République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Seddik Benyahia de Jijel
Faculté des Sciences Exactes et informatique
Département d'Informatique

Mémoire de fin d'étude

pour l'obtention du diplôme Master de Recherche en Informatique

Option : *Informatique Légale et Multimédia*

Thème

Combinaison de blockchain et biométrie pour la gestion des identités

Présenté par :
ZABAT Anis

Encadré par:
Dr.MAHAMDIOUA Meriama

Promotion : 2020.

RÉSUMÉ

La technologie Blockchain est une nouvelle technologie qui intègre la décentralisation, le calcul distribué, le chiffrement asymétrique, le hachage, l'horodatage et le principe de consensus. Elle permet de stocker et de transmettre les informations de manière sécurisée, fiable et transparente. Dans notre mémoire, nous avons proposé de combiner la technologie blockchain et système biométrique, afin de sécuriser le stockage des modèles biométriques, ainsi que le canal entre la base des templates et le module de calcul de similarité. Nous avons proposé deux solutions, la première basée sur le développement d'une blockchain locale et la deuxième sur l'utilisation d'un smart contract sur la blockchain publique Ethereum.

Mot clés :blockchain, système biométrique, sécurisation, smart contract, Ethereum.

ABSTRACT

Blockchain technology is a new technology that integrates decentralization, distributed computing, asymmetric encryption, hashing, time stamping and the principle of consensus. It allows information to be stored and transmitted in a secure, reliable and transparent manner. In our thesis, we proposed to combine blockchain technology and biometric system, in order to secure the storage of biometric models, as well as the channel between the template base and the similarity calculation module. We proposed two solutions, the first based on the development of a local blockchain and the second on the use of a smart contract on the public Ethereum blockchain.

Key words : blockchain, biometric system, security, smart contract, Ethereum.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

ABRÉVIATIONS

ADN	**A**cide **D**esoxyribo**N**ucleique
BTC	**B**itcoin
CMC	**C**umulative **M**atch **S**core**C**urves
CPU	**C**entral **P**rocessing **U**nit
DAO	**D**ecentralized **A**utonomous **O**rganization
DPOS	**D**elegated **P**roof **O**f **S**take
EER	**E**qual **E**rror **R**ate
ETH	**E**thereum
FAR	**F**alse **A**cceptance **R**ate
FNIR	**F**alse **N**egative **I**dentification **R**ate
FRR	**F**alse **R**ecognition **R**ate
IR	**I**dentification **R**ate
IPFS	**I**nter**P**lanetary **F**ile **S**ystem
NFS	**N**etwork **F**ile **S**ystem
P2P	**P**eer **T**o **P**eer
PBFT	**P**ratical **B**yzantine **F**ault **T**olerance
PoA	**P**roof **o**f **A**ctivity
PoS	**P**roof **o**f **S**take
PoW	**P**roof **o**f **W**ork
ROC	**R**eceiver **O**perating **C**haracteristics
SOC	**S**tore-**O**n-**C**ard
SSS	**S**hamir's **S**ecret **S**haring
TTP	**T**rusted **T**hird **P**arties
USB	**U**niversal **S**erial **B**us
ZKP	**Z**ero **K**nowledge **P**roof

INTRODUCTION GÉNÉRALE

Dans ces dernières années, le monde a connu une révolution dans le domaine de la sécurité de l'information. On pense que cette révolution prendra plus d'attention dans les années à venir. En fait, la sécurité des systèmes d'information est devenue un domaine de recherche très intéressent. Dans un concours de sécurité qui n'a jamais été gagné, on sait que les mots de passe sont faibles et faciles à piratés, de sorte que les organisations passent maintenant à l'étape suivante et cherchent à utiliser nos données biométriques physiologiques et / ou comportementales pour la gestion des identités. Cette technique est de plus en plus présente dans la vie quotidienne : au traitement des opérations bancaires, l'accès à certains endroits militaires ou industriels, etc. Comme rien de ce qui constitue notre vie numérique n'est totalement dépourvu de failles, les systèmes biométriques sont aussi vulnérables à des différentes attaques. Ces derniers peuvent dégrader considérablement leurs fonctionnalités, et la sécurité de ces systèmes devient une vraie nécessité et aussi un grand défi. Dans la littérature, les techniques de sécurité des données biométriques existent ne rependent pas aux exigences de domaine. Récemment, une nouvelle technologie a été proposée comme solution, à savoir blockchain ou chaine de blocs.

Au début, la technologie blockchain a été proposée et déployée afin de permettre d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière, en utilisant le crypto-monnaie « bitcoin ». Intégrant plusieurs techniques telles que la décentralisation, le calcul distribué, le chiffrement asymétrique, le hachage, l'horodatage et algorithme de consensus, cette technologie commence à être utilisée pour sécuriser d'autre domaine d'application.

Cependant, la recherche sur la manière dont la blockchain peut être utilisée dans la gestion des identités est encore très récente. Dans notre mémoire, nous essayons de combiner un système biométrique et la technologie blockchain afin de proposer un sys-

tème sécurisé, dont les points de sécurisation ciblés sont : la modification des templates et l'interception de canal (entre la base de données et le module de calcul de similarité). Dans les systèmes biométriques, toute altération dans la base des templates provoque un très grand risque, de telle manière, une attaque sur ce point du système peut empêcher un utilisateur légitime d'y accéder ou d'autoriser un imposteur. D'autre côté, l'interception de canal permet un accès avec modification des informations transmises sur la voie de communication avec l'intention de détruire les messages, de les modifier, d'insérer des nouveaux messages, de provoquer un décalage dans le temps ou la rupture dans la diffusion des messages.

Pour résoudre ces points de compromission, on a proposé deux solutions, la première est de développer un Blockchain privée et combiner son fonctionnement avec celui d'un système biométrique, et la deuxième sert à l'utilisation d'une smart contract sur la blockchain public « Ethereum ». L'idée principale de notre solution pour la sécurisation est basée sur les caractéristiques de blockchain elle-même qui garde trace de tout accès au réseau d'un côté, et d'autre côté d'utiliser la technique de l'arbre de Merkle. Cela permet d'enregistrer les templates d'une façon sécurisée dans un arbre de Merkle, et de détecter toute modification illégale.

Notre mémoire est organisé comme suit : le premier chapitre présente les systèmes biométriques et leur sécurisation. Dans le deuxième chapitre, nous présentons la technologie blockchain. Le troisième chapitre explique comment pouvons combiner les deux technologies blockchain et biométrie pour la gestion des identités. Le quatrième chapitre expose notre proposition et nos solutions développées. Notre mémoire est enfin terminé par une conclusion générale.

CHAPITRE 1

DONNÉES BIOMÉTRIQUES ET LEUR SÉCURISATION

1 Introduction

La biométrie est l'utilisation de la physiologie et / ou du comportement pour déterminer ou vérifier l'identité des individus. Malgré les avantages de ces systèmes biométriques par rapport aux systèmes d'authentification traditionnels qui utilisent des mots de passe et des cartes d'identité, ils sont toujours vulnérables à des limitations spécifiques qui peuvent dégrader considérablement leurs fonctionnalités.

Dans ce chapitre, nous décrierons, la notion de la biométrie, en parlant des modalités biométriques, d'architecture des systèmes biométriques, des mesures de performance d'un système biométrique et en terminant par une description de la sécurité des systèmes biométriques.

2 Définition

La biométrie désigne une technique d'identification et d'authentification qui consiste à transformer une caractéristique biologique, morphologique ou comportementale en une clé d'identificateur unique. Son objectif est d'attester l'unicité d'une personne à partir de la mesure d'une partie inchangeable ou immaitrisable de son corps [1] . Autrement dit, c'est une reconnaissance automatisée des individus en fonction de leurs caractéristiques biologiques et comportementales.

Pour que la reconnaissance soit envisageable, fiable et de qualité, les caractéristiques doivent au moins garantir les conditions suivantes [2, 3] :

- **Universelles :** exister chez tous les individus ou la population.

- **Uniques :** permettre de différencier un individu par rapport à un autre.
- **Permanentes ou persistantes :** autoriser l'évolution dans le temps.
- **Enregistrables :** collecter les caractéristiques d'un individu (avec l'accord de celui-ci).
- **Mesurables :** autoriser une comparaison future.
- **Non-reproductibles :** la facilité ou non à falsifier une modalité biométrique.

3 Modalités biométriques

On peut compter un grand nombre de modalités biométriques, qui peuvent être regroupées en trois grandes catégories : physiologique (ou morphologique), comportementale et biologique.

3.1 Physiologique (ou morphologique)

Les biométries morphologiques sont les biométries qui utilisent une partie du corps humain[1]. Cette catégorie regroupe la reconnaissance de :

- **L'empreinte digitale** : ce procédé est le plus répandu et le plus ancien[4]. La donnée de base est le dessin représenté par les crêtes (les lignes dessinés sur la peau) et les vallées (espaces entre les crêtes), et de l'épiderme (jonctions, terminaisons aveugles, croisements). Une empreinte est caractérisée par une centaine de points particuliers portés par les crêtes (appelés minuties), dont un nombre de minuties entre (15 et 20) correctement localisées suffisent pour une identification. Certains modules de reconnaissance d'empreintes vérifient la température du doigt, sa conductivité, les battements de cœur, ainsi que d'autres paramètres biologiques.

FIGURE 1.1 – Empreinte digitale avec crête et vallée marquées

- **L'oreille** : les oreilles, comme d'autre parties du corps, présentent aussi une empreinte unique lorsqu'on les met sous contrainte contre une surface. Ce système se base sur l'identification de la forme et des dimensions de l'oreille externe (pavillon, hélix, tragus, etc..). En effet, même si celles-ci sont uniques, elles grandissent de 0 à 20 ans et au-delà de 50 ans tout en se déformant légèrement.

• **L'iris** : c'est la région annulaire située entre la pupille et le blanc de l'œil. La biométrie par ce trait est la plus récente et efficace. Les motifs de l'iris se forment au cours des deux premières années de la vie et sont stables.

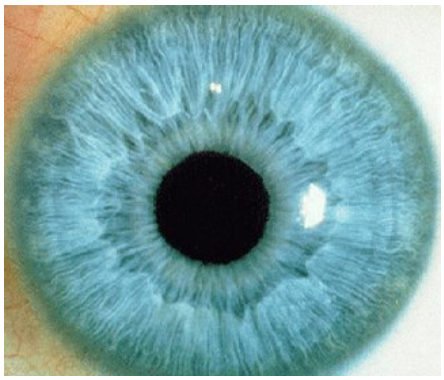

FIGURE 1.2 – Iris

• **La rétine** : elle est très peu utilisée et elle a été moins bien acceptée par le public à cause de la mesure qui doit s'effectuer à très faible distance du capteur [4] (Figure 1.3). Cette technique se base sur le fait que le schéma et le dessin formés par les vaisseaux sanguins de la rétine sont uniques pour chaque personne et assez stables toute la vie[4].

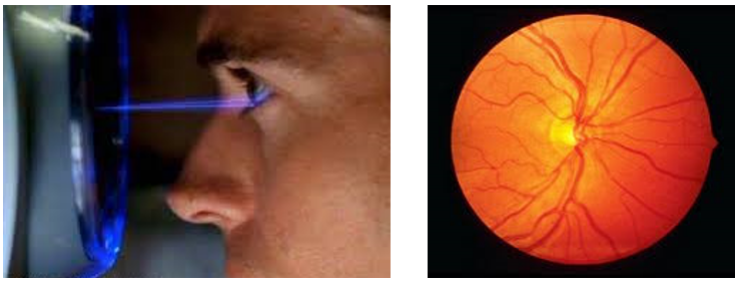

FIGURE 1.3 – Reconnaissance de la rétine

• **Géométrie de la main (hand-scan)** : c'est l'un des mesures biométriques les plus répandus, cela consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) tel que la forme de la main, longueur et largeur des doigts etc. La technologie associée à cela est principalement de l'imagerie infrarouge[4].

• **Visage** : rien n'est plus naturel qu'utiliser le visage pour identifier une personne. C'est la biométrie la plus commune et la plus populaire. Elle implique la métrique des et entre caractéristiques distinctes dans le visage, se fondant moins sur des facteurs d'une nature changeante tels que la coupe des cheveux ou l'utilisation des produits de beauté. Néanmoins, le visage humain est sujet au changement avec le temps et cette réalité demeura un défi pour les systèmes d'identification de visage, comme le changement d'expression, la maladie, la vieillesse et d'autres facteurs normaux. En outre, les

FIGURE 1.4 – Géométrie de la main

facteurs humains et environnement joueront un très grand rôle dans l'efficacité d'un système de reconnaissance faciale.

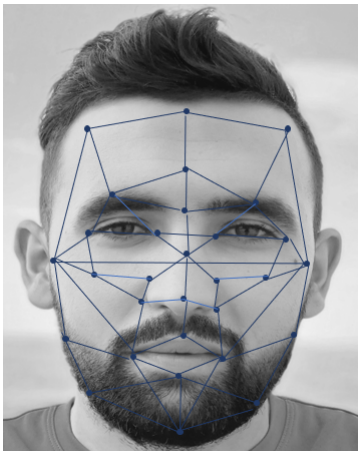

FIGURE 1.5 – Reconnaissance de visage

• **Reconnaissance vocale** : cette technique est très facilement falsifiable, en utilisant un enregistrement. La measure biométrique de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent, et de facteurs comportementaux comme la vitesse et le rythme. Ces éléments ont l'avantage d'être stables dans la vie d'un individu [5].

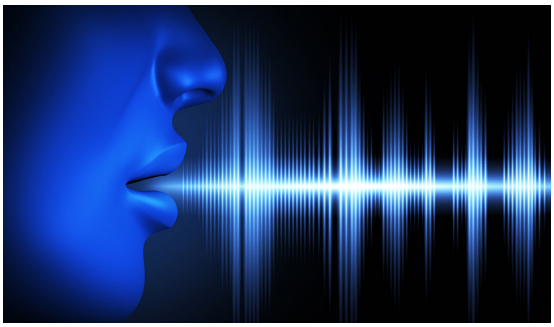

FIGURE 1.6 – Reconnaissance vocale

• **Reconnaissance Palmaire « Palmprints »** : Palmprint est l'une des nouvelles modalités biométriques les plus efficaces et qui s'appuie sur la texture de la paume de la main. Récemment, il a été montré que les lignes principales et les rides dans une image palmprint sont uniques. En général, la plupart des gens ont trois lignes principales : la ligne du cœur, la ligne de tête et la ligne de vie. Les rides sont considérées comme les modèles de ligne les plus fins et les plus irréguliers. Les rides prononcées autour des lignes principales, peuvent également contribuer à la discrimination de palmprint.

FIGURE 1.7 – Palm print

• **Veines** : le motif des veines du doigt ou de la paume de la main sert de critère d'authentification des personnes. Grâce à un scanner infrarouge et une caméra grand angle intégrée, le système capte, en quelquesmillisecondes, la structure veineuse et donc l'identité univoque d'une personne.

FIGURE 1.8 – Reconnaissance des veines

3.2 Comportementale

Cette catégorie utilise un trait personnel du comportement [6]. Se base sur l'analyse de certains comportements d'une personne. Elle concerne l'étude des actions répétitives et usuelles des personnes. On peut compter les suivants :

• **Reconnaissance de la dynamique de la frappe au clavier** : dans cette technique les durées entre frappes, la fréquence des erreurs et la durée de la frappe elle-même sont étudiées de façon statistique. En revanche, cette technologie est tributaire de l'état physique et psychique de la personne qui utilise le clavier. La fatigue, le stress sont autant de facteurs qui feront varier la qualité de la frappe.

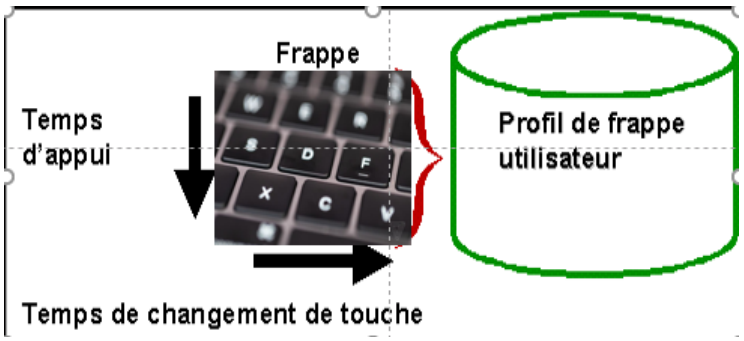

FIGURE 1.9 – Reconnaissance de la dynamique de la frappe au clavier

• **Reconnaissance de la dynamique de signature** : dans ce système d'identification, l'utilisateur doit signer avec un stylo électronique sur une tablette graphique, le système analyse ensuite les variations de vitesse du stylo, ses accélérations et ses pressions sur la tablette[4]. Le point faible de cette technique est qu'un individu qui ne signe pas toujours de la même façon se verra souvent refuser l'accès au système.

FIGURE 1.10 – Reconnaissance de la dynamique de signature

• **Reconnaissance de la démarche** : chaque être humain à une façon très personnelle de démarche qui peut être modélisée en se basant sur plusieurs éléments tels que la vitesse, l'accélération, les mouvements du corps, etc. La marche peut être aussi affectée par plusieurs facteurs comme le choix des chaussures, la surface de marche et les vêtements. Les systèmes de reconnaissance de la démarche, qui sont encore au stade de développement, utilisent le traitement d'image afin de détecter la silhouette humaine et les attributs spatiotemporels associés.

3.3 Biologique

Une biométrie de cette catégorie est basée sur l'identification de traits biologiques particuliers qui, pour toutes personnes, sont uniques et permanents [7]. Ce type de biométrie est très complexe à mettre en œuvre dans un système usuel de reconnaissance et n'est utilisé que dans un cas d'extrême nécessité (ex : Enquête criminelle, test de paternité... etc.) [8]. Cette catégorie regroupe :

• **Reconnaissance de l'ADN** : présent dans les cellules du corps, il est spécifique d'un individu à un autre et permet de l'identifier de manière certaine à partir d'un simple fragment de peau, d'une trace de sang ou d'une goutte de salive. Actuellement, le temps requis pour une analyse et le coût associé à celle-ci restreignent son utilisation dans des domaines autres que celui de l'identification judiciaire. Cependant, ce procédé biométrique fait l'objet de recherche intensive puisqu'il représente la technologie d'identification par excellence avec une marge d'erreur bien en dessous des autres moyens biométriques.

FIGURE 1.11 – Reconnaissance de l'ADN

• **Reconnaissance de l'odeur** : chaque personne dégage une odeur particulière définie par des composantes chimiques. Les systèmes biométriques basés sur cette modalité analysent ces composants pour extraire des données comparatives.

