens unique, ce qui signifie qu'on ne peut pas accéder à son entrée en utilisant la sortie. La fonction de hash est utilisée pour stocker en toute sécurité les mots de passe, trouver des enregistrements en double, stocker et récupérer rapidement des informations, etc. [1]

Fonction mathématique à sens unique, utilisée en informatique et en cryptographie pour calculer l'empreinte de données afin de garantir leur intégrité, ne permettant pas de remonter à la donnée d'entrée. [7]

Nous pouvons à cet effet définir une fonction de hachage comme un algorithme qui prend en entrée une donnée de taille quelconque et produit une sortie de longueur fixe appelée hache ou empreinte. Cette fonction est à sens unique, ce qui signifie qu'il est impossible de retrouver l'entrée à partir de la sortie. Les fonctions de hachage sont utilisées pour sécuriser les mots de passe, détecter les doublons et stocker ou récupérer rapidement des informations.

MD5 (Message Digest Algorithm 5) et SHA-256 (Secure Hash Algorithm 256-bit) sont deux fonctions de hachage cryptographiques utilisées pour garantir l'intégrité des données en générant des empreintes numériques uniques à partir de données d'entrée.

- ✓ **Signature numérique**

La signature électronique est un ensemble de mesures techniques qui visent à garantir l'intégrité d'un document et d'en authentifier son auteur. Cette dernière est donc obligatoirement liée à un document mais également à la personne qui l'appose. [12]

La signature numérique repose sur la cryptographie asymétrique utilisant une paire de clés, la clé privée doit être conservée secrète par son possesseur car elle sert à construire la signature numérique d'une donnée ou d'un document, tandis que la clé publique est communiquée au destinataire et sert à authentifier l'émetteur et à vérifier l'intégrité des données transmises. La signature numérique permet à l'utilisateur de prouver qu'il est en possession de la clé privée. [7]

Cette primitive cryptographique permet de fournir les services d'intégrité, d'authenticité et de non répudiation. Un schéma de signature numérique permet de générer une signature sur un message telle que la signature soit valide par rapport à une clé publique si et seulement si elle ait été produite en utilisant la clé privée correspondante. [11]

Les signatures numériques vérifient l'authenticité, l'origine, et l'intégrité des données, tout en assurant la non-répudiation. Elles jouent un rôle crucial en cryptographie, comparables aux signatures manuscrites mais bien plus sécurisées et pratiquement infalsifiables.



Figure 2.3 : Signature numérique associé à la cryptographie asymétrique [1]

2.1.2 Réseaux décentralisés et leur rôle dans les systèmes d'identité numérique

Les réseaux décentralisés pour les systèmes d'identité numérique présentent une alternative intéressante aux systèmes centralisés traditionnels. En utilisant des technologies comme la blockchain et les registres distribués, ces réseaux permettent aux individus de contrôler et de gérer leurs identités numériques de manière autonome.

- ✓ **Définition d'un Réseau décentralisé**

Contrairement aux réseaux centralisés, un réseau décentralisé répartit le contrôle entre de nombreux nœuds. Dans cette configuration, chaque nœud fonctionne de manière indépendante et le réseau reste fonctionnel même si un nœud tombe en panne. [18]

L'architecture décentralisée est un paradigme de conception de système qui distribue les composants, les fonctions et les processus à travers le réseau. Contrairement aux systèmes centralisés où la prise de décision et le traitement des données sont concentrés en un point central, les systèmes décentralisés répartissent ces fonctions sur plusieurs points ou nœuds du réseau. [17]

Nous pouvons définir un réseau décentralisé comme un système où le contrôle et le traitement des données sont répartis entre plusieurs nœuds. Chaque nœud fonctionne indépendamment, et le réseau continue de fonctionner même si certains nœuds tombent en panne. Contrairement à un réseau centralisé, où tout est contrôlé par un point unique, un réseau décentralisé distribue les responsabilités à travers le réseau, rendant le système plus robuste et sécurisé.

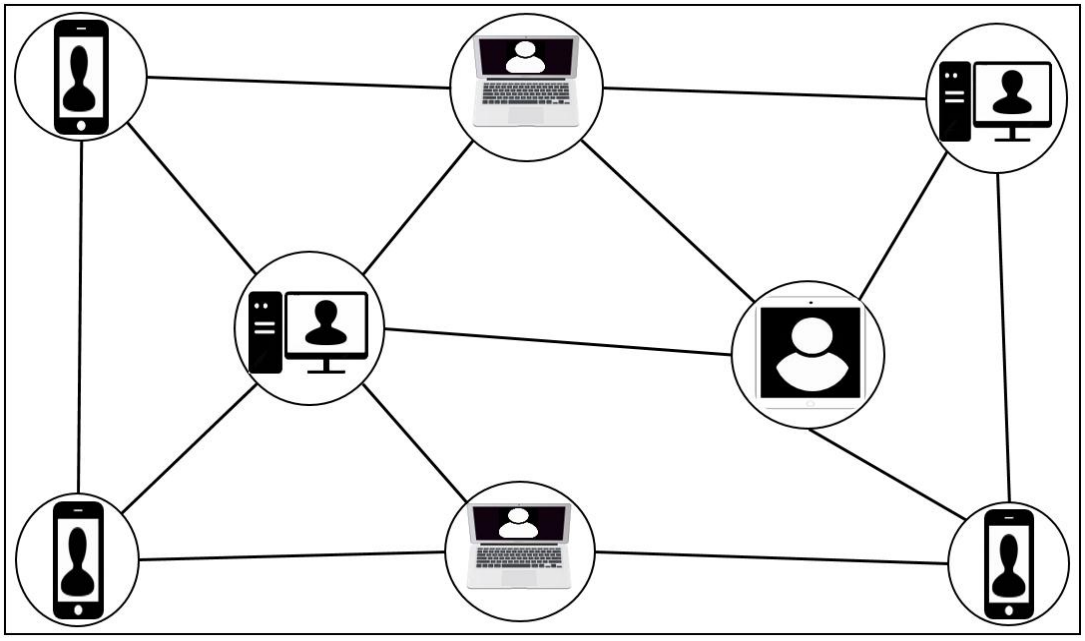


Figure 2.4 : Exemple d'un réseau décentralisé

- ➢ **Quelques avantages des réseaux décentralisés**

Les réseaux décentralisés offrent de nombreux avantages par rapport aux réseaux centralisés traditionnels. Ces avantages font des réseaux décentralisés une alternative prometteuse pour de nombreuses applications modernes, allant des finances décentralisées (DeFi) aux systèmes de gestion de données, en passant par les infrastructures de communication, parmi lesquels figurent :

- ✓ **Souveraineté et contrôle utilisateur**

Dans un réseau décentralisé, les utilisateurs possèdent et contrôlent directement leurs données et ressources. Cela élimine la dépendance à une autorité centrale, permettant aux individus et aux organisations de décider comment leurs informations sont utilisées et partagées. Cette autonomie renforce la confidentialité et le contrôle personnel.

- **Indépendance**

Les utilisateurs ne dépendent pas d'une seule entité ou d'un gouvernement central. Chaque participant a un rôle actif dans le réseau, ce qui renforce leur autonomie.

- **Contrôle local**

Les décisions concernant les règles du réseau sont prises collectivement par les nœuds participants, plutôt que par une seule autorité centrale. Cela favorise la prise de décision commune et locale.

- ✓ **Sécurité renforcée**

Les réseaux décentralisés distribuent les données et les transactions sur plusieurs nœuds, rendant les attaques cybernétiques plus difficiles. L'absence d'un point de défaillance unique diminue le risque de compromission et augmente la résilience du réseau. De plus, les technologies cryptographiques avancées utilisées dans ces réseaux offrent une protection supplémentaire contre les intrusions et les manipulations.

- **Résilience aux attaques**

Étant donné qu'il n'y a pas de point central unique à attaquer, les réseaux décentralisés sont plus résistants aux cyberattaques. Si un nœud est compromis, les autres continuent de fonctionner.

- **Chiffrement et confidentialité**

Les communications entre les nœuds peuvent être chiffrées, ce qui renforce la confidentialité des données. De plus, les utilisateurs ont un meilleur contrôle sur leurs informations personnelles.

- ✓ **Réduction des frais et efficacité accrue**
- **Moins de frais de transaction**

Dans les réseaux décentralisés, les transactions sont directes entre les parties concernées, sans intermédiaires coûteux comme les banques ou les plateformes de paiement. Cela réduit les frais de transaction.

- **Élimination des frais de conversion**

Les réseaux décentralisés utilisent souvent des cryptomonnaies universelles, ce qui élimine les frais de conversion entre différentes devises.

- **Automatisation**

Les contrats intelligents et les protocoles décentralisés automatisent de nombreuses opérations, réduisant les délais et les erreurs humaines.

- **Temps de traitement plus rapide**

Les transactions directes entre les parties prenantes se font plus rapidement que dans les systèmes centralisés, où les transactions doivent passer par plusieurs étapes.

2.2 Technologies Associées

Cette sous-section se penche sur les technologies innovantes qui soutiennent la gestion des identités numériques avec un focus sur les registres distribués, la blockchain, et l'identité auto-souveraine. Concernant la DLT et la blockchain, nous essayerons d'en discuter en termes d'applications potentielles dans les systèmes d'identité numérique, tandis que pour le SSI nous explorerons le concept d'individus ayant un contrôle total sur leurs identités numériques.

2.2.2 Registres distribués (Distributed Ledger Technology, ou DLT)

La technologie du grand livre distribué influence presque tous les aspects de la société. Elle se présente comme une alternative aux monopoles des différentes plateformes. En effet, les bases de données partagées entre plusieurs sites, régions ou participants permettent de créer un marché numérique mondial du commerce. Ce type d'architecture révolutionne la gestion des documents, en transformant de façon radicale la collecte et la transmission des données. [22]

Toutes les informations du grand livre sont stockées de manière sécurisée et précise à l'aide de la cryptographie. Elles sont consultables grâce aux signatures cryptographiques. Une fois les données stockées, elles deviennent une base de données immuable, régie par les règles du réseau. Grâce à leur répartition sur de nombreux ordinateurs, ces informations deviennent plus difficiles à corriger et à hacker, ajoutant ainsi de la sécurité au modèle. [22]

Les registres distribués représentent une avancée significative dans la manière dont les données sont stockées, partagées et sécurisées à travers divers systèmes. Cette technologie repose sur la décentralisation, où les informations sont enregistrées sur plusieurs nœuds d'un réseau plutôt que sur un seul serveur central. Dans la suite, nous essayerons de faire une brève présentation des DTL pour une meilleure compréhension des technologies dans lesquelles sont issus les VC et les DID.

- **Définitions**

Un registre distribué est une base de données partagée, répliquée et synchronisée entre les membres d'un réseau décentralisé. Il enregistre les transactions, telles que l'échange d'actifs ou de données, entre les participants du réseau. Les registres distribués peuvent être utilisés dans presque tous les secteurs où des données sont collectées et utilisées. [20]

Les DLT bouleversent les modèles traditionnels de gestion des transactions en éliminant la nécessité d'une autorité centrale. Ce type de technologie repose sur un réseau décentralisé de participants (ou nœuds) qui valident et enregistrent des transactions de manière sécurisée, garantissant ainsi transparence, traçabilité et immuabilité. [21]

La technologie du registre distribué se définit comme une infrastructure de base de données qui permet l'enregistrement, le partage et la synchronisation des transactions et des données entre plusieurs participants de manière décentralisée, sans recourir à une autorité centrale. Les DLT reposent sur des mécanismes de consensus pour garantir la sécurité et l'intégrité des données.

- **Les principes des registres distribués**

Un registre distribué doit respecter plusieurs principes et caractéristiques pour être efficace et fiable. Les principaux aspects auxquels un registre distribué doit adhérer sont :

- ✓ **Décentralisation**

Les données et les processus doivent être répartis sur un réseau d'ordinateurs indépendants plutôt que centralisés chez une seule entité. Cela garantit la résilience et réduit les risques de défaillance unique.

- ✓ **Consensus**

Les participants au réseau doivent parvenir à un accord sur l'état du registre à un moment donné. Le mécanisme de consensus garantit la cohérence des données à travers le réseau, même en présence de participants malveillants.

- ✓ **Sécurité**

Les données stockées sur le registre doivent être sécurisées contre la falsification et l'accès non autorisé. Cela est généralement assuré par des techniques cryptographiques avancées et des protocoles de sécurité robustes.

- ✓ **Transparence**

Les transactions et les mises à jour du registre doivent être visibles pour tous les participants autorisés, favorisant ainsi la transparence et la confiance dans le système.

- ✓ **Immuabilité**

Une fois enregistrées, les transactions ne doivent pas être modifiées ni effacées de manière non autorisée. Cette caractéristique est cruciale pour garantir l'intégrité des données sur le long terme.

- ✓ **Efficacité**

Le registre distribué doit être capable de gérer un grand volume de transactions de manière efficace et rapide, tout en minimisant les frais et les délais associés.

- ✓ **Interopérabilité**

Dans certains cas, il est essentiel que le registre distribué puisse interagir avec d'autres systèmes ou réseaux de manière cohérente et sans friction.

En respectant ces principes, un registre distribué peut fournir une infrastructure solide pour diverses applications, offrant sécurité, transparence et efficacité dans les échanges de données et les transactions entre les parties prenantes.

➢ **Catégories de technologie du registre distribué**

Les registres distribués sont généralement classés en deux catégories : les DLT avec autorisation et les DTL sans autorisation.

- **Registre distribué avec autorisation (permissioned)**

Dans cette catégorie, les nœuds du réseau nécessitent une autorisation pour participer au consensus.

Le grand livre distribué autorisé implique l'exigence d'une autorisation pour les nœuds des entités centrales. Ce procédé permet d'accéder au réseau et apporter des modifications dans le grand livre. Les contrôles d'accès dans un registre distribué autorisé incluent généralement la vérification d'identité. [22]

- **Registre distribué sans autorisation (permissionless)**

D'un autre côté, dans le cas des registres distribués sans autorisation, chaque nœud du réseau contient une copie complète et mise à jour de l'ensemble du registre. Tous les ajouts locaux proposés par les participants sont communiqués à tous les nœuds du réseau. [22]

Contrairement au modèle autorisé, ce type de registre distribué ne requiert pas d'autorisation préalable. Dans cette catégorie, les nœuds peuvent participer librement au réseau sans restriction.

➢ **Consensus**

- **Définition**

Le consensus dans le contexte des registres distribués est un mécanisme par lequel les nœuds participants d'un réseau décentralisé s'accordent sur l'état actuel du registre. Il s'agit de l'ensemble de règles et de processus qui garantissent que toutes les copies du registre distribuées à travers le réseau sont identiques, assurant ainsi l'intégrité et la cohérence des données.

- **Exemples de Consensus**
- **Proof of Work (PoW)**

Utilisé par Bitcoin, où les mineurs résolvent des puzzles cryptographiques pour ajouter des blocs à la blockchain.

- **Proof of Stake (PoS)**

Utilisé par Ethereum 2.0, où les validateurs sont choisis en fonction de la quantité de crypto-monnaie qu'ils détiennent et mettent en jeu.

- **Delegated Proof of Stake (DPoS)**

Utilisé par EOS, où les détenteurs de tokens élisent des délégués pour valider les transactions.

- **Byzantine Fault Tolerance (BFT)**

Utilisé par Hyperledger Fabric, où un sous-ensemble des nœuds doit approuver les transactions pour atteindre le consensus.

- **Hashgraph's Virtual Voting**

Utilisé par Hedera Hashgraph, où les transactions sont ordonnées via un mécanisme de vote virtuel sans vote explicite.

➢ **Plateforme de registre distribué**

- **Définition**

Une plateforme de registre distribué est un environnement logiciel qui permet le développement, le déploiement et l'exécution d'applications basées sur la technologie des registres distribués. Elle fournit les outils, les bibliothèques et les infrastructures nécessaires pour créer des applications décentralisées (dApps).

- **Exemples de Plateformes**

✓ **Ethereum :**

Fournit une machine virtuelle décentralisée (EVM) pour exécuter des contrats intelligents et dApps.

✓ **Hyperledger Fabric**

Une plateforme modulaire pour les solutions blockchain d'entreprise avec une architecture de plug-in.

✓ **Corda**

Conçu pour les applications financières, permettant des transactions privées et sécurisées entre parties.

✓ **EOSIO**

Fournit une infrastructure pour la construction de dApps avec des transactions rapides et sans frais.

✓ **Radix**

Conçu pour être hautement évolutif avec une structure de registre hiérarchique.

➢ **Protocole de registre distribué**

Un protocole de registre distribué est un ensemble de règles et de conventions qui définissent la communication et l'interaction entre les nœuds d'un réseau distribué. Il spécifie comment les transactions sont créées, validées, propagées et ajoutées au registre, assurant ainsi le fonctionnement harmonieux et sécurisé du système.

Parmi les protocoles nous avons :

✓ **Bitcoin**

Le protocole de Bitcoin spécifie la création de blocs, la validation des transactions via PoW, et le mécanisme de récompense pour les mineurs.

✓ **Ethereum**

Le protocole d'Ethereum définit l'exécution des contrats intelligents, la transition vers PoS, et la structure des transactions.

✓ **Hyperledger Fabric**

Utilise un protocole modulaire permettant différents consensus et mécanismes de validation en fonction des besoins de l'application.

✓ **Hashgraph**

Utilise le protocole Gossip about Gossip pour propager les transactions et Virtual Voting pour atteindre le consensus.

✓ **Radix**

Utilise le protocole Tempo pour organiser les transactions en fragments et assurer la finalité rapide et la scalabilité.

➢ **Plateforme VS protocole**

Comme vous le voyez, les plateformes et protocoles portent souvent les mêmes noms alors que cela ne représente pas les mêmes concepts ! Et pour rajouter à la confusion, certains produits portent aussi le même nom que les protocoles ou plateformes ! Un vrai bazar ! [32]

La plateforme de blockchain est un environnement complet qui comprend à la fois le protocole de blockchain et les outils de développement associés, tandis que le protocole de blockchain définit les règles de base pour le fonctionnement et la communication au sein de la blockchain. La plateforme fournit l'infrastructure pour développer et exécuter des applications sur la blockchain, tandis que le protocole fournit les règles et les mécanismes sous-jacents pour sécuriser et maintenir le réseau de la blockchain. [32]

➢ **Quelques types de registres distribués**

✓ **Blockchain**

Une blockchain est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous détenteurs de ce registre et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie. [23]

- **Caractéristiques**
  - **Structure**

Les données sont stockées dans des blocs, chaque bloc contenant un ensemble de transactions.

  - **Immutabilité**

Une fois qu'un bloc est ajouté à la chaîne, il ne peut plus être modifié.

- **Décentralisation**

Aucune autorité centrale ne contrôle la blockchain.

- **Avantages**
  - **Sécurité**

Le consensus décentralisé et les mécanismes cryptographiques assurent la sécurité des données.

- **Transparence**

Toutes les transactions sont visibles sur le registre public.

- **Immutabilité**

Les données une fois enregistrées ne peuvent pas être modifiées.

- **Inconvénients**
  - **Scalabilité**

Le nombre de transactions par est limité.

- **Consommation énergétique**

Les mécanismes de consensus comme PoW consomment beaucoup d'énergie.

- **Latence**

Le temps de validation des transactions peut être élevé.

- **Protocoles Utilisés**
  - **Bitcoin**

Il utilise le protocole Bitcoin avec un consensus PoW.

- **Ethereum**

Ici c'est le protocole Ethereum qui est utilisé avec un consensus PoS dans Ethereum 2.0.

- **Hyperledger Fabric**

Un framework pour les blockchains permissionnées, utilisant des consensus pluggables comme Practical Byzantine Fault Tolerance (PBFT).

- **Ripple**

Utilise le Ripple Protocol Consensus Algorithm (RPCA).

- **Consensus**
  - **Proof of Work (PoW)**

Les mineurs résolvent des puzzles cryptographiques pour ajouter des blocs.

- **Proof of Stake (PoS)**

Les validateurs sont choisis en fonction de la quantité de crypto-monnaie qu'ils détiennent.

- **Delegated Proof of Stake (DPoS)**

Les détenteurs de tokens élisent des délégués pour valider les transactions.

- **Exemples domaines d'application**

La blockchain est une technologie polyvalente qui trouve des applications prometteuses dans divers domaines au-delà des crypto-monnaies. Voyons de plus près comment elle révolutionne déjà des thématiques. [32]

- La gestion d'identité, [32]
- La traçabilité alimentaire [32]
- Les droits d'auteur [32]
- La gestion des dossiers médicaux [32]

✓ **DAG (Directed Acyclic Graph)**

Contrairement aux modèles traditionnels de blockchain, dans lesquels les informations sont ajoutées en blocs linéaires, les DAG permettent une approche plus distribuée. Résultat ? Les transactions peuvent se dérouler simultanément, ce qui aura tendance à augmenter la vitesse et l'efficacité du réseau. [24]

Un DAG ou Directed Acyclique Graph est une ancienne structure mathématique qui s'est démocratisée dans le domaine de l'informatique. Elle est utilisée pour créer un modèle de réseaux reliant les nœuds qui le compose. [25]

- **Caractéristiques**
  - **Structure**

Les transactions sont organisées dans une structure en graphe orienté acyclique plutôt qu'en blocs.

- **Immutabilité**

Une fois ajoutées, les transactions ne peuvent pas être modifiées.

- **Scalabilité**

Conçu pour être plus évolutif que la blockchain traditionnelle.

- **Avantages**
  - **Scalabilité**

Un DAG peut traiter un grand nombre de transactions par seconde.

- **Efficacité énergétique**

Il ne nécessite pas de mineurs et consomme moins d'énergie.

- **Rapidité**

Leurs transactions peuvent être confirmées rapidement.

- **Inconvénients**
  - **Complexité**

La structure et le fonctionnement peuvent être plus complexes à comprendre et à implémenter.

  - **Sécurité**

Moins de recherche et d'audit par rapport aux blockchains traditionnelles.

  - **Adoption**

Moins d'adoption et de soutien de la part de la communauté.

- **Protocoles et plateformes utilisés**
  - **Iota**

IOTA est une cryptomonnaie qui utilise une variante de DAG appelée « Tangle », qui fonctionne en combinaison avec la preuve de travail (PoW). Conçu pour faciliter les transactions entre les dispositifs de l'Internet des objets (IoT), le Tangle permet également de monétiser les données de la blockchain. [26]

  - **Fantom (FTM)**

Fantom est une autre cryptomonnaie qui utilise la technologie DAG dans le cadre de ces contrats intelligents (smart contract), afin d'offrir des transactions rapides et à faible coût. [26]

  - **Avalanche (AVAX)**

Avalanche utilise un type de DAG combiné avec un mécanisme de consensus unique pour atteindre une scalabilité et une sécurité exceptionnelle. [26]

- **Consensus**
  - **Consensus décentralisé**

Chaque nouvelle transaction doit valider deux transactions précédentes.

  - **Algorithme de confiance**

Les transactions sont considérées comme validées lorsqu'elles sont suffisamment validées par d'autres.

- **Exemples domaines d'application**
  - Internet des Objets [24]
  - Finance [24]
  - Jeux [24]

✓ **Hashgraph**

Comme la blockchain, le Hashgraph est aussi un autre type de technologie de registre distribué et une méthode de consensus qui a été développée comme une alternative à la Blockchain. Son objectif principal était de résoudre les problèmes auxquels la Blockchain a été confrontée et continue de faire face. Le Hashgraph se distingue par son approche

différente du consensus, qui se veut plus rapide, plus efficace et plus sécurisé, tout en visant à surmonter des défis tels que la scalabilité, la latence et la consommation énergétique élevés, souvent reprochés aux systèmes basés sur la Blockchain traditionnelle. [28]

Le Hashgraph se distingue de la blockchain par son approche innovante du stockage et de la vérification des transactions, grâce à des concepts tels que « gossip about gossip » et le vote virtuel. Ces mécanismes permettent une plus grande efficacité en termes de vitesse et de coût par rapport à la blockchain traditionnelle, qui peut souffrir de lenteurs et de frais élevés. De plus, l'utilisation de l'aBFT renforce la sécurité en permettant à ce système d'atteindre un consensus même en présence de nœuds défaillants ou malveillants, ce qui en fait une alternative solide pour les applications nécessitant des performances et une sécurité accrue. Le Hashgraph propose ainsi une solution intéressante pour les cas d'usage où la blockchain rencontre des limitations, notamment en matière de scalabilité et d'efficacité énergétique. [29]

Nous pouvons donc dire que le hashgraph est une technologie de DLT et de consensus, conçue comme une alternative à la blockchain. Contrairement à la blockchain qui stocke les données sous forme de blocs séquentiels de transactions, hashgraph utilise une structure de données basée sur les « gossip about gossip » et le vote virtuel pour stocker et vérifier les transactions. Cette approche permet à hashgraph d'atteindre des vitesses de traitement des transactions plus rapides, de réduire les frais de transaction et d'offrir des niveaux de sécurité plus élevés grâce à un système de tolérance aux pannes byzantines asynchrones (aBFT). Hashgraph vise à surmonter les limitations inhérentes à la blockchain.

- **Caractéristiques**
  - **Structure**

Hashgraph utilise aussi un graphe orienté pour enregistrer les transactions.

  - **Immutabilité**

Les transactions une fois ajoutées ne peuvent pas être modifiées.

  - **Fairness**

Il assure une commande juste des transactions.

- **Avantages**
  - **Scalabilité**

Capable de gérer un grand nombre de transactions par seconde.

  - **Efficacité énergétique**

Ne nécessite pas de minage.

  - **Fairness**

Assure un ordre juste des transactions

- **Inconvénients**
  - **Complexité**

Le mécanisme de consensus peut être difficile à comprendre.

- **Adoption**

Moins largement adopté que les blockchains traditionnelles.

- **Permission**

Souvent utilisé dans des réseaux permissions, ce qui limite la décentralisation.

- **Protocoles Utilisés**
  - **Hedera Hashgraph**

Se sert du protocole Hashgraph avec Virtual Voting.

- **Consensus**
  - **Virtual Voting**

Il adopte des votes virtuels pour atteindre un consensus sans nécessiter de vote explicite des nœuds.

- **Fairness**

Garantit que les transactions sont ordonnées de manière équitable.

- **Exemple d'application**
  - Les contrats intelligents et la finance décentralisée (DeFi) [33]
  - L'Internet des objets (IoT) [33]
  - Le domaine de la santé [33]
  - Les médias et le divertissement [33]
  - Gouvernance et identité numérique [33]

✓ **Holochain**

Holochain est une infrastructure open source rapide et scalable qui facilite le développement d'applications peer-to-peer. L'objectif de Holochain est d'offrir un Internet décentralisé qui permet aux individus de communiquer entre eux sans que leurs données transitent par des entités centralisées. [27]

Holochain est un cadre open-source permettant de créer des applications peer-to-peer sécurisées, fiables et rapides. Plutôt que de dépendre de serveurs centralisés, les applications Holochain connectent directement les appareils des utilisateurs entre eux, offrant ainsi l'autonomie et la disponibilité des logiciels locaux, tout en tirant parti de la puissance et de la redondance des solutions cloud, sans coûts de maintenance d'hébergement. [30]

Holochain est un cadre open-source conçu pour développer des applications entièrement distribuées et peer-to-peer. [31]

En partant de ces trois définitions ci-dessus, nous pouvons définir l'holochain comme une infrastructure open source rapide et évolutive qui facilite le développement d'applications peer-to-peer. Son objectif est de proposer un Internet décentralisé, permettant aux individus de communiquer directement entre eux sans passer par des entités centralisées. Au lieu de dépendre de serveurs, les applications Holochain connectent directement les appareils des

utilisateurs dans des réseaux sécurisés. Cela offre l'autonomie et la disponibilité des logiciels installés localement, tout en bénéficiant de la puissance et de la redondance des logiciels en nuage, sans les coûts associés à l'hébergement sur le cloud pour les développeurs.

- **Caractéristiques**
  - **Structure**

Holochain est basé sur des chaînes individuelles pour chaque utilisateur plutôt que sur une seule chaîne globale.

  - **Flexibilité**

Cette infrastructure permet une plus grande personnalisation des applications distribuées.

  - **Décentralisation**

Elle est complètement décentralisée, chaque utilisateur a son propre registre.

- **Avantages**
  - **Scalabilité**

Très évolutif grâce à la décentralisation complète.

  - **Personnalisation**

Permet une grande flexibilité et personnalisation des applications.

  - **Efficacité énergétique**

Consomme moins d'énergie que les blockchains traditionnelles.

- **Inconvénients**
  - **Complexité**

Peut-être complexe à comprendre et à implémenter.

  - **Interopérabilité**

Moins de compatibilité avec les systèmes basés sur la blockchain.

  - **Adoption**

Moins d'adoption et de soutien de la part de la communauté.

- **Protocoles Utilisés**
  - **Holochain**

Elle utilise son propre protocole avec un DHT (Distributed Hash Table) et un consensus basé sur les pairs.

- **Consensus**
  - **Validation par les pairs**

Les transactions sont validées par les pairs locaux plutôt que par un réseau global.

  - **DHT**

Une DHT utilise une table de hachage distribuée pour synchroniser les données.

- **Exemple d'application**
  - Réseaux sociaux décentralisés [34]
  - E-commerce décentralisé [34]
  - Jeux sur Holochain [34]

✓ **Synthèse et Comparaison des Registres Distribués**

Les registres distribués, ou Distributed Ledgers, sont des bases de données décentralisées partagées entre les nœuds d'un réseau. Ils permettent de maintenir un enregistrement consensuel et immuable de transactions. Parmi les types de registres distribués, on trouve la blockchain, les graphes acycliques dirigés (DAG), le Hashgraph et Holochain. Chacun de ces types présente des caractéristiques en termes de structure, de consensus, de sécurité, de transparence, et d'efficacité.

Dans cette synthèse, nous comparerons ces différentes technologies en les classant selon qu'elles sont avec ou sans autorisation, et fournirons des exemples concrets pour chaque catégorie. Ensuite, nous détaillerons leurs avantages et inconvénients, et comparerons leurs principes clés pour mieux comprendre leurs forces et limites respectives. Cette analyse vise à offrir une vue d'ensemble des registres distribués et à faciliter la compréhension de leurs applications potentielles dans divers contextes.

Tableau 2.1 : Synthèse des registres distribués

Type de Registre	Structure	Avantages	Inconvénients
Blockchain	Blocs chaînés linéairement	Sécurité, transparence, immutabilité	Scalabilité limitée, consommation énergétique élevée, latence
DAG	Graphe orienté acyclique	Scalabilité, efficacité énergétique, rapidité	Complexité, recherche limitée, adoption limitée
Hashgraph	Graphe orienté	Scalabilité, efficacité énergétique, fairness	Complexité, adoption limitée, souvent permissioned
Holochain	Chaînes individuelles	Scalabilité, personnalisation, efficacité énergétique	Complexité, interopérabilité limitée, adoption limitée

Tableau 2.2 : Synthèse des registres distribués (blockchain, DAG, Hashgraph, Holochain) classés en fonction de leur type : avec autorisation (permissioned) et sans autorisation (permissionless), avec des exemples pour chaque cas

Registres Distribués	Blockchain (Permissionless)	Directed Acyclic Graph (DAG)	Hashgraph (Permissioned)	Holochain
Blockchain	Bitcoin, Ethereum		Hyperledger Fabric, Corda	
Décentralisation	Élevée, aucun contrôle central (ex. Bitcoin, Ethereum)	Élevée, chaque transaction valide deux autres	Moyenne, souvent utilisé dans des réseaux permissioned mais peut être décentralisé	Très élevée, chaque utilisateur a sa propre chaîne
DAG	IOTA, Nano		Private DAG Implementations	
Hashgraph	Hedera Hashgraph (Public)		Hedera (Permissioned)	Hashgraph
Holochain	Holochain		Holochain (Private Instances)	
Consensus	PoW, PoS, DPoS	Validation par les pairs (chaque transaction valide deux autres)	Virtual Voting	Validation par les pairs, DHT
Sécurité	Très élevée grâce au consensus décentralisé et cryptographie	Élevée mais dépend du nombre de validations	Très élevée avec Virtual Voting et BFT	Très élevée grâce à la validation par les pairs et DHT
Transparence	Très élevée, toutes les transactions sont publiques	Moyenne, les transactions peuvent être tracées mais de manière moins transparente	Moyenne à élevée, dépend de l'utilisation	Variable, chaque utilisateur contrôle sa chaîne mais peut être partagé
Immuabilité	Très élevée, une fois ajoutées, les transactions ne	Élevée, les transactions validées ne	Très élevée, une fois ajoutées, les transactions	Élevée, les transactions validées sont

Tableau 2.3 : Comparaison des registres distribués en fonction des principes clés des registres distribués

	peuvent pas être modifiées	peuvent pas être modifiées	ne peuvent pas être modifiées	immuables
Efficacité	Moins efficace (PoW consomme beaucoup d'énergie)	Très efficace, pas de minage nécessaire	Très efficace, pas de minage nécessaire	Très efficace, validation locale et DHT
Interopérabilité	Moyenne, les blockchains sont souvent isolées mais des solutions inter-chaînes existent	Variable, dépend de l'implémentation spécifique	Moyenne, peut être utilisé dans des contextes différents mais souvent permissioned	Élevée, peut interagir avec d'autres systèmes grâce à la flexibilité des chaînes individuelles

✓ **Détails supplémentaires**

- **Blockchain**

Les blockchains sont très sécurisées et transparentes, mais peuvent souffrir de problèmes de scalabilité et d'efficacité, particulièrement avec PoW. Elles sont décentralisées et immuables, mais leur interopérabilité peut être limitée sans solutions spécifiques inter-chaînes.

- **DAG**

Les registres basés sur DAG sont très efficaces et scalables, avec une décentralisation élevée et une bonne sécurité. Cependant, la transparence peut être moindre que celle des blockchains traditionnelles. L'interopérabilité dépend de l'implémentation.

- **Hashgraph**

Hashgraph offre une très haute sécurité et efficacité grâce à Virtual Voting, mais est souvent utilisé dans des contextes permissioned. Sa décentralisation peut varier, et bien qu'il soit immuable, la transparence et l'interopérabilité dépendent de la mise en œuvre spécifique.

- **Holochain**

Très décentralisé et efficace, Holochain permet une grande flexibilité et personnalisation. Sa transparence et interopérabilité sont variables, dépendant des préférences des utilisateurs et des configurations spécifiques.

Tous ces registres distribués que nous venons de voir peuvent être utilisés pour créer une identité auto-souveraine grâce à leurs caractéristiques de décentralisation, de sécurité et de gestion des données. Cependant, le choix du registre dépendra des besoins spécifiques en termes de rapidité, de scalabilité et de personnalisation de la solution d'identité.

2.2.3 Identité auto-souveraine (SSI)

L'identité auto-souveraine (Self-Sovereign Identity ou SSI) est un concept révolutionnaire dans le domaine de la gestion des identités numériques. Contrairement aux modèles traditionnels où des autorités centrales ou des organisations gèrent et contrôlent les identités numériques, le modèle SSI permet aux individus de posséder et de contrôler entièrement leurs propres identités numériques. Ce modèle repose sur des technologies telles que la cryptographie avancée et les registres distribués pour assurer la sécurité, la confidentialité et l'interopérabilité des identités numériques. Les principales caractéristiques de SSI incluent la décentralisation, la transparence, la portabilité et le contrôle par l'utilisateur, ce qui offre une plus grande autonomie et une réduction des risques liés à la centralisation des données.

➢ **Définition et Concepts de Base**

L'identité auto-souveraine (Self-Sovereign Identity, SSI) représente une révolution dans la gestion des identités numériques, permettant aux individus et aux organisations de posséder, contrôler et gérer leurs propres identités sans dépendre d'autorités centralisées, en s'appuyant sur des technologies décentralisées et des principes fondamentaux de sécurité et de confidentialité.

✓ **Définition de l'identité auto-souveraine (SSI)**

Dans [35], le Self Sovereign Identity, ou Identité numérique auto-souveraine, est défini comme une méthode qui permet à une personne de gérer et contrôler facilement son identité numérique, sans qu'une autorité administrative n'intervienne. En gros, cela fonctionne comme dans la vie réelle :

Vous, en tant qu'utilisateur, décidez si vous souhaitez partager vos informations ou non.

Les prestataires peuvent demander les informations nécessaires pour vous offrir leurs services.