• **Reconnaissance de la thermographie faciale** : une caméra thermique est utilisée pour réaliser un cliché infrarouge du visage, ce qui permet de faire apparaître une répartition de la chaleur unique à chaque individu , voire de cartographier le réseau veineux du visage invisible à l'œil nu. Cette technique permet de distinguer même les vrais jumeaux.

FIGURE 1.12 – Reconnaissance de la thermographie faciale

Remarque
Les modalités biométriques peuvent être regroupées aussi selon la coopération ou non de l'individu [9], on peut trouver :

— **Techniques intrusives** : ces techniques requièrent un contact physique avec l'individu pour l'identifier, tels que les empreintes digitales, la rétine, l'iris ou la forme de la main. Leur usage est généralement mal accepté.

— **Techniques non intrusives** : ces techniques ne requièrent pas la coopération de l'individu en question, leur application peut se faire à distance en utilisant des capteurs qui ne nécessitent pas de contact direct avec l'utilisateur (visage, démarche, ...).

4 Architecture des systèmes biométriques et modes de fonctionnements

Un système biométrique est essentiellement un système de reconnaissance de formes. Ce système fonctionne en acquérant des traits biométriques, construisant des modèles et ensuite en comparant ces modèles par les caractéristiques stockées au préalable dans une base de données pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison [1].

4.1 Architecture des systèmes biométriques

Un système biométrique est composé de 5 modules suivants (voir figure 1.13) :

a. **Module d'acquisition ou capture** : Le module d'acquisition peut mesurer les caractéristiques biométriques d'origine à laide de caméras, lecteurs d'empreintes digitales, caméras de sécurité,...etc. Pour des raisons d'efficacité et de rapidité, des traitements préliminaires ont été effectués à ce niveau [1].

b. **Module de pré-traitement** : Il consiste en un prétraitement et une atténuation du bruit, et par l'application d'une série d'opérations continues (comme le filtrage, la normalisation, etc.) pour faire apparaître des paramètres pertinents et des paramètres utiles [1].

c. **Module d'extraction des caractéristiques** : Sert à représenter les données biométriques prétraitées dans l'étape précédente par de nouvelles représentations ou ce qu'on appelle les modèles. Ces modèles sont obtenus par l'extraction des caractéristiques les plus pertinents. Idéalement, ces modèles devrait être unique à chacun et relativement constante pour les changements intra-classe [1].

d. **Module du stockage** : Qui contient l'ensemble des modèles biométriques des utilisateurs enrôlés du système. En principe, les informations stockées ne sont

jamais les images d'origine, mais un modèle mathématique des éléments qui distinguent l'échantillon biométrique d'un autre [1].

e. **Module de Matching et de décision** : Il s'agit de la dernière étape, ou nous pouvons prendre les décisions appropriées en fonction des exigences de l'application, aprés le calcul de la similitude entre le et la base de référence [1].

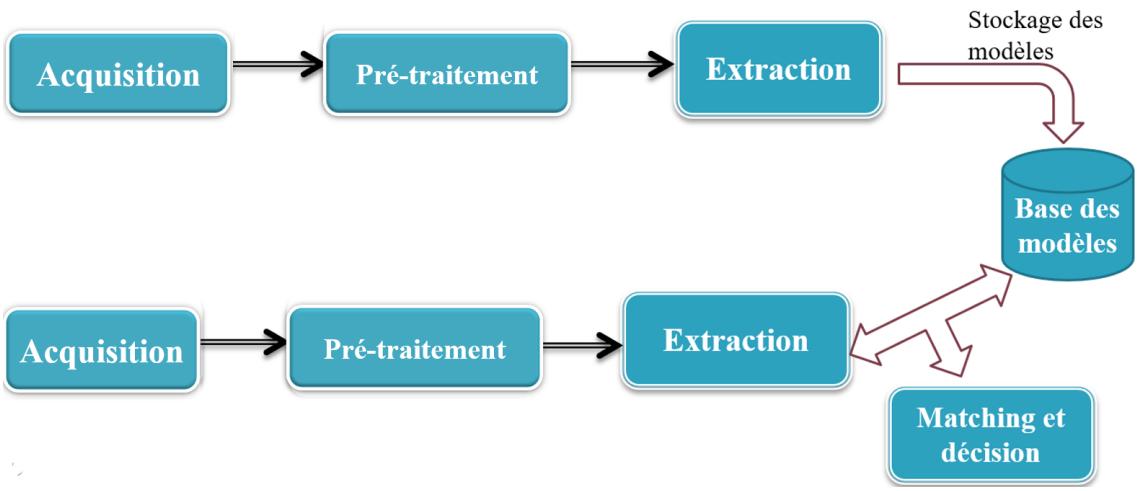

FIGURE 1.13 – Architecture d'un système biométrique

4.2 Modes de fonctionnement

Les systèmes biométriques peuvent fonctionner en deux modes principaux : l'authentification (vérification) et l'identification. Il existe une étape avant les deux modes précédents qui s'appelle "l'enrôlement".

a . **Enrolement**

C'est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données [4] (voir la figure 1.14), cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

b . Authentification

Permet de prouver l'identité revendiquée par un utilisateur(voir la figure 1.15). Le système doit répondre à une question de type : "Suis-je bien la personne que je prétends être ? ". Techniquement, le dispositif vérifie par rapport à un code (identifiant) saisi sur un clavier, ou lu par le passage d'un badge (carte à puce, magnétique, proximité, etc.) que l'échantillon biométrique fourni correspond bien au gabarit désigné par l'identifiant[4].

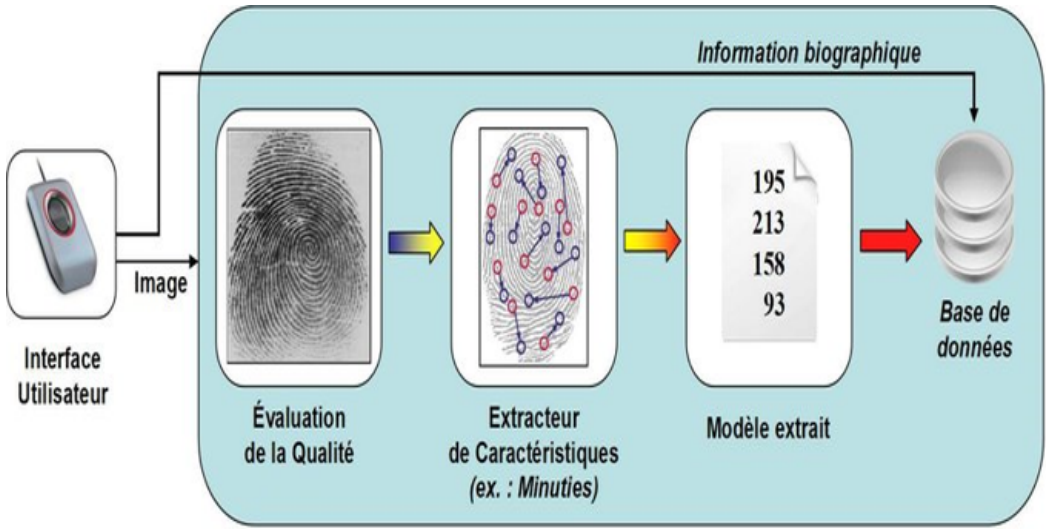

FIGURE 1.14 – Enrolement d'une personne dans un système biométrique [10]

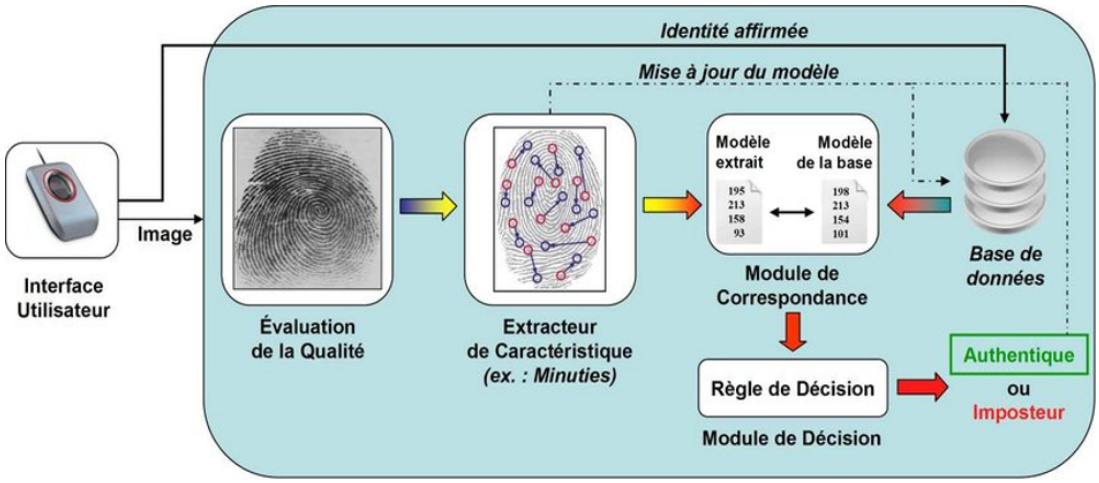

FIGURE 1.15 – Authentification d'un individu dans un système biométrique [10]

c . Identification

Permet de vérifier que l'identité d'un individu qui se présente existe bien dans la base de référence [9]. Le système doit deviner l'identité de la personne. Il répond donc à une question de type "Qui suis-je ? ". À partir de l'échantillon biométrique fourni, le dispositif cherche le gabarit correspondant dans sa base de données[4].

L'identification et l'authentification sont donc deux problèmes différents. L'identification peut être une tâche redoutable lorsque la base de données contient des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type temps réel sur le système. Ces difficultés sont analogues à celles que tend à résoudre les systèmes d'indexation de documents multimédias [11].

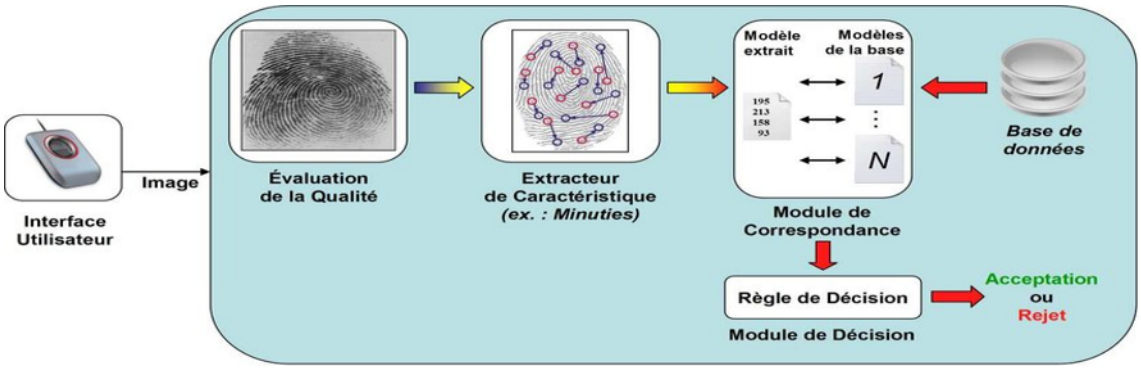

FIGURE 1.16 – Identification d'un individu dans un système biométrique [10]

5 Mesure de performance d'un système biométrique

En biométrie, chaque système est en face de deux populations :

1) Les clients appartenant au système, ceux qui sont autorisés à pénétrer dans la zone protégée.
2) Les imposteurs n'appartenant pas au système, mais généralement qui essayent de rentrer [7].

Pour évaluer les performances d'un système biométrique, plusieurs mesures sont employées . Les exigences des applications sont diverses, et par conséquent un tel système de reconnaissance assurant certains critères est recommandé pour telle ou telle application. Les critères principaux utilisés pour évaluer la performance des systèmes de reconnaissance biométriques sont [12] [13] :

- La fiabilité qui est mesurée par des taux d'erreurs et des courbes de performances.
- L'efficacité (rapidité), qui est mesurée par le temps CPU et l'espace mémoire.
- L'exigence en termes de quantité et de qualité d'exemples d'apprentissage et de test.

Dans la section qui suit, un aperçu sur les mesures d'évaluation des systèmes biométriques est présenté.

5.1 Taux d'erreur

Les systèmes d'authentifications sont généralement évalués par le taux de faux rejets et le taux de fausses acceptations. Tandis que les systèmes d'identifications peuvent être évalués par le taux d'identification, taux de faux-négatif d'identification, taux de faux-positif d'identification, et erreur de l'algorithme de présélection.

5.1.1 Taux d'erreur de systèmes d'authentification

On peut trouver plusieurs métriques pour mesurer la performance d'un système biométrique donné lors d'authentification. Les plus importants sont : le taux de fausse acceptation (TFA), le taux de faux rejet (TFR) et le taux d'erreur égal (TEE) :

a. **TFA (FAR)** : Taux de Fausses Acceptations, ("False Accept Rate" ou FAR) ; ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

$$TFA = \frac{Nombre\,imposteurs\,acceptes\,(FA)}{Nombre\,total\,d'accesimposteur}$$

b. **TFR (FRR)** : Taux de Faux Rejets, ("False Reject Rate" ou FRR). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.

$$TFR = \frac{Nombre\,de\,client\,rejetées}{Nombre\,total\,d'acces\,clients}$$

c. **TEE (EER)** : Taux d'Erreur Egale, ("Equal Error Rate" ou EER). Donne un point sur lequel : TFA = TFR.

$$TEE = \frac{(Nombre\,de\,fausses\,acceptations\,(FA) + Nombre\,de\,faux\,rejets(FR))}{Nombre\,total\,d'acces}$$

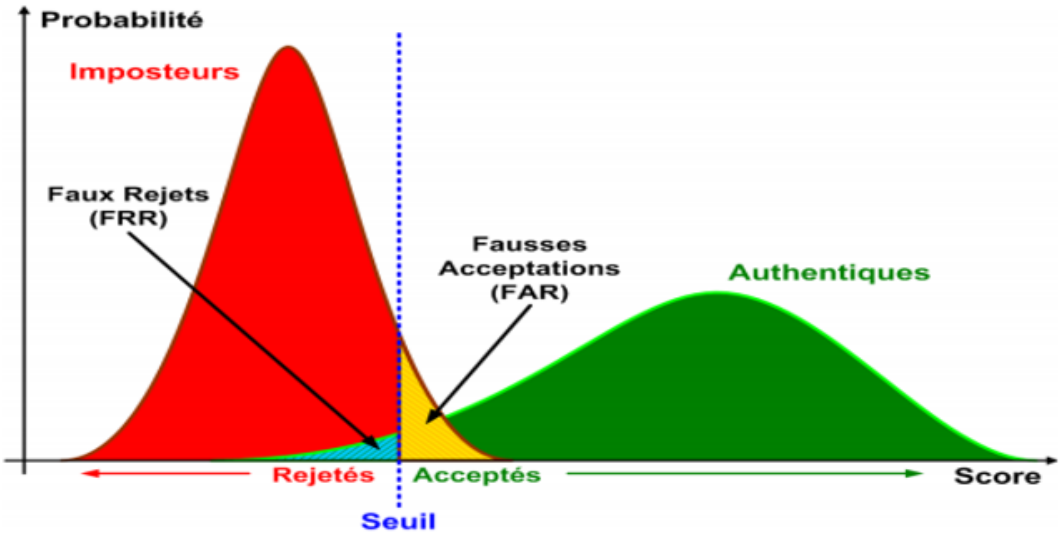

FIGURE 1.17 – Illustration du FRR et FAR
[4]

5.1.2 Taux d'erreur de systèmes d'identification

Dans le cas des systèmes d'identification, on peut trouver les taux suivants :

a. **Taux d'identification (identification rate, IR)** : Appelé aussi « taux de reconnaissance ». Il est donné sous forme de taux d'identification de rang-1(Rank-1). Il présente la proportion de tentatives d'identification authentiques pour lesquelles l'inscription correcte est indiquée dans la liste des identifiants [14] [12].

$$Rang-1 = \frac{N_i}{N}.100\%$$

Où Ni représente le nombre d'images attribuées avec succès à l'identité correcte (bien classées) et N représente le nombre total d'images essayant d'assigner une identité [12].

b. **Taux de faux-négatif d'identification (false-negative identification-error rate, FNIR)** : Proportion de transactions d'identification, par des utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur ne figure pas dans la liste des identifiants retournée [12].

c. **Taux de faux-positif d'identification (false-positive identification-error rate, FPIR)** : Proportion de transactions d'identification, par des utilisateurs non enrôlés dans le système, pour lesquels la liste des identifiants retournée est non vide [12].

d. **Erreur de l'algorithme de présélection (pre-selection error)** : L'algorithme de présélection permet de réduire le nombre de modèles biométriques à comparer avec l'image acquise pendant la phase d'identification. L'erreur de l'algorithme de présélection est l'erreur qui se produit quand le modèle correspondant à la donnée biométrique acquise ne figure pas dans la liste retournée des modèles [12].

5.2 Courbes de performance

Pour évaluer la performance d'un système biométrique par courbes, on peut trouver les courbes suivantes selon le mode de fonctionnement :

a. **Pour l'authentification**

⇒ **Courbe ROC (« Receiver Operating Characteristic » en anglais)** : La courbe ROC (voir figure 1.18) trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe a tendance à suivre la forme de l'indice de référence, plus le système est efficace, c'est-à-dire avec un taux de reconnaissance global élevé.

b. **Pour l'identification**

⇒ **Courbe CMC ("Cumulative Match Characteristic" en anglais)** : La courbe CMC donne le pourcentage de personnes reconnues en fonction d'une

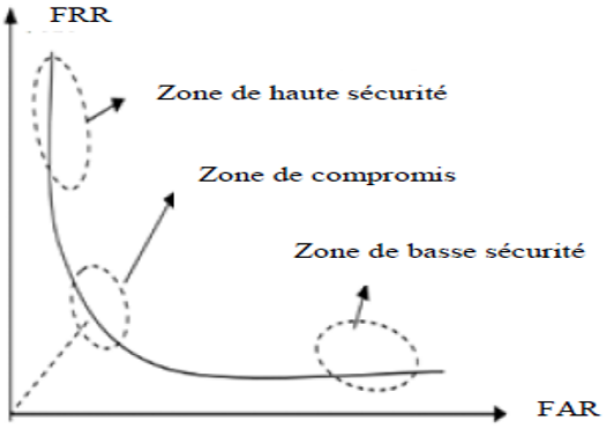

FIGURE 1.18 – Courbe ROC
[4]

variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible. Le taux d'identification de rang-n pour différentes valeurs de n peut être résumé en utilisant la courbe CMC (voir figure 1.19). Où n varie de 1 à N. N est le nombre d'utilisateurs dans la base de données [10].