✓ **Principes**

Pour garantir la propriété des individus sur leur identité, Christopher Allen [168] décrit dix principes les identités auto-souveraines doivent respecter :

- **Existence**

Les utilisateurs doivent avoir une existence indépendante ;

- **Contrôle :**

Les utilisateurs doivent contrôler leur identité ;

- **Accès**

Les utilisateurs doivent toujours avoir accès à leur identité et à leurs réclamations ;

- **Transparence**

Les systèmes et algorithmes utilisés pour gérer les identités doivent être ouverts et transparent ;

- **Persistance**

Les identités et les revendications des utilisateurs doivent être durables ;

- **Portabilité**

Les informations et les services sur les identités doivent être transportables ;

- **Interopérabilité**

Les identités et les revendications des utilisateurs doivent être utilisables dans différents secteurs, organisations et même pays ;

- **Consentement**

Un utilisateur doit accepter l'utilisation et la divulgation de son identité et de ses revendications ;

- **Minimalisation**

La divulgation des identités et des réclamations doit être minimisée pour garantir la confidentialité ;

- **Protection**

Les droits de l'utilisateur doivent être protégés.

➢ **Architecture SSI**

L'architecture des SSI repose sur plusieurs composants clés qui permettent la gestion décentralisée et sécurisée des identités numériques. Ces composants, ainsi que le modèle de confiance associé, assurent une interaction fiable entre les différents acteurs impliqués.

✓ **Composants clés**

- **Identifiants Décentralisés (DID)**

Les DID sont au cœur de l'architecture SSI, permettant une identification unique et sécurisée sans dépendre d'une autorité centrale. Les DID sont des identifiants uniques créés et contrôlés par les utilisateurs eux-mêmes. Ils sont stockés sur des registres décentralisés (comme la blockchain) et permettent aux utilisateurs de prouver leur identité de manière sécurisée. Contrairement aux identifiants traditionnels (comme les numéros de sécurité sociale ou les adresses e-mail), les DID ne sont pas liés à une entité centralisée et peuvent être résolus pour

obtenir des documents DID contenant des informations publiques permettant de vérifier l'identité.

- **Informations d'identification vérifiables (VC)**

Les VC sont des attestations numériques délivrées par des entités de confiance (émetteurs) à des individus ou des organisations (détenteurs ou sujets). Ces informations peuvent inclure des diplômes, des certificats de compétence, des cartes d'identité, etc. Les VC sont signées cryptographiquement par l'émetteur, ce qui permet à toute entité (vérificateur) de vérifier leur authenticité et leur intégrité sans avoir besoin de contacter directement l'émetteur.

- **Portefeuille numérique**

Un portefeuille numérique, appelé digital wallets (en anglais) est une application ou un dispositif qui permet aux utilisateurs de stocker leurs informations d'identification vérifiables. Les portefeuilles numériques offrent une interface sécurisée pour gérer ces informations, permettant aux utilisateurs de contrôler l'accès à leurs données et de partager des informations vérifiables avec des vérificateurs de manière sécurisée.

✓ **Modèle de confiance**

Le modèle de confiance de l'identité auto-souveraine repose sur des interactions décentralisées entre détenteurs, émetteurs et vérificateurs, chacun jouant un rôle crucial dans l'établissement et la vérification des identités numériques.

- **Détenteurs (Holders)**

Encore appelés titulaires, sont les individus ou organisations qui possèdent ces attestations. Ils les stockent dans un portefeuille numérique sécurisé et ont le pouvoir de décider quelles informations partager, avec qui, et dans quel contexte. [36]

- **Emetteurs (Issuers)**

Les émetteurs sont les entités qui créent et délivrent des attestations vérifiables. Ces attestations peuvent être des documents d'identité, des qualifications professionnelles, des preuves de domicile, ou tout autre justificatif nécessaire pour prouver un aspect de l'identité ou des compétences d'une personne. [36]

- **Vérificateurs (Verifiers)**

Les vérificateurs sont les parties intéressées par la vérification de l'authenticité des attestations fournies par les titulaires. Il peut s'agir d'employeurs, d'institutions financières, de services gouvernementaux, ou de toute autre entité nécessitant une preuve d'identité ou de qualification.

✓ **Processus d'interaction entre les acteurs**

Le processus d'interaction et de vérification dans le cadre de l'identité auto-souveraine implique trois étapes principales : l'émission, la présentation et la vérification :

- **Émission**

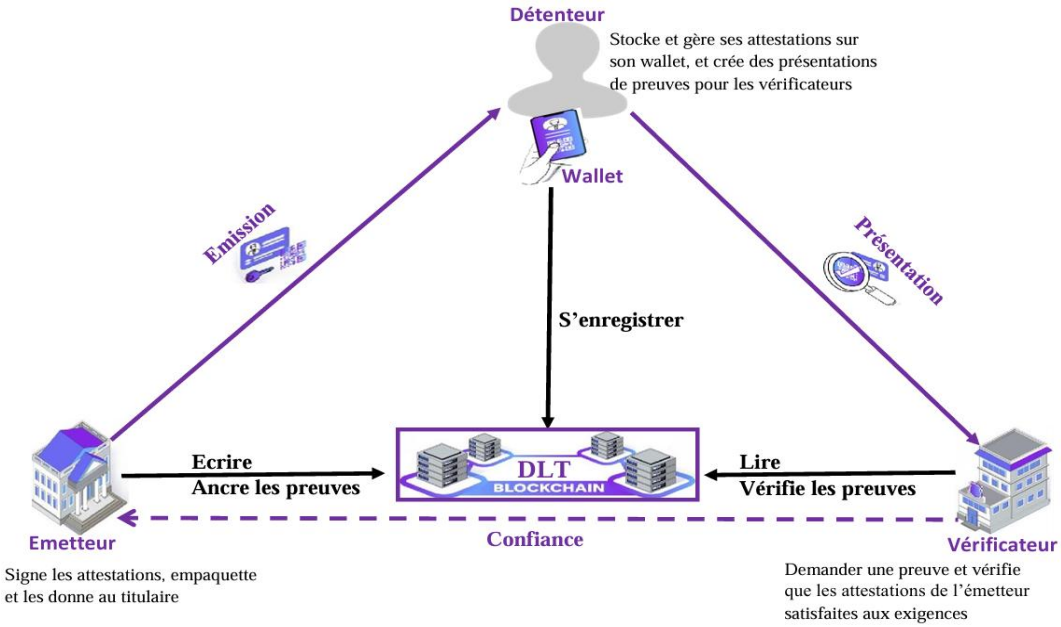
L'émission est le processus par lequel une entité de confiance (l'émetteur) délivre une information d'identification vérifiable à un individu ou une organisation (le détenteur ou titulaire), elle peut des fois avoir lieu suite à une demande de l'attestation.

- **Présentation**

La présentation est le processus par lequel le détenteur partage une information d'identification vérifiable avec une entité qui en a besoin (le vérificateur) qui peut être suite à sa réclamation.

- **Vérification**

La vérification est le processus par lequel le vérificateur s'assure de l'authenticité et de la validité de l'information d'identification vérifiable présentée par le détenteur.



: Triangle de confiance du Self-Sovereign Identity (SSI)**5.2Figure**

➢ **Avantages de SSI**

A partir de [35], nous pouvons donner les avantages de l'approche SSI en utilisant la blockchain comme registre distribué :

✓ **Contrôle du consentement des données personnelles**

Les utilisateurs peuvent attester de leur consentement sur l'utilisation de leurs données personnelles, avec les autorisations retracées dans la blockchain.

✓ **Fiabilité et mise à jour des informations**

Les prestataires de services disposent d'informations fiables et à jour grâce aux certifications inviolables de la blockchain.

✓ **Facilité d'invalidation des certifications**

La technologie blockchain permet d'invalider facilement une certification en cas de fausses informations.

- ✓ **Gestion du cycle de vie des données**

Le SSI permet de contourner les problèmes relatifs au cycle de vie des données. Les organisations peuvent accéder aux informations des utilisateurs sur le long terme sans avoir besoin de les stocker, tant que l'autorisation d'accès n'est pas retirée.

- ✓ **Consultation des données utiles à tout moment**

Les organisations peuvent consulter les données utiles à chaque fois que nécessaire sans avoir besoin de les stocker, réduisant ainsi les risques et les coûts liés au stockage de données.

- ✓ **Interopérabilité entre différentes plateformes et systèmes**

Le Self-Sovereign Identity permet une interopérabilité entre différentes plateformes et systèmes, facilitant ainsi l'intégration et la communication entre divers services et applications sans dépendre d'un intermédiaire centralisé. Cela garantit une expérience utilisateur plus fluide et cohérente à travers différents écosystèmes.

- ➢ **Défis et Limitations**

En nous basant sur [37], le Self Sovereign Identity peut avoir comme défis et limitations, en utilisant la blockchain comme registre distribué :

- ✓ **Barrières techniques**
  - **Expertise technique et infrastructure**

La mise en œuvre des systèmes SSI nécessite une expertise technique avancée et une infrastructure conséquente.

- **Intégration avec les systèmes existants**

L'intégration des solutions SSI avec les systèmes existants peut être complexe.

- **Interopérabilité**

Garantir l'interopérabilité entre les différentes plateformes SSI demeure un défi important.

- **Problèmes d'évolutivité et de performances**

Les solutions SSI basées sur la blockchain peuvent rencontrer des problèmes d'évolutivité et de performances à mesure que le nombre d'utilisateurs et de transactions augmente.

- ✓ **Considérations réglementaires et juridiques**
  - **Évolution du paysage juridique**

Le cadre juridique et réglementaire de l'identité numérique est en constante évolution.

- **Nouveaux cadres juridiques**

Le SSI remet en question les concepts traditionnels d'identité, nécessitant de nouveaux cadres juridiques pour régir la propriété des données, le consentement, la responsabilité et la résolution des litiges.

- **Adaptation des lois existantes**

Adapter les lois existantes pour s'adapter aux SSI et garantir la conformité transfrontalière peut être une tâche ardue.

✓ **Sensibilisation et éducation des utilisateurs**

- **Manque de connaissance**

De nombreuses personnes ne connaissent pas l'identité auto-souveraine et ses avantages.

- **Instaurer la confiance**

Il est nécessaire d'informer les utilisateurs sur les avantages du SSI, son fonctionnement et la manière dont ils peuvent garder le contrôle de leurs données pour instaurer la confiance.

- **Inquiétudes sur la sécurité et la confidentialité**

Les utilisateurs peuvent avoir des inquiétudes ou des idées fausses concernant la sécurité et la confidentialité des systèmes SSI, nécessitant des campagnes de sensibilisation approfondies.

Ces défis et limitations doivent être relevés pour parvenir à une adoption généralisée et réaliser tout le potentiel de l'identité auto-souveraine dans la refonte de l'avenir de la gestion de l'identité numérique.

2.3 Applications et Cas d'Utilisation

Cette section examine les applications pratiques des technologies de gestion des identités numériques à travers divers secteurs et analyse les résultats obtenus.

2.3.2 Études de cas dans divers secteurs :

Les technologies de cryptographie et les réseaux décentralisés ont des applications vastes et variées dans divers secteurs. Elles permettent de créer des systèmes d'identité numérique sécurisés et efficaces, offrant de nombreux avantages en termes de protection des données et de gestion des identités. Nous allons voir quelques applications et des cas d'utilisation dans plusieurs secteurs clés.

✓ **Finance**

Dans [38], Pierre Duffaut d'Accenture Labs montre le potentiel significatif d'un système d'identité auto-souveraine utilisant les identités distribuées et les certificats vérifiables pour la gestion des données personnelles, en particulier dans le domaine de l'identité numérique.

Le processus commence par l'enregistrement des données du passeport d'un utilisateur dans une application dédiée, qui génère une identité distribuée. Cette DID est associée à un VC, qui est ensuite validé par un tiers de confiance, qui est une banque, en utilisant la reconnaissance faciale pour vérifier l'authenticité des données. Une fois cette validation effectuée, l'utilisateur

peut utiliser l'application pour interagir de manière sécurisée avec divers organismes membres du réseau, facilitant ainsi des transactions personnalisées.

Les avantages de ce système sont multiples. Premièrement, il offre un gain de temps substantiel car la vérification de l'identité se fait instantanément, éliminant ainsi les délais associés aux méthodes traditionnelles de vérification. Deuxièmement, les systèmes SSI assurent une sécurité renforcée des données personnelles en permettant aux utilisateurs de conserver le contrôle de leurs informations, réduisant ainsi les risques de fraude et d'usurpation d'identité. Troisièmement, cette technologie peut être étendue à d'autres types de données personnelles, telles que les informations médicales ou éducatives, ouvrant ainsi la voie à de nombreuses applications potentielles.

En plus de simplifier les processus de vérification d'identité, ce système favorise également la confidentialité des utilisateurs en leur permettant de contrôler quels éléments de leur identité numérique sont partagés et avec qui. Cela renforce la confiance des utilisateurs dans les transactions numériques.

- ✓ **Santé**

Dans [39], les auteurs décrivent un système décentralisé de stockage de données médicales basé sur la blockchain. Les avantages incluent l'accessibilité globale des données en cas d'urgence et la possibilité de mener des recherches médicales sans révéler d'informations personnelles. Les dossiers médicaux tels que diagnostics et traitements sont stockés dans une base de données distribuée, gérée par des entités comme des hôpitaux ou des cliniques. Les patients sont identifiés via un numéro d'assurance maladie et représentés par des contrats intelligents sur la blockchain sans contenir d'informations personnelles.

Les patients peuvent revendiquer la propriété de leurs données via un tableau de bord personnel et un téléphone mobile. Ils peuvent également choisir de stocker leurs données dans un coffre-fort de données personnel supprimant leur entrée de la base de données d'identification centralisée. Lorsqu'un patient consulte un médecin, il peut révéler l'adresse de son contrat intelligent permettant au médecin d'accéder à ses dossiers médicaux. Le système assure que les patients ont un contrôle fort et granulaire sur l'accès à leurs informations personnelles.

- ✓ **Education**

Dans le secteur éducatif, des systèmes basés sur la blockchain ont été proposés pour améliorer la gestion des données et des identités de manière décentralisée et sécurisée.

Dans le système décrit dans [40], un agent logiciel basé sur le cloud (DSA) représente un ensemble de données (DS) et gère les clés privées et les informations d'identification dans un portefeuille numérique. Les parties intéressées interagissent avec cet agent via un identifiant décentralisé. Un éditeur comme une université utilise un agent logiciel pour émettre des informations d'identification garantissant leur authenticité et leur vérifiabilité via des protocoles DID. Ce système a été testé avec succès à l'aide de la plateforme Evernym.

Le système décrit dans [39] propose un stockage décentralisé des dossiers académiques des étudiants via la blockchain. Actuellement centralisées, ces données deviennent distribuées et les étudiants peuvent revendiquer leur propriété via des contrats intelligents. Les administrateurs universitaires déploient ces contrats avec l'identifiant des étudiants et l'URL des bases de données, tandis que les notes et descriptions de cours sont téléchargées dans une base de données décentralisée. Les étudiants contrôlent l'accès à leurs données et les employeurs ou donateurs peuvent vérifier leurs progrès. Ce système favorise une meilleure utilisation des données académiques connectant les étudiants à des opportunités et permettant des retours personnalisés pour améliorer leurs performances.

✓ **Administration publique**

Dans [41] [42] [43] [44] [45], les auteurs tentent de nous présenter la FIDe (France Identité Numérique) qui est un programme public lancé par le gouvernement français en 2018 pour fournir une solution sécurisée d'identification numérique aux citoyens. Gratuit et facultatif, ce service permet aux utilisateurs de gérer leur identité numérique via une application mobile. Les objectifs principaux incluent l'augmentation de la sécurité sur Internet, la protection des données, le contrôle des informations d'identité par les citoyens et la simplification de l'accès aux services en ligne.

Les utilisateurs s'inscrivent en utilisant leur carte d'identité nationale électronique (CNIe) ou leur passeport biométrique. Ils téléchargent l'application mobile FIDe et créent un compte en suivant les instructions fournies. L'application utilise des technologies biométriques (empreintes digitales, reconnaissance faciale) ou un code de sécurité unique pour vérifier l'identité de l'utilisateur.

Lorsqu'un utilisateur souhaite accéder à un service en ligne, il utilise l'application FIDe pour s'authentifier. L'application génère un code de sécurité unique ou utilise des technologies biométriques pour vérifier l'identité de l'utilisateur. Une fois l'identité vérifiée, l'utilisateur peut accéder aux services en ligne de manière sécurisée. Les informations nécessaires sont transmises de manière sécurisée, minimisant ainsi le risque de fraude ou d'usurpation d'identité.

2.3.3 Analyse des résultats

En analysant les résultats de ces études de cas, nous pouvons présenter quelques avantages et inconvénients de l'utilisation de la cryptographie et des réseaux décentralisés dans la gestion des identités numériques :

➢ **Avantages**

✓ **Sécurité renforcée**

Les technologies comme la blockchain utilisent des méthodes de cryptographie avancées pour sécuriser les données personnelles. Les informations sont distribuées et cryptées, réduisant ainsi les risques de piratage et d'usurpation d'identité.

✓ **Contrôle renforcé pour les utilisateurs**

Les individus ont un contrôle direct sur leurs informations d'identité numérique. Ils peuvent choisir quelles informations partager et avec qui, renforçant ainsi la confidentialité et la protection des données personnelles.

- ✓ **Efficacité opérationnelle**

L'automatisation des processus de vérification d'identité et la réduction des frictions dans les transactions numériques améliorent l'efficacité opérationnelle des organisations. Cela peut réduire les coûts et accélérer les délais de traitement.

- ✓ **Innovation potentielle**

Les technologies de gestion des identités numériques ouvrent la voie à de nouvelles applications innovantes dans divers secteurs tels que la santé, l'éducation et l'administration publique. Elles permettent de créer des solutions personnalisées et sécurisées adaptées aux besoins spécifiques des utilisateurs.

- ➢ **Inconvénients**
  - ✓ **Complexité technologique**

La mise en œuvre de systèmes de gestion des identités basés sur la blockchain et la cryptographie peut être techniquement complexe. Cela nécessite une expertise en matière de sécurité informatique et une gestion rigoureuse des clés cryptographiques.

- ✓ **Dépendance aux infrastructures numériques**

Les systèmes basés sur la technologie blockchain dépendent de l'infrastructure numérique et de la connectivité Internet. Les pannes ou les interruptions de service peuvent affecter la disponibilité des services et la gestion des identités numériques.

2.4 Conclusion

Cette analyse de l'état de l'art nous a permis de mettre en évidence les limites des systèmes traditionnels d'identification numérique, notamment leur centralisation et leur vulnérabilité face aux attaques modernes. Ces constats montrent l'importance d'explorer des approches plus innovantes comme les Références Vérifiables et les Identifiants Distribués. Ces technologies représentent une évolution majeure dans la gestion des identités numériques, imposant ainsi l’envie de vouloir avoir une compréhension approfondie de leur fonctionnement, que nous aborderons dans le chapitre suivant.

3. Compréhension des Références Vérifiables (VC) et des Identifiants Distribués (DID)

L'essor des technologies numériques a transformé la manière dont nous gérons les identités et les attestations. Les Références Vérifiables et les Identifiants Distribués sont au cœur de cette révolution, offrant des solutions innovantes pour la sécurité et la vérifiabilité des informations. Cette section explore en profondeur ces concepts, leurs avantages, et les défis qu'ils présentent.

3.1 Etude des références vérifiables

Les VC sont des éléments clés des systèmes d'identité décentralisée, offrant une méthode sécurisée et flexible pour attester de diverses informations. Dans cette sous-partie, nous explorerons en détail le concept des VC, leurs composants, leur fonctionnement, et les standards qui les régissent.

3.1.1 Définition des VC

D'après le W3C [46], un référence vérifiable ou justificatif vérifiable est un document numérique qui contient des informations d'identification semblables à celles présentes sur un document physique (comme une photo, un nom, un numéro d'identification ou des attributs comme la nationalité). Ce justificatif est émis par une autorité reconnue (comme une administration municipale ou un organisme de certification) et peut inclure des preuves sur la manière dont il a été obtenu ainsi que des contraintes d'utilisation (comme une date d'expiration).

Grâce à des technologies comme les signatures numériques, ces justificatifs peuvent être partagés avec des vérificateurs de manière rapide et sécurisée, ce qui permet de prouver leur authenticité à distance. Le terme « vérifiable » indique que le document peut être authentifié par un tiers, mais cela ne garantit pas automatiquement la véracité des informations qu'il contient. Toutefois, des éléments de preuve peuvent être inclus pour aider à évaluer la fiabilité des informations.

Les VC peuvent être représentées en utilisant différents formats en fonction des besoins du système et des spécifications en vigueur tel que : JSON-LD (JavaScript Object Notation for Linked Data), JWT (JSON Web Token), CBOR (Concise Binary Object Representation), etc. En général, JSON-LD est le format le plus largement adopté et recommandé pour les VC en raison de sa compatibilité avec les standards du W3C et de sa capacité à représenter des données liées de manière interopérable.

3.1.2 Aperçu de l'écosystème VC

Dans [46], le W3C décrit clairement les rôles dans l'écosystème des informations d'identification vérifiables deses principaux acteurs et les relations entre eux dans un système où ces informations sont utilisées. Parmi ces rôles, nous avons :

- **Titulaire**

Le titulaire est l'entité possédant des justificatifs vérifiables et capable de générer des présentations vérifiables. Les titulaires peuvent être des individus comme des étudiants, des employés, ou des clients.

- **Émetteur**

Il représente l'entité qui crée des justificatifs vérifiables à partir de revendications sur un ou plusieurs sujets, puis les transmet au titulaire. Les émetteurs incluent des organisations comme des entreprises, des gouvernements ou des particuliers.

- **Sujet**

Entité sur laquelle des revendications sont faites. Le sujet peut être un être humain, un animal ou un objet. Le titulaire est souvent aussi le sujet, mais ce n'est pas toujours le cas (par exemple, un parent peut détenir les justificatifs de son enfant).

- **Vérificateur**

C'est l'entité qui reçoit et traite les justificatifs vérifiables pour validation. Les vérificateurs peuvent être des employeurs, du personnel de sécurité ou des sites Web.

- **Registre de données vérifiables**

Système qui gère la création et la vérification des identifiants, des clés, et autres données essentielles pour l'utilisation des informations d'identification vérifiables. Cela inclut des bases de données fiables, des registres distribués et d'autres systèmes similaires.

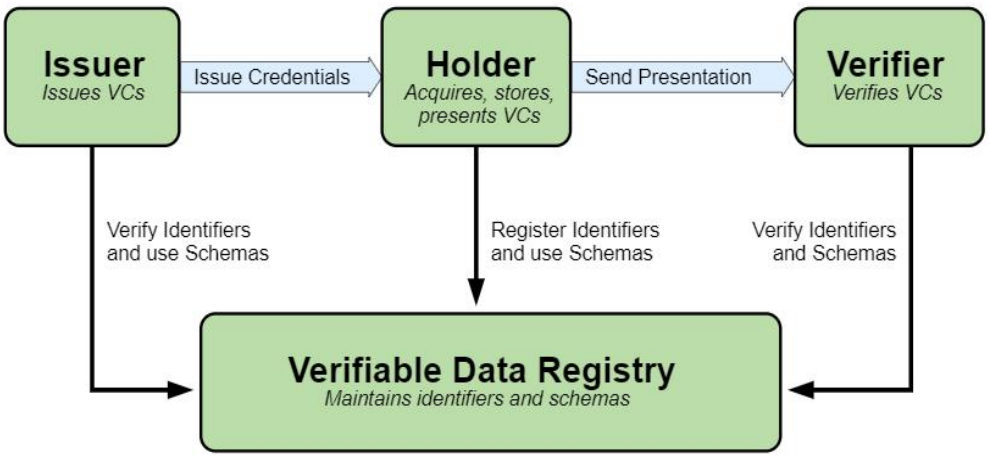


Figure 3.1 : Flux d'Informations et Rôles dans un Écosystème des VC [46]

Cette figure illustre les rôles principaux et les flux d'information dans un écosystème d'identifications vérifiables. Les acteurs clés incluent l'émetteur, qui délivre des VCs aux titulaires, le titulaire qui les stocke et les présente au vérificateur, ce dernier qui valide ces informations et le registre de données vérifiables qui maintient les identifiants et schémas nécessaires. Les interactions entre ces entités garantissent la fiabilité et la vérifiabilité des informations d'identification dans le système.

3.1.3 Composants des VCs

A partir de longues et attentives exploitations de [48, 49, 50, 51, 52, 53, 54, 55, 56], nous avons pu avoir une compréhension plus claire des VC.

La structure et le contenu des données dans une Information VC sont définis de manière à garantir l'interopérabilité, la sécurité et la vérifiabilité. Une VC est souvent représentée en

format JSON-LD et suit des spécifications standards comme celles définies par le W3C. Nous allons présenter les principales composantes d'une VC, leurs contenus et tenter d'étudier plus en profondeur l'importance de chaque composant.

Selon les spécifications du W3C (World Wide Web Consortium), un VC doit respecter certaines structures et éléments obligatoires. Les principales composantes d'une identité vérifiable sont :

- **Credential Metadata (Métadonnées du justificatif) :**

Il s'agit d'informations descriptives concernant le justificatif lui-même. Les métadonnées peuvent inclure des détails comme l'émetteur du justificatif, la date de délivrance, la période de validité, etc. Ces métadonnées permettent de comprendre le contexte et l'usage du justificatif.

- **Claim(s) (Déclarations) :**

Ce sont les affirmations ou assertions faites par le justificatif. Par exemple, un justificatif pourrait contenir une déclaration indiquant qu'une personne a réussi un certain examen ou qu'elle est majeure. Ces déclarations sont les informations que le justificatif cherche à prouver ou à attester.

- **Proof(s) (Preuves) :**

Il s'agit des éléments de vérification qui assurent que les déclarations faites dans le justificatif sont authentiques et non falsifiées. Les preuves peuvent être des signatures cryptographiques ou d'autres mécanismes qui permettent de vérifier l'intégrité et l'authenticité des déclarations.

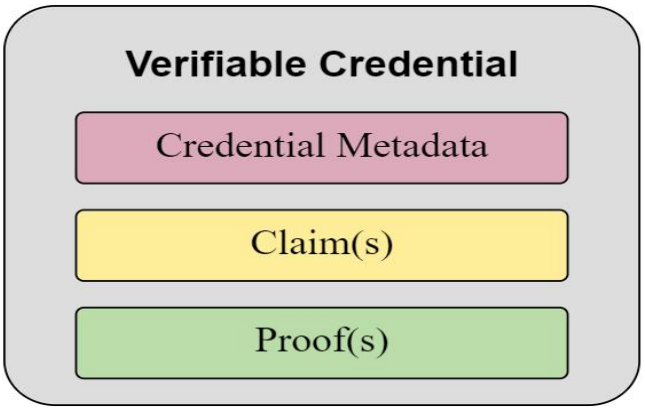


Figure 3.2 : Composants de base d'un justificatif vérifiable [54]

Ces composants travaillent ensemble pour créer un justificatif qui peut être vérifié de manière sécurisée par des tiers sans avoir besoin de consulter directement l'émetteur initial.

- **Les éléments de base contenus dans un VC en format JSON-LD**

Nous allons à présent voir plus en profondeur les éléments constitutifs d'une VC en format JSON-LD.

- ✓ **@context :**

Un ou plusieurs contextes qui désignent les termes utilisés dans le jeton. Cela permet de donner du sens aux données de la manière dont elles doivent être interprétées. Par exemple, on peut avoir un contexte pour les identifiants en général et des contextes spécifiques pour différents types d'identifiants. Typiquement, il inclut https://www.w3.org/2018/credentials/v1.

- ✓ **id :**

Un identifiant unique pour la VC. Cela peut être généralement une URL, d'un URI ou un identifiant d'un autre type (par exemple un URN) qui peut être résolu pour obtenir des informations sur la VC.

- ✓ **type :**

C'est un tableau qui spécifie les types de la VC. Un ou plusieurs types qui indiquent que le document est un credential vérifiable. Par exemple, cela pourrait inclure "VerifiableCredential" et un type spécifique comme "UniversityDegreeCredential".

- ✓ **issuer :**

L'entité qui émet le credential, peut-être une personne, une organisation ou une entité logicielle. Cela doit inclure un identifiant unique (typiquement une URL ou un DID - Decentralized Identifier, …) qui représente l'émetteur.

- ✓ **issuanceDate :**

La date et l'heure où la VC a été émise. Cela est exprimé dans un format de date et heure conforme à la norme ISO 8601.

- ✓ **credentialSubject :**

Un objet qui contient les informations sur le sujet de la VC, c'est-à-dire l'entité à qui la VC se réfère. Il peut contenir des sous-objets et des attributs spécifiques à l'identité du sujet comme le nom, la date de naissance ou d'autres attributs pertinents qui sont contenus dans le credential.

- ✓ **proof :**

Un objet qui contient les éléments de preuve qui garantissent l'authenticité et l'intégrité de la VC. Cela inclut le type de preuve utilisé (comme une signature numérique), le créateur de la preuve, et d'autres données cryptographiques pertinentes qui permettent de vérifier que le credential n'a pas été altéré et qu'il a été émis par une entité authentifiée.

- ✓ **expirationDate (optionnel)**

La date et l'heure après lesquelles la VC ne sera plus valide. Elle est également exprimée dans le format ISO 8601.

- ✓ **credentialStatus (optionnel)**

Un objet qui contient des informations sur l'état actuel de la VC, par exemple si elle a été révoquée ou non.


```
{
    "verifiableCredential": {
        "@context": [
            "https://www.w3.org/2018/credentials/v1",
            "https://www.w3.org/2018/credentials/examples/v1"
        ],
        "id": "0892f680-6aeb-11eb-9bcf-f10d8993fde7",
        "type": [
            "VerifiableCredential",
            "UniversityDegreeCredential"
        ],
        "issuer": {
            "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
            "name": "Acme University"
        },
        "issuanceDate": "2021-05-11T23:09:06.803Z",
        "credentialSubject": {
            "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
            "degree": {
                "type": "BachelorDegree",
                "name": "Bachelor of Science"
            }
        },
        "proof": {
            "type": "Ed25519Signature2018",
            "created": "2021-05-17T15:25:26Z",
            "jws": "eyJhbGciOiJFZERTQYjY0Il19..nlcAA",
            "proofPurpose": "assertionMethod",
            "verificationMethod": "https://pathToIssuerPublicKey"
        }
    }
}
```


Figure 3.3 : Exemple de VC attestant que le titulaire est diplômé d'une Licence en science à Acme University [50]

Le code ci-dessus est une représentation d'un VC utilisant des normes comme celles définies par le W3C avec une section @context qui indique les contextes pour interpréter les données du justificatif, incluant des URLs de spécifications. Le champ id fournit un identifiant unique pour le VC permettant de le référencer de manière spécifique au sein de l'écosystème le type du VC indique qu'il s'agit d'un justificatif vérifiable, en l'occurrence un diplôme universitaire sous la forme VerifiableCredential et UniversityDegreeCredential. L'émetteur (issuer) est décrit par un DID unique et le nom de l'institution, ici « Acme University » ; la date d'émission (issuanceDate) est spécifiée au format ISO 8601 assurant une standardisation internationale le credentialSubject identifie le sujet du justificatif, c'est-à-dire la personne ou l'entité à laquelle il se rapporte, avec des informations spécifiques comme le type et le nom du diplôme, ici un Bachelor of Science. Enfin, la section proof contient les détails cryptographiques qui attestent de l'authenticité du justificatif, incluant le type de signature

numérique, la date de création de la preuve et la méthode de vérification assurant que le VC est sécurisé et peut être validé de manière décentralisée

3.1.4 Fonctionnement des VCs

Les VC sont des attestations numériques qui permettent de prouver des informations sur un individu ou une entité de manière sécurisée, flexible et décentralisée. Leur fonctionnement repose sur l'interaction entre les trois acteurs. [57][58][49]

- **Création et Émission des Justificatifs Vérifiables**

Un VC est émis par une entité appelée émetteur. Cette entité peut être une institution gouvernementale, une organisation académique, un centre médical, une entreprise ou même un particulier. L'émetteur est responsable de la création et de la signature numérique du VC assurant ainsi l'authenticité et l'intégrité des informations qu'il contient.

Il est signé numériquement par l'émetteur à l'aide d'une clé cryptographique privée. Cette signature garantit que le VC est authentique et qu'il n'a pas été modifié après sa création.

La signature du VC permet aux vérificateurs de vérifier la provenance et l'intégrité du document en utilisant la clé publique correspondante qui est souvent stockée dans un registre de confiance ou sur une blockchain.

- **Réception et Stockage**

Une fois le VC émis, il est remis au titulaire qui possède le justificatif. Le titulaire est le seul à avoir accès au VC et le stocke généralement dans un portefeuille numérique sécurisé. Il peut utiliser le VC pour prouver des informations spécifiques sur lui-même à différents vérificateurs.

- **Présentation et Vérification**

Après avoir remis le VC au titulaire, il doit être présenté et vérifié pour assurer son authenticité et sa pertinence. Ce processus se décompose en deux étapes essentielles : la présentation du VC par le titulaire et la vérification de celui-ci par le vérificateur.

- ✓ **Présentation au Vérificateur ou Présentation vérifiable**

Lorsque le titulaire souhaite prouver certaines informations, il présente le VC à un vérificateur. Cette présentation peut se faire directement ou via une application numérique. Le titulaire peut choisir de révéler certaines informations spécifiques notamment en utilisant des techniques telles que la divulgation sélective.

- **Divulgation Sélective**

Les titulaires ont un contrôle total sur les informations qu'ils choisissent de partager. Grâce à la divulgation sélective, ils peuvent fournir uniquement les données nécessaires tout en préservant la confidentialité des autres informations. Les techniques de preuve à divulgation nulle de connaissance (ZKP) permettent de prouver certaines assertions sans révéler les détails sous-jacents.

Le Zero-Knowledge Proof est un protocole cryptographique qui permet de vérifier l'authenticité d'une propriété sans révéler la valeur de la donnée. Vous pouvez prouver que vous avez plus de 18 ans sans dévoiler votre date de naissance. [51]

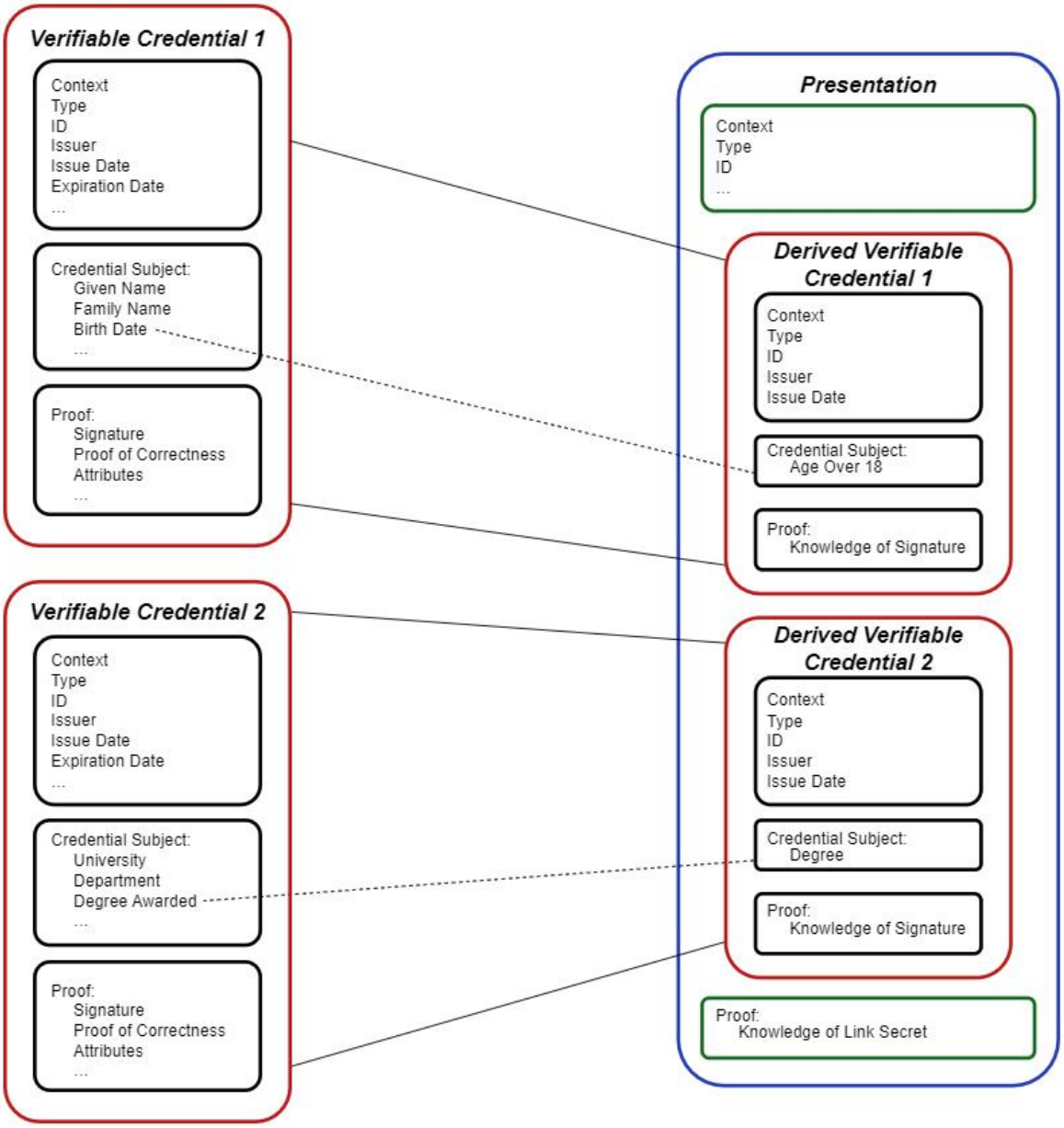


Figure 3.4 : Exemple de présentation vérifiable avec divulgation sélective [49]

L'illustration de la figure ci-dessus montre comment les informations d'identification peuvent être partiellement dérivées pour ne divulguer que ce qui est nécessaire dans une situation donnée. Par exemple, plutôt que de divulguer l'intégralité d'une carte d'identité, seule l'information prouvant que l'utilisateur est majeur pourrait être extraite et présentée.