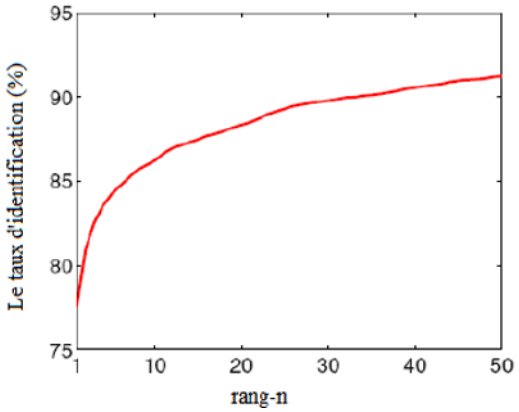

FIGURE 1.19 – Courbe CMC

Malgré les bienfaits d'un système biométrique, il nécessite d'être sécurisé. La section suivante permet d'expliquer ce point, dont on parle de différents cotés telle que les menaces et les vulnérabilités, les problèmes de sécurité de ces systèmes et leurs sécurisation.

6 Sécurité des systèmes biométriques

Au cours de temps et pour plus de sécurité, les systèmes biométriques sont de plus en plus utilisées dans de nombreuses applications. Malgré les avantages des systèmes biométriques par rapport aux systèmes d'authentification traditionnels (pin, mot de passe...), ils restent vulnérables (n'est pas sécurisés à 100%) à des attaques spécifiques. Ces derniers peuvent dégrader considérablement leur fonctionnalité. Dans cette section, nous présentons premièrement des vulnérabilités et menaces liées à l'utilisation des modèles biométriques, puis nous passons à exposer les principaux points d'attaques de ces modèles, et nous terminons par une présentation des méthodes de sécurisation d'un système biométrique.

6.1 Modèle biométrique : vulnérabilités et menaces

Les systèmes biométriques ont plusieurs faiblesses où un modèle biométrique est enregistré dans la base de données sans aucune protection. Parmi les menaces et vulnérabilités qui touchent les modèles biométriques on peut citer :

A. **Risques de violation de la vie privée**

L'analyse de la conformité de la confidentialité d'un système de reconnaissance automatique basé sur la biométrie est un problème principal à la fois pendant le processus de conception du système et pour son déploiement dans des applications réelles. On peut citer les préoccupations principales suivants liées à l'utilisation de la biométrie :

- Les données biométriques peuvent être collectées ou partagées sans l'autorisation spécifique d'un utilisateur, des connaissances adéquates ou sans objectif spécifique[15].
- Les données biométriques, qui ont été collectées à des fins spécifiques, peuvent être utilisées ultérieurement à une autre fin non voulue ou non autorisée.
- L'utilisation de la biométrie peut violer le « principe de proportionnalité » [16], qui stipule que les données biométriques ne peuvent être utilisées que si elles sont adéquates, pertinentes et non excessives par rapport à l'objectif du système.
- Les données biométriques peuvent être mal stockées et / ou transmises. Cela exposerait les données biométriques à des attaques externes.

B. **Risques d'usurpation d'identité**

Le principe est qu'un individu collecte les informations biométriques d'un autre et se fabrique une « fausse identité », parce qu'il est parfois possible de contrefaire des mesures biométriques de manière artisanale par différentes techniques[17].

Une autre technique d'usurpation d'identité « attaque par rejeu », qui consiste

à contourner la capture de l'image biométrique, avant sa conversion en gabarit, par l'accès au système par une image préalablement prélevée.
« Substitution attack » est une autre façon ou technique d'usurpation d'identité par l'insertion des caractéristiques biométriques d'un pirate ayant réussi à accéder à une banque de données aux renseignements personnels d'une autre personne.
Alors qu'un mot de passe est facilement renouvelable, la donnée biométrique deviendra caduque et ne pourra être réutilisée une fois subtilisée. En effet, les données biométriques ont la particularité d'être irrévocables et tout se complique si l'utilisateur légitime se fait pirater ses données [18].

Un système biométrique peut soumettre à d'autres types d'attaques. dont les lignes suivantes présentent les différents points d'attaques d'un système biométrique.

6.2 Modèle biométrique et problèmes de sécurité

Ratha et al. [19] ont classé les attaques sur un système biométrique générique en 8 niveaux ou classes. La figure 1.20 définit les emplacements possibles de ces attaques dans un système biométrique générique :

A. **Données biométriques falsifiées** : une reproduction de la donnée biométrique utilisée sera présentée au capteur biométrique (comme la présentation d'une copie d'une signature).

B. **Transmission de données biométriques interceptées** : une ancienne donnée biométrique enregistrée est rejouée dans le système sans passer par le capteur biométrique (comme la présentation d'une ancienne copie de l'image de l'empreinte).

C. **Attaque sur le module d'extraction des caractéristiques** : ce module pourrait être remplacé par un cheval de Troie de manière à produire des informations choisies par l'attaquant.

D. **Altération de caractéristiques extraits** : Après l'obtention de données par le module d'extraction de caractéristiques, ceux-ci sont altérés voire remplacés par d'autres données définies par l'attaquant.

E. **Module de calcul de similarité est remplacé par un module malveillant** : ce module pourrait être remplacé par un cheval de Troie afin de produire artificiellement de hauts ou bas scores.

F. **Altération de la base de données** : la base de modèles biométriques est disponible localement, à distance ou distribuée sur plusieurs serveurs. Dans ce type d'attaque, l'attaquant modifie un ou plusieurs modèles afin d'autoriser un imposteur voire d'empêcher un utilisateur légitime d'y accéder.

G. **Attaque sur le canal entre la base de données et le module de calcul de similarité** : dans ce type d'attaque, les modèles sont altérés sur le lien de transmission reliant la base de modèles et le module de calcul de similarité.

H. **Altération des décisions (acceptées ou rejetées)** : ce type d'attaque altère la décision booléenne (oui ou non) pris par le module de calcul de similarité. La dangerosité de cette attaque est élevée puisque même si le système est robuste en termes de performance, il a été rendu inutile par ce type d'attaque.

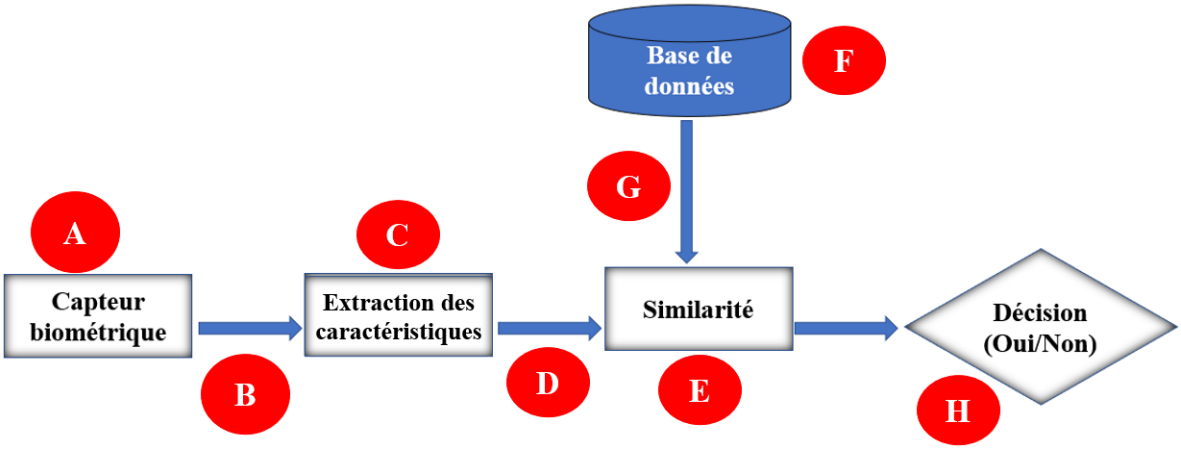

FIGURE 1.20 – Emplacements des points de compromission d'un système biométrique [19]

Les menaces relatives de ces attaques reposent généralement sur plusieurs facteurs que sont la modalité biométrique (il est plus difficile de reproduire la rétine que de forger une signature), le type du capteur (2D ou 3D, les capteurs 3D permettent de mieux détecter les tentatives de fraudes) et les paramètres de sécurité (illustrés par le FAR) du système.

Pour surmonter ces différentes attaques, il faut penser à sécuriser le système biométrique dont la section suivante présente un perçu sur les différentes méthodes de sécurisation d'un tel système.

6.3 Sécurisation du modèle biométrique

La sécurité du modèle biométrique est toujours une tâche très importante lors de la conception d'un système biométrique sécurisé. Avant de présenter les techniques utilisées pour la sécurisation des modèles biométriques, on présente d'abord des notions de base de la cryptographie qui sont utilisés pour atteindre ce but.

6.3.1 Notions générales de cryptage

La cryptographie désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

A. **Cryptographie symétrique(cryptographie à clé privée)**

Le chiffrement symétrique est basé sur des fonctions mathématiques réversibles. Le chiffrement symétrique repose sur un principe de clé unique pour chiffrer et déchiffrer(comme le montre dans la figure 1.21). Le chiffrement symétrique se

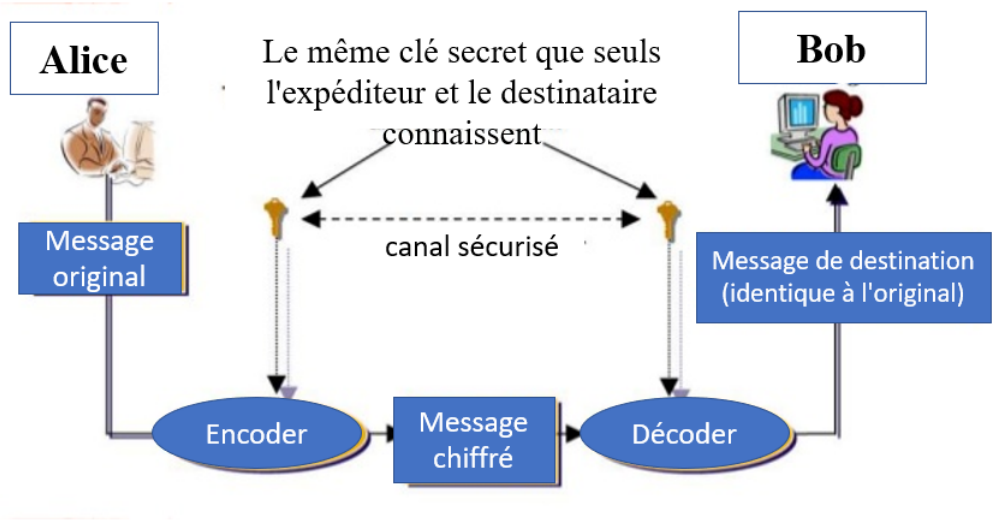

FIGURE 1.21 – La gryptographie symétrique

déroule en 3 étapes, de la manière suivante :

1ère étape

- Génération de la clé secrète par Alice
- Envoi de cette clé secrète à Bob, de manière sécurisée

2 ème étape

- Chiffrement du message original par Alice, avec la clé secrète générée
- Envoi de ce message chiffré à Bob

3 ème étape

- Réception du message chiffrée par Alice
- Déchiffrement du message avec la clé secrète reçue auparavant

B. **Cryptographie asymétrique(cryptographie à clé public)**

La cryptographie asymétrique est l'une des plus grandes fondations de la cybersécurité. Par exemple, chaque interaction sécurisée sur le Web public repose sur la cryptographie à clé publique (connexion cryptée SSL). Contrairement à la cryptographie symétrique, il utilise deux clés différentes, une clé pour chiffrer, et une autre pour le déchiffrer (ressemblent mathématiquement mais qui ne sont pas identiques).

La cryptographie asymétrique se déroule selon les étapes suivantes :

- Anis écrit un message, et souhaite l'envoyer à Mohammed, les deux possèdent une paire de clés, et chacun connait la clé publique de l'autre.
- Afin de chiffrer un message pour le destinataire, Anis va alors utiliser la clé publique du Mohammed.

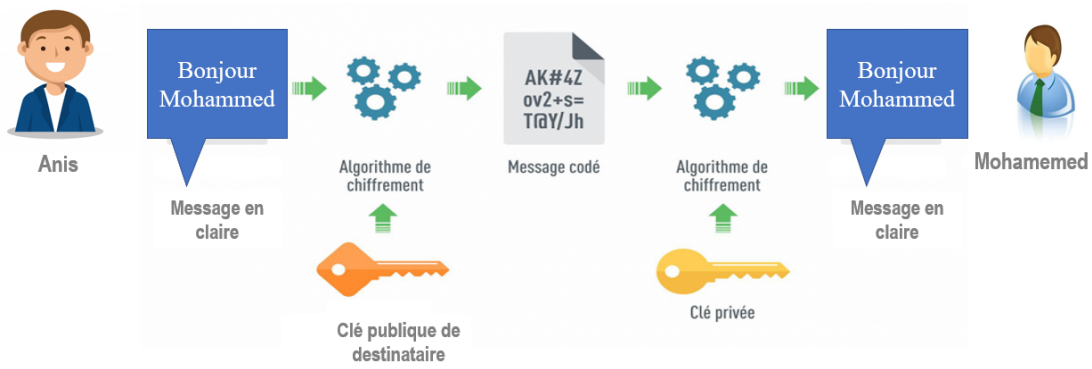

FIGURE 1.22 – La cryptographie asymétrique

• Cette clé active un algorithme, et le message écrit est alors transformé en texte incompréhensible, qui peut alors être envoyé au Mohammed.

• Lorsque Mohammed reçoit le message chiffré, il devra utiliser sa propre clé privée, celle que lui seul détient, afin d'activer l'algorithme pour le déchiffrer.

C. **Fonction de hashage cryptographique**

La fonction de hachage cryptographique est une fonction mathématique qui prend n'importe quelle chaîne d'entrée (données) de n'importe quelle longueur et génère une chaîne alphanumérique de taille fixe [20]. La chaîne de sortie est appelée valeur de hachage ou empreinte numérique ou somme de contrôle. De plus, la sortie est de longueur fixe et unique. La fonction produit toujours le même hachage à partir des mêmes données malgré le nombre de recalculs. Le hachage ne peut pas être inversé pour obtenir l'entrée données (très difficile) et, par conséquent, il peut être utilisé pour vérifier l'intégrité des données. Ainsi, il est également appelé fonction de hachage unidirectionnelle. La fonction de hachage a trois propriétés principales :

— **Résistance à la collision** : cette propriété rend très improbable (probabilité très faible) que deux entrées aléatoires génèrent le même résultat de hachage et qu'il est impossible (par calcul) de trouver un ensemble de données différent qui génère le même résultat de hachage donné d'un autre ensemble de données malgré la recalcul plusieurs fois. Plus formellement, la résistance à la collision d'une fonction de hachage peut être définie comme suit :

Il est très difficile de trouver deux entrées différents X, Y : Hash (x) = Hash (y).

— **Résistance à la pré-image** : la deuxième propriété stipule que la fonction de hachage doit être une fonction unidirectionnelle. Cette propriété implique qu'étant donné la sortie d'une fonction de hachage, il ne devrait y avoir aucun moyen de récupérer l'entrée d'origine.

— **Distribution uniforme** : La troisième propriété indique que les résultats de

hachage sont uniformément distribués dans l'espace de sortie. Étant donné une entrée aléatoire, la probabilité d'obtenir un résultat choisi est la même pour toutes les valeurs dans l'espace de sortie. Cela signifie que toutes les sorties possibles ont la même chance d'être "touchées". (plus de détails sur ce point dans le chapitre 2)

D. **Signature numérique**

La signature numérique est la méthode de cryptographie la plus sécurisée pour assurer la sécurité des informations. Pour prouver l'origine(authentification), l'intégrité des données et la non-répudiation du message, il est courant d'envoyer une signature numérique avec le message lui-même. Le processus de signature illustrer dans les étapes suivantes et la figure 1.23.

1. Calcul de l'empreinte de hachage(hash) des données à signer.
2. Chiffrement de l'empreinte à l'aide de la clé privée. On obtient alors la signature qui sera liée avec un certificat pour authentifie l'identité du signataire.
3. Déchiffrement de la signature avec la clé publique. Cela permet de retrouver l'empreinte associée aux données signées.
4. Calcul de l'empreinte des données signées. On vérifie que cette empreinte correspond à la précédente, auquel cas la signature est valide : les données sont donc intègres et l'identité de l'expéditeur est vérifiée[21].

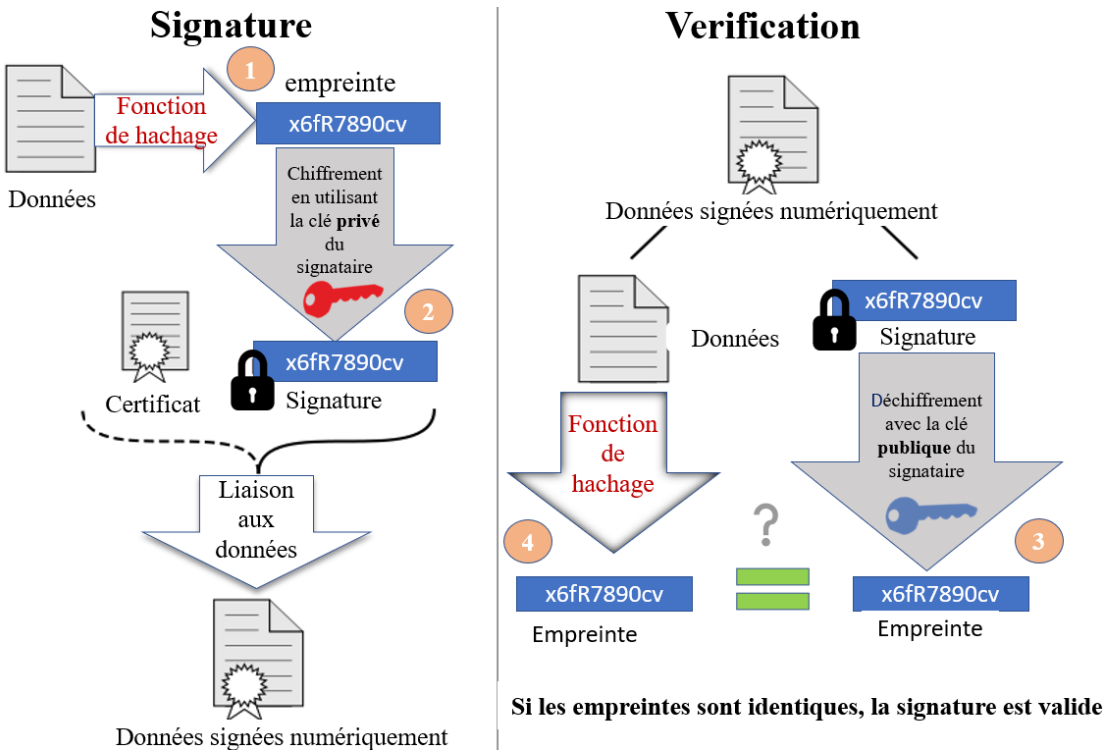

FIGURE 1.23 – Illustration de signature et vérification d'un message [22]

E. **Arbre de Merkle**

Un arbre de Merkle où arbre de hachage est une structure de données binaires arborescente qui permet de condenser un ensemble de blocs de données en un seul code de hachage au moyen d'une fonction de hachage cryptographique. Les feuilles contiennent les valeurs à stocker et les autres noeuds internes sont le hachage de ses deux fils. l'arbre de Merkle tire son nom de Ralph Merkle, qui considérer comme l'inventeur de ce type de structure en 1979 [23].

La figure 1.24 explique le fonctionnement de l'arbre de Merkle, il s'agit de hacher les blocs de données L1,..,L4 (les « feuilles »), puis de concaténer les empreintes (hashes)résultantes (Hash(L1),..,hash(L4)) deux à deux et de les hacher, et ainsi de suite jusqu'à l'obtient d'un seul hash qui s'appelle **Racine de Merkle** (Merkle root), et la modification de n'import quelle données d'un neoud entraînera la modification complète de la valeur de la racine. De cette façon, l'intégrité d'une quantité arbitraire de données peut être efficacement assurée.

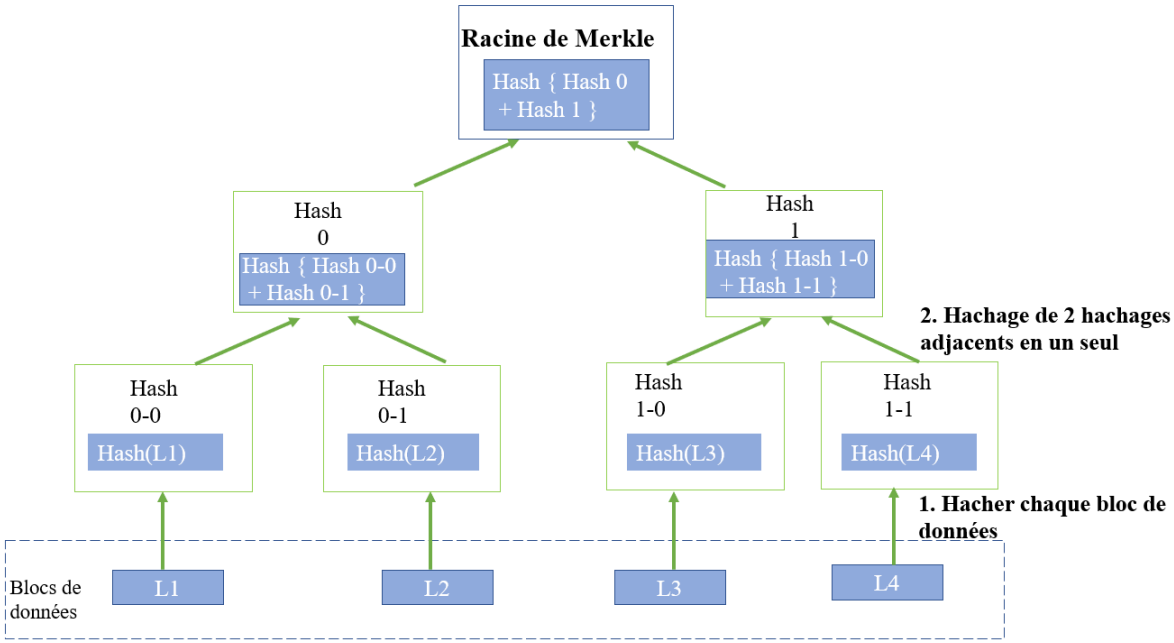

FIGURE 1.24 – Representation de l'arbre de merkle

Ces techniques de cryptage même si elles sont inventées pour sécuriser d'autres types de données, elles sont adaptées pour sécuriser les données biométriques. La section suivante présente les différentes méthodes de sécurisation des données biométriques tels que les approches matériels et les approches logiciels.

6.3.2 Approche matériel

Il s'agit d'assurer le stockage sécurisé du modèle biométrique sur un dispositif dédié (secure element) comme une carte à puce. Différentes solutions peuvent être proposées :

— Store-on-Card (SoC) : il s'agit d'éliminer la base de données centrale et de la remplacer par un dispositif sécurisé, dont en stockant le modèle biométrique sur le dispositif sécurisé[24].

— Match-on-Card (MoC) : Se réfère aux solutions où le module de comparaison est sur l'élément sécurisé. Le capteur et le module d'extraction sont sur une plateforme hôte[24].

— System-on-Device (SoD) : Le capteur, les modules d'extraction et de comparaison sont embarqués sur le même dispositif [24].

6.3.3 Approches logicielles

On peut trouver plusieurs solutions logiques, tels que :

A. **Chiffrement du modèle biométrique**

Le chiffrement des données traduit les données sous une autre forme, ou code, de sorte que seules les personnes ayant accès à une clé secrète (clé de déchiffrement) ou à un mot de passe peuvent les lire.

Le chiffrement du modèle biométrique se base sur des mécanismes de cryptographie. Le cryptage biométrique consiste à créer une clé à partir de la donnée biométrique qui servira à chiffrer et à déchiffrer un identifiant. Cette clé sera générée de manière aléatoire et différente à chaque demande d'authentification, ni la clé, ni la donnée biométrique ne sont conservées, seule la version « hachée » de la clé est conservée. Il est également impossible de relier les clés entre elles, ni de les tracer. Le cryptage biométrique permet ainsi d'utiliser la biométrie de manière anonyme et sans trace.

Il permet de réduire trois risques liés à la protection des données personnelles :

— Assurer la minimisation de la collecte de données car aucune donnée biométrique, ni gabarit ne sont conservés, cela permet de réduire les risques de perte ou de détournement de finalité.

— La personne garde le contrôle sur ses données.

— La sécurité est augmentée.

B. **Bases de données anonymes**

L'idée dans les données anonymes est de vérifier le statut d'adhésion d'un utilisateur sans connaître sa véritable identité. Une question clé dans une base de données anonyme est la nécessité d'une collaboration sécurisée entre deux parties le serveur biométrique et l'utilisateur [24]. Dans [25] où les base de données anonymes l'accès se basant sur la biométrie, l'objectif est de permettre au serveur de connaitre l'appartenance ou non du client à la base de données sans d'autres informations supplémentaires que cela soit son identité ou sa biométrie en claire (non chiffrée). Les auteurs utilisent la modalité d'iris combinée au système homomorphique de Paillier [24]. Car dans les bases de données anonymes les modèles

stockés dans la base restent en clair, alors l'information reste vulnérable aux attaques.

6.3.4 BioHachage

Basé sur la transformation du modèle biométrique à l'aide de projections pseudo-aléatoires générées à l'aide d'une clé ou d'un jeton spécifié par l'utilisateur. Cette solution a attirée beaucoup d'attention car il améliore la précision de la vérification par rapport à l'utilisation uniquement des données biométriques. Elle permet la révocation du modèle et préserve la confidentialité [26].

Toutes les méthodes de BioHashing partagent le principe commun de générer un BioCode unitaire (la donnée biométrique, après transformation) à partir de deux données : la biométrique (par exemple la texture ou les minuties pour la modalité d'empreinte digitale) et un nombre aléatoire qui doit être stocké (par exemple sur une clé USB, ou plus généralement sur une token), appelé nombre aléatoire tokenisé[24]. Le même schéma (détaillé ci-dessous) est appliqué à la fois :

— A l'étape de l'enrôlement, où seul le BioCode est stocké, au lieu des données biométriques originales brutes.

— A l'étape de la vérification, où un nouveau BioCode est généré, à partir du nombre aléatoire stocké.

Ensuite, la vérification repose sur le calcul de la distance de Hamming entre le BioCode de référence et le nouvellement émis, ce principe permet l'annulation et la diversité du BioCode en utilisant différents nombres aléatoires pour différentes applications.
Plus précisément, le processus BioHashing est illustré par la figure 1.26. On peut voir qu'il s'agit d'un schéma de protection d'authentification à deux facteurs, en ce sens que la fonction de transformation combine un nombre aléatoire spécifique dont la graine est stockée dans un jeton avec la caractéristique biométrique exprimée comme vecteur de longueur fixe F = (f1, ..., fn), F $\in$ Rn.

Ces techniques, même si elles permettent d'offrir un certain niveau de sécurisation des données biométriques, elles restent incapable d'assurer la protection nécessite à la conception d'un système biométrique sécurisé. On remarque que la possibilité d'avoir le modèle originale si un adversaire peut accéder au modèle transformé est toujours possible, ainsi qu'une fonction de hachage doit être conçus soigneusement pour que les performances de reconnaissance ne se dégradent pas.
Pour mieux répondre aux besoins de sécurisation des données biométriques, une autre technique est récemment adoptée, qui est la blockchaine.

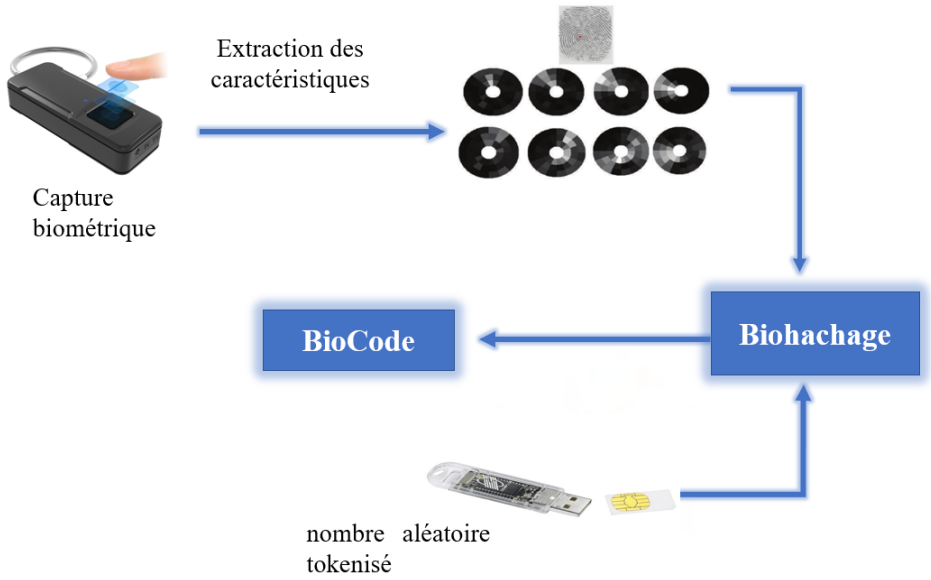

FIGURE 1.25 – BioHachage
[27]

6.3.5 Blockchain

La technologie Blockchain (chaine de blocs) est une nouvelle technologie qui intègre la décentralisation, le calcul distribué, le chiffrement asymétrique, le hachage (fonction de hachage et arbre de merkle) l'horodatage et l'algorithme de consensus. La Blockchain est une technologie qui permet de stocker et de transmettre les informations de manière sécurisée, fiable et transparente. Actuellement, son utilisation touche beaucoup de secteurs y compris la biométrie. Plus de détails sur cette technologies sont présentées dans le chapitre 2.

7 conclusion

Dans ce chapitre, on a expliqué la notion de la biométrie, les modalités biométriques, l'architecture des systèmes biométriques et modes de fonctionnements, mesure de performance d'un système biométrique, et on a terminé par la sécurité des systèmes biométriques. Cette sécurisation est reste toujours insuffisance et ne répond pas aux exigences de la protection des systèmes biométriques.

Pour répondre à ce défi, on va essayer de le combiner avec une autre technique qui s'appelle la chaine de blocs (blockchain) expliquée dans le prochain chapitre.

CHAPITRE 2

BLOCKCHAIN

1 Introduction

Au fil du temps, les technologies de l'information et de la communication ont connu de nombreux développements afin de faciliter, d'améliorer et de sécuriser l'échange et le partage d'informations, de données et de fonds de manière variée. Avec l'émergence d'Internet, les communications numériques ont émergé, permettant toutes les formes d'échange de données grâce aux transactions en ligne. L'évolution d'Internet a soulevé d'importants problèmes et défis de sécurité ainsi que les stratégies correspondantes pour y faire face. Ces problèmes ont un impact croissant sur la confiance qui est la clé de voûte de notre société, car chaque interaction humaine se déroule dans le cadre de la confiance. La société de l'information a également besoin de confiance pour continuer. Il a besoin d'une confiance numérique qui devrait être activée par les technologies de l'information. Dans ce chapitre, nous allons essayer de présenter la technologie nouvelle et innovante de Blockchain. Nous montrerons comment cette technologie peut être utilisée pour partager et contrôler en toute sécurité des informations entre des parties qui ne se font pas nécessairement confiance, et comment elle profite à la façon dont nous traitons les transactions. Dans ce chapitre on va bien expliquer la technologie de la blockchain (concept, architecture, caractéristique ... etc).

2 Concept général de blockchain

La confiance est l'un des éléments les plus fondamentaux de l'existence humaine. En affaires par exemple et jusqu'à récemment, toutes nos transactions étaient basées sur des intermédiaires "de confiance" ou des tiers de confiance (TTP) qui prenaient

la tête et géraient tous les enregistrements des transactions. Aujourd'hui, les banques suivent les soldes de toutes les parties dans un grand livre fermé au public. Nous comptons sur les banques pour confirmer ou rejeter les transactions. La banque vérifie les soldes des parties commerciales dans le grand livre et les met à jour chaque fois qu'une transaction a lieu.

La blockchain est le contraire - essentiellement un système avec une autorité répartie entre les utilisateurs qui leur permet de négocier des actifs numériques[28] . Ceci est très intéressant car dans de nombreuses situations, cette même source de confiance n'est pas elle-même pleinement approuvée par ses utilisateurs. Ce manque de confiance peut conduire à des situations où les entités d'une certaine interaction souhaitée n'ont pas du tout de tels TTP.

La technologie Blockchain a été développée pour répondre à ce besoin. Il introduit une nouvelle architecture de confiance pour remplacer les intermédiaires de confiance hérités. La technologie blockchain a été proposée et déployée pour la première fois par une personne ou un groupe anonyme sous le nom de Satoshi Nakamoto, en 2008[28]. Il a développé un système de trésorerie électronique pair-à-pair décentralisé qui a exploité une nouvelle technologie, plus tard appelée " **Blockchain** ", pour créer Bitcoin, la célèbre et controversée crypto-monnaie. Le système proposé permettrait d'envoyer des paiements en ligne directement d'une partie à une autre sans passer par une institution financière. Bitcoin permet la création d'un environnement décentralisé où les transactions et les données validées cryptographiquement ne sont sous le contrôle d'aucune autorité centrale ou d'intermédiaires.

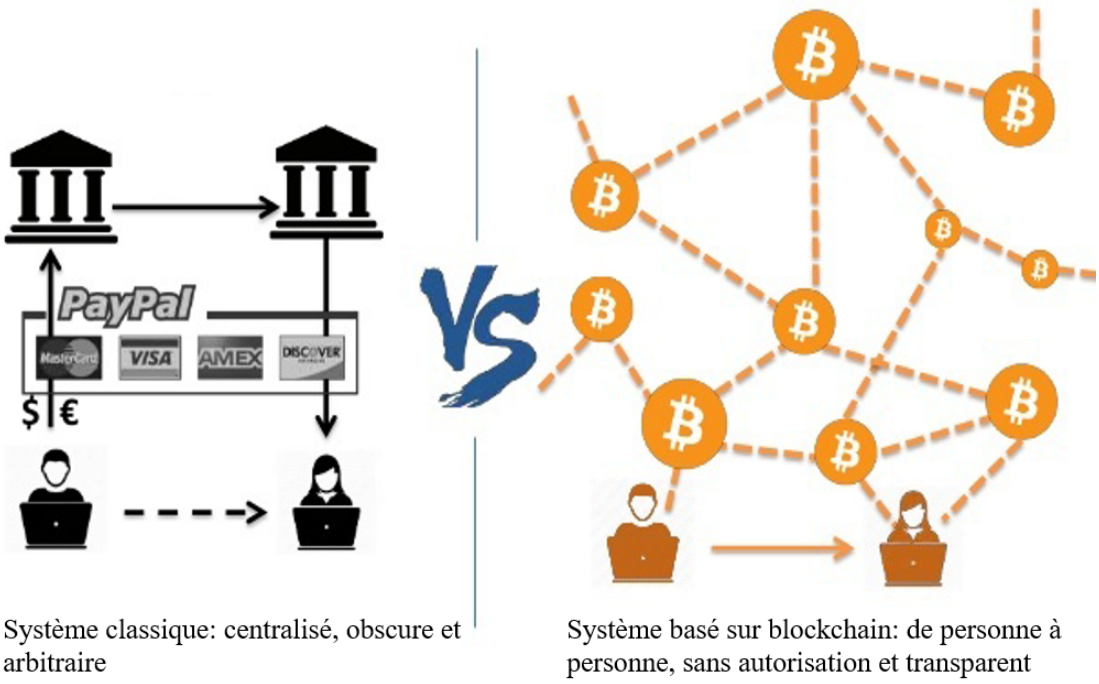

FIGURE 2.1 – Comparaison entre système classique et système basé sur blockchain

Un grand livre numérique inviolable mis en œuvre de manière distribuée (c'est-à-dire sans référentiel central) et généralement sans autorité centrale (c'est-à-dire une banque, une entreprise ou un gouvernement). À leur niveau de base, ils permettent à une communauté d'utilisateurs d'enregistrer des transactions dans un grand livre partagé au sein de cette communauté, de telle sorte qu'en fonctionnement normal du réseau de blockchain, aucune transaction ne peut être modifiée une fois publiée [29].

2.1 Définition de blockchain

La technologie Blockchain est une nouvelle technologie qui intègre la **décentralisation, le calcul distribué, le chiffrement asymétrique, l'horodatage et l'algorithme de consensus** [30]. Il fournit un registre distribué qui simplifie le processus de réconciliation des comptes grâce à des techniques de chiffrement et au protocole de transmission de messages distribués, et conserve une grande quantité de données grâce à la décentralisation. Il est capable d'augmenter l'efficacité du traitement des données et fournit une fonction de partage de données tout en garantissant la sécurité des données. Par conséquent, par rapport aux technologies traditionnelles, la technologie blockchain est dotée des atouts de durabilité, de compatibilité, de partage de données et d'inter-connectivité.

À travers les définitions ci-dessus, nous pouvons définir la blockchain comme un registre, décentralisé et public composé de nombreux pairs (nœuds)[31]. Dans la blockchain simple chaque pair a les mêmes enregistrements de données exactes dans son propre appareil, ces enregistrements distribués sont sauvegardés dans des blocs (groupe de transactions) sous une forme de chaînes immuables et sécurisées. La transparence de la blockchain vient de l'historique de toutes les transactions qui ont été effectuées à l'intérieur de celle-ci,comme toute personne ayant accès à la blockchain pourra voir toutes les transactions qui y ont eu lieu.