Ce type d'approche est central dans les systèmes d'identification décentralisés et les technologies qui utilisent les ZKP, car ils permettent de préserver la confidentialité tout en offrant une vérification fiable de certaines informations.

- ✓ **Vérification**

Le vérificateur est l'entité qui examine le VC pour s'assurer qu'il est authentique et valide. La vérification implique l'examen de la signature numérique pour confirmer que le VC a été émis par une source autorisée et qu'il n'a pas été modifié. Le vérificateur décide également s'il fait confiance à l'émetteur comme le ferait un vendeur qui évalue la validité d'un permis de conduire émis par un autre État.

- **Révocation et Suppression**

La gestion des justificatifs vérifiables peut nécessiter les deux actions clés suivantes pour assurer leur pertinence et leur sécurité qui sont la révocation et la suppression.

- ✓ **Révocation**

La révocation d'un justificatif vérifiable est un processus par lequel un émetteur annule la validité d'un VC, souvent via un registre public ou décentralisé, pour des raisons comme l'expiration, la fraude, ou des changements de statut. Cela empêche l'utilisation future du VC pour prouver les informations qu'il contient.

- ✓ **Suppression**

La suppression d'un justificatif vérifiable est l'action par laquelle un titulaire retire un VC de son portefeuille numérique, généralement pour des raisons de confidentialité, de sécurité ou parce qu'il n'est plus nécessaire. Contrairement à la révocation, la suppression ne rend pas le VC invalide mais le rend simplement inaccessible pour de futures utilisations. Cependant, si le titulaire souhaite réutiliser ce VC à l'avenir, il peut généralement récupérer une nouvelle copie du VC auprès de l'émetteur, à condition que le justificatif reste valide et non révoqué.

3.2 Etude des Identifiants Distribués (DID)

L'étude des DID explore comment ces nouvelles normes d'identification permettent une gestion décentralisée et sécurisée des identités numériques, en offrant une alternative robuste aux systèmes centralisés traditionnels. Cette section examine les concepts fondamentaux, les structures et les mécanismes associés aux DID afin de comprendre leur rôle et leur fonctionnement dans le contexte de la gestion de l'identité numérique moderne.

Pour étudier les DID, nous avons exploré les articles suivants : [48, 51, 59, 60, 61, 62, 63 et 64] qui nous ont permis d'avoir une vision plus vaste des DID.

3.2.1 Définition des DID

En nous basant sur les documents [47] et [57], d'après le NIST et le W3C, nous pouvons dire qu'un identifiant distribué est un concept qui permet à une entité de créer et de gérer ses propres identifiants numériques de manière indépendante, sans recourir à une autorité centrale ou à un registre centralisé. Ces identifiants appelés Decentralized Identifiers (DID), sont utilisés pour établir des canaux de communication sécurisés et privés pour l'authentification et l'échange de données sensibles comme des informations d'identification.

Les DID permettent à une entité de posséder plusieurs identifiants, souvent un ou plusieurs par relation avec une autre entité, ce qui garantit un niveau élevé de confidentialité et de sécurité. La possession d'un DID est prouvée par la maîtrise de la clé privée associée à la clé publique liée à ce DID.

Les DID fonctionnent selon des méthodes standardisées qui régissent leur création, résolution, mise à jour et suppression. Ces méthodes assurent également la gestion du cycle de vie des DID comme leur enregistrement, remplacement, rotation, récupération et expiration.

Un DID est composé de plusieurs éléments standardisés tels que des clés publiques pour l'authentification et la communication, des méthodes d'authentification pour prouver la possession du DID et des points de service pour interagir avec le sujet du DID. De plus, des éléments optionnels comme des signatures numériques et des horodatages peuvent être inclus pour garantir l'intégrité et l'authenticité des documents associés à un DID.

3.2.2 Structure d'un DID

Un Decentralized Identifier est une chaîne de texte simple utilisée pour identifier de manière unique une entité dans un système décentralisé. Sa structure se compose de trois éléments clés : le Schéma, la Méthode DID et l'identifiant spécifique à la méthode DID.



Figure 3.5 : Exemple de DID [57]

Chaque élément joue un rôle très important pour le bon fonctionnement du DID.

- **Scheme (schéma) :**

Le Schème est plus fréquemment représenté par le préfixe « did: ». Ce préfixe est obligatoire pour tous les DID et sert à identifier la chaîne comme étant un identifiant décentralisé.

Il indique que l'identifiant est conforme aux normes des DID, ce qui permet aux systèmes de le reconnaître et de savoir comment le traiter. Il est commun à tous les DID, quel que soit le type de méthode ou l'identifiant spécifique.

- **DID Method :**

La méthode DID, située après le schème et séparée par deux points, est un identifiant textuel qui représente la méthode ou le protocole utilisé pour gérer le DID. Ils définissent comment les DID sont créés, résolus, mis à jour, et désactivés.

Dans l'exemple « did:example:123456789abcdefghi », « example » est considéré comme la méthode DID.

Cette partie spécifie le réseau ou le registre décentralisé particulier associé à ce DID, comme « sov » pour Sovrin, « btcr » pour Bitcoin, ou tout autre méthode reconnue. La méthode détermine comment le DID est résolu, c'est-à-dire comment on accède au document DID associé pour obtenir des informations supplémentaires.

Les spécifications des méthodes DID doivent respecter les exigences normatives définies dans [58]. Les méthodes qui ne respectent pas ces exigences ne seront pas acceptées. Il est recommandé aux auteurs de méthodes DID de fournir une adresse e-mail pour faciliter la maintenance, sinon une étiquette indiquant l'absence d'information de contact sera ajoutée à l'entrée de registre.

- **DID method-specific identifier :**

L'identifiant spécifique à la méthode est la dernière partie de la chaîne DID et est unique à chaque méthode. Dans l'exemple fourni, « 123456789abcdefghi » est cet identifiant.

Il identifie de manière unique une entité ou un objet au sein de la méthode DID spécifique. Cet identifiant peut être généré de différentes manières, souvent de façon aléatoire ou déterministe et est utilisé pour pointer vers un document DID, qui contient les métadonnées associées à ce DID.

- **Quelques méthodes DID :**

Dans le tableau suivant, nous donnons le résumé de diverses méthodes DID, le registre utilisé, leurs propriétés et leurs spécificités techniques qui sont susceptibles d'être rencontrés dans les recherches.

Tableau 3.1 : Différentes méthodes de DID, le registre utilisé, leurs propriétés, et leurs spécificités

Méthode DID	Registre utilisé	Propriété	Spécificité
did:example	Aucun	Exemple générique	Utilisé uniquement pour la documentation et les exemples ; non implémenté dans des systèmes réels.
did:ethr	Blockchain Ethereum	Décentralisé	Utilise des contrats intelligents sur Ethereum pour la gestion des DID ; permet l'intégration avec les applications basées sur Ethereum.
did:btcr	Blockchain Bitcoin	Décentralisé	Basé sur des transactions Bitcoin ; les DID sont créés et résolus via la blockchain Bitcoin, assurant la sécurité et la transparence des enregistrements.
did:sov	Blockchain Sovrin	Permisionnée	Utilise une blockchain permisionnée, axée sur l'identité auto-

			souveraine ; soutenue par la Sovrin Foundation.
did:key	Aucun (auto-contenu)	Auto-souverain	DID dérivé d'une clé publique ; pas besoin de registre externe pour la résolution.
did:web	Serveurs web via HTTPS	Centralisé/Décentralisé	Basé sur les URL HTTPS ; résolution via des serveurs web, permettant une adoption facile sur l'infrastructure web existante.
did:v1	Blockchain Veres One	Décentralisé	Utilise la blockchain Veres One, conçue pour les identités numériques auto-souveraines.
did:ion	Sidetree sur Bitcoin	Décentralisé	Utilise le protocole Sidetree sur la blockchain Bitcoin ; scalable et basé sur des ancrages de lots de transactions.
did:elem	Sidetree sur Ethereum	Décentralisé	Utilise le protocole Sidetree sur Ethereum ; conçu pour la scalabilité et la résilience.
did:indy	Hyperledger Indy	Permisionné	Blockchain permisionnée pour les identités décentralisées ; utilisée par Sovrin, Evernym et d'autres projets d'identité.
did:kilt	Blockchain KILT	Décentralisé	Conçu pour les identités auto-souveraines et les attestations de

			crédibilité ; basé sur la blockchain KILT.
did:work	Aucun (off-chain)	Centralisé/Décentralisé	DID gérés hors-chaîne mais peuvent être liés à des registres décentralisés ; flexibilité pour des environnements de travail.
did:ccp	Aucun (off-chain)	Centralisé/Décentralisé	Utilisé pour les projets de gestion de cycle de vie et les cas d'utilisation spécifiques aux entreprises.
did:ion	Sidetree sur Bitcoin	Décentralisé	Protocole Sidetree ; résout les DID en les ancrant sur la blockchain Bitcoin, assurant la décentralisation et la sécurité.
did:evan	Blockchain evan.network	Décentralisé	Conçu pour les identités numériques dans les environnements industriels ; basé sur la blockchain evan.network.
did:git	Git-based	Décentralisé	Utilise des dépôts Git comme registre ; chaque commit représente une mise à jour du DID Document.
did:ipid	IPFS	Décentralisé	Utilise le système de fichiers distribué IPFS pour stocker et résoudre les DID Documents.
did:erc725	Ethereum	Décentralisé	Basé sur le standard

			ERC725 pour la gestion des identités sur la blockchain Ethereum.

Ce tableau offre une vue d'ensemble des différentes méthodes DID, leurs registres associés et leurs spécificités techniques, montrant la diversité et la flexibilité des approches pour les identifiants décentralisés.

3.2.3 L'écosystème des Identifiants Distribués

Les DID sont constitués de plusieurs éléments essentiels qui interagissent pour fournir une identité numérique décentralisée, chacun ayant un rôle spécifique dans la gestion et la vérification de cette identité. [59]

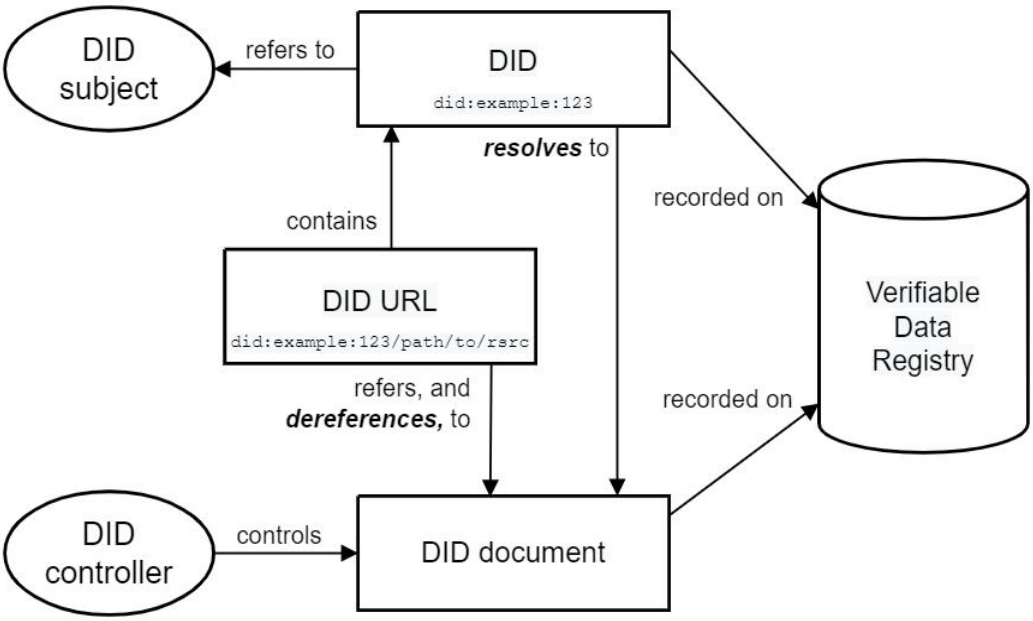


Figure 3.6 : Composants de l'écosystème des DID [59]

Ce schéma illustre comment est structuré l'environnement des DID dans un système décentralisé pour assurer l'identification et l'authentification de manière sécurisée et vérifiable.

- **URL DID**

Une URL DID est une extension de la syntaxe de base d'un DID. Alors qu'un DID standard est composé du schéma did:, d'un identifiant de méthode et d'un identifiant unique spécifique, une URL DID ajoute des composants URI supplémentaires tels que le chemin, la requête et le fragment. Ces extensions permettent de localiser des ressources spécifiques comme une clé publique cryptographique au sein d'un document DID ou d'accéder à des ressources externes. Les URL DID facilitent ainsi une navigation plus précise et ciblée au sein des informations associées à un DID.

- **Sujets DID**

Le sujet d'un DID est l'entité identifiée par le DID. Cette entité peut être variée : une personne, un groupe, une organisation, un objet ou même un concept abstrait. Le sujet du DID peut

également être le contrôleur du DID, c'est-à-dire celui qui a la capacité de gérer et de modifier le Document DID associé. Cette flexibilité dans la définition du sujet permet d'appliquer les DID à une vaste gamme d'entités et de scénarios.

- **Contrôleurs DID**

Les contrôleurs DID sont les entités qui ont la capacité de modifier un document DID. Cette capacité est généralement assurée par la détention d'un ensemble de clés cryptographiques utilisées pour signer les modifications apportées au document DID. Un DID peut avoir plusieurs contrôleurs, chacun ayant une part dans la gestion et la mise à jour du DID. Le contrôleur peut être le sujet du DID lui-même ou une autre entité désignée.

- **Registres de données vérifiables**

Les registres de données vérifiables sont les systèmes ou réseaux sous-jacents sur lesquels les DID sont enregistrés. Ces registres permettent de stocker les DID et de fournir les données nécessaires pour produire les documents DID correspondants. Les registres peuvent inclure des registres distribués, des systèmes de fichiers décentralisés, des bases de données variées ou des réseaux peer-to-peer. Ils assurent la disponibilité et l'intégrité des informations liées aux DID facilitant leur résolution et leur utilisation.

- **Document DID (DDO)**

Un Document DID (DID Document), aussi appelé DID Document Object (DDO), est un document structuré numérique qui contient des informations cruciales associées à un Identifiant Distribué (DID). Ce document décrit comment un DID peut être utilisé pour interagir de manière sécurisée avec l'entité qu'il représente en incluant généralement des méthodes de vérification telles que des clés publiques cryptographiques et des services permettant d'interagir avec le sujet du DID. Le Document DID est essentiel pour la résolution et la validation des informations liées au DID dans un écosystème décentralisé et il peut être mis à jour selon les opérations spécifiées par les méthodes DID.

Un DDO peut contenir un ensemble de composants qui forment sa structure fondamentale permettant d'associer des informations de vérification et des services spécifiques à un DID, facilitant ainsi une interaction sécurisée et décentralisée avec l'entité représentée. Ces composants sont :

- ✓ **Identifiant DID**

L'identifiant unique qui est référencé par le document DID.

- ✓ **Clés Publiques**

Une liste de clés publiques associées au DID. Ces clés sont utilisées pour la signature numérique, l'authentification et d'autres interactions cryptographiques.

- ✓ **Métadonnées**

Informations supplémentaires sur le DID telles que des descriptions ou des politiques d'utilisation.

- ✓ **Propriétés de Révocation**

Mécanismes pour révoquer ou mettre à jour le DDO, permettant de gérer les changements ou la sécurité du DID.

- ✓ **Services (endpoints)**

Les services d'un Document DID sont des points de terminaison associés à l'entité DID, ils permettent des interactions spécifiques. Ces services sont décrits dans le DDO avec des URI qui indiquent comment les accéder. Les principaux types de services incluent :

- **Services d'authentification**

Permet aux systèmes de vérifier l'identité de l'entité DID via des mécanismes d'authentification, souvent en utilisant les clés publiques spécifiées dans le DDO.

- **Services de communication**

Points de terminaison pour envoyer des messages chiffrés ou sécurisés à l'entité DID. Cela peut inclure des services de messagerie ou d'autres formes de communication électronique.

- **Services de résolution**

Points de terminaison pour obtenir le DDO lui-même ou d'autres informations associées au DID, facilitant la résolution et la vérification du DID dans l'écosystème décentralisé.

- **Services de divulgation sélective**

Permet de partager des informations spécifiques et limitées basées sur des zero-knowledge proofs ou d'autres mécanismes de confidentialité.


```
{
  "@context": ["https://www.w3.org/ns/did/v1", "https://w3id.org/security/suites/jws-2020/v1"],
  "id": "did:example:123",
  "publicKey": [
    {
      "id": "did:example:123#_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY_-tA4A",
      "type": "JsonWebKey2020",
      "controller": "did:example:123",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ"
      }
    },
    {
      "id": "did:example:123#4SZ-StXrp5Yd4_4rxHVTCYTHyt4zyPfN1fIuYsm6k3A",
      "type": "JsonWebKey2020",
      "controller": "did:example:123",
      "publicKeyJwk": {
        "kty": "EC",
        "crv": "secp256k1",
        "x": "Z4Y3NNOxv0J6tCgqOBFnHnaZhJF6LdulT7z8A-2D5_8",
        "y": "i5a2NtJoUKXkLm6q8nOEu9WOkso1Ag6FTUT6k_LMnGk"
      }
```


Figure 3.7 : Exemple extrait code de DDO [63]

Sur cette capture, nous essayons d'illustrer un DDO par un extrait de code montrant comment une liste de clés publique peut être décrite.

3.2.4 Principes de Fonctionnement des DID

Les Identifiants Distribués sont des identifiants numériques uniques à l'échelle mondiale qui permettent aux individus et aux organisations d'établir leur identité sur internet indépendamment des autorités centralisées et facilitent la création, le contrôle et la vérification d'identités numériques dans un environnement décentralisé. Ils sont essentiels pour la gestion sécurisée et décentralisée de ces identités numériques offrant une alternative aux systèmes traditionnels centralisés.

- **Création d'un DID**

La création d'un DID est le point de départ du processus, impliquant la génération de clés cryptographiques uniques et l'enregistrement de l'identifiant sur un réseau décentralisé.

- ✓ **Génération de clés**

Le processus commence par la génération d'une paire de clés cryptographiques (une clé publique et une clé privée). La clé publique sera utilisée dans le DID tandis que la clé privée reste secrète et est utilisée pour signer des transactions ou des documents.

- ✓ **Enregistrement sur un réseau décentralisé**

Le DID est ensuite enregistré sur une plateforme décentralisée, nous voyons, souvent une blockchain. Cela crée un lien entre le DID et la clé publique et assure la transparence, et l'accessibilité tout en garantissant l'autonomie du DID.

- ✓ **Document DID**

Lors de l'enregistrement, un Document DID est également créé contenant des métadonnées sur l'identité, comprenant la clé publique et vraisemblablement des points de terminaison de services (comme des adresses pour la communication ou l'authentification).

- **Résolution d'un DID**

La résolution d'un DID est un processus assuré par un résolveur DID. Un résolveur DID est un composant logiciel ou un service qui prend un DID en entrée et le transforme en un Document DID associé. Ce processus permet d'obtenir toutes les informations nécessaires pour interagir avec le sujet du DID.

- ✓ **Interrogation d'un résolveur DID**

L'interrogation se fait en soumettant le DID à un résolveur DID qui interroge le registre décentralisé pour retrouver le Document DID associé.

- ✓ **Récupération des informations**

La récupération se fait en obtenant le Document DID du registre. Le résolveur renvoie le Document DID associé, fournissant ainsi tous les détails nécessaires tels que la clé publique, les services associés et d'autres métadonnées.

- **Vérification et Interaction**

Une fois le Document DID récupéré, il sert à vérifier l'identité du sujet et à faciliter des interactions sécurisées.

- ✓ **Vérification d'identité**

La vérification se fera donc en utilisant les clés publiques contenues dans le Document DID pour authentifier le sujet du DID. Cela permet de confirmer que l'entité qui prétend être associée au DID est bien celle qu'elle prétend être.

- ✓ **Interactions sécurisées**

Les interactions se font en suivant les services définis dans le Document DID, permettant des échanges sécurisés entre les parties comme s'authentifier auprès de services, échanger des informations de manière sécurisée ou signer numériquement des documents garantissant ainsi l'intégrité et l'authenticité des actions.

Pour faire la résolution DID, on utilise des fonctions de résolution DID qui sont des outils servant à transformer un DID en un document DID contenant des informations importantes sur ce DID.

```
resolve(did, resolutionOptions) →
   « didResolutionMetadata, didDocument, didDocumentMetadata »

resolveRepresentation(did, resolutionOptions) →
   « didResolutionMetadata, didDocumentStream, didDocumentMetadata »
```

Figure 3.8 : Fonctions de résolution DID avec entrées et sorties [59]

- ✓ **Fonction resolve(did, resolutionOptions)**

La fonction « resolve » prend en entrée un DID par exemple did:btcr:123456789abcdefghi et des options de résolution. Elle renvoie plusieurs éléments : des métadonnées sur le processus de résolution, le document DID sous une forme abstraite et des métadonnées spécifiques au document DID. Si le processus de résolution échoue, les métadonnées décrivent l'erreur survenue et le document DID est vide.

- ✓ **Fonction resolveRepresentation(did, resolutionOptions)**

La fonction « resolveRepresentation », quant à elle, fonctionne de manière similaire mais avec une différence clé. Au lieu de retourner un document DID sous forme abstraite, elle fournit une représentation spécifique du document DID sous forme d'un flux d'octets. Ce flux peut être en format JSON, CBOR ou un autre format, en fonction des besoins. Comme pour resolve, cette fonction retourne également des métadonnées sur le processus de résolution et sur le document DID lui-même. Si la résolution échoue, le flux d'octets est vide et les métadonnées décrivent l'erreur.

En résumé la fonction « resolve » est utilisée pour obtenir un document DID sous une forme abstraite tandis que « resolveRepresentation » est utilisée pour obtenir une version formatée du document DID. Les deux fonctions permettent de manipuler et de comprendre les DID en fonction des besoins spécifiques qu'il s'agisse d'un modèle de données ou d'une représentation spécifique.

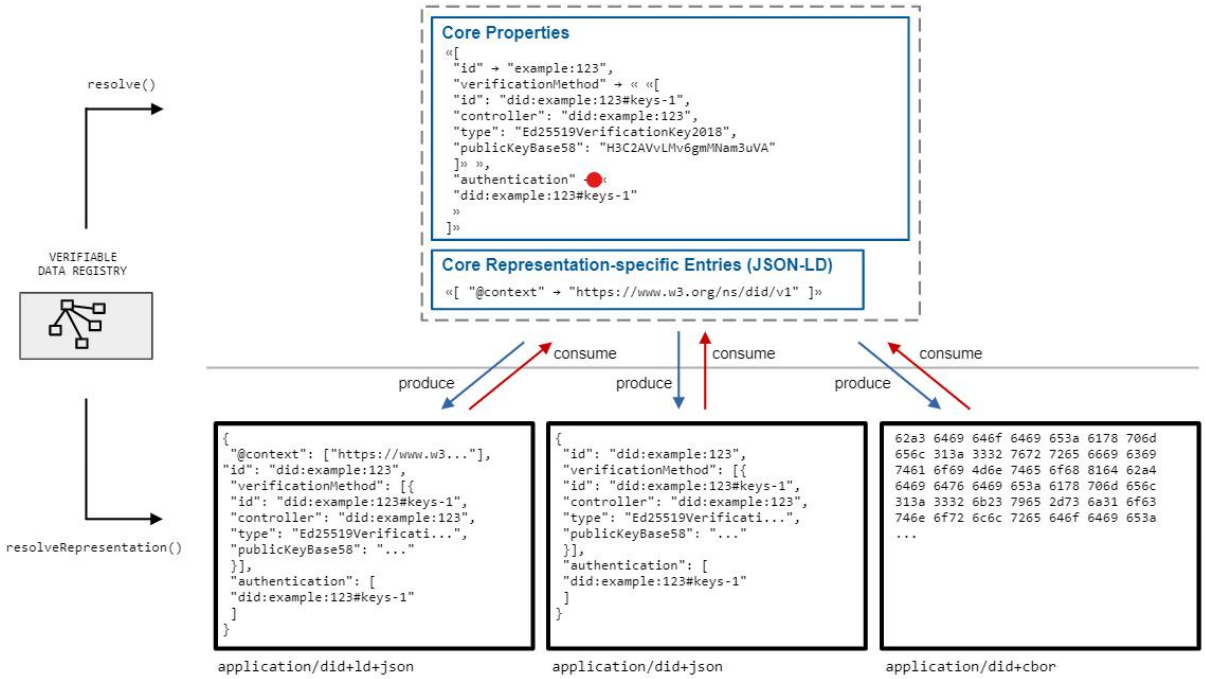


Figure 3.9 : Illustration des fonctions resolve() et resolveRepresentation() [59]

La figure montre comment un DID enregistré sur un registre de données vérifiables peut être résolu pour obtenir ses propriétés de base et comment ces propriétés peuvent être représentées dans différents formats adaptés à divers usages. Cela souligne la flexibilité et l'interopérabilité des DID dans des environnements numériques variés en fonction des besoins des consommateurs de données.

➢ Contrôle et Mise à Jour

Le contrôle continu et la mise à jour des informations d'un DID sont essentiels pour maintenir la sécurité et l'intégrité de l'identité numérique.

✓ Propriété et contrôle

Le contrôle est assuré par le propriétaire du DID, qui détient la clé privée. Ce contrôle permet au propriétaire de gérer le Document DID, d'ajouter ou de retirer des informations et de révoquer le DID si nécessaire.

✓ Mise à jour des informations

Les utilisateurs peuvent mettre à jour le Document DID lorsque cela est nécessaire (par exemple, pour changer de clé publique ou ajouter de nouveaux services), généralement en faisant une nouvelle transaction sur le registre décentralisé (la blockchain). Cette mise à jour est également transparente et immuable, renforçant la sécurité et la confiance.

3.3 Protocoles et Normes des VC et DID

Les Verifiable Credentials et Decentralized Identifiers sont des éléments clés de l'écosystème de l'identité numérique décentralisée. Ils reposent sur des protocoles et des normes bien définis pour garantir l'interopérabilité, la sécurité, la confidentialité des données et l'adoption à grande échelle.

3.3.1 Protocoles de Communication et d'Authentification

- **DID Communication Protocol (DIDComm)**

Un protocole de communication construit spécifiquement pour les DID, permettant l'échange sécurisé de messages entre entités sur la base de leurs identités décentralisées. DIDComm offre des fonctionnalités de chiffrement, de vérification et de confidentialité.

- **Verifiable Credentials Data Model**

Ce modèle définit comment les VC peuvent être structurés en spécifiant les formats de données et les méthodes d'émission et de vérification. Les VC permettent d'attester des informations tout en garantissant leur véracité sans nécessiter de tiers de confiance.

- **OAuth 2.0 et OpenID Connect**

Bien que principalement utilisés dans un contexte centralisé, ces protocoles peuvent être adaptés dans des environnements utilisant des DID pour l'authentification. Ils facilitent l'accès sécurisé aux ressources en ligne avec un contrôle sur l'identité de l'utilisateur.

- **JSON Web Tokens (JWT)**

Utilisés pour transmettre des informations d'identification et d'authentification de manière sécurisée. Les JWT peuvent être intégrés dans les systèmes utilisant des VC pour la vérification des données.

3.3.2 Normes et Standards

Des normes et standards reconnus assurent la cohérence et l'interopérabilité dans l'utilisation des VCs et DID :

- **W3C DID Specification**

Cette spécification définit le format des DID, les méthodes de création et de résolution des identifiants décentralisés. Elle promeut l'autonomisation des utilisateurs en leur permettant de créer et de gérer leurs propres identités.

- **W3C Verifiable Credentials Data Model 1.0**

Document qui décrit comment structurer et utiliser les VC. Il en définit les architectures, les processus d'émission, de vérification et les exigences de format.

- **ISO/IEC 29100**

Un cadre qui définit les principes de protection de la vie privée applicables aux systèmes d'identité numérique. Bien qu'il ne soit pas spécifique aux VC ou aux DID, il fournit des lignes directrices pertinentes pour les implémentations.

- **Decentralized Identifiers (DID) v1.0**

Un standard du W3C qui guide la mise en œuvre des identifiants décentralisés. Il inclut la syntaxe et les méthodes pour la résolution des DID.

Ces protocoles et normes forment la colonne vertébrale des VC et des DID offrant des mécanismes sécurisés et standardisés pour l'identité numérique dans un monde de plus en plus décentralisé et interconnecté.

3.4 Avantages des VC et des DID

Les VC et les DID offrent des avantages significatifs dans le domaine de l'identité numérique, contribuant à une importante augmentation de la sécurité, à une réduction des fraudes et des usurpations d'identité, ainsi qu'à une simplification des processus d'authentification et de vérification. Cette section explore comment ces technologies transforment positivement la gestion de l'identité numérique et renforcent la confiance dans les interactions.



Figure 3.10 : illustration de la positivité des VC et DID [59]

3.4.1 Amélioration de la sécurité et de la vérifiabilité

Les Vérifiables Credentials et les Decentralized Identifiers offrent une infrastructure de sécurité robuste grâce à des technologies cryptographiques avancées. Ces systèmes permettent de créer des identités numériques qui sont non seulement sécurisées mais également vérifiables par des tiers. Par exemple, un utilisateur peut présenter une VC à un service en ligne sans avoir à divulguer d'autres informations personnelles. La vérifiabilité des informations contenues dans les VC permet également de garantir leur authenticité, ce qui renforce la confiance tant dans les échanges en ligne que dans les interactions physiques.

3.4.2 Réduction des fraudes et des usurpations d'identité

L'introduction des VC et des DID constitue un atout majeur dans la lutte contre la fraude et l'usurpation d'identité. En s'appuyant sur des normes de vérification décentralisées, ces technologies rendent difficile la falsification des identités. Par exemple, un acteur malveillant ne peut pas facilement créer une fausse identité en raison des mécanismes de cryptographie qui sous-tendent ces systèmes. De plus, les utilisateurs peuvent se qui accéder à leurs données et peuvent les rappeler à tout moment, minimisant ainsi le risque d'abus.

3.4.3 Simplification des processus d'authentification et de vérification

Les VC et les DID simplifient considérablement les processus d'authentification et de vérification. Dans un monde numérique où les utilisateurs doivent souvent gérer des dizaines de mots de passe et d'identifiants, ces solutions décentralisées de tailles permettent un accès plus fluide aux services. Les utilisateurs peuvent prouver leur identité ou leurs qualifications (par exemple, diplômes, certifications) facilement grâce à des preuves numériques qui sont instantanément vérifiables. Cela réduit les frictions dans divers secteurs, allant de l'éducation à la finance, en offrant une expérience utilisateur plus rapide et plus agréable.

3.5 Défis Techniques et Réglementaires

Les VC et les DID rencontrent divers défis techniques et réglementaires qui influencent leur adoption et leur intégration. Cette section explore les obstacles techniques liés à leur mise en œuvre efficace ainsi que les enjeux réglementaires qui doivent être surmontés pour assurer leur conformité et acceptabilité.

3.5.1 Défis techniques :

- **Scalabilité**

La scalabilité représente la capacité d'un système à s'ajuster en fonction de l'augmentation de la charge de travail ou du nombre d'utilisateurs. Dans un environnement technologique en constante évolution, il est essentiel que les infrastructures puissent évoluer sans compromettre les performances. Les défis incluent la gestion efficace des ressources, l'architecture logicielle adaptée et la capacité à intégrer de nouvelles fonctionnalités sans nécessiter des refontes majeures du système.

- **Interopérabilité**

L'interopérabilité désigne la capacité des systèmes et des applications à travailler ensemble sans difficulté. Dans un monde où de nombreux fournisseurs et technologies coexistent, garantir que les nouveaux systèmes puissent interagir avec les systèmes existants est un défi majeur. Cela nécessite souvent l'adoption de normes communes, la mise en place de protocoles compatibles et la gestion des différences entre les plateformes.

- **Complexité de mise en œuvre**

La mise en œuvre d'une nouvelle technologie ou d'un nouveau système peut s'avérer complexe en raison des multiples facteurs à considérer tels que les besoins des utilisateurs, les exigences opérationnelles et la nécessité de former le personnel. Cette complexité est souvent exacerbée par le manque de documentation ou de ressources de support, ainsi que par la résistance au changement qui peut exister au sein des organisations.

3.5.2 Défis réglementaires

- **Conformité aux lois sur la protection des données**

La conformité aux lois sur la protection des données telles que le RGPD en Europe, représente un défi essentiel pour les organisations. Il est crucial de s'assurer que toutes les données collectées et traitées sont gérées de manière à respecter les droits des individus. Cela inclut la transparence dans la collecte des données, la sécurité des informations personnelles et le respect des demandes d'accès ou de suppression de données.

- **Acceptation légale**

L'acceptation légale des solutions technologiques peut varier d'une juridiction à l'autre. Les entreprises doivent s'assurer que leurs solutions respectent non seulement les lois en vigueur, mais également les réglementations sectorielles spécifiques. Cela peut nécessiter des consultations juridiques approfondies et une veille réglementaire continue pour s'adapter aux évolutions législatives. De plus, l'acceptation de nouvelles technologies comme les systèmes basés sur l'intelligence artificielle ou la blockchain soulève également des questions éthiques et de responsabilité qui doivent être prises en compte.

3.6 Conclusion

Les VC et les DID constituent des solutions révolutionnaires pour surmonter les défis identifiés. Leur structure décentralisée et leur confiance sur des mécanismes cryptographiques robustes offrent une sécurité augmentée et une autonomie des utilisateurs sans précédent. Cependant, pour comprendre leur impact réel de ces technologies, il est essentiel d'analyser leurs apports pratiques sur la sécurité et la vérifiabilité des identités en ligne, thématiques abordées dans le prochain chapitre.

4. Impact des VC et DID sur la Sécurité et la Vérifiabilité des Identités en Ligne

La transformation numérique accélérée a causé la multiplication des vulnérabilités dans les systèmes traditionnels de gestion des identités en ligne, en mettant en lumière la nécessité de solutions plus robustes, sécurisées et décentralisées. Les Verifiable Credentials et les Decentralized Identifiers émergent comme des réponses prometteuses à ces défis, offrant de nouvelles perspectives pour renforcer la sécurité, la vérifiabilité et la confidentialité des identités numériques dans un écosystème en constante évolution.

Dans cette section nous allons aborder la question à savoir : « comment les VC et les DID peuvent transformer la sécurité des identités numériques et garantir une vérifiabilité accrue ? ».

4.1 Problématiques Actuelles de la Sécurité des Identités en Ligne

La sécurité des identités en ligne est confrontée à des défis croissants, exacerbés par l'augmentation des activités numériques et des menaces sophistiquées. Les systèmes d'identification traditionnels peinent à protéger efficacement les utilisateurs contre des attaques telles que le vol d'identité et le phishing, mettant en évidence les limitations structurelles de ces méthodes dans un environnement numérique de plus en plus complexe et interconnecté.

Nous allons essayer d'évoquer les problèmes de sécurité courants des identités en ligne et les limites des systèmes de gestion traditionnels.

4.1.1 Problèmes courants de sécurité

Les problèmes de sécurité en ligne les plus courants tels que le phishing, le vol d'identité, l'usurpation d'identité et la réutilisation des mots de passe exposent les utilisateurs à des risques importants, compromettant leur vie privée et leur sécurité personnelle.