Aprés tous ces définitions et explications ce qu'il faut retenir est le suivant :

- La blockchain est une technologie qui permet de stocker et de transmettre les informations de manière sécurisée, fiable et transparente[32].
- Elle garde l'historique de tous les échanges qui ont pu être effectués depuis l'ouverture d'une blockchain.
- On trouve des blockchains publiques, privées et Consortium[33].
- Dans une blockchain, toutes les transactions sont traitées sous la forme de blocs devant être validés par des nœuds de réseau avant d'apparaître dans la blockchain et d'être visible de tous les utilisateurs.
- Sa transparence et sa sécurité permettent à la blockchain de pouvoir être utilisée dans plusieurs applications qui sortent du cadre de la finance.

La blockchain est composée d'un ensemble de blocs reliées entre eux avec une hash(ID) dont chaque bloc contient le hach de bloc précédent de telle manière compose la chaine de blocs [34], le bloc contient d'autres informations comme l'ensemble de transactions, l'horodatage et d'autres informations sera expliquer dans la section 3.1. Une structure de blockchain représentée dans la FIGURE 2.2 suivant.

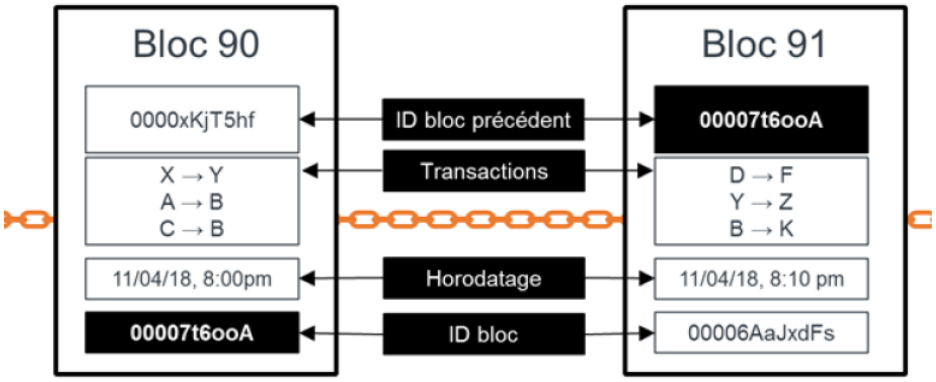

FIGURE 2.2 – Structure d'un blockchain

2.2 Fonctionnement de blockchain

Comme nous l'avons vu, la blockchain a la particularité qu'elle fonctionne sans organe central de contrôle.
Les transactions (achat ou transfert d'argent par exemple) sont distribuées entre tous les membres d'un réseau, au lieu d'être regroupées à un seul endroit ou de passer par un seul intermédiaire. On parle aussi de pair à pair.
Plusieurs étapes interviennent pour ajouter une transaction. Elles diffèrent selon le type de chaînes de blocs. Prenant un exemple d'une transaction sur Bitcoin va comme suit :

— **Étape 1 : création d'un portefeuille Bitcoin**
Un portefeuille Bitcoin doit créer pour qu'une personne puisse envoyer ou recevoir des bitcoins. Un portefeuille bitcoin stocke 2 informations : une **clé privée** et une **clé publique**[32]. La clé privée est un numéro secret(nombre aléatoire entre 0 et 2256-1) qui permet au propriétaire de signer les transactions(fonctionne comme un mot de passe qui doit être gardé secret). La clé publique utilisée pour former une adresse publique personnelle et unique (version hachée de la clé publique) à l'aide d'un algorithme de cryptographie asymétrique appelé ECDSA (Elliptic Curve Digital Signature Algorithm ou algorithme de signature numérique sur courbes elliptiques)[35], peut considérer comme un numéro de compte bancaire, les utilisateurs peuvent créer autant d'adresses publiques.

— **Étape 2 : Création d'une transaction Bitcoin**
Si Alice veut envoyer 1 BTC à Bob, Alice doit se connecter à son portefeuille Bitcoin à l'aide de sa clé privée et créer une transaction qui contient la quantité de bitcoins qu'elle souhaite envoyer et l'adresse à laquelle elle souhaite les envoyer.

— **Étape 3 : Diffusion de transaction sur le réseau de Bitcoin**
Une fois qu'Alice crée la transaction bitcoin, la transaction sera regroupée dans un **bloc** avec d'autres transactions qui attendent d'être incluses dans la Blockchain, ensuite le bloc doit diffuser sur l'ensemble du réseau Bitcoin[32].

— **Étape 4 : confirmation de transaction**
Un mineur écoutant le réseau de Bitcoin authentifie la transaction à l'aide de la clé publique d'Alice, confirme qu'Alice a suffisamment de bitcoins dans son portefeuille (dans ce cas au moins 1 BTC) et ajoute un nouveau bloc à la Blockchain de Bitcoin contenant les détails des transactions[32].

— **Étape 5 : Diffusion de changement de blockchain à tous les mineurs**
Une fois la transaction confirmée, le mineur doit diffuser la modification de la chaîne de blocs à tous les mineurs pour s'assurer que leurs copies de la chaîne de blocs sont toutes synchronisées.

Dans la blockchain, toutes les transactions sont regroupées sous la forme de blocs. Chaque bloc doit ensuite être validé par les nœuds du réseau en utilisant une méthode algorithmique. Une fois que le bloc est validé, il est ajouté à la chaîne de blocs et devient donc visible de tous les utilisateurs. Voici un schéma qui permettra d'illustrer cette définition.

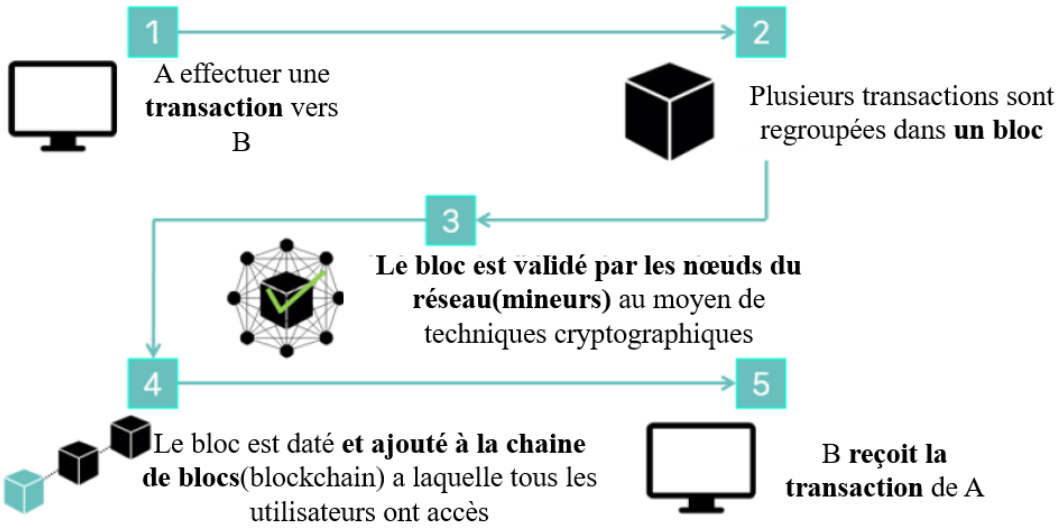

FIGURE 2.3 – Fonctionnement d'un blockchain(Blockchain france 2016)

2.3 Minage et mineurs

Le **minage** est un terme utilisé pour décrire le processus consistant à la validation d'un bloc (transactions qui attendent d'être incluses dans la Blockchain) par un des membres(nœuds) du réseau qui s'appelle **mineur**[36]. C'est donc considéré comme l'opération fondamentale d'une chaîne de blocs[37], quelle qu'elle soit, et qui la distingue d'un système centralisé classique.

Le minage consiste à contribuer à la sécurisation d'une blockchain publique en apportant une contribution en terme de puissance de calcul, dont pour qu'un mineur pouvoir créer un bloc valide dans une blockchain prenant l'exemple de Bitcoin , il est nécessaire de résoudre un problème mathématique très complexe(**preuve de travail**) , dont la solution ne peut être trouvée que par force brute, c'est-à-dire en testant au hasard des solutions jusqu'à tomber sur la bonne.
Pour cela des sociétés spécifiées des fermes de minage qui regroupent des machines dédiées pour le minage ont grande capacité de calcul (de processeurs, d'ordinateurs ou de cartes graphiques utilisées pour les jeux vidéo), alors une grande consommation d'électricité et très coûteux. Les mineurs les plus performants sont récompensés s'ils

FIGURE 2.4 – ferme-minage-bitcoin

ajoutent avec succès un nouveau bloc à la blockchain en bitcoins par exemple ils récompensent des nouveaux Bitcoins. Les mineurs ont été initialement récompensés avec 50 Bitcoins, la récompense est divisée par deux environ tous les quatre ans(6.25 BTC à partir de mai 2020).

Notez que dans la blockchain publique, chaque nœud pourrait participer au processus

de minage, et seul un ensemble sélectionné de nœuds est responsable de la validation du bloc dans la blockchain du consortium [38].

2.4 Caractéristiques de blockchain

— **Décentralisation** : parmi les aspects principaux de la blockchain est qu'il s'agit d'un registre décentralisé, ce qui signifie que les données sont conservées par tous les nœuds du réseau. Aucune autorité centrale ne tient ou ne met à jour le grand livre. Les algorithmes de consensus de plus, chaque homologue du système a le pouvoir d'ajouter de nouvelles transactions. Chaque transaction qui passe la phase de consensus sera enregistrée dans le grand livre[38].

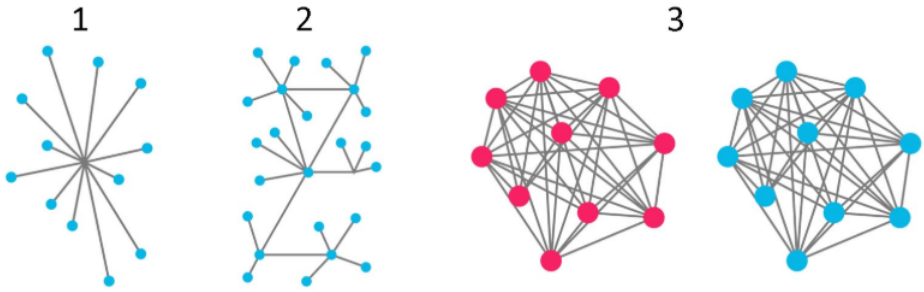

FIGURE 2.5 – Différence entre un système centralisé (1) et décentralisé (2) et (3).

— **Immuable** :une fois qu'une transaction est ajoutée à une blockchain, elle ne peut pas être supprimée ou modifiée. Cette immuabilité est l'un des principaux aspects qui contribuent à la fiabilité du système de blockchain. Le mécanisme de consensus est fait de telle sorte qu'il deviendra impossible de tromper le système et le rendra très fiable. Le grand livre distribué peut être considéré comme un enregistrement permanent irréversible[38].

— **Sécurisé** : les chaînes de blocs sont cryptographiquement sécurisées, les signatures numériques garantissant que les données contenues dans les blocs n'ont pas été modifiées.

— **Transparent** : le grand livre est partagé entre plusieurs pairs du réseau, ce qui signifie que tout utilisateur du réseau peut voir toutes les transactions depuis la création de la blockchain jusqu'au dernier bloc enregistré.

— **Persistance** : Les transactions peuvent être validées rapidement et les transactions invalides ne seraient pas admises par les mineurs. Des blocs contenant des transactions non valides ont pu être découverts immédiatement.

— **Anonymat** : Chaque utilisateur peut interagir avec la blockchain avec une adresse générée, qui ne révèle pas la véritable identité de l'utilisateur. Notez que la blockchain ne peut pas garantir la parfaite préservation de la vie privée grâce à la contrainte intrinsèque [38].

3 Architecture de blockchain

La technologie blockchaine se compose de plusieurs composants dont ils présentés dans cette section.

3.1 Bloc

Les blocs sont une structure de données fondamentale (fichier) dans la blockchain, ils sont liés entre eux pour former une chaîne de blocs. Chaque bloc peut être considéré comme une page dans le grand livre. Un bloc est un enregistrement de certaines transactions valides qui n'ont pas encore été enregistrées dans les blocs déjà chaînés. Les blocs individuels sont composés de plusieurs composants ; presque ceux-ci peuvent être différenciés dans la tête du bloc (en-tête de bloc) qui contient les métadonnées et son corps (corps de bloc)[38].

A) **En-tête de bloc**

Contient les éléments suivants (voir figure 2.6) :

- **Version de bloc** : indique quel ensemble de règles de validation de bloc à suivre, ceci est utilisé pour que les ordinateurs puissent lire correctement le contenu de chaque bloc[38].
- **Hachage de la racine de l'arbre Merkle** : la valeur de hachage de toutes les transactions dans le bloc[38].
- **Horodatage** : heure actuelle en secondes dans le temps universel depuis le 1er janvier 1970[38].
- **Nonce** : le hash que le mineur va devoir faire varier et trouver pour résoudre la preuve de travail, un champ de 4 octets, qui commence généralement par 0 et augmente pour chaque calcul de hachage[38].
- **ParentHash** : une valeur de hachage de 256 bits qui pointe vers le bloc précédent. S'il s'agit du premier bloc(bloc genèse), ce hash vaut 0.
- **Données supplémentaires** : il peut s'agir par exemple de l'index (hauteur) qui indique l'emplacement du bloc à l'intérieur de la blockchain. Le premier bloc est indexé « 0 » ; cela s'appelle le bloc de genèse, le prochain "1", et ainsi de suite[38].

B) Corps de bloc

Le corps de bloc est composé d'un compteur de transactions et transactions. Le nombre maximal de transactions qu'un bloc peut contenir dépend de la taille du bloc et de la taille de chaque transaction[38].

Dans le contexte d'une blockchain, il existe différents types de blocs :

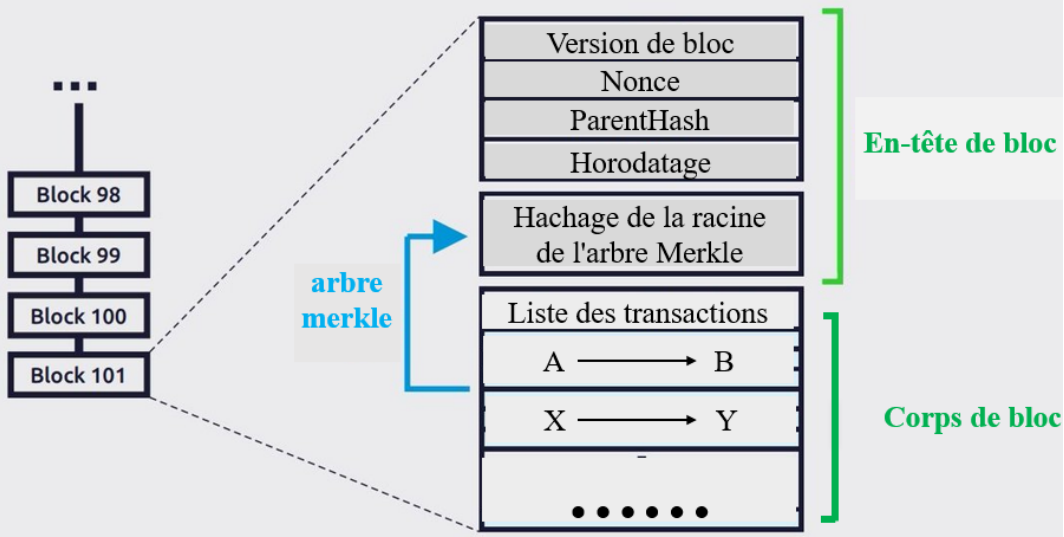

FIGURE 2.6 – Structure simplifié d'un bloc
[38]

— **Bloc genèse** : c'est le premier bloc de toute blockchain (hauteur = 0). Il fournit la base sur laquelle une blockchain entière est construite. En termes de Bitcoin, le bloc genèse a été créé le 3 janvier 2009 et contient 50 BTC.

— **Blocs de branche principale** : les blocs de branche principale font référence aux blocs qui se trouvent dans la chaîne la plus haute.

— **Blocs orphelins** : les blocs orphelins sont les blocs qui ont la même hauteur, ils se produisent lorsque deux mineurs produisent un bloc à des moments similaires. Les blocs orphelins sont considérés comme des blocs valides pour la première fois mais ils ne font pas partie de la chaîne principale.

3.2 Réseau décentralisé

Le réseau de blockchain est composé de nombreux nœuds situés dans le monde entier, chacun d'entre eux conserve une copie locale de la blockchain qui contient un enregistrement complet de toutes les transactions. Il s'agit d'un réseau pair à pair distribué où tous les deux nœuds sont autorisés à communiquer entre eux sans avoir besoin d'une autorité centrale.
Un **nœud** est un ordinateur lié au réseau de la blockchain, il représente un utilisateur particulier. On peut distinguer deux types de noeuds : les noeuds complets et les noeuds légers[39].

— **Noeuds complets** : contiennent une copie complète de la blockchain(l'historique complet de toutes les transactions), généralement suivent toutes les règles de l'algorithme de consensus pour ajouter des blocs au réseau. Parmi les tâches principales de ceux nœuds la vérification de toutes les transactions et le maintien du consensus entre les autres nœuds, peuvent considérer comme un serveur [40].

— **Noeuds légères** : ne contiennent pas la copie complète de la blockchain, mais uniquement les en-têtes de bloc. Également appelés clients VPS (Vérification de Paiement Simplifiée) qui consiste à un utilisateur peut vérifier si certaines transactions ont été incluses ou non dans un bloc. Les nœuds légers dépendent entièrement de nœuds complets et ne peuvent exister sans un nœud complet, généralement ne disposant pas de capacités matérielles suffisantes[40].

Ils considèrent toujours que la chaîne la plus longue est la branche principale et continuent de l'étendre. Lors d'une transaction, elle doit d'abord être validée puis diffusée à chaque autre nœud connecté. De cette façon, les données se propagent d'un nœud à l'autre pair-à-pair (c'est à dire sans intermédiaire) et atteignent l'ensemble du réseau. Un nœud dans un réseau blockchain remplit diverses fonctions selon le rôle qu'il prend.