- **Phishing**

Le phishing est un type de menace de cybersécurité qui cible les utilisateurs directement par e-mail, SMS ou messages directs. Lors de l'une de ces escroqueries, l'assaillant se fera passer pour un contact de confiance pour voler des données telles que des identifiants, des numéros de compte et des informations de carte de crédit. Le phishing est un type d'attaque d'ingénierie sociale dans laquelle un cybercriminel utilise des e-mails ou d'autres messages textuels pour voler des informations sensibles. En utilisant une adresse e-mail crédible, un attaquant vise à inciter la cible à lui faire suffisamment confiance pour divulguer des données personnelles, telles que des identifiants de déconnexion, des numéros de carte de crédit ou des informations de compte financier. [65]

Chaque année des millions d'internautes sont victimes de tentatives de phishing. Ces escroqueries reposent sur des sites Web qui imitent des entités de confiance telles que des banques ou des commerçants, mais qui sont en réalité contrôlés par des réseaux criminels. Ces faux sites ont pour but de convaincre les victimes de fournir des informations personnelles que les escrocs peuvent utiliser pour voler de l'argent ou revendre des identifiants à d'autres cybercriminels. [66]

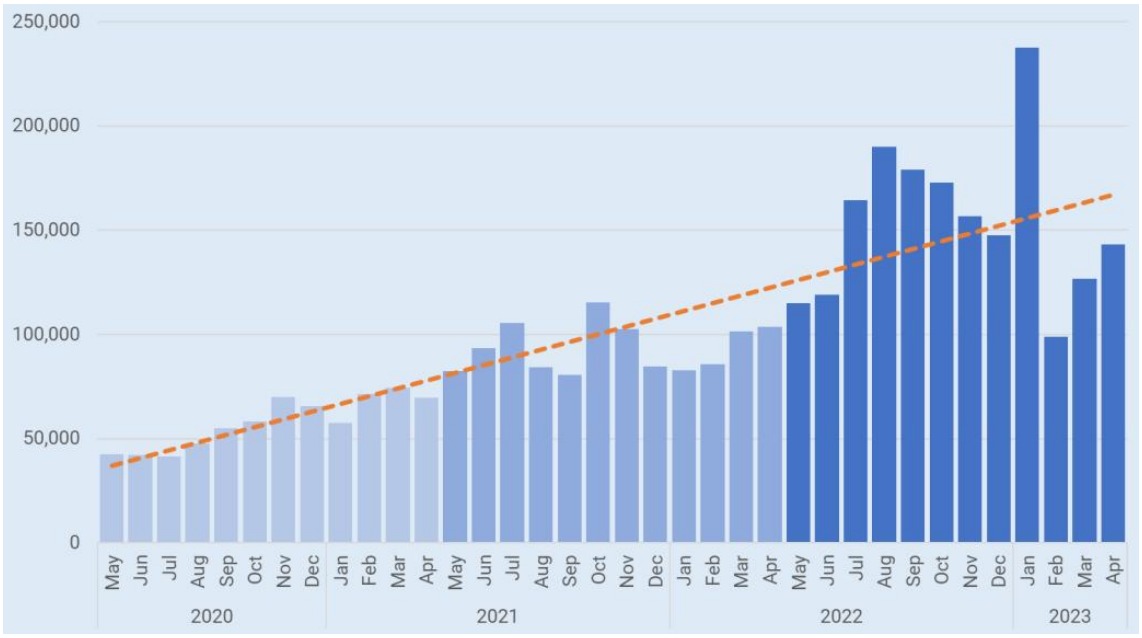


Figure 4.1 : Attaques de phishing par mois, mai 2020 - avril 2023 [66]

Le graphique ci-dessus montre une tendance préoccupante d'augmentation des attaques de phishing au cours des dernières années avec une montée en flèche en 2022 et 2023. Cette tendance indique que les attaques de phishing deviennent de plus en plus fréquentes, soulignant l'importance de renforcer les mesures de sécurité en ligne pour contrer ces menaces croissantes.

- **Usurpation d'identité**

Le vol d'identité ou usurpation d'identité se produit lorsqu'une personne obtient et utilise à votre insu et sans votre consentement vos renseignements personnels. Les renseignements personnels peuvent comprendre toute information ou tout document servant à établir votre identité. [68]

Le vol d'identité est un crime de plus en plus fréquent et aux conséquences graves qui fait chaque année des milliers de victimes. Dans la majorité des cas, les victimes de vol d'identité découvrent ce vol beaucoup trop tardivement. Fidèle à son mandat de servir le public, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) a élaboré des documents d'information et des conseils à l'intention des particuliers pour réduire le risque de devenir victime de vol d'identité. La présente brochure offre des conseils sur la prévention du vol d'identité ainsi que des mesures que peuvent prendre les victimes pour se relever de ce crime. [67]

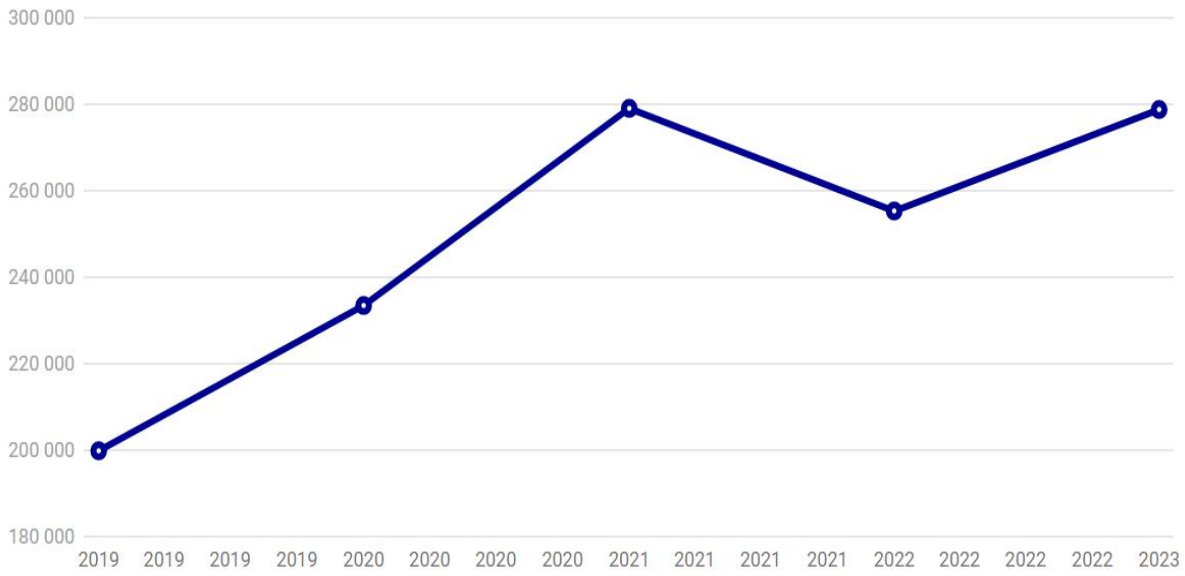


Figure 4.2 : Nombre d'infractions liées au cyber entre 2019 et 2023 [74]

D'après [74], en 2023, les infractions enregistrées relèvent :

- ✓ Pour 59% d'atteintes aux biens (escroqueries, détournement de moyens de paiement...) ;
- ✓ Pour 34,5% d'atteintes aux personnes (harcèlement, injures, menaces, atteintes aux mineurs...) ;
- ✓ Pour 6%, d'atteintes aux institutions et à l'ordre public (troubles à l'ordre public, atteintes à la sûreté de l'État et aux institutions, trafics...) ;
- ✓ Pour 0,5%, d'atteintes aux législations et réglementations spécifiques numériques (infractions au droit d'auteur, infractions au Règlement général sur la protection des données – RGPD).

➢ **Réutilisation et faiblesse des mots de passe**

La réutilisation des mots de passe fait référence à la pratique non sécurisée consistant à utiliser le même mot de passe sur plusieurs comptes, plateformes ou services différents. [72]

La réutilisation des mots de passe est extrêmement dangereuse. Les criminels peuvent avoir du mal à percer dans les systèmes de votre banque, mais il suffit d'un site avec une sécurité faible pour se faire briser et ils pourraient obtenir votre nom d'utilisateur et mot de passe. En quelques heures, ils pouvaient essayer cette combinaison de nom d'utilisateur et de mot de passe sur des centaines voire des milliers de sites sur le web. Il y a des chances qu'ils trébuchent sur au moins quelques autres sites où ce nom d'utilisateur et ce mot de passe fonctionnent. [69]

La réutilisation des mots de passe est un problème plus important que vous ne le pensez et très difficile à repérer. Une enquête de [73] révèle que 53 % des personnes reconnaissent utiliser le même mot de passe pour plusieurs comptes ce qui est une bonne chose pour les pirates informatiques. [70]

Verizon [71] estime que 86 % des attaques ont pour origine des informations d'identification volées. Si un même mot de passe est utilisé pour de nombreux appareils et applications, il suffit que le maillon le plus faible soit compromis. Un courriel d'hameçonnage, un réseau public non sécurisé ou un appareil personnel infecté par un logiciel malveillant peuvent tous

conduire à la compromission d'un mot de passe dans la vie personnelle d'un utilisateur final. S'il a réutilisé son mot de passe professionnel, cet incident cybernétique initialement sans rapport avec votre organisation peut entraîner une chaîne d'événements impactant cette dernière. [70]



Figure 4.3 : pourcentage de réutilisation des mots de passes [75]

Sur [75], il est mentionné que 65% des personnes utilisent et réutilisent les mêmes mots de passe. Réutiliser le même mot de passe ou des variations de celui-ci est une pratique courante mais risquée. Même si beaucoup de gens savent que cela peut compromettre leur sécurité en ligne, ils continuent de le faire par commodité. C'est un problème de sécurité important car si un mot de passe est compromis sur un site, il peut être utilisé pour accéder à d'autres comptes si les mêmes identifiants sont utilisés.

4.1.2 Limitations des systèmes d'identification traditionnels

Les systèmes d'identification traditionnels présentent plusieurs limitations, notamment une dépendance excessive à des tiers de confiance, un manque de transparence et de vérifiabilité, un contrôle restreint pour les utilisateurs ainsi qu'un risque accru de violation de données.

- **Dépendance à des tiers de confiance**

Les systèmes d'identification traditionnels reposent sur des tiers de confiance tels que les gouvernements, les institutions financières et d'autres entités centralisées, pour vérifier et valider les identités. Cette dépendance crée plusieurs problèmes :

- ✓ **Centralisation**

La centralisation des informations dans un seul système ou une seule entité rend ces systèmes vulnérables à des attaques. Comme illustré dans [76], une centralisation excessive expose à tout perdre en cas de destruction ou d'attaque, augmentant ainsi le risque d'accès non autorisé ou de manipulation de données sensibles.

- ✓ **Biais de confiance**

Lorsque les systèmes d'identification sont centralisés, les utilisateurs doivent faire aveuglément confiance à l'entité qui gère leurs informations. Cependant comme mentionné dans [76], cette confiance peut être mal placée surtout si l'entité se détourne des principes démocratiques ou des libertés individuelles.

- ✓ **Falsification potentielle**

La centralisation peut également faciliter la falsification des données par des acteurs malveillants qui pourraient cibler un point unique pour compromettre l'intégrité des identités comme le suggère le risque de manipulation des dossiers médicaux mentionné dans [76].

- **Manque de transparence et de vérifiabilité**

Les processus d'identification traditionnels manquent souvent de transparence et de vérifiabilité pour les utilisateurs :

- ✓ **Processus opaque**

Les utilisateurs n'ont souvent aucune visibilité sur la manière dont leurs informations sont gérées ou vérifiées ce qui augmente les risques de mauvaise gestion ou d'abus. Comme dans [76], les systèmes centralisés peuvent masquer des processus complexes et difficiles à auditer.

- ✓ **Vérifiabilité limitée**

La vérifiabilité des informations est souvent restreinte, ce qui empêche les utilisateurs de s'assurer que leurs données sont correctes et non altérées. Dans [76], l'auteur évoque la crainte que des informations sensibles comme celles des dossiers médicaux puissent être modifiées à l'insu des utilisateurs.

- ✓ **Absence de contrôle**

Les utilisateurs n'ont pas le contrôle direct sur leurs données dans les systèmes traditionnels, ce qui peut mener à des situations où des informations sont utilisées sans leur consentement, renforçant le manque de confiance dans ces systèmes.

- **Contrôle limité pour les utilisateurs**

Dans les systèmes d'identification traditionnels, le contrôle des données d'identification est souvent entre les mains des tiers ce qui limite l'autonomie des utilisateurs :

- ✓ **Possession des données**

Les utilisateurs ne possèdent pas réellement leurs données, elles sont détenues par des tiers ce qui crée une dépendance et un manque d'autonomie. L'auteur de [76] montre comment la centralisation des données pourrait faire sentir aux médecins qu'ils ne sont pas responsables des informations qu'ils produisent.

- ✓ **Partage non autorisé**

Il y a un risque que les données des utilisateurs soient partagées ou utilisées sans leur consentement. [76] met en lumière les inquiétudes liées à la perte de confidentialité, en particulier dans des contextes où les informations sont centralisées.

- ✓ **Restriction de l'autonomie**

Les systèmes centralisés imposent des restrictions sur ce que les utilisateurs peuvent faire avec leurs propres informations, limitant ainsi leur capacité à gérer et protéger leurs données personnelles de manière proactive.

- **Risque de violation de données**

Les systèmes centralisés et dépendants des tiers augmentent le risque de violations de données, ce qui peut avoir des conséquences dévastatrices :

- ✓ **Exposition massive**

La centralisation des informations dans un seul endroit augmente la probabilité qu'une violation de données compromette un grand nombre d'utilisateurs simultanément. [76] évoque comment la centralisation d'informations médicales pourrait attirer les hackers, augmentant ainsi le risque d'exposition massive.

- ✓ **Vulnérabilité aux attaques**

Les systèmes centralisés sont des cibles attrayantes pour les cybercriminels comme l'illustre la crainte exprimée dans [76] que des terroristes ou hackers prennent pour défi de pénétrer des bases de données centralisées.

- ✓ **Conséquences juridiques et financières**

Les violations de données dans les systèmes centralisés peuvent entraîner des conséquences graves tant sur le plan juridique que financier pour les entités responsables ainsi que pour les individus dont les données sont compromises.

4.2 Améliorations Apportées par les VC

Les Verifiable Credentials apportent des solutions innovantes aux problématiques de sécurité des identités en ligne, en renforçant la vérifiabilité des informations tout en réduisant les risques de falsification et d'usurpation. Ces avancées permettent de garantir une plus grande intégrité des données et de restaurer la confiance dans les échanges numériques.

4.2.1 Renforcement de la vérifiabilité des informations d'identité

Pour garantir la fiabilité et l'intégrité des informations d'identité dans un système décentralisé utilisant des Références Vérifiables, plusieurs mécanismes et pratiques doivent être mis en place. Ces mécanismes assurent que les informations partagées sont authentiques, conformes et vérifiables sans dépendre d'une autorité centrale unique.

- ➢ **Signature Cryptographique**

Les VC utilisent des signatures numériques pour prouver que les informations contenues dans une référence (ou credential) ont été émises par une source authentique. Ces signatures garantissent que les données n'ont pas été altérées après leur émission.

- ➢ **Preuve de Validité**

Les VC incluent des mécanismes pour prouver la validité des informations sans révéler plus que ce qui est nécessaire. Cela peut inclure l'utilisation de preuves à divulgation nulle de connaissance, qui permettent de vérifier qu'une assertion est vraie sans divulguer l'information elle-même.

- ➢ **Vérification Décentralisée**

Contrairement aux systèmes traditionnels où une autorité centrale valide les informations, les VC permettent à n'importe quel vérificateur de vérifier l'authenticité et l'intégrité d'une

référence à l'aide de la blockchain ou d'autres technologies décentralisées. Cela renforce la confiance et réduit la dépendance à une seule entité.

- **Gestion efficace de la révocation**

Les VC englobent des mécanismes pour révoquer une référence si elle n'est plus valide (par exemple, si l'information est périmée ou si l'identité a été compromise). Cela peut se faire de manière transparente et décentralisée en utilisant des registres publics pour publier les statuts de révocation.

- **Contrôle de l'Accès Sélectif**

Les VC permettent également un contrôle d'accès sélectif, où l'utilisateur peut choisir quelles informations d'identité partager avec quel vérificateur. Cette fonctionnalité est cruciale pour protéger la vie privée et minimiser l'exposition d'informations sensibles. Par exemple, un utilisateur pourrait choisir de prouver son âge sans révéler sa date de naissance complète. Cette divulgation sélective est souvent rendue possible grâce à des technologies comme les preuves à la ZKP, qui permettent de prouver la véracité d'une information sans en révéler les détails.

- **Audits et Traçabilité**

Enfin pour garantir la fiabilité d'un système d'identité décentralisé, des mécanismes d'audit et de traçabilité doivent être intégrés. Les audits permettent de vérifier que les processus de vérification et de révocation sont effectués correctement et en conformité avec les normes établies. La traçabilité quant à elle, permet de retracer l'historique d'une VC y compris les entités qui l'ont émise, vérifiée et éventuellement révoquée. Cela est essentiel pour maintenir la transparence et la confiance dans le système tout en fournissant un moyen de résoudre les litiges ou de répondre à des exigences réglementaires.

4.2.2 Réduction des risques de falsification et d'usurpation

Pour réduire les risques de falsification et d'usurpation dans les systèmes d'identité, il est crucial de mettre en œuvre des mesures telles que la signature cryptographique pour garantir l'intégrité des données, l'authenticité de l'émetteur pour valider les sources et la décentralisation pour éviter les points de défaillance uniques. La révocation et la mise à jour des credentials, l'utilisation de preuves zero-knowledge pour la vérification sans divulgation d'informations sensibles ainsi que la traçabilité et l'auditabilité sont également essentielles. Enfin, l'authentification multi-facteurs renforce la sécurité en combinant plusieurs méthodes de vérification.

- **Signature Cryptographique**

La signature cryptographique est l'une des premières lignes de défense contre la falsification. Chaque VC est signée par l'émetteur à l'aide de sa clé privée, ce qui garantit l'intégrité des informations. Toute modification non autorisée du credential invalide immédiatement la signature, rendant la falsification détectable. Les vérificateurs peuvent utiliser la clé publique de l'émetteur pour authentifier le document, assurant que les informations n'ont pas été altérées.

- **Authenticité de l'Émetteur**

L'authenticité de l'émetteur est essentielle pour réduire les risques d'usurpation. Les VC permettent de vérifier que le credential provient bien d'une source légitime, identifiée de manière unique et sécurisée. Ce mécanisme empêche les entités malveillantes de se faire passer pour des émetteurs légitimes, en garantissant que seuls les émetteurs autorisés peuvent émettre des credentials vérifiables.

- **Décentralisation**

La décentralisation des systèmes d'identité élimine les points de défaillance uniques, ce qui renforce la sécurité globale. En l'absence d'une autorité centrale unique, la vérification et la gestion des VC sont réparties entre plusieurs entités. Cela rend le système plus résilient face aux attaques et limite les possibilités de falsification ou d'usurpation à grande échelle.

- **Révocation et Mise à Jour**

Les mécanismes de révocation et de mise à jour des VC sont essentiels pour maintenir la validité des informations d'identité. Lorsqu'un credential devient obsolète ou compromis, il peut être révoqué par l'émetteur et cette information est immédiatement disponible pour tous les vérificateurs. Cela empêche l'utilisation de credentials périmés ou compromis, réduisant ainsi les risques d'usurpation.

- **Preuves Zero-Knowledge**

Les ZKP renforcent la sécurité des VC en permettant aux utilisateurs de prouver la validité de certaines informations sans divulguer les détails sous-jacents. Par exemple, un utilisateur peut prouver qu'il est majeur sans révéler sa date de naissance complète. Cette méthode protège la vie privée tout en minimisant les risques d'exposition et de manipulation des données sensibles.

- **Traçabilité et Auditabilité**

La traçabilité et l'auditabilité des VC jouent un rôle crucial dans la prévention de la falsification et de l'usurpation. Chaque étape de la vie d'un credential, de son émission à sa révocation est enregistrée et peut être vérifiée. Cela permet de retracer l'historique complet d'un credential, d'identifier rapidement les anomalies et de s'assurer que les processus sont conformes aux normes de sécurité.

4.3 Améliorations Apportées par les DID

Les Decentralized Identifiers révolutionnent la gestion des identités numériques en offrant aux utilisateurs une autonomie sans précédent dans la création et la gestion de leurs identités tout en renforçant la confidentialité et le contrôle sur leurs données personnelles. Ces innovations permettent aux individus de reprendre la main sur leurs informations dans un environnement numérique de plus en plus complexe.

4.3.1 Autonomie des utilisateurs dans la gestion de leur identité

Les DID jouent un rôle essentiel dans l'augmentation de l'autonomie des utilisateurs et la gestion de leur identité numérique. En permettant une gestion et une création décentralisées des identifiants, les DID offrent aux utilisateurs un contrôle sans précédent sur leurs informations personnelles leur permettant de gérer et de protéger leur identité de manière indépendante sans dépendre d'une autorité centrale.

- **Création et Gestion Décentralisée**

Les DID permettent aux utilisateurs de créer et de gérer leurs identifiants de manière décentralisée sans avoir besoin d'un intermédiaire. Cette approche décentralisée élimine la dépendance à une autorité centrale pour la gestion des identités offrant aux utilisateurs la liberté de générer, utiliser et révoquer leurs identifiants selon leurs besoins sans craindre une surveillance ou une intervention non désirée.

- **Contrôle Total sur les Informations**

Avec les DID, les utilisateurs ont un contrôle total sur les informations qu'ils partagent. Ils peuvent décider quelles données sont partagées avec qui et à quel moment. Ce contrôle granulaire permet aux utilisateurs de protéger leur vie privée tout en participant activement à diverses transactions numériques renforçant ainsi leur sentiment d'autonomie.

- **Révocation et Mise à Jour**

Les DID facilitent la révocation et la mise à jour des informations d'identité permettant aux utilisateurs de maintenir l'exactitude et la sécurité de leurs données. En cas de compromission ou d'obsolescence des informations, l'utilisateur peut facilement révoquer ou mettre à jour ses identifiants garantissant que seules des informations valides et actuelles sont utilisées dans les interactions numériques.

- **Transparence et Visibilité**

Les DID assurent une transparence et une visibilité accrues dans la gestion des identités. Les utilisateurs peuvent suivre l'historique de leurs interactions et de l'utilisation de leurs identifiants ce qui leur permet de comprendre comment et où leurs informations sont utilisées. Cette transparence renforce la confiance des utilisateurs dans le système et leur permet de détecter rapidement toute utilisation abusive.

- **Portabilité et Interopérabilité**

Les DID sont conçus pour être portables et interopérables, ce qui signifie que les utilisateurs peuvent utiliser leurs identifiants sur différentes plateformes et services sans avoir à créer de nouveaux comptes ou identifiants. Cette portabilité renforce l'autonomie des utilisateurs en leur permettant de déplacer librement leurs identités à travers divers écosystèmes numériques tout en conservant le contrôle sur leurs données.

- **Autonomisation par la Cryptographie**

La cryptographie joue un rôle central dans l'autonomisation des utilisateurs grâce aux DID. Les signatures cryptographiques et les techniques de chiffrement permettent aux utilisateurs de protéger leurs informations contre les accès non autorisés et de prouver leur identité de manière sécurisée. Cela leur donne la capacité de gérer leurs identifiants en toute confiance en s'assurant que leurs données restent privées et sécurisées.

- **Gestion des Relations de Confiance**

Les DID permettent une gestion plus efficace des relations de confiance. Les utilisateurs peuvent établir et gérer des relations avec d'autres entités de manière décentralisée en utilisant des preuves cryptographiques pour valider l'authenticité des interactions. Cette gestion

décentralisée des relations de confiance réduit la dépendance à des tiers et renforce l'autonomie des utilisateurs dans la gestion de leurs identités numériques.

4.3.2 Amélioration de la confidentialité et du contrôle des données personnelles

Les Identifiants Décentralisés jouent un rôle crucial dans l'amélioration de la confidentialité et du contrôle des données personnelles en offrant des mécanismes avancés qui permettent aux utilisateurs de gérer et de protéger leurs informations avec une grande autonomie et sécurité.

- **Contrôle Sélectif des Données**

Les DID permettent aux utilisateurs de décider précisément quelles informations personnelles sont partagées avec qui et dans quelles circonstances. Grâce à cette granularité, les utilisateurs peuvent révéler uniquement les données nécessaires à une transaction ou une interaction spécifique, minimisant ainsi l'exposition de leurs informations sensibles. Ce contrôle sélectif est essentiel pour protéger la vie privée et réduire les risques de divulgation excessive de données.

- **Gestion Décentralisée des Identités**

La gestion décentralisée des identités, rendue possible par les DID, élimine la nécessité de recourir à une autorité centrale pour la gestion des informations d'identité. Cela signifie que les utilisateurs sont les seuls à contrôler et à gérer leurs identifiants réduisant ainsi les risques d'exploitation ou de compromis par des tiers. Cette décentralisation renforce la confidentialité en limitant les points d'accès potentiels aux données personnelles.

- **Cryptage des Données**

Le cryptage des données est un élément fondamental des DID pour protéger les informations personnelles contre l'accès non autorisé. Toutes les données associées aux DID peuvent être chiffrées, garantissant ainsi qu'elles ne peuvent être lues ou modifiées que par les personnes ou entités autorisées. Ce niveau de protection cryptographique assure que les informations restent confidentielles tout au long de leur cycle de vie.

- **Contrôle des Permissions**

Les DID permettent aux utilisateurs de gérer précisément les permissions accordées pour l'accès à leurs données. Ils peuvent définir, modifier ou révoquer les autorisations d'accès en fonction de leurs préférences et des besoins changeants. Ce contrôle granulaire des permissions renforce la capacité des utilisateurs à protéger leur vie privée et à limiter l'accès à leurs informations à ceux en qui ils ont confiance.

- **Révocation et Mise à Jour**

La possibilité de révoquer et de mettre à jour les informations personnelles est essentielle pour maintenir la confidentialité. Avec les DID, les utilisateurs peuvent rapidement révoquer des identifiants ou mettre à jour des informations devenues obsolètes ou compromises. Cela garantit que les données partagées sont toujours à jour et conformes aux besoins de sécurité tout en minimisant les risques d'utilisation abusive d'informations périmées.

- **Preuves Zero-Knowledge**

Les ZKP permettent aux utilisateurs de prouver la véracité d'une information sans révéler les données sous-jacentes. Par exemple, un utilisateur peut prouver qu'il est diplômé sans divulguer le diplôme en entier. Cette technologie est cruciale pour améliorer la confidentialité car elle permet de valider des informations tout en protégeant les détails sensibles des utilisateurs.

- **Transparence et Audits**

La transparence et la possibilité d'audits réguliers sont des aspects essentiels pour maintenir la confiance et la sécurité dans les systèmes utilisant des DID. Les utilisateurs peuvent voir comment et par qui leurs données sont utilisées et des audits peuvent être effectués pour s'assurer que les processus de gestion des identités respectent les normes de confidentialité. Cette transparence permet de détecter rapidement les anomalies ou les abus, renforçant ainsi la protection des données personnelles.

- **Portabilité des Identités**

Les DID assurent la portabilité des identités, permettant aux utilisateurs de transporter leurs informations d'identité d'un service à un autre sans compromettre leur confidentialité. Cette portabilité donne aux utilisateurs un contrôle total sur leurs données, leur permettant de choisir librement les plateformes sur lesquelles ils souhaitent utiliser leurs identifiants, sans être enfermés dans un écosystème particulier.

4.4 Études de cas et exemples Pratiques

L'impact des Verifiable Credentials et des Decentralized Identifiers sur la sécurité des identités en ligne peut être clairement démontré à travers des études de cas réels. Ces quelques exemples montrent comment ces technologies sont déployées dans différents contextes et les résultats qu'elles permettent d'obtenir en matière de gestion des identités numériques, de protection de la confidentialité et d'amélioration de la vérifiabilité des informations.

4.4.1 Présentation de cas d'utilisation réels

Pour mieux comprendre l'application concrète des VC et des DID, il est utile d'examiner des cas d'utilisation réels. Ces exemples montrent comment différentes organisations à travers le monde ont intégré ces technologies dans leurs systèmes pour améliorer la sécurité, la confidentialité et l'efficacité de la gestion des identités numériques. Les cas suivants illustrent la diversité des contextes et des résultats obtenus.

- **BCDiploma**

BCDiploma est une solution innovante de certification des diplômes basée sur la blockchain, développée pour faciliter la transformation digitale des établissements d'enseignement. Cette application permet l’accès en un clic à des diplômes et attestations de formation sécurisées et certifiées par les écoles et universités elles-mêmes et dans d'autres pays auprès de partenaires institutionnels et universités. BCDiploma permet aux établissements d'émettre eux-mêmes leurs propres diplômes infalsifiables. [80] [79] [81]



Figure 4.4 : logo de BCDiploma [79]

Voyons maintenant à partir de [79] quelques points du fonctionnement de BCDiploma et aux points clés qui en font une solution incontournable pour la certification des diplômes.

- ✓ **Fonctionnement de BCDiploma**
  - **Certification**

Les établissements importent les diplômes à certifier via un fichier Excel ou une API intégrée, puis les publient sur la blockchain.

- **Lien unique**

Un lien URL unique est généré pour chaque diplôme certifié, que le diplômé peut partager pour prouver l'authenticité de son diplôme.

- **Vérification**

Le lien mène à une page web où le diplôme est affiché avec toutes les preuves de sa certification sur la blockchain.

- ✓ **Points clés**
  - **Simplicité et sécurité**

L'application est facile à utiliser et garantit des données infalsifiables.

- **Personnalisation**

Les diplômes peuvent être configurés en termes de contenu et de mise en page.

- **Économique et respectueux des données**

Pas de frais récurrents, contrôle de la diffusion par le diplômé et respect du RGPD.

- ➢ **Medicalchain**

Medicalchain est une plateforme qui utilise la technologie blockchain pour améliorer la gestion des dossiers médicaux. L'objectif principal est de donner aux patients un contrôle total sur leurs données médicales, leur permettant de partager une version complète et unique de leur dossier avec les organisations de leur réseau médical. En éliminant les inefficacités des systèmes de santé traditionnels, Medicalchain favorise une approche collaborative et intelligente des soins. [82] [83]



Figure 4.5 : Logo de Medicalchain [82]

✓ **Fonctionnement de Medicalchain**

Medicalchain fonctionne en utilisant une architecture à double blockchain, combinant Hyperledger Fabric pour gérer l'accès aux dossiers médicaux et Ethereum pour les services et applications qui sous-tendent la plateforme. [82]

- **Architecture à double blockchain**
  - **Hyperledger Fabric**

Utilisé pour gérer les dossiers médicaux avec un haut degré de confidentialité, cette blockchain permissioned permet aux utilisateurs de contrôler qui peut accéder à leurs données médicales, quelles informations sont accessibles et pour combien de temps.

  - **Ethereum et Smart Contracts**

L'ERC20 token [87, 88] basé sur Ethereum alimente les applications et services sur la plateforme. Les contrats intelligents permettent de réaliser des transactions sécurisées et transparentes.

- **Gestion des identités et permissions**

Les participants tels que les praticiens, les patients et les institutions de recherche ont des droits de lecture et/ou écriture spécifiques sur les dossiers médicaux basés sur les permissions accordées par le patient.

- **Sécurité et cryptographie**

Les dossiers médicaux sont chiffrés avec une cryptographie symétrique et chaque clé de chiffrement est protégée par une clé RSA de 2048 bits. Les accès sont enregistrés comme transactions sur la blockchain, garantissant la traçabilité et la transparence.

- **Applications et services**
  - **Consultations de télémédecine**

Les patients peuvent consulter des médecins à distance tout en partageant leurs dossiers médicaux de manière sécurisée.

  - **Marché des données de santé**

Les patients peuvent choisir de monétiser leurs données en les partageant avec des institutions de recherche en échange de tokens (MedTokens).

- **Utilisation des MedTokens**

Les tokens sont utilisés pour effectuer des transactions sur la plateforme, comme payer pour des consultations de télémédecine ou échanger des données de santé.

✓ **Points-clés** [83]

- **Contrôle patient**

Les patients peuvent gérer l'accès à leurs dossiers médicaux électroniques, assurant ainsi la sécurité et l'exactitude des informations.

- **Accessibilité pour les chercheurs**

Les sociétés pharmaceutiques peuvent accéder à des données précises et actualisées directement via la plateforme.

- **Efficacité pour les assureurs**

Les informations sont transmises de manière plus rapide et rentable sans intermédiaire.

- **Opportunités pour les développeurs**

Medicalchain offre des possibilités de monétisation des données de santé et invite à des partenariats pour développer davantage de solutions innovantes.

4.4.2 Analyse des résultats et des bénéfices obtenus

L'examen de ces cas d'utilisation permet de tirer des leçons importantes sur les avantages et les défis liés à l'adoption des VC et des DID. Cette analyse met en lumière les gains en termes de sécurité, d'autonomie des utilisateurs et d'efficacité opérationnelle, tout en soulignant les bénéfices spécifiques obtenus dans chaque contexte. Elle permet également de mieux comprendre les implications de ces technologies pour un avenir meilleur de la gestion des identités numériques.

- **Amélioration de la sécurité et de la vérifiabilité**

Les technologies des VC et DID renforcent la sécurité des identités numériques en rendant les informations infalsifiables et facilement vérifiables. Par exemple, BCDiploma assure que les diplômes ne peuvent pas être contrefaits grâce à l'utilisation de la blockchain. Chaque diplôme est associé à un lien unique qui peut être vérifié en temps réel, garantissant l'authenticité du document. De même, Medicalchain protège les données médicales des patients par une cryptographie avancée tout en permettant une traçabilité complète des accès, ce qui améliore considérablement la sécurité des informations sensibles.

- **Réduction de la dépendance aux systèmes centralisés**

L'adoption des DID et des VC permet de réduire la dépendance aux systèmes centralisés en donnant le contrôle aux utilisateurs. Medicalchain, par exemple, utilise une architecture décentralisée qui permet aux patients de gérer eux-mêmes l'accès à leurs dossiers médicaux, réduisant ainsi la nécessité de faire confiance à une seule entité centralisée pour la gestion de leurs données.

- **Renforcement de l'autonomie des utilisateurs**

Les utilisateurs gagnent en autonomie grâce à ces technologies, car ils peuvent décider qui a accès à leurs informations et pour combien de temps. Medicalchain illustre parfaitement cet aspect en permettant aux patients de partager leurs dossiers médicaux de manière sélective et contrôlée. Cette autonomie renforce la confiance des utilisateurs dans le système et les encourage à être plus proactifs dans la gestion de leur identité numérique.

- **Confidentialité améliorée**

La confidentialité des données est un élément crucial dans la gestion des identités numériques. Avec BCDiploma, seules les personnes possédant le lien unique peuvent accéder aux diplômes, respectant ainsi la confidentialité des informations. Medicalchain va plus loin en utilisant une blockchain permissionnée pour s'assurer que seuls les individus autorisés

peuvent accéder aux dossiers médicaux, protégeant ainsi la vie privée des patients de manière rigoureuse.

- **Efficacité opérationnelle accrue**

Les systèmes utilisant des VC et DID apportent une efficacité opérationnelle significative en automatisant les processus de vérification et en réduisant les intermédiaires. BCDiploma simplifie le processus de certification et de vérification des diplômes, ce qui réduit les délais et les coûts associés. Medicalchain améliore l'efficacité des systèmes de santé en permettant un partage fluide et sécurisé des données médicales, facilitant ainsi les consultations et la recherche sans compromettre la sécurité des informations.

Ces résultats montrent que l'intégration des VC et DID dans divers domaines peut transformer la gestion des identités numériques en offrant des solutions plus sécurisées, autonomes et efficaces, tout en respectant la confidentialité des utilisateurs.

4.5 Conclusion

Dans ce chapitre, nous avons vu que les technologies VC et DID apportent des réponses concrètes aux menaces pesantes sur les systèmes d'identité numérique. Leur capacité à réduire les risques de fraude et à renforcer la vérification des informations représente une avancée significative. Toutefois, leurs impacts positifs ne peuvent être pleinement réalisés sans une adoption à grande échelle. Le chapitre suivant explorera donc les obstacles majeurs freinant leur mise en œuvre, notamment au niveaux réglementaire et technique.

5. Obstacles à l'adoption des VC et des DID

L'adoption des VC et des DID rencontre plusieurs obstacles qui peuvent freiner leur diffusion. Ces obstacles se répartissent en différentes catégories : techniques, réglementaires, organisationnelles et culturelles. Cette section examine ces obstacles en profondeur, en mettant en lumière les problèmes spécifiques et les solutions potentielles.

5.1 Obstacles techniques

L'adoption des Verifiable Credentials et des Decentralized Identifiers est fortement affectée par divers obstacles techniques qui peuvent entraver leur mise en œuvre et leur efficacité. Ces obstacles doivent être compris et adressés pour faciliter l'intégration à grande échelle de ces technologies. Dans cette section, nous aborderont les limitations technologiques et les problèmes d'interopérabilité, tout en proposant des solutions potentielles.

5.1.1 Limitations technologiques et solutions potentielles

Les limitations technologiques représentent des défis critiques dans le développement et l'adoption des VC et des DID. Voyons quelques-unes de ces limitations ainsi que des solutions potentielles.

- **Scalabilité**

Comme nous l'avons souligné dans la partie 3, la scalabilité est un défi majeur pour les systèmes utilisant des VC et des DID, en particulier lorsqu'il s'agit de gérer un grand nombre de transactions en temps réel. Les systèmes actuels, comme ceux basés sur la blockchain, peuvent rencontrer des limitations de performance, de latence et de capacité, ce qui peut nuire à leur adoption à grande rapidité.

- ✓ **Solutions potentielles**

Pour améliorer l'évolutivité et l'efficacité des réseaux blockchain, les solutions suivantes semblent être parmi les plus prometteuses.

- **Utilisation des solutions de couche 2**

Les solutions de couche 2 dans la blockchain sont des technologies développées pour surmonter les limites fondamentales des réseaux de blockchain de couche 1, tels que Bitcoin et Ethereum, principalement en termes d'évolutivité, de coût et de vitesse de transaction. [89]

L'objectif principal des solutions L2 (Layer 2) est d'améliorer la capacité du réseau à traiter un volume de transactions beaucoup plus important, à une vitesse plus élevée et à des coûts moindres, sans compromettre les caractéristiques fondamentales de sécurité et de décentralisation de la chaîne sous-jacente. Ils y parviennent grâce à différentes approches telles que les réseaux de canaux de paiement qui permettent des transactions quasi instantanées entre les parties ; les rollups qui regroupent plusieurs transactions en un seul lot à traiter ; et les sidechains qui sont des chaînes indépendantes connectées à la chaîne principale, chacune étant conçue pour certains cas d'utilisation ou des applications spécifiques. [89]

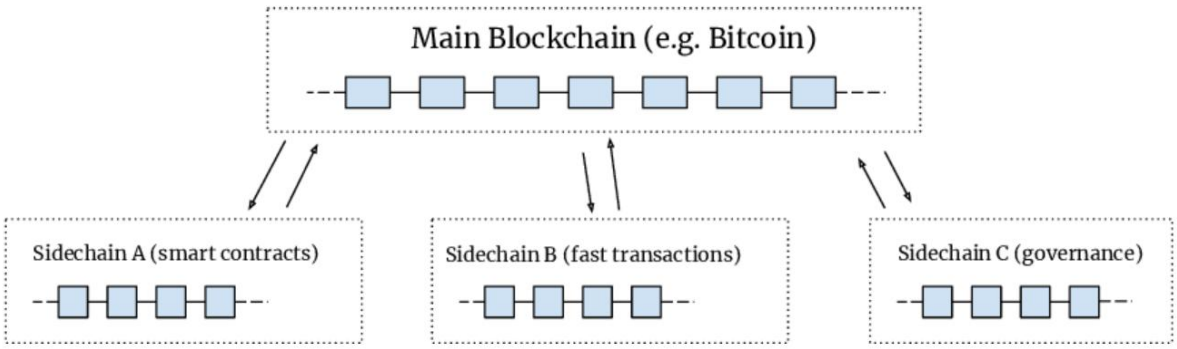


Figure 5.1 : illustration avec sidechain [89]

Les solutions de couche 2 sont comme une réponse innovante au trilemme de l'évolutivité, offrant un moyen d'augmenter la capacité du réseau sans sacrifier sa sécurité et sa décentralisation. [89][90]

- **Fragmentation (sharding)**

La fragmentation consiste à diviser la charge du réseau en sous-ensembles plus petits appelés (éclats), permettant une augmentation du nombre de transactions pouvant être traitées simultanément. Ce qui permet une utilisation plus efficace des ressources réseau et augmente la rapidité des transactions en diminuant la charge sur chaque nœud de la blockchain. [89][90][91]

- **Optimisation des protocoles**

L'optimisation des protocoles comprend l'amélioration des algorithmes de consensus et la mise en œuvre de technologies innovantes pour réduire le temps de confirmation des transactions et les coûts d'exploitation. Cela permettra de traiter davantage de transactions par seconde (TPS) tout en maintenant un haut niveau de sécurité et de décentralisation. [92][93]

Par exemple passer de mécanismes de consensus énergivores comme le PoW, à des solutions plus efficaces comme le PoS ou des systèmes hybrides.

➢ **Sécurité**

En tant que système basé sur la cryptographie, les menaces contre les clés peuvent être une très grande limitation mais aussi le système lui-même peut être vulnérable aux attaques telle que : attaques Sybil, attaques par usurpation d'Identité, compromission des clés cryptographiques, etc peuvent mettre en péril l'intégrité et la confidentialité des données.

✓ **Gestion rigoureuse des clés**

Une gestion rigoureuse des clés est cruciale dans les systèmes de gestion des identités utilisant les VC et les DID. Cette gestion dépend fortement du portefeuille.

Le portefeuille est responsable de la création du stockage et de la gestion des clés cryptographiques utilisées pour signer les VC et gérer les DID. Il permet la génération de paires de clés publiques et privées et s'assure que les clés privées restent sécurisées et accessibles uniquement par leur propriétaire.

Les portefeuilles peuvent être de plusieurs types (portefeuille logiciel, portefeuille matériel et portefeuille en cloud).

Quel que soit le type, il est utilisé pour protéger les informations sensibles qu'il contient.

Tenant compte de son importance, un chiffrement des données, une protection par mot de passe ou biométrie et une mise en œuvre de mécanismes d'authentification multi-facteurs pour accéder au portefeuille sont nécessaires afin d'éviter un accès non autorisé. En plus, il serait intéressant de penser à améliorer les portefeuilles pour qu'ils puissent intégrer des mécanismes automatisés pour gérer la rotation des clés sans perturber l'accès aux identités et aux services associés.

- ✓ **Systèmes de détection d'anomalies**

Des systèmes de détection d'anomalies peuvent être essentiels pour assurer la sécurité des systèmes d'identité décentralisée tels que ceux utilisant les références vérifiables et les identifiants distribués. Ces systèmes pourront être conçus pour identifier les comportements ou activités suspectes qui pourraient indiquer une menace ou une compromission.

Pour mettre en place ces genres de systèmes, il faudra penser à d'intégrer de mécanisme de surveillance en temps réel, d'analyse comportementale et d'alertes proactives travaillant ensemble pour créer un environnement sécurisé où les anomalies peuvent être rapidement détectées et traitées, réduisant ainsi les risques de compromission des systèmes d'identité décentralisée.

- ➢ **Complexité technique (complexité d'implémentation)**

L'implémentation de nouvelles technologies peut souvent s'accompagner d'une complexité technique importante, rendant la transition difficile pour les équipes et réduisant le temps et les coûts de déploiement.

La mise en œuvre des VC et DID est techniquement complexe, impliquant des compétences avancées en cryptographie, en gestion des clés et en intégration de systèmes. Cette complexité peut ralentir l'adoption par les entreprises et les développeurs.

Une des limites majeures liés à l'adoption des VC et DID est le manque de documentation complète et accessible. De plus, le nombre d'experts maîtrisant ces technologies est limité, ce qui complique leur implémentation et leur adoption à grande échelle.

- ✓ **Documentation et formation**

Une documentation claire et détaillée, accessible à différents niveaux de compétence (débutant, intermédiaire, expert), est essentielle. Elle permet aux développeurs et aux utilisateurs de mieux comprendre et de mettre en œuvre ces technologies de manière efficace. En plus des programmes de formation et des certifications spécifiques à ces technologies peuvent aider les professionnels à acquérir les compétences nécessaires. Cela inclut non seulement la formation technique mais aussi des sessions sur les cas d'utilisation et les avantages.

- ✓ **Interfaces utilisateur simplifiées**

S’assurer à ce que l’interface utilisateur soit facile à naviguer, même permettant aux utilisateurs moins familiarisés de comprendre comment utiliser les VC et DID sans nécessiter une connaissance technique approfondie.

Intégrer des fonctionnalités d'assistance en temps réel, comme des chatbots ou des FAQ interactives, pour aider les utilisateurs à résoudre les problèmes et à répondre à leurs questions lors de l'utilisation des systèmes.

5.1.2 Problèmes d'interopérabilité entre différentes plateformes et systèmes

Les problèmes d'interopérabilité entre différentes plateformes et systèmes se manifestent principalement par des standards incompatibles et des formats de données divers car l'interopérabilité technique dépend de la compatibilité des protocoles utilisés. Ces obstacles entravent la communication fluide entre les systèmes, rendant difficile l'échange d'informations et la collaboration efficace.

Pour résoudre ces problèmes d'interopérabilité entre différentes plateformes et systèmes, il est essentiel de mettre en place des stratégies et des standards qui permettent une communication et une intégration fluides entre les différentes technologies.

- **Incompatibilité des standards**

L'incompatibilité des standards est un problème fréquent dans les projets technologiques où des systèmes utilisent des normes différentes qui ne communiquent pas facilement entre eux. Dans le domaine des systèmes d'identité décentralisée, l'incompatibilité entre différents standards peut poser un défi majeur, notamment en raison de la diversité des protocoles et des schémas de données utilisés.

- ✓ **Multiples protocoles**

Si chaque plateforme utilise ses propres protocoles pour gérer l'authentification, l'échange de données et la gestion des identités. Les protocoles peuvent inclure des différences dans la gestion des identifiants distribués, les types de cryptographie et les méthodes de vérification des credentials. Par exemple, certaines plateformes pourraient utiliser des standards basés sur des protocoles plus récents tandis que d'autres restent sur des versions plus anciennes . [94]

Adoption de standards ouverts comme ceux proposés par des organisations telles que la Decentralized Identity Foundation (DIF) ou le W3C. L’utilisation de standards comme DIDComm, un protocole pour la communication sécurisée entre DID pourrait permettre une communication fluide entre les plateformes. [95][94]

- ✓ **Schémas de données différents**

Les plateformes peuvent employer des schémas de données variés, ce qui peut créer des incohérences dans la manière dont les informations sont stockées et partagées. Ces différences peuvent compliquer l'intégration et la collaboration entre différentes plateformes . [95]

Pour favoriser l’interopérabilité, il est nécessaire de se référer sur les schémas de données grâce à l'utilisation de formats uniformisés tels que JSON-LD. Ce format est recommandé pour les VC et permet une meilleure interopérabilité des données . [95][94]

- **Formats de données divers**

La diversité des formats de données concerne les variations dans la manière dont les systèmes structurent, échangent et stockent les informations. Cela peut entraîner des incohérences, des

pertes d'informations et rendre les processus d'intégration plus complexes, perturbant ainsi l'interopérabilité entre plateformes.

- ✓ **Incohérence des données**

La diversité des formats de données engendre souvent des incohérences lors du transfert entre systèmes. Par exemple, une plateforme pourrait utiliser un format XML tandis qu'une autre adoptera JSON, compliquant ainsi la normalisation sans autant de soucier de l'interopérabilité entre les plateformes.

La normalisation des formats de données entre plateformes via des protocoles comme les VC, qui permet un format uniforme pour échanger des informations d'identité de manière interopérable ou bien de penser à des mécanismes de sérialisations et désérialisations entre lors de communications entre les plateformes. [94]

- ✓ **Perte de données**

L'incompatibilité des formats de données peut conduire à une perte d'informations lorsque des systèmes ne sont pas en mesure d'interpréter les données provenant d'autres plateformes .

Utiliser des mécanismes de validation des données et de conversion ou de traduction des données entre les formats de différentes plateformes. Cela pourrait inclure des outils ou des API pour faciliter l'intégration entre systèmes . [94] [95]

- ✓ **Complexité du traitement**

Le traitement de données provenant de différents systèmes nécessite des solutions complexes pour uniformiser et traduire les formats, augmentant la charge pour les développeurs et les entreprises .

Simplification des formats de données et adoption de protocoles ouverts qui minimisent la conversion des données complexes, réduisant ainsi la complexité pour les développeurs . [95]

- ➢ **Problèmes de résolution des DID**

Les DID sont des identifiants décentralisés utilisés pour gérer les identités numériques. Cependant, la variété des méthodes de résolution des DID et l'absence de mécanismes inter-ledgers rendent leur intégration entre plusieurs systèmes plus complexe.

- ✓ **Méthodes de DID multiples**

Chaque plateforme pourrait adopter des méthodes de résolution de DID différentes, ce qui complique l'interopérabilité. Certains utilisent des méthodes centralisées tandis que d'autres préfèrent des approches totalement décentralisées . [95]

Une résolution possible à ce problème serait de promouvoir l'adoption de méthodes de résolution universelles pour les DID, telles que celles proposées par la DID Method Registry du W3C, qui permet de gérer différents types de DID de manière standardisée . [95]

- ✓ **Manque de mécanismes inter-ledgers**

Le manque de mécanismes de communication entre différents réseaux décentralisés est un problème majeur, notamment lorsque des DID sont enregistrés sur plusieurs blockchains incompatibles entre elles . [94]

Développement de passerelles inter-ledgers qui permettent aux DID de fonctionner à travers différentes blockchains, comme cela est exploré par des projets utilisant CKB (Common Knowledge Base) . [94] [95]

- **Ecosystèmes fermés et propriétaire solutions**

Les écosystèmes fermés se réfèrent à des environnements technologiques où les plateformes ou systèmes ne permettent pas une interopérabilité avec d'autres solutions, créant des barrières pour les utilisateurs qui souhaitent migrer vers d'autres systèmes ou échanger des données.

- ✓ **Propriétaire Solutions**

Certaines plateformes sont propriétaires, c'est-à-dire utilisant des solutions non-standardisées qui ne permettent pas une intégration facile avec d'autres systèmes. Cela crée des silos d'informations et rend difficile la gestion interopérable des identités . [94]

Encourager l'adoption de standards ouverts et interopérables pour réduire la dépendance aux solutions propriétaires. Par exemple, des solutions comme Hyperledger Indy visent à offrir des alternatives ouvertes pour la gestion des identités décentralisées .

- ✓ **Verrouillage de l'écosystème**

Ces systèmes fermés entraînent un verrouillage de l'écosystème, rendant les utilisateurs et les entreprises dépendants de solutions spécifiques sans possibilité de migration vers des standards ouverts sans perte de fonctionnalités ou de données . [95]

Portabilité des données via des protocoles standardisés comme le DIDComm, qui permet aux utilisateurs de migrer leurs identités et données d'une plateforme à une autre sans perte d'information ou d'accès . [94] [95]

5.2 Obstacles réglementaires

L'intégration des technologies d'identité décentralisée comme les informations vérifiables et identifiants décentralisés dans les systèmes existants rencontre des obstacles réglementaires importants. Cette section analyse les défis juridiques et les exigences de conformité qui doivent être pris en compte pour assurer leur adoption sécurisée et efficace.

5.2.1 Analyse des obstacles légaux et réglementaires

L'adoption des VC et DID se heurte à divers obstacles légaux et réglementaires qui freinent leur implémentation à grande échelle. Cette section explore les principaux défis juridiques auxquels ces technologies sont confrontées.

- **Incertitude juridique**

L'un des principaux obstacles à l'adoption des VC et DID est l'incertitude juridique qui entoure ces technologies. Comme les VC et les DID sont encore relativement nouveaux, il existe peu de précédents ou de jurisprudences qui pourraient aider à définir comment ils

doivent être régulés, utilisés et interprétés. Les entreprises et les institutions peuvent donc hésiter à adopter ces technologies sans une compréhension claire de leur statut légal.

Pour pallier cette incertitude, il serait nécessaire d'élaborer des cadres juridiques spécifiques aux VC et DID ou de clarifier leur interprétation au sein des cadres existants. Par exemple, l'eIDAS (Règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques) pourrait être étendu pour couvrir les VC et DID. De plus, des initiatives comme le W3C et l'Internet Engineering Task Force (IETF) visent à standardiser ces technologies, ce qui pourrait contribuer à une meilleure certitude légale. [46][96]

- **Compatibilité avec la réglementation existante**

Les VC et DID ne sont pas toujours compatibles avec les réglementations existantes. Par exemple, des législations comme le RGPD en Europe imposent des exigences strictes en matière de traitement des données personnelles, y compris le droit à l'oubli. Les DID étant par nature décentralisés, rendent difficile la mise en œuvre de certains aspects du RGPD, comme la gestion de la suppression des données personnelles sur un réseau distribué.

Dans le but d'assurer la compatibilité, il serait utile de mettre en place des mécanismes permettant d'intégrer les principes des DID dans des cadres juridiques comme le RGPD. Cela pourrait inclure la création de systèmes de gestion des droits qui permettent la révocation des informations personnelles de manière sécurisée et traçable sans affecter la nature décentralisée du DID. Des techniques de ZPK pourraient également aider à prouver des informations sans révéler de données sensibles. [46][97]

- **Manque de clarté**

Le manque de clarté sur la responsabilité des parties impliquées dans l'émission, la vérification et le stockage des VC et DID est un autre obstacle majeur. Par exemple, il ne sera pas toujours facile de savoir quel acteur est responsable en cas de fuite d'information ou d'usurpation d'identité, ce qui peut entraîner des risques juridiques.

Il serait crucial de penser à développer des modèles de responsabilité juridique clairs qui répartissent les rôles et responsabilités entre les parties prenantes (émetteurs, détenteurs, vérificateurs). Les législateurs peuvent travailler avec des acteurs comme la DIF pour élaborer des politiques qui déterminent les obligations de chaque partie.

- **Règlementations en évolution**

Les technologies numériques, y compris les VC et DID, évoluent rapidement, ce qui rend difficile l'élaboration de cadres réglementaires stables. Les gouvernements et organismes de réglementation ont souvent du mal à suivre le rythme de l'innovation technologique ce qui conduit à des cadres juridiques obsolètes ou inadaptés.

Pour faire face à ces défis, les régulateurs devraient adopter des cadres juridiques flexibles qui peuvent s'adapter aux nouvelles évolutions technologiques. Il peut s'agir de lois basées sur des principes plutôt que sur des règles strictes ce qui permettrait aux législateurs de réagir plus rapidement aux changements. De plus, des partenariats public-privé avec des organisations comme Hyperledger et des initiatives de standardisation internationales peuvent aider à aligner les réglementations avec les besoins technologiques.

5.2.2 Exigences en matière de conformité et solutions proposées

Pour garantir l'adoption et l'implémentation des VC et DID à grande échelle, il est crucial de respecter certaines exigences réglementaires. Cette section identifie trois principaux domaines de conformité : la protection des données personnelles, l'auditabilité et la traçabilité, ainsi que la collaboration avec les autorités.

- **Protection des données personnelles**

Les réglementations comme le RGPD en Europe imposent des exigences strictes concernant le traitement et la protection des données personnelles. Les détenteurs de VC et DID doivent être capables de contrôler leurs données y compris le droit de les supprimer, de les corriger ou d'en restreindre l'accès. Les systèmes doivent également respecter les principes de minimisation des données, garantissant que seules les informations essentielles sont partagées. [97]

Pour répondre à ces exigences, une solution clé est l'utilisation de la divulgation sélective. Cette technique permet aux détenteurs de VC de partager uniquement les informations strictement nécessaires sans révéler d'autres données sensibles. Les ZKP, qui permettent de prouver certaines informations sans les divulguer complètement, jouent également un rôle central dans la protection de la vie privée. Les portefeuilles numériques doivent également être conçus pour offrir des options de contrôle avancées aux utilisateurs concernant leurs informations. [46]

- **Auditabilité et traçabilité**

Pour des raisons de sécurité et de conformité, il est nécessaire de disposer de mécanismes permettant de suivre et d'auditer les échanges d'informations. Les systèmes basés sur les VC et DID doivent offrir une traçabilité claire et permettre aux parties concernées (émetteurs, vérificateurs et détenteurs) de vérifier les transactions et les échanges de données de manière transparente et fiable. Cela inclut la capacité à prouver l'authenticité de l'émetteur et l'intégrité des informations fournies.

La blockchain ou d'autres registres distribués jouent un rôle clé dans la fourniture d'une traçabilité immuable et transparente. En utilisant des protocoles basés sur la blockchain, les systèmes peuvent garantir que chaque transaction est horodatée, vérifiable et non modifiable. Des solutions comme Hyperledger Indy sont spécialement conçues pour gérer des systèmes de confiance basés sur la blockchain tout en respectant les exigences de confidentialité grâce à des techniques cryptographiques avancées. [55]

- **Collaboration avec les autorités**

Les concepteurs des systèmes d'identité décentralisés doivent collaborer avec les autorités et les régulateurs pour garantir la conformité avec les législations en vigueur telles que les lois sur l'identité numérique ou la protection des consommateurs. Cette collaboration inclut également la mise en place de mécanismes pour répondre aux demandes légales comme les injonctions ou les audits de conformité. Il est important d'assurer que les identités numériques soient reconnues et acceptées par les autorités publiques.

Pour favoriser une collaboration efficace, il est crucial de s'engager dans des initiatives telles que l'European Blockchain Partnership (EBP) ou les programmes de sandbox régulatoire. Ces

initiatives permettent aux entreprises et aux gouvernements de travailler ensemble à la définition des standards et des protocoles, garantissant ainsi que les solutions d'identité numérique soient conformes et acceptables sur le plan réglementaire. De plus, en s'appuyant sur des cadres tels que l'eIDAS, il est possible de créer une interopérabilité entre les systèmes d'identité décentralisés et les autorités gouvernementales. [96]

5.3 Obstacles organisationnels et culturels

Cette section explore les divers obstacles organisationnels et culturels qui freinent l'adoption des Verifiable Credentials et des Decentralized Identifiers avec un focus sur les résistances internes et les dynamiques culturelles.

5.3.1 Barrières internes aux organisations

Les organisations font face à des défis internes majeurs tels que la résistance au changement et le coût de mise en œuvre qui peuvent considérablement ralentir l'intégration de nouvelles technologies comme les VC et DID.

Les organisations peuvent rencontrer des obstacles internes lorsqu'elles tentent d'adopter des technologies innovantes comme celles des VC et les DID. Parmi les principaux défis, on trouve la résistance au changement et les coûts élevés de mise en œuvre. Ces barrières peuvent retarder considérablement l'intégration de ces nouvelles technologies malgré leurs avantages potentiels.

- **Résistance au changement**

La résistance au changement est un défi majeur pour toute organisation cherchant à adopter de nouvelles technologies. Cela est souvent dû à des craintes liées à l'incertitude ou à des processus en place qui fonctionnent correctement, bien que moins efficacement. Le personnel peut craindre que ces nouvelles technologies nécessitent des compétences supplémentaires, modifient leur rôle au sein de l'organisation ou encore introduisent des risques. La résistance peut également provenir de la direction en raison d'une vision à court terme ou d'un manque de compréhension des avantages des VC et DID.

Une stratégie efficace pour surmonter cette résistance consiste à investir dans la formation et l'éducation du personnel. Cela peut inclure des ateliers, des démonstrations de cas d'utilisation réels et des programmes de sensibilisation sur les avantages des VC et DID tels que l'amélioration de la sécurité et de la gestion des identités. De plus, l'implication des parties prenantes dès le début du processus d'implémentation est cruciale pour assurer leur adhésion. L'approche de la gestion du changement peut être utilisée pour structurer cette transition, en mettant l'accent sur la communication, la formation et la gestion des impacts organisationnels.

- **Coût de mise en œuvre**

Les coûts associés à la mise en œuvre des VC et DID peuvent être perçus comme prohibitifs, en particulier pour les petites et moyennes entreprises. Ces coûts incluent l'investissement dans de nouvelles infrastructures technologiques, la formation des employés, et parfois des frais de maintenance élevés pour les solutions décentralisées. De plus, le passage à un système d'identité décentralisée implique souvent des révisions des processus internes ce qui peut nécessiter des ressources supplémentaires.

Pour gérer les coûts de mise en œuvre, il est recommandé de procéder par phases. Les organisations peuvent commencer par des projets pilotes à petite échelle pour évaluer l'efficacité des VC et DID avant de les déployer à grande échelle. De plus, l'utilisation de solutions open source comme Hyperledger Indy permet de réduire considérablement les coûts initiaux en évitant les licences coûteuses. Les partenariats public-privé peuvent également être explorés pour obtenir un soutien financier ou technique. Enfin, il est important de démontrer un retour sur investissement (ROI) clair en montrant comment l'amélioration de la sécurité des identités et la réduction des fraudes peuvent compenser les coûts initiaux. [98] [100]

5.3.2 Facteurs culturels influençant l'adoption

Les différences culturelles et les perceptions sociales des technologies émergentes comme les références vérifiables et identifiants distribués influencent considérablement leur adoption. Ces facteurs incluent la perception de la vie privée, la méfiance vis-à-vis des nouvelles technologies ainsi que les spécificités sectorielles.

- **Différences culturelles dans la perception de la vie privée**

La manière dont la vie privée est perçue varie largement à travers le monde. En Europe par exemple, les citoyens sont généralement très soucieux de la protection des données personnelles, ce qui se reflète dans des réglementations strictes comme le RGPD. En Afrique, les attitudes envers la vie privée peuvent varier considérablement. Dans certaines régions, la protection des données peut être une préoccupation émergente, tandis que d'autres peuvent accorder plus d'intérêt à la sécurité et à l'accès non-autorisé aux données personnelles des gens.

Pour surmonter ces variations, les systèmes de VC et DID doivent offrir des options personnalisables en matière de divulgation des données en tenant compte des normes culturelles locales. Par exemple, en Afrique de l'Ouest plus particulièrement au Sénégal, il pourrait être utile d'introduire des initiatives de sensibilisation pour mieux expliquer les avantages de la protection des données et la gestion des identités décentralisées. L'utilisation de divulgation sélective et de zero-knowledge proofs permet également d'adapter les systèmes aux attentes culturelles spécifiques en matière de confidentialité.

A partir de [101], on peut avoir une perception culturelle de la vie privée dans tous les pays du monde. Il montre que les pays non pas la même considération envers la vie privée et aussi la sécurité des systèmes informatiques.

- **Méfiance des technologies émergentes**

La méfiance vis-à-vis des nouvelles technologies est un phénomène mondial. En Afrique, cette méfiance peut être accentuée par un manque de sensibilisation et d'expérience avec les technologies décentralisées. Au Sénégal, des projets pilotes ou des démonstrations concrètes peuvent être nécessaires pour établir la confiance dans les VC et DID en prouvant leur sécurité et leurs avantages réels.

Pour construire la confiance, il est crucial de mettre en place des programmes éducatifs et des démonstrations de cas d'utilisation adaptées aux contextes locaux. Par exemple, des ateliers éducatifs et des projets pilotes au Sénégal peuvent aider à surmonter la méfiance en montrant des bénéfices tangibles. L'open source est également un atout précieux pour permettre aux utilisateurs et développeurs de vérifier et comprendre les systèmes en détail.

- **Nature du secteur**

L'adoption des VC et DID peut également varier en fonction du secteur. Les secteurs comme la finance et la santé peuvent être plus ouverts à ces technologies en raison des besoins croissants en matière de sécurité et de gestion des identités. Si on prend l'exemple notre pays, les projets dans la fintech ou les systèmes de santé numériques peuvent bénéficier grandement de l'intégration des VC et DID.

Pour attirer ces technologies aux différents secteurs, il est important de démontrer comment les elles peuvent répondre aux défis spécifiques. Dans le secteur financier au Sénégal, par exemple, des cas d'utilisation montrant comment les VCs peuvent améliorer la sécurité des transactions financières et la conformité réglementaire peuvent encourager l'adoption. Dans le secteur de la santé, des projets pilotes démontrant l'amélioration de la gestion des dossiers médicaux peuvent être particulièrement convaincants.

5.4 Conclusion

Ce chapitre montre que ces technologies sont très riches en avantages. Malgré leurs nombreux avantages, les VC et les DID font face à des barrières importantes, telles que le manque d'interopérabilité, la complexité technique et une faible sensibilisation des acteurs. Ces défis ralentissent leur diffusion et nécessitent des stratégies adaptées pour encourager leur adoption. Afin de surmonter ces freins, il est primordial d'élaborer des recommandations stratégiques, que nous examinerons dans un autre chapitre.

6. Recommandations stratégiques pour l'adoption des VC et des DID

Les technologies des références vérifiables et des identifiants distribués sont en train de transformer la manière dont les informations d'identités sont gérées et partagés. Cependant, leur mise en œuvre nécessite une approche stratégique pour surmonté les obstacles technique, réglementaires et culturelle. Pour maximiser les avantages de ces innovations, il est crucial de développer des stratégies de mise en application solide et de suivre des pratiques recommandés. Ce chapitre propose un cadre stratégique pour l'adoption des VC et des DID, en mettant l'accent sur les étapes clés de leur mise en œuvre, les pratiques de développement recommandé, les considérations politiques, et des études de cas éclairant comme celle de Microsoft entra.

6.1 Stratégies de mise en œuvre

Une mise en œuvre réussie des VC et DID nécessite une planification minutieuse car ces technologies sont encore en émergence et en pleine évolution. Une stratégie claire comprenant des étapes bien définit est essentielle pour garantir leur adoption réussie dans un environnement sécurisé et conforme aux régulations en vigueur.

6.1.1 Étapes clés pour l'implémentation des VC et DID

La mise en place des technologies VC et DID est un travail très complexe en raison de leur nature technique et des nouveaux dynamiques qu'elles introduisent. Dans cette section, nous aborderons les étapes essentielles à suivre pour la mise en œuvre des VC et des DID dans des systèmes existant. Cela inclut l'analyse des besoins spécifiques des utilisateurs, l'explorations de diverses architectures techniques possibles et la mise en place de procédures de gouvernance adapter.

- **Évaluation des besoins**

L'implémentation de Verifiable Credentials et de Decentralized Identifiers nécessites d'abord une analyse des besoins spécifiques des utilisateurs qui varie selon les secteurs. Par exemple, dans le domaine de l'éducation, il pourrait être nécessaire de vérifier l'authenticité des diplômes, tandis que dans le domaine de la santé, l'accent pourrait être mis sur la confidentialité et la vérification des professionnels de santé. Comme dans le projet BCDiploma [78], un besoins clair a été identifier pour permettre aux institutions académique de délivrer des diplômes infalsifiables et vérifiables de manière décentralisée.

- **Sélection des technologies, standards et protocoles**

Une fois les besoins clairement définis, il faudra choisir les technologies, standards et protocoles appropriés pour l'implémentations des technologies à VC-DID. Ces technologies reposent sur des normes qui garantissent leur interopérabilité entre différents systèmes et leur conformité aux meilleures pratiques en matière de sécurité et de gestion des identités. Ces choix vont définir l'interopérabilité, la sécurité et la conformité aux normes des systèmes d'identités décentralisés.

Pour implémenter ces technologies à VC-DID, il est essentiel d'opter pour des technologies, standards, protocoles et frameworks appropriés pour garantir l'interopérabilité, la sécurité, et la conformité avec les normes existantes.

Tableau 6.1 : présentation de quelques outils

Catégorie	Outils
Technologies	Blockchain (Ethereum [109], Hyperledger Indy [98], Bitcoin [119, 120]), Hyperledger Ursa [107], IPFS [110], Universal Resolver [112], Cloud HSM [121, 122]
Standards	W3C Verifiable Credentials Standard [46, 54], W3C DID Core Standard [59], JSON-LD [118],
Protocoles	DIDComm [115], OpenID Connect avec VCs [117], OAuth 2.0 [116], Revocation Registries [123]
Frameworks	Hyperledger Aries [114], Sovrin [108], Trinsic [111], uPort [113]

Sur ce tableau, nous avons répertorié un ensemble d'éléments essentiel pour implémenter un systèmes d'identité décentralisé. Les technologies assurent le stockage sécurisé et la gestion des identités. Les standards garantissent que les informations sont interopérables entre les systèmes. Les protocoles facilitent la communication sécurisée et la révocation des credentials. Enfin, les frameworks offrent des environnements prêts à l'emploi pour la création, gestion et vérification des identités décentralisées.

- **Conception de l'architecture ou de la solution**

La conception d'une architecture pour les systèmes basés sur les VC et DID nécessites la prise en compte de plusieurs aspects techniques et organisationnels. Les choix des infrastructures, des méthodes de DID, de la gestion des clés et de la sécurité cryptographique sont des éléments centraux pour garantir un système adapté aux besoins identifiés en prenant en compte des facteurs tels que la sécurité, l'interopérabilité, la gouvernance et la scalabilité.

L'architecture déterminera la manière dont les utilisateurs, les émetteurs et les vérificateurs interagirons au sein du système et doit comprendre un cadre de gouvernance définissant les rôles et les responsabilités des parties prenantes comme par exemple un établissement universitaire (émetteur) qui délivre un diplôme numérique sous forme de VC à un étudiant (titulaire). Un employeur potentiel (vérificateur) vérifiera la validité du diplôme avant d'embaucher l'étudiant.

- **Quelques étapes clés du développement de la solution**

Le développement d'une solution basée sur les VC et les DID repose sur plusieurs étapes, qui consistent à implémenter les fonctionnalités techniques et les composants architecturaux définis précédemment. En utilisant des outils adaptés comme Hyperledger Indy, DIDComm et des protocoles cryptographiques avancés, il est possible de créer une solution robuste, décentralisée et interopérable tout en garantissant la sécurité et la protection des données des utilisateurs. Ce processus se fait en collaboration avec des développeurs, des experts en sécurité et d'autres parties prenantes pour garantir la conformité aux normes et la robustesse du système.

- ✓ **Création des DID**

Les DID sont au cœur des systèmes SSI. Ils permettent à une entité de créer une identité qui n'est pas contrôlée par une autorité centrale. Ils sont généralement basés sur des chaînes de blocs ou d'autres technologies décentralisées.

- **Génération de clés**

La première étape de la création des DID consiste à générer des paires de clés cryptographiques asymétriques (privée et publique) pour chaque entité. La clé privée est gardée secrète tandis que la clé publique est utilisée pour identifier l'entité. Cette clé publique est intégrée dans un DID Document, qui contient des informations comme la méthode de résolution du DID, les clés publiques associées et d'autres métadonnées. Par exemple, Hyperledger Indy permet la génération ces paires de clés et leur enregistrement dans un registre décentralisé. [59] [98]

- **Association de document DID**

Le DID Document est associé à chaque DID et contient les informations de la clé publique, les endpoints de communication, et d'autres données techniques. Le DID Document est ce qui permet à d'autres entités de vérifier les interactions avec un DID. [59]

- **Stockage**

Une fois créés, les DID sont enregistrés dans des DLT, comme Hyperledger Indy ou Sovrin. Comme nous l'avons mentionné précédemment, ces registres garantissent l'immuabilité et l'accessibilité des identifiants mais ne stockent pas les informations personnelles, uniquement les DID et leurs documents associés pour préserver la confidentialité.

- ✓ **Résolution des DID**

La résolution des DID est le processus qui permet de convertir un DID en un DID Document, contenant les informations nécessaires pour interagir avec l'entité propriétaire du DID. Ce processus est essentiel pour établir des connexions sécurisées entre des parties. Il est géré par un outil ou service appelé DID Resolver qui prend un DID en entrée et retourne le DID Document correspondant. Ce processus est souvent automatisé et peut se faire à travers des frameworks comme Hyperledger Aries ou le Universal Resolver. [59] [112]

- ✓ **Conception du portefeuille**

Le portefeuille (ou wallet) est un outil essentiel pour gérer les clés cryptographiques et les VC. Il sert d'interface utilisateur pour l'interaction avec les systèmes d'identité décentralisée. Grâce à lui, l'utilisateur peut créer et gérer ses données, signer des transactions cryptographiques pour prouver la possession d'un DID et stocker les informations de manière sécurisée. Les portefeuilles peuvent être des applications mobiles, des extensions de navigateur ou des logiciels autonomes. Les frameworks proposent souvent des SDKs pour le développement de portefeuilles qui respectent les standards de sécurité et de décentralisation. [115] [111]

- ✓ **Intégration des protocoles de Sécurité**

L'intégration des protocoles de sécurité est cruciale pour garantir la confidentialité, l'intégrité et l'authenticité des échanges dans un système utilisant des VC et DID. Il faudra penser à des protocoles de sécurité intégrés dans ces solutions comme DIDComm, les ZKP, la rotation des clés et d'autres mécanismes cryptographiques. Chaque protocole joue un rôle clé pour assurer la sécurité de bout en bout du système d'identité décentralisée. Pour l'intégration, il faudra ajouter les bibliothèques jouant ce rôle ou de configurer des règles permettant de les respecter.