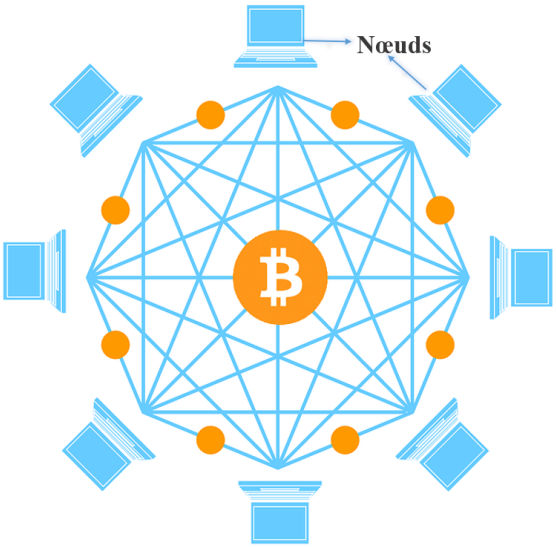

FIGURE 2.7 – Un réseau pair à pair (décentralisé)

Un nœud peut proposer et valider des transactions et effectuer du minage pour faciliter le consensus et sécuriser la blockchain. Cela se fait en suivant un protocole consensuel. (Le plus souvent, c'est la preuve de travail PoW). Les nœuds peuvent également effectuer d'autres fonctions telles que la vérification de paiement simple (nœuds légers), les valideurs et de nombreuses autres fonctions selon le type de la chaîne de blocs utilisée et le rôle attribué au nœud.

3.3 Transactions

Une transaction est l'unité fondamentale d'une blockchain. Elle représente un transfert de valeur d'un compte (adresse) à un autre compte, ce transfert est diffusé sur le réseau, collecté par les mineurs et inclus en blocs. Il est d'abord envoyé à tous les nœuds de connexion, pour augmenter les chances d'être ajouté à un bloc. Pour faire face à un problème de double dépenses, on ne peut transférer que des transactions

non dépensées. Pour éviter que chaque nœud ne doive vérifier l'historique complet de la blockchain pour les transactions partiellement non dépensées, par conception, les transactions sont soit complètement dépensées, soit non dépensées, ce qui signifie qu'il n'est pas possible de dépenser seulement une partie d'une transaction. La quantité restante peut être retransférée dans son propre « portefeuille », créant ainsi une nouvelle transaction non dépensée. Nakamoto définit une pièce comme une chaîne de signatures numériques. Pendant le transfert, le propriétaire de la pièce signe un hachage des transactions précédentes et la clé publique du récepteur et l'ajoute à la fin de cette chaîne de signatures numériques[28]. La clé privée est utilisée pour signer la transaction, et la clé publique est utilisée pour la vérification de la transaction[41], comme le montre la FIGURE 2.8. Avant la blockchain, le problème de la double dépense a été résolu en s'appuyant sur un tiers de confiance.

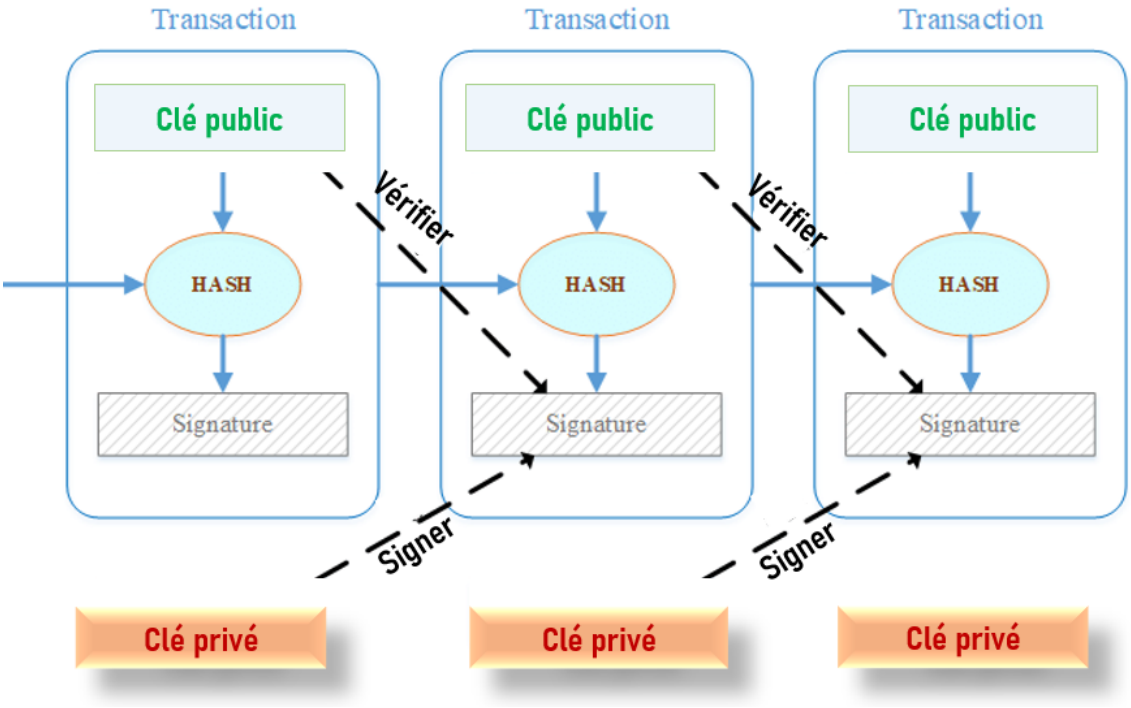

FIGURE 2.8 – Structure de transaction dans une blockchain Bitcoin [42]

3.4 Consensus

Le consensus est un grand problème dans les réseaux distribués comme la blockchain, puisqu'il n'y a pas d'entité centrale pour décider quels nouveaux blocs sont valides, chaque noeud doit décider s'il accepte ou non un nouveau bloc reçu[33]. On peut définir le consensus comme l'épine dorsale de la blockchain (système de grand livre distribué), car la sûreté et la sécurité de la blockchain sont assurées dans cette couche, généralement c'est la couche de base de la plupart des systèmes de blockchain.

Le but principal de cette couche est de faire en sorte que tous les nœuds se mettent d'accord sur un état cohérent du registre, tous suivant des règles simples[28]. Dans un réseau blockchain (Bitcoin par exemple), le consensus sert à la vérification des transactions (simple) + algorithme de consensus(PoW,Pos.....) (compliqué). Il existe de nombreuses variantes différentes de protocoles de consensus tels que la preuve de participation (PoS), PoS délégué (dPoS)....

A) **Preuve de travail (Proof of Work (poW))**

Le mécanisme de preuve de travail est considéré comme le mécanisme de consensus le plus célèbre dans la blockchain car il a été utilisé avec la première crypto-monnaie qui n'ait jamais existé. La preuve de travail est une exigence pour définir un calcul informatique coûteux, également appelé exploration, qui doit être effectué afin de créer un nouveau groupe de transactions sans confiance (bloc) sur un registre distribué de blockchain. Le processus d'extraction vérifie la légitimité d'une transaction, ou évite les soi-disant doubles dépenses et aussi pour créer une nouvelle monnaie numérique en récompensant les mineurs pour effectuer la tâche précédente. Chaque fois qu'une transaction est défini en utilisant l'algorithme POW , les événements suivants se produisent dans les coulisses :

- Les transactions sont regroupées dans un bloc.
- Les mineurs vérifient que les transactions dans chaque bloc sont légitimes.
- Pour ce faire, les mineurs devraient résoudre un casse-tête mathématique appelé problème de preuve de travail (trouver un hash qui répond à certains critères par exemple commenér par un certain nombre de zéros.) qui ne peut se résoudre qu'aléatoirement (force brute), par exemple les calculs successifs d'un hash en ajoutant une chaîne alphanumérique aléatoire (Nonce) pour obtenir différents hashs jusqu'à l'obtient d'un hash inférieur à un seuil (cible) [43]. Une récompense est donnée au premier mineur qui résout chaque problème de bloc.
- Les transactions vérifiées sont stockées dans la blockchain publique.

L'inconvénient majeur du pow est la consommation d'énergie, dont les mineurs ont pour objectif des ordinateurs puissants pour plus de puissance de calcul.

B) **Preuve d'enjeu (Proof-of- stake)**

La preuve d'enjeu ou preuve de mise est un algorithme consensuel proposé en 2012 [44] comme algorithme alternatif à la preuve de travail. Il est utilisé pour valider un bloc de transactions dans le réseau blockchain et dispose d'un mécanisme pour punir les nœuds qui ne suivent pas le protocole de consensus.

Un mineur doit miser des montants d'actifs numériques prédéfinis pour obtenir

un consensus. Contrairement à la preuve de travail, cet algorithme choisit au hasard un mineur dans le pool de minage et le mineur choisi est requis pour résoudre un problème mathématique simple. Ensuite, si le mineur résout le problème avec succès, un intérêt ou un bonus est accordé sur sa mise. Sinon, le mineur suivant est choisi au hasard. Par conséquent, il n'y a pas de course pour résoudre le problème mathématique pour obtenir une incitation économique.

Les principaux avantages de la preuve de mise sur la preuve de travail sont :

— Réduits la consommation d'énergie

— Plus de décentralisation entraînant une diminution des chances d'attaque de 51%[44].

Étant donné que la preuve de participation n'a qu'un problème mathématique simple à résoudre, les mineurs n'ont pas besoin d'ordinateurs haut de gamme pour participer à l'exploitation minière. Un ordinateur moins puissant suffit. Ainsi, beaucoup moins d'énergie est gaspillée et il n'y a pas de concurrence féroce sur la construction de nœuds à haute puissance de calcul pour obtenir une incitation économique. De plus, presque tous les nœuds peuvent participer à l'exploitation minière. Ainsi, la preuve de participation motive une participation plus large à l'exploitation minière, ce qui augmente la décentralisation de la blockchain.

C) **Preuve de mise déléguée (Delegated proof of stake DPOS)**

Le consensus du DPoS est divisé en deux processus : le premier consiste à élire les **témoins** (c'est-à-dire les producteurs de blocs) par les utilisateurs de réseau, ces témoins sont chargés de valider les transactions et de créer des blocs, ils génèrent un bloc toutes les 3s à tour de rôle, et si un témoin n'a pas terminé la tâche à l'heure spécifiée il sera ignoré et remplacé par un autre [45]. Avec DPoS beaucoup moins de nœuds sont nécessaires pour valider un bloc, prenant l'exemple de EOS (l'une des blockchains DPOS les plus populaires), n'a que 21 témoins[46], le bloc peut être confirmé rapidement, ce qui signifie que la transaction peut être confirmée rapidement.

Le second processus sert à générer des blocs. Les utilisateurs des systèmes DPoS votent également pour un groupe de «**délégués**» (parties de confiance responsables de la maintenance du réseau). Les délégués supervisent la gouvernance et les performances de l'ensemble du protocole blockchain, mais ne jouent aucun rôle dans la validation des transactions et la production de blocs. Parmi les rôles des délégués la proposition de changer la taille d'un bloc, ou le montant qu'un témoin devrait être payé en échange de la validation d'un bloc. Mis en œuvre pour la première fois dans son projet BitShares par Dan Larimer.

D) **Preuve d'autorité (PoA)**

Fonctionne selon l'idée suivante, seuls les validateurs ont le droit d'approuver

les transactions et les nouveaux blocs. Un nœud participant gagne une réputation à son identité et ce n'est que lorsque cette réputation est accumulée à un score élevé que le nœud peut devenir un validateur. Le PoA est considéré comme plus robuste que le PoS pour deux raisons. D'une part, les validateurs sont incités à vérifier honnêtement les transactions et les blocs, sinon leur identité sera associée à une réputation négative. D'autre part, un validateur ne peut pas approuver deux blocs consécutifs. Cela empêche la centralisation de la confiance.

E) **Tolérance aux pannes byzantines (BFT)**

L'algorithme pratique de tolérance aux pannes byzantine proposé par Miguel Castro et Barbara Liskov a été la première solution pratique pour parvenir à un consensus face au problème d'échecs byzantins[47]. Le problème a été expliqué de façon pertinente dans un article comme le suivant :

Imaginez que plusieurs divisions de l'armée byzantine campent à l'extérieur d'une ville ennemie, chaque division était commandée par son propre général. Les généraux ne peuvent communiquer entre eux que par messager. Après avoir observé l'ennemi, ils doivent décider d'un plan d'action commun. Cependant, certains des généraux peuvent être des traîtres, essayant d'empêcher les généraux loyaux de parvenir à un accord. Les généraux doivent décider quand attaquer la ville, mais ils ont besoin d'une forte majorité de leur armée pour attaquer en même temps. Les généraux doivent disposer d'un algorithme pour garantir que (a) tous les généraux loyaux décident du même plan d'action, et (b) qu'un petit nombre de traîtres ne puissent pas amener les généraux loyaux à adopter un mauvais plan. Les généraux loyaux feront tout ce que l'algorithme dit qu'ils doivent faire, mais les traîtres peuvent faire ce qu'ils veulent. L'algorithme doit garantir la condition (a) indépendamment de ce que font les traîtres. Les généraux loyaux doivent non seulement se mettre d'accord, mais aussi s'entendre sur un plan raisonnable[47].

Terme informatique désignant une situation où les parties concernées doivent s'entendre sur une stratégie unique pour éviter un échec complet. Toutefois, il suppose que certaines des parties concernées peuvent être corrompues ou peu fiables. L'objectif de la BFT est de pouvoir se défendre contre les défaillances byzantines, dans lesquelles les composants d'un système tombent en panne avec des symptômes qui empêchent certains composants du système de se mettre d'accord entre eux, lorsque cet accord est nécessaire pour le bon fonctionnement du système[48].

Il utilise le concept de machine d'état répliquée et de vote par répliques pour les changements d'état. Il fournit également plusieurs optimisations importantes, telles que la signature et le chiffrement des messages échangés entre les répliques

et les clients, réduisant la taille et le nombre de messages échangés, pour que le système soit pratique face aux pannes byzantines. Cet algorithme nécessite des répliques «3f + 1 » pour pouvoir tolérer les nœuds défaillants « f ». Cette approche impose une faible surcharge sur les performances du service répliqué. Les auteurs signalent un surcoût de 3% pour un service de système de fichiers réseau (NFS) sur lequel ils ont mené leurs expériences. PBFT n'a cependant été mis à l'échelle et étudié qu'à 20 répliques. C'est les frais généraux de la messagerie augmentent considérablement à mesure que le nombre de répliques augmente [38].une comparaison entre ces méthodes de consensus en terme de plusieurs critères est présentée dans le tableau 2.1.

Propriétés	PoW	PoS	DPoS	PBFT
Consommation énergétique	oui	Non	Non	Non
Type de blockchain	Publique	Publique et privée	Publique	Privée
Tolérance au fautes byzantines et à la compromission	<= 25	Dépend de l'algorithme spécifique utilisé	Dépend de l'algorithme spécifique utilisé	<=33
Niveau de sécurité	Très élevé	faible	Élevé	Faible
Niveau de décentralisation	Moyen	Élevé	Très élevé	faible
Exemple	Bitcoin	Peercoin	Bitshares	Hyperledger Fabric

TABLEAU 2.1 – Comparaison entre les algorithmes de consensus PoW,PoS,DPoS,PBFT [38]

3.5 Contrats intelligents (Smart contracts)

Les contrats intelligents sont des programmes informatiques autonomes auto-exécutables qui sont exécutés en fonction d'une condition définie par le programmeur [49]. Ces contrats sont capables de faciliter, de faire respecter et d'exécuter des accords entre deux parties en utilisant la blockchain. Contrairement aux contrats traditionnels, où un tiers (banque, notaire) est requis, les contrats intelligents permettent une entreprise indépendante entre des parties anonymes avec des frais moins chers.

Les contrats intelligents ont diverses applications possibles telles que :

— **Vote numérique** : les contrats intelligents reposant sur la blockchain peuvent améliorer la sécurité des systèmes de vote, par exemple des applications utilisent les contras intelligents et la blockchain pour protéger les votes de la fraude. Quand

une transaction de vote est enregistré sur la blockchain alors elle est protégée.Une fois le vote terminé, le contrat intelligent enverra un jeton à une adresse représentant le résultat de vote (gagnant du vote)[50].

— **Gestion d'entreprise** : les entreprises peuvent bénéficier des contrats intelligents et économiser beaucoup de temps et d'argent, ils peuvent établir un contrat intelligent simplement indiquant quand la date est telle date les salaires seront envoyés automatiquement aux employeurs.

— **Paiement** : par exemple, on peut payer le loyer de la chambre automatiquement à la fin du mois sans impliquer une banque entre les deux, un développeur écrit un programme informatique system (contrat intelligent). Ce programme définit l'intégralité des règles telles qu'elles ont été définies au début du projet : un mois de souscription, à qui les fonds seront envoyés, quel montant minimum sera récolté, quand les conditions (règles) les conditions sont remplies, telles que la date de paiement, le code sera exécuté et le paiement est effectué automatiquement

Il y'a d'autres utilisations des contrats intelligents comme le trading ou prêt de propriété, commerce d'actions ou d'obligations sur des marchés distribués [49]. En outre, il peut également être utilisé pour un système de contrat de notaire numérique autonome.

4 Quelques applications de blockchain

L'importance de la blockchain vient du fait qu'elle nous a permis pour la première fois à transférer de la valeur plutôt que de simples copies de données. En effet, la blockchain est venue empêcher les doubles dépenses et établir la confiance entre les participants anonymes dans les transactions plutôt que d'utiliser des intermédiaires de confiance. La blockchain peut être utilisée dans différents domaines d'application tels que financiers, non financiers, assurances, Internet des objets (IOT), soins de santé, Internet, crypto-monnaie, parmi les différentes utilisations on peut compter quelques exemples.

4.1 Bitcoin

En 2008, Satoshi Nakamoto a expliqué l'idée principale de son invention dans son livre blanc intitulé « Bitcoin : un système de paiement électronique pair à pair », il a déclaré : « Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur une preuve cryptographique plutôt que sur la confiance permettant à deux parties de traiter directement entre elles sans avoir besoin d'un tiers de confiance [28]. Chaque transaction est stockée dans la blockchain. Il s'agit donc d'un fonctionnement décentralisé, s'appuyant sur un système de nœuds. Chaque nouveau bloc ajouté à

la chaîne doit être vérifié, sécurisé puis enregistré. Les utilisateurs qui effectuent ces contrôles, les mineurs, sont ensuite rémunérés pour chaque nouveau bloc enregistré.

4.2 Ethereum

Ethereum est une plate-forme informatique conçue pour faciliter les contrats intelligents dans lesquels Ether est la crypto-monnaie utilisée[32]. Son prix a légèrement augmenté au fil des ans, mais il reste assez précieux. Ethereum, en tant que plate-forme, utilise le même système de blockchain que Bitcoin mais ne se limite pas aux transactions pair-à-pair et va plus loin pour prendre en charge les contrats intelligents. Étant donné la variété des applications qu'Ethereum facilite, Ether a de nombreuses utilisations immédiates.