- ➢ **Test et validation**

Les tests sont cruciaux pour s'assurer que le système fonctionne correctement et est sécurisé. Des tests de pénétration, d'interopérabilité entre différentes solutions VC-DID et des tests de performance doivent être réalisés.

Par exemple IBM a mené des tests rigoureux lors de l'implémentation de sa solution basée sur Hyperledger Indy (IBM Blockchain Identity Solutions), en vérifiant l'interopérabilité avec les autres solutions basées sur la blockchain.

La validation de la compatibilité avec les standards (W3C, DIF) et les procédures de gouvernance est également importante pour garantir que le système est prêt pour le déploiement. [105] [106]

- ➢ **Déploiement, Formation et Sensibilisation**

Le déploiement doit être planifié de manière à assurer une transition en toute conformité. Pour se faire, il faudra penser dès le début à des formations pour les utilisateurs par exemple, les administrateurs de systèmes, les développeurs d'applications ainsi que des sensibilisations pour les utilisateurs finaux à la gestion de leur identité et à l'utilisation des wallets numériques pour les VC et DID. Il est crucial de fournir des interfaces utilisateur intuitives pour garantir une adoption rapide.

Pour référence, la société Evernym [104], organise des programmes de formation et de sensibilisation pour les institutions adoptant son application mobile Sovrin, un portefeuille numérique permettant de gérer des identités décentralisées. [103]

- **Surveillance et Amélioration Continue**

Une fois le système en place, il doit être surveillé régulièrement pour identifier les failles de sécurité, les problèmes d'interopérabilité ou d'autres obstacles techniques. Des mécanismes de rotation des clés et de révocation des credentials doivent être mis en œuvre pour renforcer la sécurité et la robustesse à long terme.

La DIF [102] promeut une amélioration continue des solutions VC-DID à travers l'élaboration de nouveaux standards et la mise à jour des protocoles en fonction des retours d'expérience et des avancées technologiques.

6.1.2 Meilleures pratiques pour une adoption réussie

Adopter les VC et les DID ne se limite pas uniquement à l'intégration technique ; cela nécessite également des pratiques facilitant l'adoption tout en maximisant leur impact. Ici, nous détaillerons des recommandations telles que l'implication des parties prenantes, la conformité aux réglementations et la promotion de l'interopérabilité qui sont cruciales pour assurer une adoption fluide et sécurisée.

- **Implication des parties prenantes (collaboration intersectorielle)**

L'implication des parties prenantes est essentielle pour garantir que tous les acteurs concernés, y compris les gouvernements, les entreprises, les utilisateurs finaux et les organisations de la société civile, soient engagés dans le processus d'adoption. Une collaboration intersectorielle permet de créer un consensus autour des normes et des meilleures pratiques ainsi que de partager des connaissances. [124]

Les parties prenantes peuvent inclure :

- ✓ **Les gouvernements**

Pour garantir la conformité aux réglementations nationales et internationales.

- ✓ **Les entreprises privées**

Pour assurer une adoption plus large, en particulier dans les secteurs où la sécurité et la vérification d'identité sont cruciales (banques, services financiers, éducation, santé).

- ✓ **Les utilisateurs finaux**

Pour s'assurer que les solutions sont adaptées aux besoins réels des individus.

Une telle collaboration peut être facilitée par des forums internationaux comme la DIF, qui rassemble des acteurs du monde entier pour favoriser l'adoption de standards communs. [102] [59]

- **Assurer la conformité réglementaire**

Pour favoriser l'adoption des VC et DID, il est primordial que les systèmes basés sur les VC-DID soient conformes aux lois et régulations en vigueur, en particulier celles relatives à la protection des données et à la confidentialité telles que le Règlement Général sur la Protection des Données en Europe ou la California Consumer Privacy Act (CCPA) aux États-Unis.

- ✓ **La protection des données**

Les informations personnelles doivent être protégées conformément aux législations sur la vie privée.

- ✓ **La gestion des consentements**

Les utilisateurs doivent avoir un contrôle total sur leurs données en fonction en évitant de franchir les limites fixees par les utilisateurs.

- ✓ **La gestion des risques**

Les entités doivent mettre en place des mécanismes de gestion des risques en matière de sécurité.

La conformité garantit non seulement la légalité de l'utilisation de ces technologies mais aussi renforce la confiance des utilisateurs.

- ➢ **Focus sur l'expérience utilisateur**

Favoriser une adoption rapide des technologies VC-DID revient à miser sur l'expérience utilisateur pour s'assurer qu'elle soit fluide et intuitive. Si les utilisateurs finaux trouvent le système difficile à utiliser, l'adoption sera entravée. Les meilleures pratiques dans ce domaine incluent :

- ✓ **Simplifier l'interface**

L'interface des applications et des portefeuilles de VC doit être simple, intuitive et compréhensible à une large population.

- ✓ **Garantir la transparence**

Les utilisateurs doivent savoir comment leurs informations sont utilisées, par qui et à quelles fins.

- ✓ **Fournir un support utilisateur efficace**

Offrir des services d'assistance clairs et accessibles pour aider les utilisateurs à naviguer dans ces systèmes.

Des exemples d'implémentations réussies incluent les portefeuilles de VC développés par des acteurs comme Evernym et IBM. [126] [127]

- ➢ **Promouvoir l'interopérabilité**

L'interopérabilité est un élément clé pour que les VC et DID puissent être utilisés dans différents systèmes et secteurs. Les meilleures pratiques pour favoriser cette interopérabilité sont :

- ✓ **Adhésion aux standards internationaux**

Les solutions doivent être basées sur des standards reconnus comme ceux promus par le W3C, tels que les spécifications DID et VC.

- ✓ **Collaboration avec des consortiums industriels**

Le travailler avec des groupes comme le Trust over IP Foundation aide à garantir que les solutions sont compatibles avec d'autres systèmes et plateformes.

- ✓ **Intégration des API standardisées**

Cela facilite l'interaction entre les différentes plateformes utilisant les VC et DID.

L'interopérabilité améliore la portabilité des identités et permet aux utilisateurs de réutiliser leurs informations d'identification dans différents écosystèmes. [46] [54]

- ➢ **Garantir la Sécurité**

La sécurité est au cœur de l'adoption des VC et DID, en particulier car ces technologies gèrent des informations sensibles. Les meilleures pratiques de sécurité incluent :

- ✓ **Utilisation de la cryptographie avancée**

L'emploi de signatures numériques, la rotation des clés et les ZKP garantissent la confidentialité et l'intégrité des données.

- ✓ **Sécurisation des portefeuilles numériques**

Les portefeuilles numériques doivent inclure des mécanismes de sécurité rigoureux tels que l'authentification multifactorielle et le chiffrement des données.

- ✓ **Mécanismes de récupération sécurisée**

Les utilisateurs doivent pouvoir récupérer leurs identifiants ou informations de manière sécurisée en cas de perte.

- ➢ **Suivi et évaluation**

Enfin, il est essentiel de mettre en place des mécanismes de suivi et d'évaluation pour s'assurer que les systèmes à VC-DID répondent aux objectifs fixés et continuent à respecter les réglementations et standards en vigueur. [102] [59]

- ✓ **Auditabilité**

La capacité à vérifier de manière transparente que les processus d'émission, de gestion et de révocation des VC sont sécurisés.

- ✓ **Feedback continu**

Recueillir des retours d'expérience des utilisateurs et des parties prenantes pour améliorer les processus.

- ✓ **Mise à jour des systèmes**

Mettre en œuvre des mises à jour régulières pour s'adapter aux évolutions technologiques et réglementaires.

Le suivi et l'évaluation sont cruciaux pour garantir la pérennité et l'évolutivité des systèmes d'identité décentralisée tout en assurant leur efficacité opérationnelle et leur sécurité.

6.2 Pratiques recommandées pour les développeurs

Les développeurs jouent un rôle clef dans la conception et l'intégration des systéms à VC-DID. Des choix judicieux en matiére d'outils, de framework et de méthodologie peuvent avoir un impact signifficatif sur la robustesse, l'interopérabilité et la securité des solutions. Cette partie fournis des directives spécifique pour aider les développeurs à créér des solutions robust et sécurisées.

6.2.1 Directives pour le développement de solutions VC et DID

Le développement de solutions utilisant des VC et DID nécessite le respect de standards spécifiques et des pratiques strictes. Ci-dessous, vous trouverez des directrices détaillées que les développeurs peuvent suivre pour garantir que leurs solutions répondent aux normes tout en protégeant les données d'identité.

- ➢ **Adopter des méthodes agiles et conformes aux standards**

Pour assurer une gestion efficace des projets et garantir la qualité des livrables, il est essentiel d'adopter des méthodologies agiles tout en respectant les normes établies. Cela permet non seulement d'améliorer la flexibilité et la réactivité mais également d'assurer la cohérence et la conformité.

- ✓ **Méthodologie Agile**

Le développement de solutions basées sur VC et DID devrait suivre les approches agiles. Cela permets des itérations rapides, un retour d'information constants et une adaptation aux exigences changeantes des utilisateurs. L'approche agile est particulièrement adaptée à des systèmes évolutifs comme les VC et DID, car elle encourage des livraisons fréquentes et une meilleure gestion des priorités.

L'Agile Manifesto [128] et ses principes favorisent l'interaction entre les parties prenantes et la réactivité au changement, deux aspects essentiels dans des projets intégrant des VC et DID. De plus, les frameworks spécifiques à l'identité décentralisée tels que le W3C Verifiable Credentials Data Model [46] [54] soulignent l'importance de l'adaptation aux standards.

- ✓ **Conformité aux standards**

Le respect des normes ouvertes telles que les standards définis par le W3C pour les VC et les DID est tres important pour garantir que les solutions seront compatibles avec d'autres systèmes. Il est important de rester à jour concernant les évolutions des standards émis par des organismes tels que le W3C, la DIF, et l'IETF. [59] [46] [54]

- ➢ **Prioriser la sécurité**

La sécurité doit être une priorité absolue dans tout projet numérique, notamment en matière de protection des données et de gestion des clés. Mettre en place des mécanismes robustes garantit non seulement la confidentialité et l'intégrité des informations mais aussi la protection des accès et des communications sensibles.

- ✓ **Sécurité des données**

Les VC et DID sont construits autour de la protection des données d'identité donc la sécurité doit être au cœur du développement. Cela inclut l'utilisation de signatures cryptographiques fortes pour garantir l'authenticité et l'intégrité des informations ainsi que des mécanismes robustes pour protéger la vie privée des utilisateurs comme les ZKP. Les pratiques de sécurité tels que la gestion rigoureuse des clés, la rotation des clés et le chiffrement de bout en bout doivent être intégrées dès le début du développement.

NIST SP 800-63B [129] fournit des directives précieuses sur la sécurité des identités numériques tandis que la DIF [102] offre des ressources sur la sécurité et la gestion des clés dans les systèmes d'identité décentralisée.

- ✓ **Gestion des clés**

La gestion des clés est un pilier de la sécurité dans les solutions basées sur les VC et DID. L'authenticité et l'intégrité des données sont garantis par l'utilisation de signatures cryptographiques qui doivent être gérées de manière sécurisée. La rotation des clés et leur révocation doivent également être prises en compte pour éviter les compromis à long terme.

La spécification JSON Web Key (JWK) par l'IETF [130] décrit les mécanismes de gestion des clés dans les environnements distribués.

- ➢ **Faciliter l'interopérabilité**
- ✓ **Interopérabilité des systèmes**

Il est essentiel que les solutions développées soient interopérable avec d'autres systèmes utilisant des standards similaires pour garantir une adoption à grande échelle. En utilisant des standards ouverts comme ceux définis par le W3C et en garantissant que les systèmes puissent s'intégrer avec d'autres réseaux d'identité décentralisé, les solutions permettront une plus grande flexibilité et un meilleur échange d'information. L'initiative Universal Resolver de la DIF [112] est un bon exemple d'outil facilitant l'interopérabilité des DID en prenant en charge plusieurs méthodes DID.

- ✓ **Protocoles de communication**

L'interopérabilité repose aussi sur des protocoles standardisés de communication entre les différentes parties prenante (émetteurs, détenteurs et vérificateurs). Des protocoles tels que DIDComm sont utilisés pour la transmission sécurisée des informations d'identité entre différentes plateformes et services.

DIDComm Protocol [131] définit un cadre pour une communication sécurisée entre systèmes d'identité décentralisée.

- **Tests exhaustifs**

Avant le déploiement de toute solution que ce soit VC-DID ou autre, des tests exhaustif doivent être effectué pour garantir que le système fonctionne comme prévu et qu'il est sécurisé. Cela inclut des tests unitaires, des tests d'intégration, ainsi que des tests de pénétration pour vérifier la résistance aux attaques. En particulier, il est crucial de tester la robustesse des mécanismes cryptographiques et des systèmes de gestion des clés.

Tester l'interopérabilité avec d'autres systèmes est également essentiel. Les développeurs doivent s'assurer que leurs solutions peuvent échanger des données avec d'autres systèmes d'identité décentralisé ou réseaux de confiance. Des tests de compatibilité avec des solutions existantes doivent être effectués pour valider cette interopérabilité. [132] [133]

- **Documentation Complète**

La documentation est un élément souvent négligé mais primordial pour garantir que les développeurs et les utilisateurs finaux puissent utiliser et maintenir les systèmes d'identité décentralisée. La documentation doit inclure des guides clairs sur l'utilisation des APIs, les méthodes d'implémentation des VC et DID ainsi que les pratiques de sécurité à suivre.

Les solutions utilisant des VC et DID doivent également fournir une documentation détaillée sur les mécanismes de sécurité en place y compris la gestion des clés et les mesures prises pour protéger la vie privée des utilisateurs. Cela permet non seulement de renforcer la confiance des utilisateurs mais aussi de faciliter la vérification par des tiers.

6.2.2 Outils et Framework recommandés

Il existe de nombreux outils et frameworks qui peuvent faciliter le développement de solutions basées sur les VC et DID. Ici, nous allons identifier quelques outils et frameworks recommandés qui peuvent faciliter le développement ces solutions tout en assurant une intégration fluide et une conformité aux standards techniques.

- **Frameworks de développement (hyperledger Indy)**

Ces frameworks facilitent le développement de solutions basées sur les VC et DID en offrant des outils pour créer, gérer et vérifier les informations d'identité décentralisé.

- ✓ **Aries Framework** [135]

Aries est un ensemble de protocole et d'outils open-source qui facilite la création d'infrastructures pour des interactions de confiance basées sur les DID et VC. Développé avec

l'appui d'Hyperledger, Aries permet de créer des agents décentralisés capable de gérer les identifiants, d'effectuer des connexions sécurisées et de traiter des preuves cryptographiques.

- **Avantages**

  - Compatible avec les DID, VC et les zero-knowledge proofs.
  - Basé sur des standards de l'IETF et du W3C.
  - Dispose de SDKs dans plusieurs langages (Python, JavaScript, .NET).

Figure 6.1 : Logo de Hyperledger Aries [136]

✓ **Sovrin** [134]

Sovrin est une plateforme d'identité décentralisée construite sur la blockchain Hyperledger Indy. Elle propose un cadre permettant d'utiliser les DID et VC pour des interactions autonomes, tout en assurant l'autosouveraineté des utilisateurs.

- **Avantages**

  - Gouvernance claire et infrastructure décentralisée.
  - Supporte les DID et les VC dans des systèmes sécurisés et privés.

Figure 6.2 : Logo de Sovrin

✓ **Veramo** [137]

Veramo est un framework JavaScript qui aide à créer des applications VC et DID. Il est conçu pour être modulaire et léger, facilitant l'intégration dans des systèmes existants ou nouveaux.

✓ **Avantages**

  - Prise en charge des DID, VC et des preuves cryptographiques.
  - Extensible et compatible avec plusieurs normes DID, telles que did:web, did:key, did:ethr.
  - Interface simple à utiliser avec des plugins adaptables.

Figure 6.3 : Logo de Veramo [138]

- **Outils de Gestion des Clés(Did-JWT)**

Dans les systèmes basés sur les DID et VC, la gestion des clés est une tâche à ne pas négliger pour assurer la sécurité et l'intégrité des identités décentralisées. Nous allons voir quelques outils de gestion des clés recommandés :

- ✓ **DIDKit** [139]

DIDKit est un SDK pour gérer les identifiants décentralisés et les signatures cryptographiques associées aux VC. Il propose des fonctions robustes pour la création, l'émission, la vérification et la gestion des identifiants distribués.

- **Avantages**

  - Prise en charge de plusieurs méthodes de DID (ex : did:key, did:web).
  - Gestion des clés et signatures cryptographiques.
  - Conformité aux standards W3C VC et DID.

- ✓ **Vault by HashiCorp** [140]

Vault est un outil de gestion des secrets et de protection des données sensibles. Il peut être utilisé pour la gestion des clés privées nécessaires à la création et à la validation des VC et DID.

- **Avantages**

  - Centralisation de la gestion des clés et des secrets.
  - Rotation des clés, gestion des accès et des politiques.
  - Peut être intégré dans un environnement multi-cloud ou on-premise.

- ✓ **Indy-SDK** [141]

- **Bibliothèques de Vérification**

Les bibliothèques de vérification jouent un rôle crucial dans les systèmes de VC et de DID. Elles permettent de vérifier l'authenticité des claims contenues dans les VC tout en respectant les standards de sécurité et de confidentialité. Dans la suite nous allons montrer quelques bibliothèques de vérification couramment utilisées dans ces systèmes.

- ✓ **Trust Framework (Indy)**

Hyperledger Indy propose une bibliothèque robuste pour la vérification des VC et des DID. Le Trust Framework est conçu pour garantir que chaque interaction entre un détenteur de credential, un vérificateur et un émetteur est sécurisée et décentralisée. Hyperledger Indy repose sur une chaîne de blocs privée qui assure la gestion et la vérification des identifiants décentralisés.

- **Fonctionnalités principales**

- Vérification de l'authenticité des credentials en interrogeant la blockchain.
- Utilisation de mécanismes cryptographiques tels que les ZKP pour prouver des attributs sans divulguer toutes les informations privées.
- Support de la non-corrélation entre différentes vérifications pour améliorer la confidentialité de l'utilisateur.

- **Exemple d'utilisation**

Le vérificateur envoie une requête au détenteur du VC qui peut prouver certaines informations (ex. : âge supérieur à 18 ans) sans révéler de détails supplémentaires comme la date de naissance exacte.

✓ **ZKP (Zero-Knowledge Proof) librarie**

Les Zero-Knowledge Proof sont des protocoles cryptographiques permettant à une partie (le prouveur) de démontrer la véracité d'une information sans révéler l'information elle-même. Ces bibliothèques sont particulièrement utilisées pour renforcer la confidentialité des utilisateurs dans les systèmes VC et DID.

Une bibliothèque populaire de ZKP est ZoKrates, utilisée pour implémenter des preuves zero-knowledge dans des systèmes blockchain comme Ethereum. [142]

- **Fonctionnalités principales**

- Preuve de la possession d'attributs ou de données sans divulguer les informations réelles.
- Protection renforcée de la vie privée des utilisateurs lors de la vérification des credentials.
- Permet d'éviter la corrélation des données d'un même utilisateur à travers plusieurs systèmes ou interactions.

✓ **Verifiable Credential libraries (W3C)** [46] [54]

Le W3C a standardisé un modèle de données pour les Verifiable Credentials. Ce modèle repose sur un ensemble de normes cryptographiques qui garantissent l'intégrité des informations, l'authenticité de l'émetteur et la confidentialité des données personnelles. Le W3C propose également des bibliothèques qui facilitent l'implémentation et la vérification des VC.

- **Fonctionnalités principales**

- Conformité totale aux standards W3C pour les VC.
- Vérification des signatures cryptographiques pour s'assurer que le credential n'a pas été falsifié.
- Permet de vérifier si un credential a été révoqué par l'émetteur.

- **Exemple d'utilisation**

Une organisation peut émettre un VC signé numériquement attestant d'une qualification. Lorsqu'une autre organisation vérifie ce VC, elle peut confirmer que la signature est valide, et que le credential n'a pas été révoqué.

6.3 Considérations pour les décideurs politiques

Les décideurs politiques et les régulateurs ont un rôle crucial à jouer dans la promotion de l'adoption des VC et des DID. Pour que cette adoption réussisse, ils doivent mettre en place des cadres réglementaires et des politiques favorables à l'innovation tout en garantissant la sécurité et la confidentialité des données personnelles. Cette partie propose des recommandations à l'intention des régulateurs et des décideurs pour encourager un environnement propice à l'adoption de ces technologies.

6.3.1 Recommandations pour les régulateurs et les décideurs politiques

Les régulateurs et décideurs politiques ont un rôle essentiel à jouer pour établir des normes et des cadres de gouvernance autour des VC et DID. Cette section examine ce rôle qu'ils doivent jouer pour encourager l'adoption des VC et des DID. Nous soutenons que des cadres réglementaires clairs et proactifs peuvent favoriser l'innovation tout en protégeant les droits des utilisateurs.

- **Cadre Légal plus Clair**

Un cadre juridique clair n'est pas négligeable pour encourager l'adoption des VC et DID. Les régulateurs doivent définir des normes et règles précises concernant l'utilisation, la gestion et la sécurité de ces technologies. Cela inclut la protection des données personnelles, la conformité au RGPD (en Europe) sur la confidentialité des données. Un tel cadre garantit que les utilisateurs puissent faire confiance aux systèmes basés sur les VC et DID tout en étant protégés contre les abus ou la surveillance indue.

Le RGPD offre un cadre de protection des données qui pourrait être étendu pour inclure des recommandations spécifiques sur la gestion des identifiants décentralisés. Par exemple, les VC pourraient être utilisées pour faciliter la gestion des consentements dans les transactions numériques.

Le RGPD [143] encourage l'adoption de ces technologies pour une meilleure protection des données dès la conception.

- **Soutien à la Recherche et Développement**

Les régulateurs et gouvernements peuvent jouer un rôle actif en soutenant la recherche et le développement des technologies VC-DID. Ils peuvent fournir des subventions, investir dans des infrastructures technologiques ou collaborer avec des universités et des entreprises technologiques pour exploré les cas d'usage dans différents secteurs comme l'éducation, la santé ou les services financiers.

En France par exemple, des initiatives comme le programme de recherche sur la blockchain par l'Agence nationale de la recherche (ANR) peuvent aider à financer des projets innovants autour des VC et DID. [145] [146] [147]

La Commission européenne a financé plusieurs projets de recherche autour de l'identité numérique notamment EBSI (European Blockchain Services Infrastructure), un projet explorant l'utilisation de la blockchain et des VC pour l'identification des citoyens. [144]

- **Encourager l'Innovation**

Les régulateurs doivent également encourager l'innovation en créant des environnements propices au développement de nouvelles applications pour les VC et DID. Cela pourrait inclure des zones de test réglementaires (sandboxes) où les entreprises peuvent expérimenter ces technologis sans être immédiatement soumises à une réglementation stricte. Cela permettrait aux startups de tester des solutions tout en assurant une surveillance réglementaire.

Par exemple le Royaume-Uni a mis en place des « regulatory sandboxes » pour permettre aux startups fintech de tester des technologies innovantes sous la supervision de la Financial Conduct Authority (FCA). Ces environnements réglementair flexibles pourraient être étendus pour inclure les technologies d'identité décentralisée.

Les sandbox réglementaires de la FCA sont un exemple réussi d'encouragement à l'innovation tout en minimisant les risques réglementaires. [148]

- **Faciliter la Collaboration**

La coopération entre les secteurs public et privé est cruciale pour une adoption réussie des VC et DID. Les régulateurs doivent favoriser un dialogue entre les différentes parties prenantes y compris les gouvernements, les entreprises technologiques, les organisations de standardisation et les consommateurs. De plus, il est essentiel d'harmoniser les normes à l'échelle internationale pour garantir l'interopérabilité des systèmes d'identification numérique.

En prenant l'exemple du W3C et de la DIF qui travaillent en étroite collaboration avec des entreprises comme Microsoft, IBM et d'autres pour développer des normes ouvertes pour les identifiants décentralisés. Ce type de collaboration doit être encouragé par les régulateurs. [54] [102]

6.3.2 Politiques favorisant l'adoption des VC et DID

Pour accélérer l'adoption des VC et DID, des politiques incitatives doivent être mises en place. Nous proposons des politiques spécifiques et des initiatives qui peuvent être mises en œuvre pour promouvoir l'adoption des VC et des DID comme la création de partenariats public-privé, les subventions, les programmes de sensibilisation et l'assistance technique qui sont capables d'aider à surmonter les obstacles liés à l'adoption de ces technologies et stimuler l'innovation.

- **Sensibilisation et Education**

L'adoption de la sensibilisation et l'éducation peut être très importante pour que les utilisateurs, entreprises et institutions publiques comprennent les avantages des VC et DID. Des campagnes de sensibilisation, des formations et des conférences peuvent aider à vulgariser les concepts techniques et à encourager la confiance envers ces technologies. Il est également important d'intégrer ces notions dans les programmes éducatifs, notamment dans les filières en ingénierie, droit, gestion des données et cybersécurité.

Pour faciliter la compréhension de ces technologies aux utilisateurs, nous avons proposé quelques initiatives à mettre en place :

- ✓ **Programmes éducatifs**

Intégrer des formations sur les identités décentralisées dans les cursus universitaires. Par exemple, l'Université de Stanford a lancé des cours sur la technologie blockchain qui inclut des modules sur les DID.

- **Intégration dans les cursus académiques**

Introduire les concepts des VC et DID dans les programmes des universités et des écoles notamment dans les filières d'ingénierie informatique, cybersécurité, droit numérique et gestion des données. Cela permettrait de former une nouvelle génération de professionnels qui comprend et maîtrise ces technologies.

- **Ateliers pratiques**

Organiser des ateliers où les étudiants et professionnels peuvent expérimenter des outils décentralisés, créer des infrastructures à identifiants distribués et travailler avec des solutions de gestion de clés cryptographiques.

- **Collaborations avec des institutions**

Travailler avec des écoles et universités pour développer des modules sur la gestion des identités numériques, l'autonomie des utilisateurs et la sécurité des informations.

- ✓ **Campagnes de sensibilisation**

Les organisations peuvent mener des campagnes de sensibilisation pour éduquer sur l'importance des identités numériques sécurisées.

- **Publics diversifiés**

Créer des campagnes adaptées à différents publics (utilisateurs, entreprises, institutions publiques et privées) afin de vulgariser les avantages des VC et DID comme l'amélioration de la sécurité et la réduction des fraudes.

- **Supports visuels et interactifs**

Utiliser des vidéos explicatives, infographies et démonstrations interactives pour simplifier les concepts techniques complexes.

- **Utilisation des médias sociaux**

Exploiter les réseaux sociaux pour sensibiliser un large public en publiant du contenu éducatif régulier et en engageant des discussions autour des questions de sécurité des données et d'autonomie numérique.

- ✓ **Conférences et webinaires**

Organiser des événements physiques ou virtuels qui réunissent des experts, des décideurs politiques et des développeurs pour discuter des cas d'utilisation, des défis et des avantages des VC et DID.

- **Partenariats avec des organisations**

Collaborer avec des organisations telles que la DIF, le W3C ou des entreprises pionnières comme Evernym et IBM pour proposer des webinaires éducatifs et des sessions de questions-réponses avec le public.

- **Événements régionaux et internationaux**

Participer à des forums mondiaux et régionaux, en particulier en Afrique, pour partager les expériences locales et les meilleures pratiques sur l'adoption de ces technologies.

➢ **Subventions, incitations fiscales et financières**

Les incitations financières peuvent encourager les entreprises et les institutions à adopter les VC et DID. Ces mesures peuvent inclure des subventions pour le développement de solutions technologiques, des incitations fiscales pour les entreprises qui adoptent ou développent des solutions d'identités décentralisées et des fonds publics pour la recherche et l'innovation dans ce domaine. [149] [150]

✓ **Subventions pour les startups**

Des fonds peuvent être mis à disposition des startups qui développent des solutions VC et DID. Par exemple, l'Union européenne a lancé des appels à projet pour financer des technologies innovantes y compris les systèmes de gestion d'identité.

✓ **Incitations fiscales**

Des allègements fiscaux pour les entreprises qui adoptent des solutions sécurisées d'identité décentralisée peuvent encourager leur adoption rapide. Par exemple, certains pays offrent des crédits d'impôt pour les dépenses liées à la recherche et développement (R&D) dans les nouvelles technologies.

✓ **Programmes gouvernementaux de financement**

Des programmes comme Horizon Europe ont financé des projets pilotes sur l'identité numérique. Ces genres de pratiques peuvent être efficaces pour booster les VC et DID.

➢ **Support technique et réglementaire**

Le cadre réglementaire et technique est essentiel pour favoriser une adoption à grande échelle. Il doit y avoir un soutien pour le développement de standards communs, d'interopérabilité et un accompagnement technique pour les entreprises qui souhaitent intégrer ces technologies. En parallèle, une réglementation claire sur les questions de confidentialité, de protection des données et de cybersécurité est nécessaire pour éviter les abus et protéger les utilisateurs. [151]

✓ **Standards et protocoles**

Le W3C a déjà mis en place des standards pour les Verifiable Credentials et les Decentralized Identifiers, mais des efforts supplémentaires sont nécessaire pour garantir une interopérabilité à grande échelle.

- ✓ **Guides techniques**

Des resources techniques et des infrastructures de test (sandboxes) comme nous l'avons suggéré précédemment doivent être offertes pour permettre aux entreprises de tester et d'intégrer les technologies VC-DID dans leurs services.

- ✓ **Cadre réglementaire**

Des régulateurs comme la European Data Protection Board (EDPB) fournissent des lignes directrices pour s'assurer que ces nouvelles technologies respectent les lois sur la protection des données. Nous devons avoir partout le monde des régulateurs comme le RGPD pour s'assurer au maximum le respect de lois fixées.

- ➢ **Partenariats Public-Privé**

Les partenariats entre le secteur public et le secteur privé sont essentiels pour développer des solutions innovantes tout en bénéficiant du soutien financier et réglementaire du gouvernement. Ces partenariats permettent de mutualiser les ressources et d'accélérer le développement de projets concrets autour des VC et DID. Le secteur public peut jouer un rôle d'utilisateur précoce (early adopter), ce qui pourrait augmenter la confiance des autres secteurs dans l'adoption de ces technologies. [152] [153]

- ✓ **Projets pilotes conjoints**

Par exemple, le projet Evernym, soutenu par la Fondation Sovrin, a collaboré avec des gouvernements pour créer des systèmes d'identification basés sur les DID pour des services publics.

- ✓ **Partenariats pour l'innovation**

Le programme EU Blockchain Partnership [152], qui réunit des gouvernements et des entreprises privées, vise à développer des solutions d'identité numérique interopérables au niveau européen.

- ✓ **Mise en place de frameworks d'identité**

Des initiatives comme l'Alastria en Espagne [154] démontrent comment les partenariats public-privé peuvent permettre de développer un cadre national pour l'identité décentralisée.

6.4 Étude du cas de microsoft entra

Microsoft Entra est un exemple concret de la manière dont les grandes entreprises peuvent intégrer les technologies VC-DID dans leurs solutions de gestion des identités. Dans cette étude de cas nous allons explorer comment microsoft entra a mis en œuvre ces technologies et analyse les leçons qui peuvent être tirées de cette initiative.

6.4.1 Présentation de Microsoft Entra

- ➢ **Contexte et objectifs de la plateforme**

Microsoft entra est la plateforme de gestion des identité et d'accès basée sur le cloud de microsoft, lancé pour simplifier la gestion des identités et des accès informatiques des employés tout en améliorant la sécurité et la conformité des entreprises.

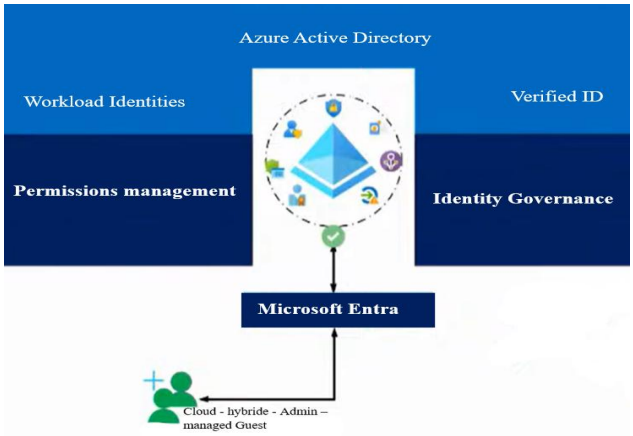


Figure 6.4 : Gestion des identités dans un environnement hybride et cloud

Microsoft entra est juste une version améliore d'Azure AD. Son objectif principal est de permettre aux organisations de gérer en toute sécurité les identités, de contrôler les accès aux ressources et de garantir la conformité tout en renforçant la protection des données sensible. Elle s'inscrit dans la volonté de microsoft d'intégrer les technologies décentralisées comme les VC et les DID afin de proposer une approche moderne et sécurisé de la gestion des identités. [155]

La plateforme vise à améliorer l'interopérabilité et la portabilité des informations d'identité en utilisant les technologies des CV et DID, offrant ainsi aux utilisateurs un plus grand contrôle sur leurs informations personnelles. Parmi ses objectifs clés nous avons :

- ✓ **Sécurisation des accès**

Entra permet de garantir que seul les utilisateurs autorisés accèdent aux ressources, grâce à une gestion restreinte des permissions.

- ✓ **Réduction des risques de fraude et d'usurpation**

Grâce à la vérification cryptographique des identités, cette plateforme réduit considérablement les risques qui sont lies aux fraude et a l'usurpation.

- ✓ **Faciliter la gestion des identités et des accès**

Pour permettre aux utilisateurs de gérer les identités numériques de leurs employés de manière autonome, entra intègre des algorithmes pour la signature comme secp256k1, Ed25519 et P-256, des outils pour la rotation, le stockage sécurisé et la révocation des clés sans oublier la possibilité de partager uniquement les informations nécessaires, préservant ainsi la vie privée des utilisateurs.

- ➢ **Composants de microsoft intra**

Microsoft entra est une plateforme complète de gestion des identités et des accès qui combine plusieurs outils et services pour renforcer la sécurité des organisations.

- ✓ **Azure active directory (Azure AD)**

Composant central de la gestion des identités, il permet aux organisations de gérer les identités et les accès aux ressources cloud, ainsi qu'aux applications SaaS et aux infrastructures on-premises.

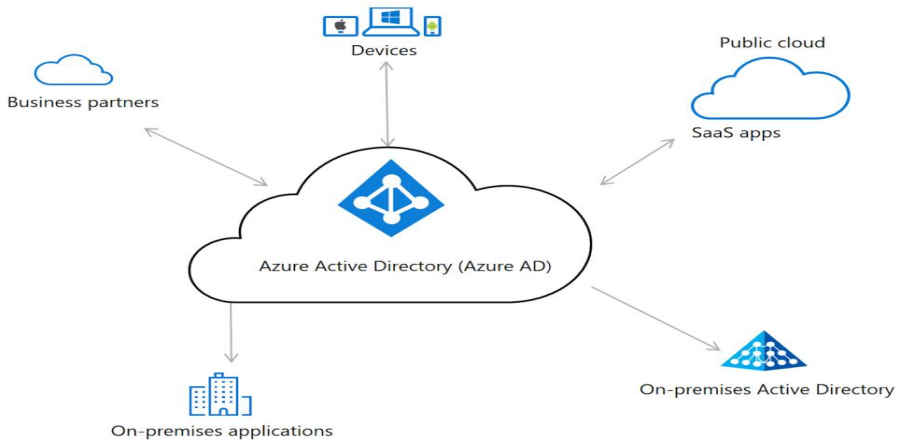


Figure 6.5 : Architecture Azure AD [175]

Dans ce diagramme, nous avons une illustration de l'écosystème d'Azure AD et son rôle dans la gestion des identités et des accès pour divers types de ressources.

- **Azure Active Directory (Azure AD)**

Azure AD est au centre du diagramme, c'est une solution cloud de gestion des identités et des accès qui permet de sécuriser et d'unifier les authentifications pour diverses ressources, qu'elles soient dans le cloud ou sur site.

- **Connexions principales**

  - **Business Partners (Partenaires commerciaux) :**

L'un des avantage d'Azure AD est sa possibilité de partager des ressources ou des applications avec des partenaires commerciaux tout en garantissant une gestion sécurisée des accès, souvent via des fonctionnalités de collaboration B2B.