4.3 Litecoin

Lancé en 2011 [51], Litecoin était basé sur Bitcoin mais avec plusieurs améliorations. Il a été conçu pour être plus difficile à produire, avoir une vitesse de transaction plus rapide et consommer moins de mémoire lors de son traitement.

4.4 Blockchain et l'écosystème de la santé

La blockchain a le pouvoir de faire une percée massive dans l'écosystème de la santé car elle peut facilement apporter des changements spécifiques dans la gestion des soins de santé du patient. Grâce à cette technologie, le pouvoir reviendra aux mains des gens. Cela signifie que les individus seront ainsi responsables de gérer leurs propres enregistrements, obtenant ainsi le contrôle global de leurs propres donnés.

4.5 Vote

Le système de vote traditionnel(sur les papiers) a beaucoup d'inconvénients tels que la perte de registres et la fraude électorale. Blockchain peut changer le système de vote traditionnel par un système de vote numérisé avec une plate-forme sécurisée servant de support à tout le processus(voter, dépister et compter les votes). Les résultats d'un système de vote basé sur la technologie de la blockchain sont transparents parce que les votes peuvent compter et vérifier qu'aucun vote n'avait été supprimé, modifié ou adaptée par l'être humain.

5 Taxonomie des systèmes de blockchain

La diversité de la recherche et du développement de la blockchain offre la possibilité de classer la blockchain en catégories selon un ensemble de critères comme la

décentralisation,l'immuabilité, processus de consensus...

5.1 Blockchain publique

Dans la blockchain publique(sans permission), tous les enregistrements sont visibles pour le public et comme tout le monde pourrait participer au processus de consensus(n'importe qui peut en devenir un nœud)[38] on peut s'attendre à voir une topologie très décentralisée sur un réseau établi. Étant donné que les transactions sont stockées dans différents nœuds du réseau distribué, il est presque impossible de falsifier la blockchain publique. De coté de rapidité car il existe un grand nombre de nœuds sur le réseau public de blockchain la propagation des transactions et des blocs prend beaucoup de temps car le processus de consensus prend beaucoup de temps par rapport au blockchain privé ou consortium[38].

5.2 Blockchain privée

Considérée comme un réseau centralisé car il est entièrement contrôlé par une seule organisation[38] où tous les nœuds du système sont identifiés et connus. Comme seuls les utilisateurs autorisés gèrent la blockchain, il est possible de restreindre l'accès en lecture et de restreindre les personnes qui peuvent émettre des transactions.
Les réseaux blockchain autorisés peuvent ainsi permettre à quiconque de lire la blockchain ou restreindre l'accès en lecture aux personnes autorisées. Ils peuvent également permettre à quiconque de soumettre des transactions à inclure dans la blockchain ou, encore une fois, ils peuvent restreindre cet accès uniquement aux personnes autorisées. Les réseaux blockchain autorisés peuvent être instanciés et maintenus en utilisant un logiciel open source ou fermé [29]. Plus efficace Avec moins de validateurs.

5.3 Blockchain de consortium

Également connu sous le nom d'hybride. Ce type n'est pas contrôlé par une seule autorité mais par un groupe spécifié créé pour contrôler le processus de consensus. La blockchain du consortium est un système «semi-privé» et a un groupe d'utilisateurs contrôlé, mais fonctionne à travers différentes organisations. Ils sont souvent associés à une utilisation en entreprise, avec un groupe d'entreprises collaborant pour tirer parti de la technologie de la chaîne de blocs pour améliorer les processus métier. Comme la blockchain privée il est plus efficace que la blockchain publique.
Une comparaison entre les trois types de blockchain est répertoriée dans le tableau 2.2.

Type de blockchain / Propriété	Blockchain public	Blockchain privé	Blockchain à Consortium
Qui peut la consulter ?	Tout le monde	Seulement les utilisateurs invités	Cela varie
Centralisé	Non	Oui	Partiel
Vitesse de transaction	Lente	Rapide	Rapide
Immutabilité	Presque impossible à falsifier	Pourrait être falsifié	Pourrait être falsifié
Anonymat des utiisateurs	Oui	Non	Non
Détermination du consensus	Tous les noeuds	Une organisation	ensemble de nœuds sélectionné
Permission	Sans autorisation	autorisé	autorisé

TABLEAU 2.2 – Comparaison entre les 3 types de blockchain public, privé, consortieum [38]

6 Conclusion

La technologie Blockchain est un grand registre distribué qui enregistre une liste ordonnée d'enregistrements de transactions (ou de faits) immuables reliées entre elles par une chaîne, sur des blocs, les blocs sont référencés par leur hachage et chaque bloc spécifie explicitement le bloc (hachage) sur lequel il est construit. Dans ce chapitre, nous avons présenté la blockchain et ses concepts qui est une nouvelle technologie révolutionnaire qui a captivé l'attention des chercheurs et des innovateurs dans le monde de la technologie, ainsi que leur fonctionnement. Les différents types de blockchain, et quelques applications de cette technologie dans la vie humaine sont aussi présentés dans ce chapitre.

Dans le chapitre suivant, on va expliquer comment combiner entre les deux technologies blockchain et la biométrie pour la gestion des identités.

CHAPITRE 3

COMBINAISON DE BLOCKCHAIN ET DE BIOMÉTRIE

1 Introduction

De nombreuses recherches ont pris une grande importance ces dernières années, parmi ces très récentes recherches l'intégration des avantages et des caractéristiques des blockchains publiques dans les systèmes biométriques en raison du fort potentiel et des bénéfices. La combinaison des deux technologies (la blockchain et la biométrie) peut apporter plusieurs avantages. Dans ce chapitre, on va parler de cette combinaison, de ses avantages, défis et limites, en commençant d'abord par la présentation des deux possibilités d'intégration.

2 Blockchain et biométrie

La combinaison de la blockchain et de la biométrie pourrait potentiellement présenter de nombreux avantages. En première approximation, la technologie de la chaîne de blocs pourrait fournir aux systèmes biométriques certaines caractéristiques souhaitables telles que l'immuabilité, la responsabilité, la disponibilité et l'accès universel[52]. Elle pourrait aussi sécuriser les gabarits biométriques [53], et assurer la vie privée dans les systèmes biométriques [54].

— Par définition, une blockchain garantit l'immuabilité des registres qu'elle stocke, qui pourraient être utilisés par un système biométrique pour construire un stockage de modèle sécurisé.

— Dérivée de la propriété précédente, une blockchain augmente la responsabilité et l'auditabilité des données stockées, ce qui peut être très utile pour démontrer à

un tiers (par exemple, un régulateur) que les modèles biométriques n'ont pas été modifiés.

— Enfin, une blockchain (publique) offre également une disponibilité complète et un accès universel à tout utilisateur.

De plus, l'intégration de la technologie biométrique serait également très bénéfique pour les blockchains. Parmi de nombreux autres nouveaux cas d'utilisation, la biométrie pourrait considérablement améliorer les schémas d'identité numérique distribués actuels basés sur la blockchain[55].

Une autre application intéressante de la biométrie à la blockchain est liée aux appareils intelligents. Un appareil intelligent est un actif numérique ou physique ayant accès à une chaîne de blocs qui peut effectuer des actions et prendre des décisions en fonction des informations qui y sont stockées. Par exemple, une voiture pourrait être entièrement gérée (louée ou achetée) grâce à un contrat intelligent. Cependant, une identification adéquate de l'utilisateur n'est pas encore entièrement résolue. Dans ce cas, un protocole d'authentification basé sur la biométrie pourrait considérablement augmenter le niveau de sécurité actuel.

Le tableau suivant(Tableau 3.1) donne un aperçu des avantages mutuels de la blockchain et de la biométrie.

Blockchain à la biométrie	- Immuabilité. - Responsabilité. - Disponibilité. - Accès universel.
La biométrie à la blockchain	- Des modèles d'identité numérique plus sûrs. - Nouveaux cas d'utilisation (par exemple, les appareils intelligents). - Portefeuilles biométriques « wallets » :l'une des méthodes les plus utiles pour authentifier les utilisateurs consiste à utiliser leurs informations biométriques. Presque tous les systèmes permettent les utilisateurs à utiliser leurs informations biométri--ques en termes de matériel. De plus, la sécurité des méthodes biométriques est un fait.

TABLEAU 3.1 – Bénéfices mutuels Blockchain / biométrie.
[55]

2.1 Blockchain pour biométrie

De plus en plus, il apparaît que la blockchain est considérée comme la solution ultime à chaque problème. Comme nous avons déjà parlé dans la section précédente, la technologie blockchain donne des solutions aux systèmes biométriques comme la sécurisation des gabarits et la vie privée. Malgré ces opportunités, la technologie blockchain

souffre de certaines limitations potentielles qui doivent être soigneusement étudiés et caractérisés avant la combinaison des technologies biométriques et blockchain.

2.1.1 Défis et limites des blockchaines

Malgré les nouvelles opportunités déjà décrites dans les sections précédentes, la combinaison des technologies blockchain et biométriques n'est pas simple en raison des limitations de la technologie blockchain actuelle.

A. Limites des blockchain actuelles : parmi les limites de blockchain actuelles , on peut citer :
   - Sa capacité de traitement des transactions est actuellement très faible (environ des dizaines de transactions par seconde).
   - Sa conception réelle implique que toutes les transactions du système doivent être stockées, ce qui rend l'espace de stockage nécessaire pour que sa gestion se développe très rapidement.
   - Sa robustesse face aux différents types d'attaques n'a pas encore été suffisamment étudiée[56].

B. Défis des blockchains actuelles : parmi les défis des réseaux publics blockchain pour le déploiement et l'exploitation de systèmes biométriques, on peut citer :

— **Coût économique de l'exécution des contrats intelligents** : afin de prendre en charge les contrats intelligents dans les chaînes de blocs et de récompenser les nœuds qui utilisent leur capacité de calcul pour maintenir le système, chaque instruction exécutée nécessite le paiement d'une redevance dans une crypto-monnaie[56]. Prenant le cas de blockchain Ethereum, où la crypto-monai utilisé appelé gaz. Des instructions simples (comme une somme) coûtent 1 gaz, tandis que d'autres peuvent coûter beaucoup plus cher (par exemple, le calcul d'un hachage SHA3 coûte 20 gaz). En revanche, l'espace de stockage est particulièrement cher (environ 100 gaz pour 256 bits). Par conséquent, l'un des premiers problèmes de recherche serait de minimiser le coût de fonctionnement d'un système biométrique (totalement ou partiellement) dans une blockchain, et de savoir comment les contrats intelligemment efficaces impliquant la biométrie pourraient être codés.

Operation	Gas/kb	ETH/kb	$/kb
Ecrire	6,400	0.000032	$0.00784
Lire	640,000	0.0032	$0.784

Tableau 3.2 – Coûts de stockage non volatils à Ethereum. [56]

— **Confidentialité** : par conception, toutes les opérations effectuées dans une blockchain publique sont connues de tous les nœuds participants. Ainsi, il n'est pas possible d'utiliser directement des clés cryptographiques secrètes, car cela réduirait le nombre d'applications potentielles[56]. En ce qui concerne la confidentialité dans les chaînes de blocs publiques, trois couches principales sont considérées en général :

a) Les participants : Le premier garantit aux participants de rester anonymes à l'intérieur et à l'extérieur de la blockchain. Ceci est réalisé avec des mécanismes cryptographiques comme les suivants :

— Signatures en anneau : Introduites en 2001 par Rivest, Shamir et Tauman [57]. Permet à un signataire de signer un message tout en préservant l'anonymat derrière un groupe, appelé «anneau», qui est sélectionné par le signataire. Les membres de l'anneau doivent être déterminés et leurs clés publiques doivent être fournies. Le signataire utilise sa clé secrète et la clé publique de tous les membres d'anneau pour signer un message. Un vérificateur peut vérifier la validité de la signature, mais ne peut pas savoir qui l'a généré parmi tous les membres possibles de l'anneau[58].

— Adresses furtives : Le système d'adresse furtive permet à l'expéditeur d'une transaction de créer une adresse aléatoire unique au nom du destinataire. Les clés privées de ces adresses sont également liées au compte du destinataire, mais il est impossible pour un tiers d'identifier leurs adresses publiques associées sans connaître leurs clés d'observation. Grâce à ce processus de cryptage, seule la contrepartie concernée peut connaître la transaction.

— Stockage de données privées hors chaîne : Le stockage d'informations sous diverses formes en dehors de la chaîne. Cela devient nécessaire lorsqu'une partie veut vérifier les informations dans la blockchain, mais pas nécessairement les rendre disponibles.

b) Les termes : la confidentialité des termes garde secrète la logique des contrats intelligents, en utilisant par exemple les engagements de Pedersen, qui sont des algorithmes de cryptographie qui permettent à un prouveur de s'engager sur une certaine valeur sans la révéler ou pouvoir la modifier.

c) Les données : pour la biométrie c'est le plus important, l'objectif de la couche de confidentialité des données est de garder les transactions, les contrats intelligents et d'autres données telles que les modèles biométriques cryptés à tout moment, en chaîne et hors chaîne. Les outils cryptographiques utilisés incluent les preuves à divulgation nulle de connaissance(ZKP)(un accord qui permet aux acteurs de prouver que la situation est vraie sans révéler d'informations liées à cette dernière), les engagements Pedersen(des algorithmes de

cryptographie qui permettent à un prouveur de s'engager sur une certaine valeur sans la révéler ou pouvoir la modifier.) ou les couches de confidentialité hors chaîne comme les environnements d'exécution sécurisés (TEE) basés sur le matériel.

Cependant, l'application de ces outils cryptographiques est encore très limitée pour les blockchains.

— **Capacité de traitement** : une autre limitation importante est liée à sa capacité de traitement. Ethereum, par exemple, est capable d'exécuter une douzaine de transactions par seconde, ce qui pourrait ne pas être suffisant pour certains scénarios[56]. De plus, il y a un temps de confirmation minimum avant de considérer que la transaction a été correctement ajoutée à la blockchain. Ce temps peut osciller entre différentes chaînes de blocs, de quelques dizaines de secondes à quelques minutes, ce qui réduit son utilisation pour les systèmes biométriques.

— **Évolutivité** : Il s'avère que l'évolutivité est le plus grand obstacle à l'adoption de la technologie blockchain depuis ses origines jusqu'à aujourd'hui car, théoriquement, tous les nœuds du réseau de la blockchain doivent stocker tous les blocs du réseau de la blockchain. Prenant l'exemple du blockchain publique (Bitcoin), actuellement, sa taille est d'environ 250 Go (2020), et elle augmente très rapidement. Pour certains scénarios d'application tels que les dossiers de santé électronique et l'Internet des objets (IoT), cela peut être un problème[56].

— **Sécurité** : en tant que nouvelle technologie, la caractérisation de la sécurité de la blockchain est toujours en cours. Parmi toutes les attaques possibles, il convient de mentionner l'attaque dite à 51% [59].

Attaque 51% : une attaque à 51% fait référence à une attaque sur la blockchain par un groupe de nœuds de réseau qui contrôlent plus de la moitié de la puissance de calcul du réseau. Cela permet au groupe de nœuds de contrôler efficacement la blockchain(choisir les transactions enregistrées dans la blockchain et rend possible la double dépense)[60]. Il s'agit d'une attaque terrible(dangereuses pour la sécurité) classique car elle peut rendre la blockchain inutilisable. de 51% de la capacité de calcul de toute blockchain publique ou privée, il pourrait inverser ou falsifier les transactions. Cette attaque s'applique même à la blockchain avec des algorithmes de consensus non basés sur la preuve de travail, comme les blockckains basées sur la preuve de participation (PoS) ou la preuve d'autorité(PoA)(expliquées dans le chapitre 2 section 3.4) , généralement utilisés dans les topologies privées ou de consortium.

Il faut signaler aussi que les principaux problèmes de sécurité rencontrés à ce jour par les chaînes de blocs sont principalement liés à des erreurs de programmation, par exemple, l'attaque DAO survenue en 2016, qui a mis en danger

l'ensemble de l'écosystème Ethereum [61]. L'attaquant a découvert une vulnérabilité dans le code source du contrat intelligent de l'organisation The DAO (Decentralized autonomous organization) et collecter de façon récursive un montant estimé à 3.6 millions ETH (environ un tiers de montant total estimé à 12 millions disponibles pour The DAO).

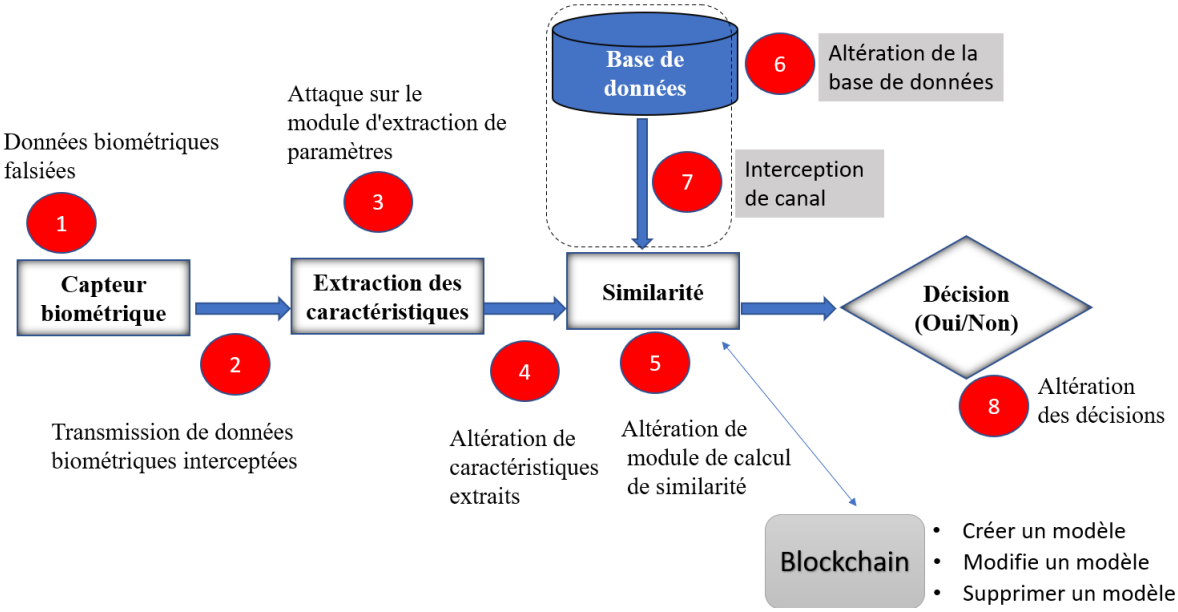

FIGURE 3.1 – Points de compromission d'un système biométrique et protection des modèles biométriques basé sur la blockchain [55]

2.1.2 Protection des modèles biométriques basés sur la blockchain

La figure 3.1 montre les différents points de compromission d'un système biométrique de 1 à 8 (expliqués dans le premier chapitre section 6.1), et comment la technologie blockchain peut sécuriser les points de compromission 6 (Altération de la base de données des modèles biométriques) et 7 (Attaque sur le canal entre la base de données et le module de calcul de similarité). L'un des principaux aspects qui contribuent à la fiabilité du système de blockchain est l'immuabilité dont, une fois qu'une transaction est ajoutée à une blockchain, elle ne peut pas être supprimée ou modifiée. De cette manière, le problème de l'altération de la base de données des modèles biométriques sera résolu. l'attaque 7 peut être résolue par la blockchain, dont, ou lieu d'envoyer les modèles biométriques, seul un hash utilisé dans la blockchain sera envoyé, et quand tout accès à la chaine est détecté, et chaque transaction sera enregistrée sur la blockchain, la technologie blockchain peut diminuer les problèmes de sécurité d'un système biométrique.