  - **Devices (Appareils)**

Azure AD gère sérieusement l'authentification des appareils tel que les ordinateurs, tablettes ou smartphones pour garantir que seul les appareils autorisés peuvent accéder aux ressources.

  - **Public Cloud et Applications SaaS**

Azure AD s'intègre avec des applications SaaS (comme Microsoft 365, Salesforce, ou Dropbox) et des services cloud publics, permettant une authentification unique (SSO) et une gestion centralisée des accès.

- **On-premises Active Directory**

Azure AD est souvent utilisé en parallèle avec Active Directory sur site pour fournir une gestion hybride des identités. Cela permet aux entreprises de tirer parti des ressources sur site tout en utilisant des fonctionnalités modernes du cloud.

- **On-premises Applications (Applications sur site)**

Les applications locales c'est-à-dire celle qui sont hébergées sur des serveurs internes de l'organisation peuvent également être intégrées à Azure AD, ce qui permet de les rendre accessibles via le cloud.

✓ **Microsoft entra verified ID**

Son rôle est de permettre aux entreprises d'émettre et de vérifier des VC basés sur des DID, en ligne avec les standards définis par le World Wide Web Consortium. Ce composant utilise la blockchain pour fournir des identifiants numériques auto-souverains.

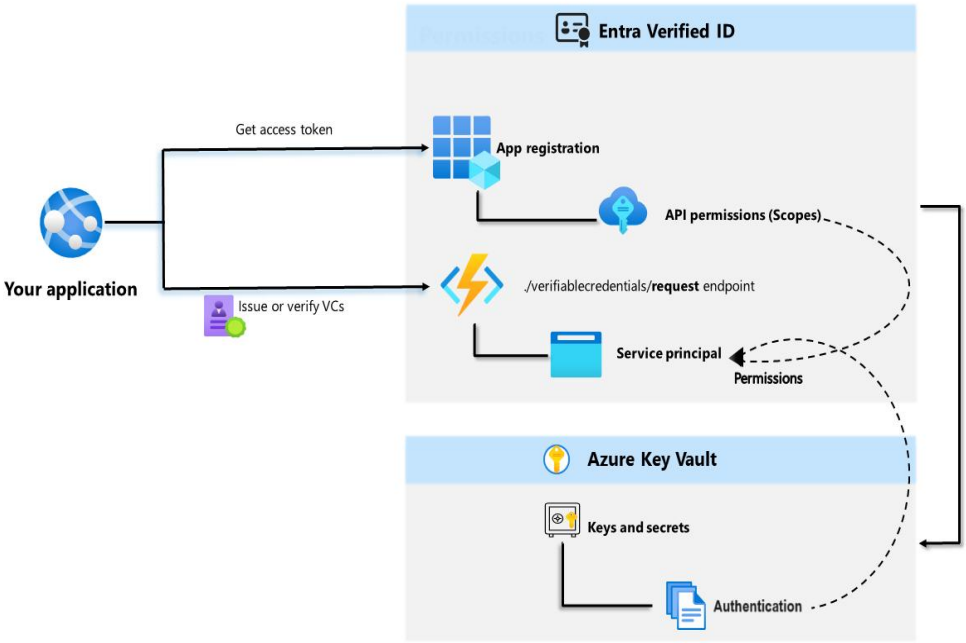


Figure 6.6 : Diagramme illustrative de l'architecture Vérification d'identité Microsoft Entra [172]

Ce diagramme illustre le processus d'intégration et d'utilisation des Identifiants Vérifiés (Verified Credentials) dans une application via Microsoft Entra Verified ID : [172]

- **App Registration**

Une application doit être enregistrée dans Microsoft Entra pour obtenir un accès aux API nécessaires. Cela permet à l'application d'obtenir un jeton d'accès.

- **API Permissions**

Des autorisations spécifiques (scopes) sont attribuées à l'application pour accéder à des fonctionnalités comme l'émission ou la vérification des Identifiants Vérifiés via l'API /verifiablecredentials/request.

- **Azure Key Vault**

Les clés et secrets utilisés pour signer ou sécuriser les Identifiants Vérifiés sont stockés dans Azure Key Vault. L'authentification garantit que seuls les services autorisés peuvent y accéder.

- **Service Principal**

Un principal de service agit comme une entité (liée à l'application) pour définir et gérer les permissions associées à l'utilisation des Identifiants Vérifiés.

✓ **Entra permissions management**

La Gestion des autorisations Microsoft Entra est une solution CIEM (Cloud Infrastructure Entitlement Management) qui offre une visibilité sur les autorisations dans des environnements multicloud (Azure, AWS, GCP). Elle aide les organisations à détecter, corriger et superviser les autorisations inutilisées ou excessives pour renforcer la sécurité selon le principe du privilège minimum dans une stratégie de Confiance Zéro.

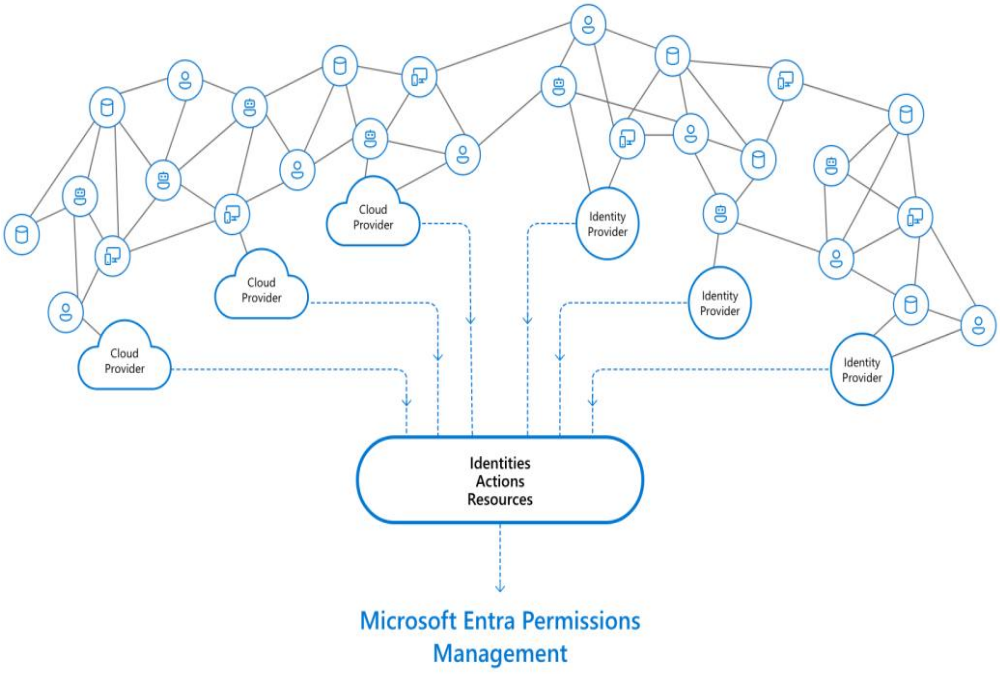


Figure 6.7 : exemple de diagramme illustrative du permissions management [171]

Le diagramme ci-dessus illustre comment Microsoft Entra Permissions Management supervise et sécurise l'accès dans un environnement multi-cloud complexe. Les principaux éléments sont : [171]

- **Réseau d'Identités et Ressources**

Il met en évidence un réseau d'identités, de fournisseurs de cloud et de fournisseurs d'identité. Cela reflète un environnement dans lequel des utilisateurs ou des systèmes interagissent avec des ressources réparties sur plusieurs plateformes.

- **Permissions Management**

Microsoft Entra agit comme un centre de contrôle pour gérer les identités, les actions autorisées (permissions) et les ressources associées.

- **Interopérabilité Multi-Cloud**

Ce modèle montre qu'entra permet une gestion centralisée des permissions, même dans des environnements ou des ressources et identités proviennent de différents cloud ou fournisseurs d'identité. Cela permet d'améliorer la visibilité et de réduire les risques d'accès non autorisé.

Cette gestion fonctionne en trois phases principales (découverte, correction et supervision) pour aider les organisations à gérer efficacement les autorisations et à renforcer leur posture de sécurité.

- **Découverte**

C'est la phase d'analyse des autorisations inutilisées ou excessives grâce à des outils comme l'Index PCI et l'analyse des autorisations.

- **Correction**

Dans cette phase se fait, la suppression automatique des autorisations inutilisées, gestion des accès à la demande et automatisation des autorisations juste-à-temps.

- **Supervision**

La phase de suppression (monitor) concerne la détection d'anomalies via le machine learning et génération de rapports d'investigation détaillés.



Figure 6.8 : Cas d'utilisations clés de gestion des autorisations [171]

Cette gestion permet une sécurité cohérente et une réduction des risques en unifiant les stratégies d'accès sur plusieurs plateformes cloud tout en garantissant une visibilité et un contrôle granulaire sur les permissions et les accès aux ressources, réduisant ainsi les risques liés aux permissions excessives.

✓ **Entra Identity governance**

Microsoft Entra ID Governance est une solution de gouvernance des identités utilisé pour la gestion de l'accès tout au long du cycle de vie des utilisateurs en automatisant et en optimisant la gestion des accès pour garantir que les bonnes personnes disposent du bon niveau d'accès. il automatise les processus d'identité et d'accès, offre une délégation pour les groupes d'entreprise et améliore la visibilité et la sécurité des accès, son but c'est d'améliorer la productivité, renforcer la sécurité et répondre aux exigences de conformité.

Avec ID governance, il est possible d'implémenter les scénarios suivants pour les employés, les partenaires commerciaux et les fournisseurs : [173]

- **Cycle de vie des identités**
  - Automatisation de la création, mise à jour et suppression d'identités.
  - Intégration avec des systèmes RH (comme Workday, SuccessFactors) pour gérer les identités des employés, partenaires et invités.
  - Gestion automatisée des appartenances aux groupes, rôles d'applications et ressources (via SCIM, LDAP, SQL).

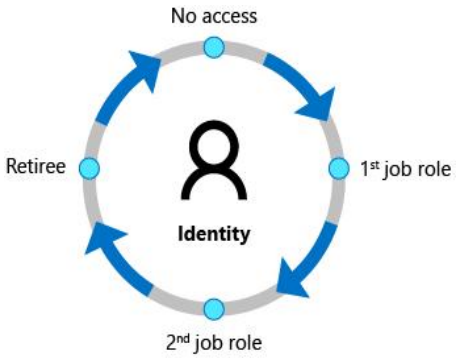


Figure 6.9 : Gouvernance des identités [173]

- **Cycle de vie des accès**
  - Définition des droits d'accès pour les utilisateurs, y compris les stratégies d'accès conditionnel (par exemple : acceptation des conditions d'utilisation).
  - Automatisation des changements d'accès en fonction des attributs des utilisateurs.
  - Révisions régulières des droits d'accès des utilisateurs, invités et administrateurs.

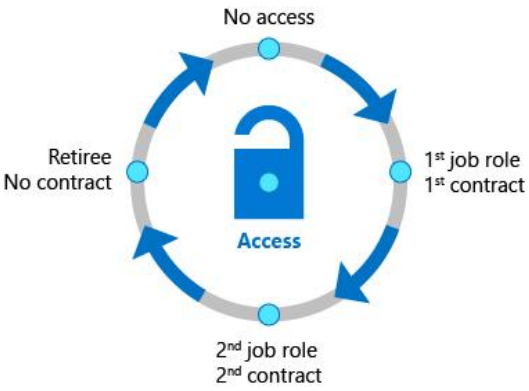


Figure 6.10 : Gouvernance des accès [173]

- **Cycle de vie des accès privilégié**

  - Utilisation de Microsoft Entra Privileged Identity Management (PIM) pour sécuriser les rôles administratifs.
  - Contrôles comme l'accès juste-à-temps, l'authentification multi-facteurs, et les alertes de modification de rôle.
  - Recertification périodique des accès privilégiés via des révisions d'accès.

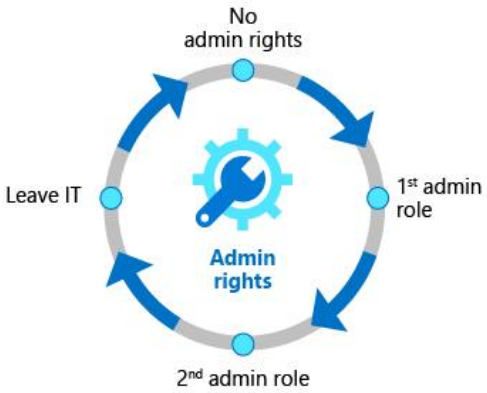


Figure 6.11 : Gouvernance des accès privilégiés [173]

Nous pouvons dire que Microsoft Entra ID Governance offre une solution complète pour automatiser la gestion des identités et des accès.

✓ **Microsoft Entra Workload Identities**

Microsoft Entra Workload Identities encore appele identités de charge de travail, désigne les identités attribuées à des entités logicielles telles que des applications, services, scripts ou conteneurs pour leur permettre de s'authentifier et d'accéder à des ressources ou services spécifiques. Elles se distinguent des identités humaines car elles sont dédiées aux opérations automatisées des charges de travail non humaines. [156]

Les principaux concepts que désignes par les identités de charge de travail dans Microsoft Entra sont :

- **Applications**

Une application représente un modèle global défini par un objet d'application. Ce modèle détermine la manière dont les jetons sont émis, les ressources accessibles, et les actions possibles par l'application.

- **Principaux de service**

Il s'agit d'une instance locale d'un objet d'application dans un locataire spécifique. Le principal de service définit les permissions et les actions qu'une application peut exécuter dans ce locataire.

- **Identités gérées**

Ce sont des principaux de service spéciaux qui simplifient la gestion des informations d'identification. Les développeurs n'ont pas besoin de gérer manuellement les secrets pour accéder aux ressources Azure.

- **Différence entre identités humaines et identités de charge de travail**

  - **Identités humaines**

Les identités humaines représentent des personnes physiques ou utilisateurs humains (employés, partenaires, clients) avec un accès manuel aux ressources qui interagissent avec des systèmes pour accéder aux ressources.

Parmi les entités des identités humaines, nous avons les employés internes (travailleurs de bureau, personnel de terrain) et les partenaires externes (consultants, fournisseurs, clients, etc.).

- **Caractéristiques**

  - Chaque identité humaine est associée à un utilisateur unique.
  - Elle nécessite une authentification via des méthodes comme des mots de passe, des biométries ou des authentifications multifactor (MFA).
  - Elle est utilisée pour des sessions manuelles et interactives avec des applications ou services.
  - Les autorisations dépendent souvent des rôles ou des groupes auxquels l'utilisateur appartient dans le système.

- **Exemples de cas d'usages**

  - Un employé accède à une application cloud pour consulter des données ou effectuer des tâches administratives.
  - Un consultant utilise un compte temporaire pour collaborer sur un projet spécifique.

  - **Identités machines**

Les identités de charge de travail représentent des entités logicielles ou machines (applications, services, conteneurs) qui accèdent aux ressources de manière automatisée sans intervention humaine.

Les entités des identités machines, nous pouvons avons une application web qui interagit avec une API (ex : Microsoft Graph), un script automatisé qui extrait des données d'un stockage cloud, une charge de travail Kubernetes accédant à un coffre-fort de secrets, etc.

- **Caractéristiques**

  - Elles sont non humaines et fonctionnent indépendamment d'une session utilisateur.
  - Authentification via des mécanismes sécurisés comme des clés, certificats ou identités gérées.

- Elles nécessitent des informations d'identification spécifiques (ex : tokens d'accès) pour accéder aux ressources.
- Les permissions sont définies au niveau des ressources nécessaires à leur exécution.

- **Exemples de cas d'usages**

- Une identité gérée permettant à un pipeline CI/CD de déployer une application.
- Une application accédant à Azure Key Vault pour récupérer des secrets.

Tableau 6.2 : résumé des différences entre identités humaines et machines

Aspect	Identités humaines	Identités de charge de travail
Entité représentée	Personnes physiques	Logiciels, scripts, services, ou conteneurs
Type d'authentification	Mots de passe, biométrie, MFA	Clés, certificats, identités gérées
Interaction	Manuelle (sessions interactives)	Automatisée (sans intervention humaine)
Permissions	Dépendantes des rôles ou groupes	Définies par ressource ou scénario
Exemples d'utilisation	Accès à des outils bureautiques, CRM	Accès aux API, stockage cloud, pipelines CI/CD

Ces différences permettent d'optimiser la gestion des accès dans les systèmes modernes, en tenant compte des spécificités de chaque type d'identité.

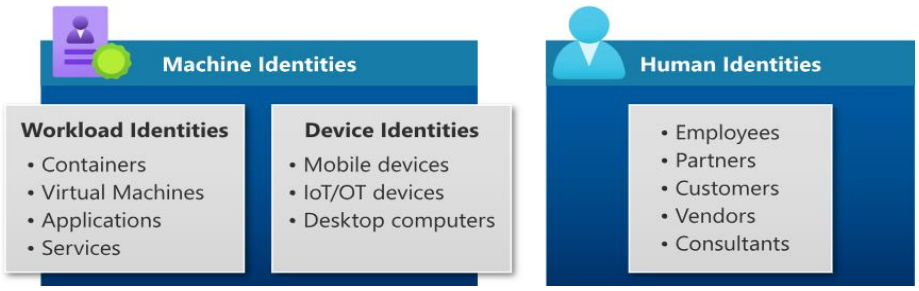


Figure 6.12 : illustration des identités humaine et machines [156]

- **Importance de la sécurité des identités machines**

Avec la croissance des entités non humaines dans les systèmes, ces identités deviennent une cible privilégiée pour les cyberattaques, notamment à cause des défis suivants :

- Multiplication des informations d'identification nécessaires pour diverses ressources.
- Risques liés à une gestion inadéquate des secrets et des clés.
- Difficulté de suivi des cycles de vie des identités (création, révocation).

Les cyberattaques exploitant ces failles peuvent entraîner des violations majeures des services ou application.

En plus, le nombre d'identités machine dépasse largement celui des identités humaines, avec un ratio estimé à 10:1 en moyenne. Ce chiffre inclut une large variété de machines telles que des appareils IoT, des conteneurs, des infrastructures cloud, des API, et des algorithmes. Dans les grandes entreprises, ce nombre peut atteindre plusieurs millions d'identités machine [174]

- **Évolution de la plateforme**

Microsoft entra a vu le jour en 2022, mais elle est issue des progrès continus de Microsoft dans le domaine de la gestion des identités numériques avec Azure AD en tant que fondement. La plateforme a intégré progressivement des fonctionnalités liées aux identifiants décentralisés et aux Verifiable Credentials pour répondre aux besoins croissants de sécurisation et de décentralisation des identités numériques.

L'évolution récente se concentre sur l'interopérabilité et la conformité avec des standards internationaux tels que les normes du W3C pour les DID et les VC. Microsoft envisage d'élargir les cas d'usage dans divers secteurs tels que la santé, l'éducation et les services financiers. [158]

- **Positionnement de Microsoft Entra par rapport aux autres solutions de gestion des identités.**

Microsoft Entra se distingue des autres plateformes de gestion des identités par son intégration profonde avec Azure AD, sa capacité à gérer des identités décentralisées à grande échelle et son utilisation des Verifiable Credentials pour renforcer la sécurité des identités numériques. Par rapport à des concurrents comme Okta ou Auth0, Microsoft mise sur son infrastructure cloud Azure et sa capacité à s'intégrer avec des environnements hybrides tout en proposant des fonctionnalités uniques comme les DID.

Le principal atout de Microsoft Entra est sa vision de l'avenir des identités numériques en se concentrant non seulement sur la gestion des accès centralisés mais aussi sur l'émission et la vérification d'identités décentralisées. [159]

6.4.2 Technologies utilisées

Cette section présente les aspects techniques et normatifs sous-jacents à l'intégration des VC et des DID dans Microsoft Entra. Elle a décrit les organismes de normalisation impliqués, les normes et algorithmes pris en charge ainsi que le rôle spécifique des VC et DID dans le contexte de Microsoft Entra pour garantir l'interopérabilité, la sécurité et l'efficacité des processus d'identification.

- **Organismes de normalisation**

Microsoft Entra s'appuie sur plusieurs organismes de normalisation pour garantir l'interopérabilité, la sécurité et la conformité de ses services d'identité. Parmi les principaux organismes nous avons : [160]

- ✓ **W3C**

Responsable de la normalisation des VC et des DID. Microsoft Entra utilise les spécifications du W3C pour permettre l'émission et la vérification d'identifiants décentralisés.

- ✓ **DIF**

Cette organisation joue un rôle clé dans le développement d'outils et de protocoles pour les identités décentralisées. Microsoft Entra collabore avec la DIF pour promouvoir les normes d'identité auto-souveraine.

- ✓ **IETF**

Les standards de sécurité comme OAuth 2.0, OpenID Connect et d'autres protocoles utilisés dans Microsoft Entra sont définis par l'IETF, qui joue un rôle crucial dans l'évolution des normes d'authentification et d'autorisation sur Internet.

- ✓ **OpenID Foundation (OIDF)**

La fondation est à l'origine du protocole OpenID Connect qui étend OAuth 2.0 en ajoutant une couche d'identité. Microsof Entra, via Azure AD, utilise OpenID Connect pour l'authentification des utilisateurs dans des environnements décentralisés, garantissant ainsi des échanges sécurisés et standardisés d'informations d'identité

- ➢ **Normes prises en charge**

Tableau 6.3 : Normes prise en charge par microsoft entra

Microsoft Entra prend en charge un large éventail de normes pour assurer la sécurité et l'interopérabilité de ses solutions d'identité :

Ces normes permettent à Microsoft Entra Verified ID de s'intégrer efficacement dans l'écosystème d'identités décentralisées, tout en restant compatible avec des protocoles d'authentification et d'autorisation plus traditionnels et largement adoptés.

- **Algorithmes pris en charge**

Microsoft Entra prend en charge divers algorithmes cryptographiques pour la vérification des identités et la sécurisation des transactions. Ces algoritmes sont utilisés dans le cadre des signatures JWS pour garantir l'intégrité et l'authenticité des informations transmises. Nous allons voir les principaux types de clés et algorithmes pris en charge :

Composant de pile technologique	Norme ouverte	Organisme de normes
Modèle de données	Modèle de données des informations d'identification vérifiables v1.1	W3C VC WG
Format d'informations d'identification	JSON Web Token VC (JWT-VC) - encodé en tant que JSON et signé en tant que	JWS (RFC7515) W3C VC WG / IETF
Identificateur d'entité (émetteur, vérificateur)	did	W3C CCG
Authentification utilisateur	Fournisseur OpenID auto-émis v2	OIDF
Présentation	OpenID pour les informations d'identification vérifiables	OIDF
Langage de requête	Presentation Exchange v1.0	DIF
Confiance dans le propriétaire de DID	Well Known DID Configuration	DIF
Révocation	Liste d'état des justificatifs vérifiables	W3C CCG
Identités décentralisées (DID)	Decentralized Identifiers (DID)	W3C CCG / Decentralized Identity Foundation (DIF)
Informations d'identification vérifiables (VC)	Verifiable Credentials (VC)	W3C VC WG
Authentification	OAuth 2.0 et OpenID Connect	IETF / OpenID Foundation
Authentification et échange d'assertions	Security Assertion Markup Language (SAML)	OASIS
Authentification sans mot de passe	FIDO2 (Fast Identity Online)	FIDO Alliance

Tableau 6.4 : Types de clé et des algorithmes JWT pris en charge par Microsoft Entra

Type de clé	Algorithme JWT
secp256k1	ES256K
Ed25519	EdDSA
EC	P-256

- ✓ **Secp256k1**

Elle est utilisée avec l'algorithme ES256K. Ce type de clé elliptique est largement employé dans les systèmes blockchain et de cryptographie asymétrique pour générer des signatures sécurisées.

- ✓ **Ed25519**

Elle est combinée avec l'algorithme EdDSA (Edwards-Curve Digital Signature Algorithm), Ed25519 est un algorithme à courbe elliptique reconnu pour ses performances et sa sécurité élevée, souvent utilisé dans les systèmes nécessitant des signatures numériques rapides et sécurisées.

- ✓ **EC P-256**

L'algorithme elliptique P-256, conforme au NIST (National Institute of Standards and Technology), est un standard largement utilisé dans les systèmes de sécurité modernes pour assurer des signatures numériques solides et conformes aux réglementations.

- ➢ **Rôle des VC et DID dans Microsoft Entra**

[161] montre que les VC et les DID jouent un rôle central dans l'infrastructure de Microsoft Entra. Ils permettent de créer des identités décentralisées et vérifiables, offrant aux utilisateurs un contrôle total sur leurs informations personnelles. Ces technologies offrent une alternative sécurisée aux identifiants traditionnels centralisés, en utilisant la cryptographie pour garantir que seuls des tiers autorisés peuvent vérifier les informations d'identité.

- ✓ **Rôle des VC**

Elles permettent aux organisations d'émettre des informations d'identité sous forme de credentials qui peuvent ensuite être partagés et vérifiés de manière cryptographique. Ces VC sont basées sur des standards du W3C et permettent aux utilisateurs de présenter uniquement les informations nécessaires sans divulguer plus de détails qu'exigé, grâce à des mécanismes de divulgation sélective.

- ✓ **Rôle des DID**

Ce sont des identifiants uniques créés par les entreprises, qui ne dépendent pas d'une autorité centrale. Ils permettent ces dernières de posséder, contrôler et gérer leurs identités sans dépendre de services centralisés comme les fournisseurs d'authentification traditionnels. Les DID, utilisés avec les VC, assurent l'authenticité et la sécurité des interactions numériques tout en garantissant la confidentialité des données des utilisateurs.

6.4.3 Analyse de l'intégration des VC et DID dans Microsoft Entra

Dans cette section, nous allons essayer d'analyser l'intégration des VC et DID dans Microsoft Entra en examinant les aspects techniques et organisationnels de cette intégration, abordant l'architecture et l'implémentation, la configuration du système, ainsi que les bénéfices observés à travers l'adoption de ces technologies.

➢ **Architecture et implémentation**

Microsoft Entra repose sur une architecture décentralisée qui permet la gestion d'identités numériques basées sur les VC et les DID. L'infrastructure utilise des normes ouvertes, telles que celles définies par le W3C, permettant aux utilisateurs de contrôler leurs identités tout en fournissant une vérification fiable.

L'utilisation de Microsoft Entra permet de créer des DID qui sont résolus via le Microsoft Resolver, et les VC sont stockés dans Microsoft Authentificator App. Ces identifiants sont signés et vérifiés par des mécanismes cryptographiques robustes qui garantissent l'intégrité des données d'identité . [162]

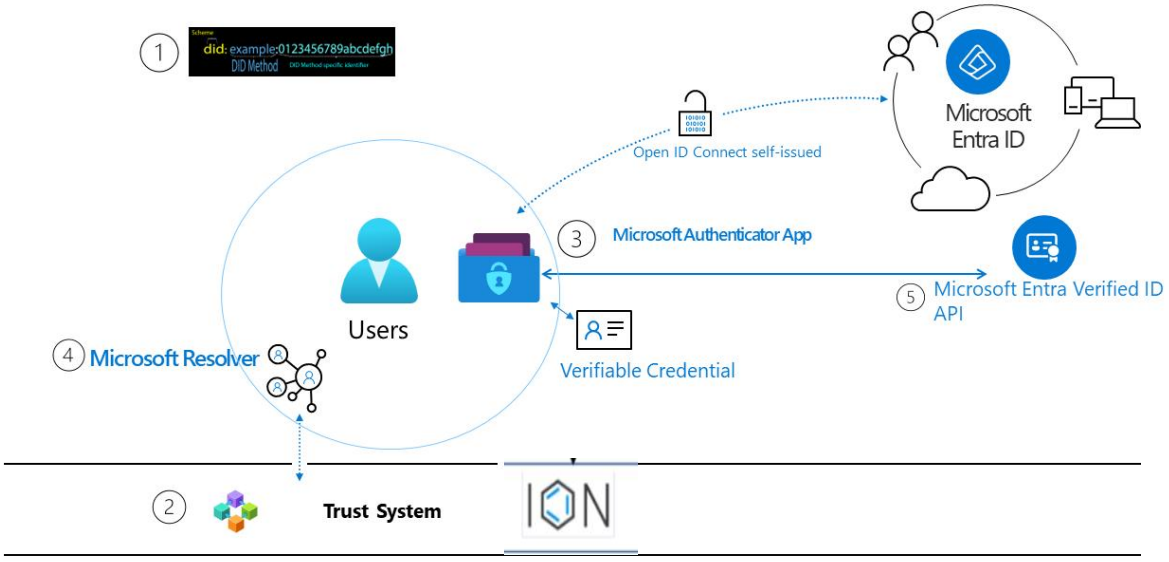


Figure 6.13 : Architecture de Microsoft intra [161]

✓ **Composants de l'architecture**

- **DID**

Chaque utilisateur possède un DID unique qui agit comme un identifiant auto_souverain. Le schéma DID (par exemple, « did:example:0123456789abcdef » est conforme aux standards définis par le W3C, garantissant que chaque DID est unique et peut être résolu de manière décentralisée.

Le DID est utilisé pour associer des informations d'identité à une entité (individu ou organisation) tout en garantissant la confidentialité et l'autonomie des utilisateurs.

- **Trust System (Système de Confiance)**

Les DID sont associés à un système de confiance décentralisé qui permet de résoudre les DID pour vérifier l'authenticité des informations d'identité. Ce système est fondé sur une infrastructure publique, telle que la blockchain, qui garantit que les DID peuvent être vérifiés sans dépendre d'une autorité centralisée.

Le système de confiance sert également à valider les attributs de l'identité via un mécanisme distribué, rendant difficile la falsification des informations.

- **Microsoft Authenticator App**

  - **Issuance des VC**

Les utilisateurs peuvent émettre leurs Verifiable Credentials via l'application Microsoft Authenticator, qui agit comme un portefeuille sécurisé (wallet) pour stocker les VC. L'application se base sur le protocole OpenID Connect Self-Issued pour gérer les échanges d'identité de manière sécurisée.

  - **Stockage et présentation**

Les credentials sont stockés localement sur l'appareil de l'utilisateur, et l'application Authenticator permet aux utilisateurs de présenter ces credentials aux vérificateurs de manière sécurisée en utilisant des signatures cryptographiques pour garantir l'intégrité des données.

- **Microsoft Resolver**

Le resolver est un composant crucial qui permet de résoudre les DID en informations vérifiables sur l'identité de l'utilisateur. Il se base sur une infrastructure décentralisée pour garantir que les informations d'identité sont accessibles et authentifiées de manière sécurisée.

Microsoft Resolver est compatible avec différents types de DID y compris ceux générés par d'autres systèmes, ce qui favorise l'interopérabilité entre plateformes.

- **Microsoft Entra Verified ID API**

L'API Verified ID de Microsoft Entra est une interface qui permet aux développeurs et aux applications d'intégrer des fonctionnalités de vérification d'identité dans leurs systèmes.

Elle permet de vérifier les VC des utilisateurs, d'émettre de nouveaux credentials et de configurer les politiques de gestion des identifiants. L'API utilise des protocoles sécurisés tels que OpenID Connect, pour faciliter la communication entre le système de gestion des identités et les applications tierces.

✓ **Processus d'implémentation**

- **Création du DID**

Lorsqu'un utilisateur se connecte à Microsoft Entra pour la première fois, un DID est créé et enregistré dans un registre décentralisé. Ce processus implique la génération de paires de clés cryptographiques qui sont utilisées pour signer et vérifier les credentials.

- **Issuance et stockage des VC**

Une fois le DID créé, des Verifiable Credentials peuvent être émis par des entités tierces (par exemple, une organisation ou un gouvernement). Ces VC sont ensuite stockés sur l'application Microsoft Authenticator de l'utilisateur, garantissant que l'utilisateur a un contrôle total sur ses informations d'identité.

- **Vérification de l'identité**

Pour vérifier une identité, un vérificateur peut interagir avec l'utilisateur via l'application Authenticatore. L'application signe les VC de l'utilisateur à l'aide de la clé privée associée au DID et le vérificateur utilise l'API Verified ID de Microsoft Entra pour résoudre le DID et confirmer la validité des credentials.

✓ **Caractéristiques de l'Architecture**

- **Décentralisation**

La création et la gestion des DID sont basées sur une infrastructure décentralisé, ce qui garantit qu'aucune autorité centrale ne peut contrôler ou altérer les identités. Cela permet aux utilisateurs d'être autonomes et de gérer leurs identifiants en toute sécurité.

- **Interopérabilité**

L'architecture de Microsoft Entra est conçue pour être compatible avec divers systèmes d'identité décentralisée. Elle respecte les normes définies par le W3C et peut interagir avec d'autres fournisseurs de DID et de VC, facilitant ainsi une adoption à grande échelle.

- **Sécurité avancée**

L'utilisation de technologies telles que les signatures numériques et les paires de clés asymétriques assure que seules les personnes autorisées peuvent accéder aux credentials ou les partager avec des tiers. Cela fait que la sécurité globale du système est renforcée.

➢ **Configuration de Microsoft Entra**

Configurer Microsoft Entra pour l'utilisation des VC et DID nécessite quelques étapes techniques spécifiques. L'administration de ces systèmes se fait via le portail Microsoft Entra [169] qui permet de définir les politiques d'émission et de vérification des credentials.

La configuration peut être de deux types : configuration rapide et configuration avancée, chacun répond à des besoins spécifiques des administrateurs et organisations en fonction de la complexité.

✓ **Configuration rapide**

Cette méthode est conçue pour les organisations qui recherchent une configuration rapide et simple des services de vérification d'identité sans nécessiter de personnalisation approfondie.

Ces étapes sont :

- **Prérequis**

Avant de commencer la configuration rapide de l'ID vérifié, il est important de s'assurer que les éléments suivants sont en place :

  - Accès administrateur au portail Microsoft Entra.
  - Accès aux ressources Azure pour la configuration des ID et l'émission des credentials.

Ces prérequis garantissent que l'administrateur dispose des autorisations nécessaires pour configurer et gérer les VC. Pour plus de détails sur les prérequis, vous pouvez consulter le guide de configuration rapide .

- **Fonctionnement de la configuration rapide de l'ID vérifié**

La configuration rapide de l'ID vérifié se concentre sur une mise en place simple et efficace des VC. Les administrateurs utilisent le portail Entra pour définir rapidement les politiques d'émission, en utilisant des paramètres par défaut. Cela permet aux organisations de démarrer avec les fonctionnalités essentielles de l'identité vérifiée sans entrer dans des détails complexe.

- **Configurer un ID vérifié**

Pour configurer un ID vérifié :

Il faut se connecter au portail Microsoft Entra.

  - Créer un schéma d'identité (VC), définir les attribus nécessaires et spécifier la durée de validité.
  - Publier le schéma pour permettre son utilisation par d'autres utilisateurs et applications.

Ces étapes permettent de commencer l'émission d'ID vérifiés en quelques minutes.

- **Utilisation de MyAccount**

Avec MyAccount, les utilisateurs finaux peuvent gérer leurs informations d'identification de manière plus autonome. Cela simplifie la distribution et la gestion des informations d'identification d'espace de travail en offrant une interface utilisateur conviviale.

- **Inscrire une application dans Microsoft Entra ID**

Pour utiliser les VC dans un environnement applicatif :

  - Il est possible d'inscrire une nouvelle application dans Microsoft Entra ID via le portail.

- Il est possible aussi d'attribuer des autorisations nécessaires pour l'émission et la vérification des informations d'identification.

L'inscription de l'application est une étape cruciale pour s'assurer que l'intégration se fait correctement et que les bonnes permissions sont accordées. Plus de détails sont disponibles dans le guide de configuration rapide .

✓ **Configuration Avancée**

Elle est destinée aux administrateurs qui ont besoin d'une personnalisation poussée et d'un contrôle total sur les configurations de sécurité, d'identité et de gestion des clés.

- **Prérequis**

Pour la configuration avancée, en plus des prérequis de la configuration rapide, il est nécessaire d'avoir :

- Un abonnement Azure actif pour créer et gérer des ressources avancées.
- Autorisation d'accès au service Azure Key Vault qui sera utilisé pour gérer les clés de sécurité.

- **Création d'un coffre de clés**

Un coffre de clés (Azure Key Vault) est créé pour gérer les clés utilisées pour signer les informations d'identification, cela se fait en :

- Se connectant à Azure Portal et créant un nouveau coffre de clés.
- Configurant les politiques d'accès pour permettre à Microsoft Entra d'utiliser ces clés.

La gestion des clés est essentielle pour garantir la sécurité des VC, notamment en ce qui concerne la rotation régulière des clés pour minimiser les risques de compromission . [164]

- **Gérer l'accès au coffre de clés**

- Attribution des rôles d'accès au coffre de clés, permettant à Microsoft Entra ID d'utiliser les clés pour signer les informations d'identification.
- Configuration des politiques de rotation pour assurer la mise à jour régulière des clés.

Ces mesures permettent de renforcer la sécurité des identités en garantissant que seules les clés autorisées sont utilisées pour les opérations cryptographiques.

- **Configurer un ID vérifié**

Cette étape est similaire à celle de la configuration rapide mai avec des paramètres plus détaillés là il faudra définir des politiques spécifiques, par exemple des politiques de divulgation sélective ou des preuves à connaissance nulle.

- **Inscrire une application dans Microsoft Entra ID**

Comme pour la configuration rapide, ici aussi on peut inscrire une application, mais cette fois-ci avec des options avancées. Il faudra définir des rôles de sécurité spécifiques, attribuer des autorisations plus granuleuses pour garantir que seules certaines actions peuvent être effectuées par l'application.

- **Accorder des autorisations pour obtenir des jetons d'accès**

Pour permettre aux applications d'accéder aux service Entra, il faudra accorder des autorisations spécifiques afin que les applications puissent obtenir des jetons OAuth 2.0 pour l'émission et la vérification des VC.

- **Inscrire l'ID décentralisé et vérifier la propriété du domaine**

  - Enregistrement d'ID décentralisée (DID) via Microsoft Entra.
  - Vérification de la propriété du domaine associé au DID, ce qui est nécessaire pour assurer l'authenticité de l'identité décentralisée et pour valider que le domaine est contrôlé par l'organisation.

Cette étape permet de renforcer la confiance dans les VC et d'assurer que les identifiants sont authentiques et sont correctement validés . [164]

Ces deux configurations de de Microsoft Entra permettent une mise en place flexible selon les besoins de sécurité, de contrôle et de complexité d'une organisation. Pour plus de détails et de références, les guides complets sont disponibles via Microsoft Learn [163] [164].

➢ **Bénéfices observés**

L'intégration des VC et des DID dans Microsoft Entra offre plusieurs avantages, tant en matière de sécurité qu'en termes d'amélioration de la confiance et de l'adaptabilité aux besoins spécifiques des organisations. [165] [166]

✓ **Contrôle renforcé et sécurité**

Microsoft Entra offre des fonctionnalités avancées qui permettent aux organisations de mieux contrôler les accès et de renforcer la sécurité des identités numériques.

- **Contrôle des accès**

Microsoft Entra permet de gérer précisément les accès à travers des politiques adaptatives qui prennent en compte divers facteurs comme l'identité de l'utilisateur, la localisation et le contexte. Cela permet de mettre en place une sécurité stricte en réduisant les risques d'accès non autorisé. L'intégration avec Azure Active Directory permet également d'assurer une surveillance continue et une réponse aux incidents en temps réel.

- **Authentification Multi-Facteurs (MFA)**

Entra intègre des mécanismes de vérification d'identité avancés tels que l'authentification multi-facteurs afin de minimiser les risques de compromission de comptes. Ce niveau de sécurité supplémentaire est essentiel pour prévenir les attaques de phishing et de prise de contrôle de comptes/

- **Gestion de l'accès basée sur le contexte**

Grâce à des solutions comme les accès conditionnels, Entra permet de définir des politiques de sécurité basées sur le contexte, garantissant que les bonnes personnes aient accès aux bonnes ressources au bon moment. Cette approche est essentielle dans la prévention des violations de sécurité basées sur des comportements inhabituels.

✓ **Amélioration de la confiance**

Microsoft Entra améliore la confiance en simplifiant et sécurisant l'authentification et la gestion des identités.

- **Identifiants vérifiables**

Entra permet d'émettre et de vérifier des identifiants vérifiables qui sont utilisés pour prouver des aspects de l'identité de manière sécurisée et sans compromettre la confidentialité de l'utilisateur. Ce processus assure l'intégrité des informations échangées entre les parties, ce qui renforce la confiance dans les interactions numériques.

- **Transparence et auditabilité**

Microsoft Entra offre des capacités de journalisation et de rapport détaillées permettant aux administrateurs de suivre les actions d'authentification et d'accès. Cette transparence est un atout majeur pour établir une confiance au sein des organisations car elle permet de démontrer le respect des politiques de sécurité et de conformité.

- **Normes de sécurité**

La compatibilité de Microsoft Entra avec des standards reconnus tels que OAuth 2.0 et OpenID Connect, garantit que les pratiques de sécurité respectent les normes de l'industrie, ce qui inspire confiance aux utilisateurs et aux partenaires.

✓ **Adaptabilité**

Les différentes options de configurations permettent aux organisations de s'adapter à leurs besoins spécifiques en matière de sécurité et de gestion des identités.

- **Prise en charge des protocoles standards**

Entra supporte une variété de protocoles tels que SAML, OAuth, et OpenID Connect, qui permettent l'intégration facile avec des applications tierces et facilitent la transition des systèmes existants. Cette adaptabilité est cruciale pour les organisations qui veulent éviter de réinventer leurs infrastructures d'identité lors de leur migration vers des solutions basées sur le cloud.

- **Gestion des Identités Décentralisées**

Entra est conçu pour prendre en charge l'utilisation des DID qui permettent aux utilisateurs de contrôler leurs informations d'identité de manière décentralisée. Cela améliore l'adaptabilité

du système en offrant un modèle de gestion des identités plus ouvert et plus flexible, compatible avec l'évolution vers des modèles d'identité auto-souveraine.

- **Scalabilité**

Microsoft Entra permet de répondre aux besoins croissants des entreprises, qu'il s'agisse d'ajouter de nouveaux utilisateurs, de prendre en charge davantage de services ou de s'adapter aux changements de réglementation. Cette capacité de mise à l'échelle sans compromis sur la sécurité ou la performance fait d'Entra une solution particulièrement adaptée aux organisations en croissance rapide.

6.4.4 Recommandations spécifiques pour optimiser utilisation de microsoft intra

Pour optimiser l'utilisation de Microsoft Entra dans le contexte des VC et DID, il est crucial de suivre des recommandations spécifiques qui pourront garantir une sécurité renforcée, une gestion efficace des identités et une expérience utilisateur améliorée. Dans la suit, nous allons proposer quelques mesures primordiales à adopter pour profiter d'une meilleure manière à cette technologie.

➢ **Adopter une gestion rigoureuse des clés cryptographiques**

Comme nous l'avons énoncé dans plusieurs parties de ce travail, la sécurité des systèmes utilisant les VC et DID repose fortement sur la gestion des clés cryptographiques. Pour se faire, nous recommandons de :

✓ **Générer régulièrement de nouvelles clés**

Cette pratique permet de limiter le temps de vie des clés afin de réduire l'impact d'éventuelles compromissions.

✓ **Utiliser un matériel sécurisé**

Le stockage des clés privées dans des modules de sécurité matériels (HSM) ou des dispositifs de gestion des clés empêche à des accès non autoriser.

✓ **Suivre les meilleures pratiques**

Des ressources comme le NIST SP 800-57 fournissent des recommandations sur la gestion des clés (NIST, 2020). [167]

➢ **Configurer l'authentification multi-facteurs (MFA)**

L'activation de l'authentification multi-facteurs est essentielle pour renforcer la sécurité des comptes :

✓ **Utiliser des méthodes variées**

Il faut intégrer des facteurs basés sur quelque chose que l'utilisateur connaît (mot de passe), possède (téléphone mobile, application d'authentification) et est (biométrie).

- ✓ **Configurer des politiques adaptées**

Microsoft Entra permet de créer des politique d'accès conditionnel qui exigent la MFA selon le niveau de risque détecté.

- ✓ **Éduquer les utilisateurs**

Fournir une formation régulière aux utilisateurs sur l'importance de la MFA et comment l'utiliser correctement.

- ➢ **Utiliser les normes et protocoles de la fondation DID et VC**

Respecter les standards est fondamental pour garantir l'interopérabilité :

- ✓ **S'appuyer sur les spécifications W3C**

La Fondation W3C publie des spécifications et des normes pour les DID et les VC, ce qui garantit une adoption large et interopérable.

- ✓ **Conformité à GDPR**

S'assurer que l'utilisation des VC respecte les régulations en matière de protection des données personnel même sans être en Europe, le respect de ces règles ne peut être que bénéfique.

- ✓ **Suivre les évolutions des normes**

Participer à des forums et des groupes de travail ou de mettre des veilles technologiques pour rester à jour sur les évolutions des normes.

- ➢ **Optimiser la gestion des identités avec les VC**

Les VC doivent être intégrés dans une stratégie de gestion des identités cohérente :

- ✓ **Assurer une gouvernance claire**

Définir des politiques et des processus pour l'émission, le stockage et la révocation des VC surtout dans les africains.

- ✓ **Évaluation des entités émettrices**

Une évaluation est nécessaire pour s'assurer que les VC proviennent de sources fiables et revue, garantissant leur véracité.

- ✓ **Mettre en place des mécanismes de révocation**

Il faut garantir que les informations de l'identité soient à jour et que les données non valides soient rapidement supprimées ou révoquées.

- ➢ **Surveiller et auditer l'utilisation des VC et DID**

La surveillance et l'audit sont essentiels pour garantir la sécurité et la conformité :

- ✓ **Configurer des journaux d'audit**

Cela permet d'utiliser les fonctionnalités d'audit de Microsoft Entra pour tracer toutes les transactions liées aux VC et DID.

- ✓ **Analyser régulièrement les rapports**

Mettre en place des mécanismes d'analyse pour identifier des comportements suspects ou non conformes.

- ✓ **Effectuer des audits de sécurité périodiques**

Cela vous aide à évaluer l'efficacité de votre implémentation et à identifier des domaines d'amélioration.

En appliquant ces recommandations, nous pouvons garantir non seulement une sécurité mais également une gestion des identités efficace et une expérience utilisateur améliorée lors de l'utilisation de Microsoft Entra dans le cadre des VC et DID.

6.5 Conclusion

Les recommandations que nous avons proposées dans ce chapitre visent à lever les obstacles identifiés précédemment en mettant l'accent sur des solutions pratiques et adaptées aux différents contextes d'utilisation. Ces stratégies ne sont pas seulement nécessaires pour favoriser l'adoption de ces technologies, mais également pour maximiser leurs bénéfices dans des environnements numériques de plus en plus exigeants. Dans la conclusion générale, nous allons essayer de clôturer cette analyse en synthétisant les principaux résultats et en proposant des pistes pour le développement futur des VC et DID, notamment dans des contextes spécifiques comme l'apport que peut avoir l'IA pour ces technologies.

7. Conclusion générale et perspectives

Dans cette section, nous allons résumer les principaux résultats de l'étude que nous avons eu à aborder dans les différentes sections abordé en mettant en lumière les bénéfices et les défis associés aux références vérifiables et aux identifiants distribués dans le domaine de la gestion sécurisée des identités numériques. Elle propose également des perspectives d'évolution avec un accent particulier sur l'application de ces technologies pour faciliter la transition des étudiants entre les universités et les entreprises. Ces perspectives visent à renforcer la sécurité et l'efficacité des processus tout en garantissant un contrôle accru des utilisateurs sur leurs données personnelles.

7.1 Conclusion

Lors de notre étude, nous avons mis en évidence l'importance des VC et des DID dans l'amélioration de la gestion des identités numériques. Les technologies traditionnelles telles que les mots de passe et les certificats centralisés ont montré leurs limites en matière de sécurité et de gestion des données personnelles. Dans ce contexte, les technologies basées sur les VC et DID se présentent comme des solutions novatrices pour renforcer la sécurité et l'autonomie des utilisateurs.

Les références vérifiables permettent de créer des attestations numériques sécurisées et vérifiables qui réduisent les risques de falsification et facilitent la vérification des informations sans divulguer plus de données que ce qui est nécessaire. Les DID, quant à eux, offrent une approche décentralisée pour l'identification numérique, permettant aux utilisateurs de posséder et de gérer leurs identités sans dépendre d'une autorité centralisée. Cette autonomie accrue améliore la confidentialité et le contrôle des données tout en réduisant les risques associés aux points de défaillance uniques.

Parmi les avantages que nous avons identifiés au cours de l'étude figurent :

- **Sécurité renforcé**

Les mécanismes cryptographiques utilisés pour les VC garantissent l'intégrité et l'authenticité des données, ce qui réduit les risques de fraude et d'usurpation d'identité.

- **Vérifiabilité des informations**

Les informations peuvent être vérifiées de manière sécurisée, sans nécessiter un contact direct avec l'émetteur, ce qui simplifie les processus administratifs et réduit les coûts.

- **Contrôle utilisateur et confidentialité**

Les utilisateurs disposent d'un contrôle total sur leurs données avec la possibilité de partager uniquement les informations nécessaires à un moment donné, grâce à des techniques de divulgation sélective.

- **Décentralisation**

Les DID permettent une gestion plus flexible et moins centralisée des identités, éliminant les dépendances aux fournisseurs d'identité traditionnels et offrant une forte résilience aux systèmes.

Cependant, nous avons aussi vu que l'adoption de ces technologies n'est pas sans défis. L'étude a révélé plusieurs obstacles, notamment :

- **Interopérabilité**

Il existe encore des défis techniques à relever pour assurer l'interopérabilité des différents systèmes et standards utilisés pour les VC et DID.

- **Réglementation**

La mise en œuvre de ces technologies doit s'accompagner d'une conformité avec les cadres juridiques et réglementaires existants tels que le RGPD afin de garantir la protection des droits des utilisateurs.

- **Sensibilisation et adoption**

La transition vers des systèmes basés sur les VC et DID nécessite une sensibilisation des utilisateurs et des organisations, ainsi qu'une formation appropriée pour les acteurs concernés.

En somme, les références vérifiables et les identifiants distribués offrent une approche innovante pour la gestion des identités numériques, avec le potentiel de transformer les pratiques actuelles en améliorant la sécurité, la vérifiabilité et le contrôle des utilisateurs. Les recommandations formulées dans ce mémoire visent à surmonter les défis identifiés et à encourager l'adoption de ces technologies pour répondre aux besoins croissants en matière de sécurité des identités en ligne.

7.2 Perspectives

Pour un avenir meilleur, les VC et les DID offrent des possibilités intéressantes pour améliorer la gestion des identités numériques. Une des perspectives clés est d'exploiter les capacités de l'intelligence artificielle pour améliorer la sécurité, l'efficacité et l'automatisation des processus liés à ces technologies tout en garantissant une confidentialité renforcée et une vérification précise des informations.

Références bibliographique et webographie

1. Stratégie de sécurité Zero Trust dans un environnement de cloud communautaire : https://theses.hal.science/tel-04500625v1/document
2. DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust : https://dl.acm.org/doi/pdf/10.1145/3446983.3446992
3. Design Patterns for Blockchain-based Self-Sovereign Identity : https://arxiv.org/pdf/2005.12112
4. The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity : https://arxiv.org/pdf/1711.07127
5. Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution : https://arxiv.org/pdf/1712.01767
6. A Survey on Essential Components of a Self-Sovereign Identity : https://arxiv.org/pdf/1807.06346
7. Blockchain et identification numérique : https://hal.science/hal-03319516v1/document
8. https://bu.unistra.fr/opac/resource/arxivorg/BUS1885578
9. https://bib.ulb.be/fr/support/boite-a-outils/google-scholar#:~:text=Google%20Scholar%20est%20un%20outil,la%20collaboration%20de%20nombreuses%20universit%C3%A9s.
10. La Blockchain pour la Sécurisation des E-livrets scolaires : https://rivieresdusud.uasz.sn/bitstream/handle/123456789/1803/bakhoum_memoire_2019.pdf?sequence=1&isAllowed=y
11. Cryptographie à Base de Politiques: Théorie et Applications : https://www.eurecom.edu/publication/2122/download/ce-baggwa-061208.pdf
12. Blockchain pour suivi et sécurisation des produits de santé : http://archives.univ-biskra.dz/bitstream/123456789/18916/1/AZIZI_MIYADA.pdf
13. GESTION DE LA SÉCURITÉ EN E-SANTÉ : SÉCURITÉ DES COMMUNICATIONS, SÉCURITÉ DU TRAITEMENT DES DONNÉES ET RESPECT DE LA VIE PRIVÉE DES PATIENTS : https://books.google.sn/books?hl=fr&lr=&id=XeX6EAAAQBAJ&oi=fnd&pg=PA107&dq=Blockchain+pour+suivi+et+s%C3%A9curisation+des++produits+de+sant%C3%A9+&ots=AMgRjJ1wpp&sig=XGD9MXsp565N_5BglD1zNL6euZg&redir_esc=y#v=onepage&q&f=false
14. De la Sécurité à la E-Confiance basée sur la Cryptographie à Seuil dans les Réseaux sans fil Ad hoc : http://eprints.univ-batna2.dz/206/
15. Utilisation de la blockchain dans le système de santé électronique : https://corpus.ulaval.ca/server/api/core/bitstreams/924f0150-275c-48b5-bb22-5e24fdcd2ba7/content
16. Échange de clés Diffie-Hellman : https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman
17. Architecture décentralisée : définition et fonctionnement : https://www.malekal.com/architecture-decentralisee/
18. Qu'est-ce qu'un réseau centralisé et un réseau décentralisé ? : https://www.ninjaone.com/fr/it-hub/endpoint-management/reseau-centralise-reseau-decentralise/
19. Réseaux décentralisés : comment ils fonctionnent et quels avantages ils ont : Réseaux décentralisés : comment fonctionnent-ils et quels sont leurs avantages | ITIGIQUE (itigic.com)

20. La technologie Blockchain et les registres distribués (DLT) : La technologie Blockchain et les registres distribués (DLT) - Actualité Informatique (actualiteinformatique.fr)
21. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines : https://www.mdpi.com/1999-5903/13/3/62
22. Technologie du registre distribué : tout savoir sur ce système numérique : Technologie du registre distribué : que savoir sur ce système numérique ? (objetconnecte.com)
23. Qu'est-ce qu'une chaîne de blocs (blockchain) ? : https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application#
24. Introduction aux Directed Acyclic Graphs (DAG) : un modèle de données révolutionnaire en crypto-monnaie et en informatique : https://www.tokize.com/fr/directed-acyclic-graphs-dag-crypto/
25. Qu'est-ce qu'un DAG ou graphe orienté acyclique ? (Directed Acyclique Graph) : https://coinacademy.fr/academie/dag-directed-acyclic-graph-graphe-acyclique-oriente/
26. Qu'est-ce que la technologie DAG (Directed Acyclic Graph) ? : https://coinacademy.fr/academie/technologie-dag/
27. Définition et principe de la crypto monnaie Holochain (HOT) : https://bitcoinmatin.fr/definitions-des-crypto-monnaies/holochain/
28. Hashgraph vs Blockchain- A Detailed Overview : https://www.solulab.com/hashgraph-vs-blockchain/
29. Hashgraph Vs. Blockchain: Which is Right for Your Business? : https://www.orientsoftware.com/blog/hashgraph-vs-blockchain/#:~:text=Mining%20the%20blockchain%20is%20a,and%20more%20energy%2Defficient%20option.
30. What is Holochain? : https://www.holochain.org/what-holochain/
31. What is Holochain? : https://holo.host/faq/what-is-holochain/
32. La blockchain : une technologie révolutionnaire au-delà des cryptomonnaies : https://lemondenumeriquedemelanie.com/la-blockchain-une-technologie-revolutionnaire-au-dela-des-cryptomonnaies/
33. Hedera / HBAR : https://coinaute.com/fiche-hedera/
34. Holo / HOT : https://coinaute.com/fiche-holo/
35. Tout savoir sur le Self Sovereign Identity : Tout savoir sur le Self Sovereign Identity - LeDroit.Fr
36. Self-Sovereign Identity (SSI) : tout comprendre au concept : Self-Sovereign Identity (SSI) : tout comprendre au concept | Archipels Wallet
37. Qu'est-ce que l'identité auto-souveraine (SSI) et son utilisation : Qu'est-ce que l'identité auto-souveraine (SSI) et son utilisation (informationsecurityasia.com)
38. Comment la blockchain permet de gérer l'identité digitale ? | Croissance & Innovation : https://www.youtube.com/watch?v=jcKtLfBMxT0
39. A privacy-preserving system for data ownership using blockchain and distributed databases : https://arxiv.org/pdf/1810.11655
40. Certifying Provenance of Scientific Datasets with Self-sovereign Identity and Verifiable Credentials : https://arxiv.org/pdf/2004.02796
41. Qu'est-ce que France identité, la nouvelle application gouvernementale d'identité numérique : https://adess-france.fr/conseils-actualites/quest-ce-que-france-identite-numerique/

42. Obtenir son identité numérique certifiée : https://france-identite.gouv.fr/identite-numerique-certifiee/
43. France Identité Gardez la maîtrise de vos données d'identité : https://france-identite.gouv.fr/en-savoir-plus/de-quoi-s-agit-il/
44. Présentation de l'application France Identité : https://www.youtube.com/watch?v=03qgI3WL2_8
45. TOUT SAVOIR sur FRANCE IDENTITÉ (carte d'identité et permis sur smartphone) : https://www.youtube.com/watch?v=yohKY7FNOQg
46. Verifiable Credentials Data Model v1.1 : https://www.w3.org/TR/vc-data-model/
47. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems : A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (nist.gov)
48. DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust : https://dl.acm.org/doi/fullHtml/10.1145/3446983.3446992
49. Verifiable Credentials Data Model v2.0 : https://w3c.github.io/vc-data-model/
50. Identifiants vérifiables : https://fr.wikipedia.org/wiki/Identifiants_v%C3%A9rifiables
51. Comprendre le SSI : les VCs et les DIDs : https://www.archipels.io/post/comprendre-le-ssi-les-verifiable-credentials-vcs-et-les-decentralized-identifiers-dids
52. Verifiable Credentials Implementation Guidelines 1.0 : https://web.archive.org/web/20220319201909/https://w3c.github.io/vc-imp-guide/
53. What are Verifiable Credentials? : https://didproject.azurewebsites.net/docs/verifiable-credentials.html
54. Verifiable Credentials Data Model v1.1 : https://web.archive.org/web/20220326095443/https://www.w3.org/TR/vc-data-model/
55. Verifiable Credentials Use Cases : https://web.archive.org/web/20220318153134/https://www.w3.org/TR/vc-use-cases/
56. https://web.archive.org/web/20220319201909/https://w3c.github.io/vc-imp-guide/
57. Blockchain : comment fonctionnent les "verifiable credentials" ? : "Verifiable Credentials" : Norme Internationale, Solution Blockchain (bcdiploma.com)
58. An Introduction to Verifiable Credentials : https://web.archive.org/web/20211019160040/https://verifiablecredential.io/learn
59. Decentralized Identifiers (DIDs) v1.0 : https://www.w3.org/TR/did-core/#representations
60. DID Specification Registries : https://www.w3.org/TR/did-spec-registries/#did-methods
61. Qu'est-ce qu'un DID ? Définition et usage : https://www.bcdiploma.com/fr/blog/what-is-a-did-definition-and-uses
62. Qu'est-ce qu'un Identifiant Décentralisé (DID) ? https://www.coinbase.com/fr/learn/wallet/what-is-a-decentralized-identifier-did#How-DIDs-Work
63. JSON Web Signature 2020 : https://w3c-ccg.github.io/lds-jws2020/
64. Decentralized Identity: The Basics of Decentralized Identity : https://techcommunity.microsoft.com/t5/security-compliance-and-identity/decentralized-identity-the-basics-of-decentralized-identity/ba-p/3071980
65. Qu'est-ce que le phishing ? : https://www.fortinet.com/fr/resources/cyberglossary/phishing#:~:text=Le%20phishing%20est%20un%20type,pour%20voler%20des%20informations%20sensibles.

66. A Study of the Scope and Distribution of Phishing : https://www.cybercrimeinfocenter.org/phishing-landscape-2023
67. Le vol d'identité : https://www.ipc.on.ca/sites/default/files/legacy/2016/08/id-theft-f.pdf
68. LE VOL D'IDENTITÉ : https://www.sq.gouv.qc.ca/wp-content/uploads/2016/11/2016-03-01_001_vol-d-identite1.pdf
69. Cameron apprend à réutiliser les mots de passe : https://support.microsoft.com/fr-fr/topic/cameron-apprend-%C3%A0-r%C3%A9utiliser-les-mots-de-passe-6f5b6951-e524-450c-9b2d-2f69d83ad496
70. Réutilisation des mots de passe : un danger caché que vous ne devez pas ignorer : https://specopssoft.com/fr/blog/reutilisation-des-mots-de-passe-un-danger-cache/
71. Rapport sur les enquêtes sur les violations de données 2024 : https://www.verizon.com/business/resources/reports/dbir/?cjdata=MXxOfDB8WXww&CMP=afc_m_p_cj_na_ot_2022_99&SID=tuid:3110735F072C6FB112E3611D064E6E85&cjevent=d7d289ab4e5f11ee82b857e30a82b838&vendorid=CJM&PID=100357191&AID=11365093
72. Qu'est-ce que la réutilisation des mots de passe ? : https://layerxsecurity.com/fr/glossary/what-is-password-reuse/#:~:text=La%20r%C3%A9utilisation%20des%20mots%20de%20passe%20fait%20r%C3%A9f%C3%A9rence%20%C3%A0%20la,comptes%2C%20plateformes%20ou%20services%20diff%C3%A9rents.
73. Security : https://www.techrepublic.com/topic/security/#:~:text=%22While%20people%20may%20use%20different%20usernames%20for%20their,using%20their%20personal%20passwords%20at%20work%2C%22%20Harmer%20said.
74. Cybercriminalité : un état des lieux pour l'année 2023 : https://www.vie-publique.fr/en-bref/295063-cybercriminalite-bilan-de-lannee-2023
75. Plus de 80 statistiques sur les mots de passe pour inspirer de meilleures pratiques de sécurité : https://secureframe.com/fr-fr/blog/password-statistics
76. Gestion décentralisée des documents médicaux des patients : https://shs.cairn.info/revue-document-numerique-2009-3-page-23?lang=fr#s1n2
77. ISO/CEI 24760-3:2016 : https://www.iso.org/standard/57916.html
78. Digitalisez vos certificats, diplômes et micro-certifications : https://www.bcdiploma.com/fr
79. BCDiploma : https://www.auf.org/wp-content/uploads/2018/10/bcdiploma_-_auf-1.pdf
80. La certification de vos diplômes sur la blockchain : https://www.auf.org/maghreb/nouvelles/appels-a-candidatures/certification-de-vos-diplomes-blockchain/
81. BCdiploma : https://fr.wikipedia.org/wiki/BCdiploma#Technologie
82. Medicalchain-Whitepaper : https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf
83. Own Your Health : https://medicalchain.com/en/
84. Trust Stamp leveraging IP portfolio to expand implementation scope : https://www.biometricupdate.com/202407/trust-stamp-leveraging-ip-portfolio-to-expand-implementation-scope
85. Secure, Private & Trusted Identity : https://truststamp.ai/
86. BIOMETRIC DATA & DIGITAL IDENTITY : file:///C:/Users/AFRICA%20TECH/Downloads/Privacy-Protecting-Power-of-IT2-September-2020-6.pdf

87. C’est quoi un token ERC20 sur Ethereum ? : https://coinacademy.fr/academie/cest-quoi-un-token-erc20-sur-ethereum/
88. Qu'est-ce qu'un token ERC20 ? : https://cryptoast.fr/qu-est-ce-que-token-erc20/
89. Quelles sont les solutions de niveau 2 dans la blockchain ? : https://metlabs.io/fr/quelles-sont-les-solutions-de-niveau-2-dans-la-blockchain/
90. Le trilemme de l’évolutivité : les solutions de layer 1 et de layer 2 : https://academy.youngplatform.com/fr/blockchain/evolutivite-solutions-couche-2/
91. Quelle est la différence entre la fragmentation et le sharding ? : https://www.quora.com/What-is-the-difference-between-fragmentation-and-sharding
92. PoW et PoS combinés : Les avantages d'une approche hybride : https://w3r.one/fr/blog/blockchain-web3/consensus/mecanismes-hybrides/pow-et-pos-combines-avantages-approche-hybride
93. Qu'est-ce que la preuve d'enjeu ou proof-of-stake (PoS) ? : https://cryptoast.fr/qu-est-ce-que-pos-proof-of-stake/
94. Lisez le pont inter-chaînes dans un article : Nouvelle infrastructure sous la prospérité du multi-chaîne (Traduit par google à partie du chinois) : https://www.okx.com/zh-hans/learn/a-cross-chain-bridge#:~:text=%E8%B7%A8%E9%93%BE%E6%A1%A5%E8%A7%A3%E5%86%B3%E7%9A%84%E6%98%AF%E7%94%A8%E6%88%B7%E8%B5%84
95. DID : Créer des identités blockchain conviviales, sécurisées et interopérables : https://www.binance.com/fr/square/post/1073118
96. Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l’identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : <P (europa.eu)
97. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
98. Hyperledger Indy : https://hyperledger-indy.readthedocs.io/en/latest/
99. Technologies numériques avancées : https://digital-strategy.ec.europa.eu/fr/policies/advanced-digital-technologies
100. The Value of Digital Transformation : https://hbr.org/2023/07/the-value-of-digital-transformation
101. Data Protection Laws of the World : https://www.dlapiperdataprotection.com/
102. Together we're building a new identity ecosystem : https://identity.foundation/
103. https://www.youtube.com/@Evernym/videos
104. Identity Decentralized : https://decentralized-id.com/companies/evernym/
105. Blockchain for digital identity and credentials : https://www.ibm.com/blockchain-identity
106. IBM Blockchain : https://www.ibm.com/blockchain
107. Welcome Hyperledger Ursa! : https://www.hyperledger.org/blog/2018/12/04/welcome-hyperledger-ursa
108. Global public registry for DIDs Trust anchor for Verifiable Credentials : https://sovrin.org/
109. Ethereum : https://ethereum.org/fr/
110. IPFS : https://ipfs.tech/

111. Trinsic : https://trinsic.id/
112. Universal Resolver : https://dev.uniresolver.io/ et https://github.com/decentralized-identity/universal-resolver
113. uPort : https://www.uport.me/
114. Hyperledger Aries : https://www.hyperledger.org/projects/aries, https://wiki.hyperledger.org/display/aries, https://aca-py.org/latest/, https://aries-cloud-agent-python.rehttps://sovrin.org/adthedocs.io/en/latest/
115. DIDComm : https://didcomm.org/, https://github.com/hyperledger/aries-rfcs/blob/main/features/0023-did-comm/README.md
116. OAuth 2.0 : https://oauth.net/2/
117. OpenID Connect : https://openid.net/
118. JSON for Linking Data : https://json-ld.org/
119. Bitcoin et identité auto-souveraine (ION + BTCR) : https://decentralized-id.com/blockchain/bitcoin/
120. ION – We Have Liftoff! : https://techcommunity.microsoft.com/t5/security-compliance-and-identity/ion-we-have-liftoff/ba-p/1441555
121. Qu'est-ce qu'un HSM basé sur le cloud ? : https://www.entrust.com/fr/resources/learn/what-is-cloud-hsm
122. AWS CloudHSM : https://aws.amazon.com/fr/cloudhsm/
123. Revocation registry : https://sovrin.org/revocation-registry/, https://findynet.fi/en/for-customers/revocation-registry/
124. BLOCKCHAIN FOR SOCIAL IMPACT MOVING BEYOND THE HYPE : https://unidosenred.org/wp-content/uploads/2022/06/study-blockchain-impact-moving-beyond-hype.pdf
125. Developing a complete architecture for Internet Digital Trust. And a better Internet for everyone. : https://trustoverip.org/
126. The internet's next step: The era of digital credentials : https://www.ibm.com/blog/the-internets-next-step-the-era-of-digital-credentials/
127. Evernym : https://www.evernym.com/
128. Manifesto for Agile Software Development : https://agilemanifesto.org/
129. NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management : https://pages.nist.gov/800-63-3/sp800-63b.html
130. JSON Web Key (JWK) : https://datatracker.ietf.org/doc/html/rfc7517
131. DIDComm Messaging v2.x Editor's Draft : https://identity.foundation/didcomm-messaging/spec/
132. Credentials Community Group : https://www.w3.org/community/credentials/
133. Explore the world of cyber security : https://owasp.org/
134. Sovrin Foundation : https://sovrin.org/
135. Hyperledger Aries : https://www.lfdecentralizedtrust.org/projects/aries
136. https://github.com/hyperledger/aries/blob/main/collateral/Hyperledger_Aries_Logo_Color.jpg
137. Veramo : https://veramo.io/
138. Introducing Veramo : https://medium.com/uport/introducing-veramo-5a960bf2a5fe
139. Spruce Systems DIDKit : https://github.com/spruceid/didkit
140. HashiCorp Vault : https://www.vaultproject.io/

141. Hyperledger Indy : https://github.com/hyperledger-archives/indy-sdk
142. Zokrates : https://zokrates.github.io/
143. Texte complet du RGPD - Article 25 : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR
144. EBSI – European Blockchain Services Infrastructure : https://www.eqar.eu/qa-results/synergies/european-blockchain-service-infrastructure-ebsi/
145. Projets de recherche : https://lern.univ-rouen.fr/projets-de-recherche
146. Algortihmes pour des Blockchains plus efficaces – BASE-BLOC : https://anr.fr/Projet-ANR-22-CE25-0012
147. Infrastructure de données blockchain équitable et modulaire pour une science et une société ouvertes – FairOnChain : https://anr.fr/fr/projets-finances-et-impact/projets-finances/projet/funded/project/anr-23-chro-0002/?tx_anrprojects_funded%5Bcontroller%5D=Funded&cHash=fbc7ccdc1d8af77e735ae19466273629
148. FCA Sandbox : https://www.fca.org.uk/firms/innovation/regulatory-sandbox
149. EU Blockchain Observatory & Forum : https://blockchain-observatory.ec.europa.eu/index_en
150. Horizon 2020 : https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en
151. https://www.edpb.europa.eu/edpb_en
152. European Blockchain Partnership : https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership
153. Innovative Solutions for Safe Travel : https://www.evernym.com/
154. Alastria, Blockchain Ecosystem : https://www.techtitute.com/sn/enseignants/alastria-blockchain-ecosystem
155. Qu'est-ce que Microsoft Entra ? : https://learn.microsoft.com/fr-fr/entra/fundamentals/what-is-entra
156. Que sont les identités de charge de travail ? : https://learn.microsoft.com/fr-fr/entra/workload-id/workload-identities-overview
157. Quoi de neuf dans Microsoft Entra ID ? : https://learn.microsoft.com/fr-fr/entra/fundamentals/whats-new
158. Historique de publication des versions de Microsoft Entra Connect : https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/reference-connect-version-history
159. Comparer Microsoft Entra ID et Okta : https://www.g2.com/compare/microsoft-entra-id-vs-okta
160. Normes prises en charge par Vérification d'identité Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/verified-id/verifiable-credentials-standards
161. Présentation de la vérification d'identité Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/verified-id/decentralized-identifier-overview
162. Qu'est-ce que l'architecture Microsoft Entra ? : https://learn.microsoft.com/fr-fr/entra/architecture/architecture
163. Configuration rapide de l'ID vérifié Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/verified-id/verifiable-credentials-configure-tenant-quick
164. Configuration avancée de la Vérification d'identité Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/verified-id/verifiable-credentials-configure-tenant

165. Documentation Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/
166. Blog Microsoft Entra : https://techcommunity.microsoft.com/t5/microsoft-entra-blog/bg-p/Identity
167. Recommendation for Key Management: Part 1 – General : https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final#:~:text=Part%201%20provides%20general%20guidance,type%20of%20key%20and%20other
168. À propos de Christopher Allen : https://www.lifewithalacrity.com/about/
169. Centre d'administration Microsoft Entra : https://entra.microsoft.com/
170. Découverte Microsoft Entra - Partie 1 : https://www.youtube.com/watch?v=IKCfld69lpc
171. Qu'est-ce que la gestion des autorisations Microsoft Entra : https://learn.microsoft.com/fr-fr/entra/permissions-management/overview
172. Émettre des informations d'identification Vérification d'identité Microsoft Entra à partir d'une application : https://learn.microsoft.com/fr-fr/entra/verified-id/verifiable-credentials-configure-issuer
173. Qu'est-ce que Microsoft Entra ID Governance ? : https://learn.microsoft.com/fr-fr/entra/id-governance/identity-governance-overview
174. Six enseignements du Gartner® Hype Cycle™ pour l'identité numérique, 2022. : https://www.keyfactor.com/fr/blog/six-takeaways-from-gartner-hype-cycle-for-digital-identity/
175. Azure Active Directory est devenu Microsoft Entra ID : https://www.microsoft.com/fr-fr/security/business/identity-access/microsoft-entra-id