2.1.3 Analyse des besoins de stockage

Comme indiqué dans la section précédente, l'une des limites principales de l'intégration des deux technologies est le coût de fonctionnement (totalement ou partiellement) d'un système biométrique basé sur la blockchain. Il est donc crucial d'estimer et de minimiser ce coût. Cette section décrit les différents schémas existants pour stocker de gros volumes de données (par exemple, une base de données des modèles biométriques) dans des chaînes de blocs publiques avec l'exécution des contrats intelligents, comme Ethereum.

Il existe essentiellement trois approches, qui sont présentées ci-dessous en termes de complexité (du plus bas au plus haut), et coût économique (de plus haut à plus bas) [56] :

A) **Stockage complet en chaîne**

C'est le schéma le plus simple et donc le plus inefficace et coûteux. Dans ce cas, les données sont simplement stockées dans la blockchain telles quelles, sans aucun type de prétraitement[56]. Par exemple, des modèles biométriques pourraient être directement stockés sous forme de structure de données dans un contrat intelligent, dans le cadre d'un modèle d'identité numérique plus général.

De manière générale, l'espace de stockage dans les blockchains publiques est particulièrement coûteux par rapport au calcul, afin de décourager son utilisation abusive. Par conséquent, l'utilisation de système de stockage impliquerait généralement un coût prohibitif pour la plupart des applications biométriques. Par exemple, le tableau(Table 3.2) illustre le coût de lecture et stocker 1 kilo-octet de données dans Ethereum en termes d'unités de gaz, éther et dollars américains.

B) **Hachage de données**

Pour surmonter les problèmes du schéma précédent, une approche plus efficace consiste à stocker les données hors chaîne et l'immuabilité intrinsèque. De cette façon, au lieu des données complètes, seule une valeur de hachage est stockée dans la blockchain[56].. Ensuite, le modèle complet peut être stocké dans n'importe quel autre système de stockage externe traditionnel (voir figure 3.2). Cette possibilité offre une grande flexibilité, car l'ensemble complet des modèles biométriques peut être stocké dans un groupe de serveurs inter-connectés(fermes de serveurs).

Même cette approche est plus efficace par rapport à la première(stockage complet en chaîne), elle a un inconvénient est qu'elle est encore nécessaire garantir la disponibilité des données stockées en dehors de la blockchain. Si ces données ont été perdues ou falsifiées, même lorsque cette modification serait toujours remarquée, la viabilité du système serait compromise.

C) **Arbre de merkle**

Enfin, le schéma précédent peut encore être amélioré, grâce à l'utilisation de

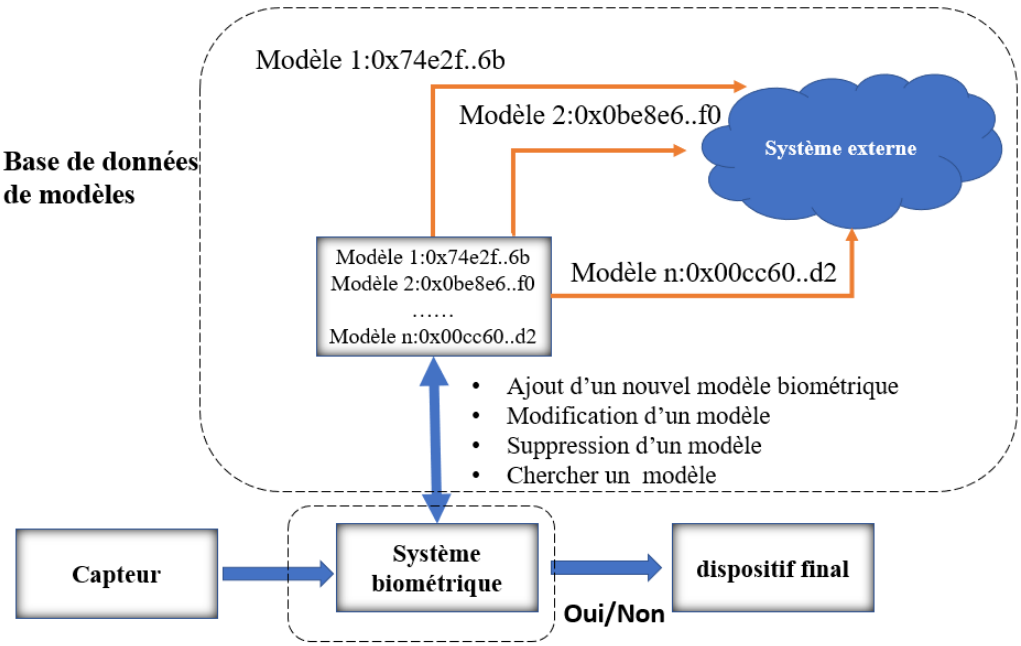

FIGURE 3.2 – Système biométrique utilise des techniques de stockage de hachage de données

l'arbre de Merkle. Cette construction est largement utilisée en cryptographie et des problèmes informatiques tels que la vérification de l'intégrité de la base de données [62], réseaux pair-à-pair [63] et, bien sûr, chaînes de blocs.

La blockchain utilise un réseau P2P où chaque nœud (homologue) doit avoir la même copie de données et de nouvelles données doivent être propagées et vérifiées sur le réseau [34]. La propagation et la vérification des données sur le réseau Pair-à-pair sont longues et coûteuses en calculs. Par conséquent, l'arborescence Merkle est utilisée.

Au lieu d'envoyer des données, seul le hachage des données est envoyé et le pair récepteur vérifie le hachage par rapport à la racine de l'arborescence Merkle, ce qui permet une vérification sécurisée et efficace de structures de données plus grandes et garantit l'intégrité des données.

Concernant la protection du modèle biométrique à l'aide de la technologie blockchain, un système biométrique utilisant cette technique conserverait un arbre de Merkle, stockant un modèle à chaque nœud et stocker le nœud racine de l'arbre de merkle dans un contrat intelligent[56].

Par conséquent, lorsqu'un nouveau modèle biométrique est créé (après la phase d'inscription), ou une version existante est modifiée ou supprimée, l'arborescence est recalculée et la nouvelle racine est mise à jour dans la blockchain. Un schéma simplifié de cette approche peut être trouvé sur la Figure 3.3.

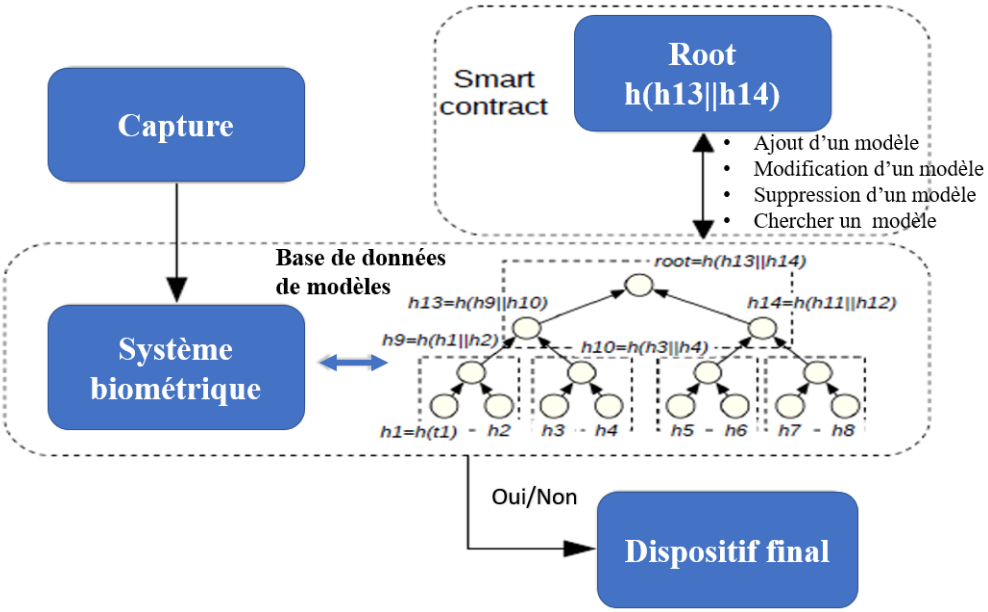

FIGURE 3.3 – Système biométrique utilise des techniques de stockage de l'arbre de merkle

2.2 Biométrie pour blockchain

Dans la blockchain, les actifs qui appartiennent à un participant sont contrôlés via la clé privée d'une paire de clés asymétriques qui appartient au participant. Bien que cela permette aux participants au réseau de blockchain d'avoir la souveraineté sur leurs actifs, cela implique la responsabilité de gérer leurs propres clés. Actuellement, il existe deux problèmes majeurs dans la gestion des clés :

a) les utilisateurs ne disposent pas d'un moyen efficace et sécurisé pour stocker leurs clés.

b) en cas de perte des clés aucun mécanisme de récupération efficace n'existe.

2.2.1 Sécurisation des clés en utilisant les données biométriques

Comme nous l'avons vue dans le chapitre précédent(Chapitre 2), les clés asymétriques jouent un rôle essentiel dans l'identification des participants au réseau et le contrôle des actifs du réseau blockchain, dont pour faire une transaction dans un réseau blockchain, chaque transaction est signée par la clé privée de l'utilisateur et vérifiée par la clé publique. La clé publique peut-être partagée avec n'importe qui et un correspondant clé privée qui doit être stockée cachée. La clé privée est stockée dans le dossier de l'utilisateur portefeuille(Wallet). Par conséquent, la sécurité du portefeuille est principalement la sécurité de la clé privée qu'il contient, dont avoir accès à la clé privée correspondant à un compte est suffisant pour gérer et utiliser ce compte. Parmi les solutions existent pour la protection des portefeuilles qui contiennent les informations sensibles comme les informations financières, médicales..etc, par les données

biométriques :

2.2.2 Chiffrement et déchiffrement des clés privées à l'aide d'empreintes digitales

Il est simple d'utiliser des méthodes de cryptage symétriques traditionnelles telles que Data Encryption Standard (DES) pour le cryptage et le décryptage symétriques, où la même clé et une seule clé sont utilisées pour effectuer le cryptage et le décryptage. Comme l'empreinte digitale est un trait biométrique unique, et offre une bonne identification par rapport aux codes d'accès sélectionnés traditionnellement. Elle est utilisée pour générer la clé utilisée dans le cryptage symétrique[64].

L'idée est de créer d'abord une clé symétrique (hachage) à l'aide des données d'empreintes digitales du propriétaire, puis d'utiliser la clé symétrique pour chiffrer la clé privée. Dans le cas de déchiffrement, si la clé générée est le même que le génère dans la phase d'enregistrement(C'est-à-dire les images d'empreinte numérique correspondant), ont utilisant le même algorithme symétrique utilisé dans le chiffrement et la clé générée , la clé privée chiffrée est déchiffrée.

3 Etat de l'ART

Le domaine de la combinaison de la blockchain et de la biométrie est très récent. Dans la littérature, on ne trouve que quelques travaux scientifiques qui offrent des propositions de fusion de ces deux concepts ensemble.

Dans [55], les auteures ont discuté des principales caractéristiques et limites des blockchains, en particulier celles qui pourraient directement affecter la mise en œuvre des systèmes biométriques. Ils ont également exploré les avantages mutuels potentiels pour les deux technologies et discuté d'une première approximation d'une architecture combinée en utilisant la blockchain pour la protection des modèles biométriques.

Ces mêmes auteurs ont exploré dans [55], la viabilité des systèmes biométriques basés sur la blockchain en mettant l'accent sur le stockage des modèles biométriques. Ils ont d'abord discuté des principaux schémas de stockage des blockchains publiques (Ethereum), et mis en place un contrat intelligent pour l'estimation de son coût de stockage. Les résultats obtenus prouvent que des schémas simples tels que le stockage direct des modèles biométriques en chaîne ou le hachage direct des données ne conviennent pas à un véritable système biométrique.

Cependant, lorsque les arbres de Merkle sont inclus en tant que structure de données intermédiaire, les coûts de stockage deviennent fixes quel que soit le volume total de données à stocker, et des temps d'exécution réduits. Deux études basées sur la biométrie faciale et de signature ont été le cœur des expérimentions appliqués dans ce

papier.

Dans le même champ de recherche, ces auteurs ont discuté dans [65], des opportunités et des défis dans l'intégration de la blockchain et de la biométrie, en mettant l'accent sur le stockage et la protection des modèles biométriques, un problème clé en biométrie encore largement non résolu. Les compromis clés impliqués dans cette intégration, à savoir la latence, le temps de traitement, le coût économique et les performances biométriques, sont étudiés expérimentalement grâce à la mise en œuvre d'un contrat intelligent sur la plateforme de blockchain Ethereum.

Pour une solution plus concrète, les auteurs de [66] ont proposé une architecture pour le système des documents d'identité électronique biométrique (e-ID) basé sur Blockchain pour la vérification d'identité des citoyens dans les transactions correspondant au notaire, à l'enregistrement, à la déclaration et au paiement des impôts, aux services de santé de base et à l'enregistrement des activités économiques, entre autres.

Pour valider l'authentification de l'utilisateur, un système d'identification électronique biométrique est utilisé pour éviter l'usurpation d'identité et les attaques associées. Le mécanisme d'authentification proposé combine l'utilisation de la carte à puce (contient les modèles d'iris et d'empreinte digitale) et les caractéristiques biométriques (modèle d'iris) . En conséquence, ce mécanisme évite le vol d'identité pour le propriétaire du document et contrôle que seul le propriétaire peut accéder aux services de gouvernement électronique. De plus, pour valider le document, un certificat numérique est utilisé avec la clé publique et privée correspondante pour chaque citoyen en utilisant le code PIN d'un utilisateur. Le processus de validation des transactions proposé a été mis en œuvre sur un système Blockchain afin d'enregistrer et de vérifier les transactions effectuées par tous les citoyens inscrits au recensement électoral, ce qui garantit la sécurité, l'intégrité, l'évolutivité, la traçabilité et l'absence d'ambiguïté.

De plus, une architecture de réseau Blockchain est présentée de manière distribuée et décentralisée comprenant tous les nœuds du réseau, la base de données et les entités gouvernementales telles que le registre national et les bureaux de notaire. Les résultats de l'application d'un nouvel algorithme de consensus au réseau Blockchain sont également présentés montrant le temps d'exploration, la mémoire et l'utilisation du processeur lorsque le nombre de transactions augmente.

Dans [67], un nouveau mécanisme de distribution des clés est proposé pour la gestion des identités basée sur la blockchain pour l'authentification des utilisateurs, en utilisant la biométrie. Cet article propose un nouveau mécanisme de gestion des clés pour la gestion des identités basée sur la blockchain pour l'authentification des utilisateurs. L'analyse rigoureuse est présentée pour montrer que le protocole proposé est protégé contre diverses attaques possibles.

4 Conclusion

La Blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. La blockchain est composée d'un ensemble de blocs reliés entre eux avec un hash(ID) dont chaque bloc contient le hachage de bloc précédent de telle manière compose la chaine de blocs.

Comme nous avons vu, l'intégration de la technique récente blockchain et la biométrie est un nouveau domaine de recherche qui attire l'attention des chercheurs actuellement et au futur. Cela est dû aux bénéfices mutuels de ces techniques.

La blockchain peut fournir aux systèmes biométriques certains caractéristiques tels que, l'immuabilité, la responsabilité, la disponibilité ou l'accès universel. Puisque l'avantage est mutuel, la blockcahain pourrait bénéficier de la biométrie, et améliore schémas d'identité numérique distribués actuels.

Basé sur ce qui est présenté auparavant, et pour profiter des caractéristiques des blockcains pour les systèmes biométriques, notre proposition de combinaison du système biométrique et blockchain -présentée dans le chapitre suivant- est autour l'intégration d'un système biométrique dans une architecture blockchain.

CHAPITRE 4

SÉCURISATION D'UN SYSTÈME D'AUTHENTIFICATION BIOMÉTRIQUE PAR UNE BOCKCHAIN

1 Introduction

Dans le cadre de ce projet intitulé « Combinaison de Blockchain et Biométrie pour la Gestion des Identités », nous avons développé une application décentralisée appelée BioBlockchain_Application pour améliorer la sécurité d'un système d'authentification biométrique qui s'appuie sur la technologie blockchain, afin d'assurer la sécurisation des modèles biométriques contre l'attaque d'altération des templates, et l'attaque de canal entre la base de données et le module de calcul de similarité.

Dans la littérature, les architectures proposées pour la sécurisation des systèmes biométriques par la technologie de blockchain sont rares et sont généralement basés sur l'utilisation de blockchaine Ethereum en écrivant des contrats intelligents. Dans notre travail, nous avons proposé deux solutions :

— Implémentation d'une architecture blockchaine et sa combinaison avec un système d'authentification des empreintes digitales, pour une solution privée.

— Utilisation de la blockchain Ethereum (Ethereum Test), pour une solution publique.

La section suivante explique en détail nos propositions, leur implémentation et les différents outils utilisés.

2 Solutions proposées

Comme nous avons vu dans le chapitre 1, les points d'attaque d'un système biométrique sont variés (voir la figure 4.1). Nos solutions proposées dans ce travail visent les points 6 et 7 de la figure 4.1 :

— **Base de données** : comme nous avons vu déjà, la base de données des modèles biométriques peuvent être disponible localement, à distance ou distribuée sur plusieurs serveurs. Ce type de stockage rendre le système vulnérable aux attaques d'altération dont, une attaque sur ce point du système peut empêcher un utilisateur légitime d'y accéder ou d'autoriser un imposteur.

— **Canal** :l'interception de canal permet un accès avec modification des informations transmises sur la voie de communication avec l'intention de détruire les messages, de les modifier, d'insérer des nouveaux messages, de provoquer un décalage dans le temps ou la rupture dans la diffusion des messages. la sécurisation de canal entre la base de données et le module de calcul de similarité est assurée par nos applications.

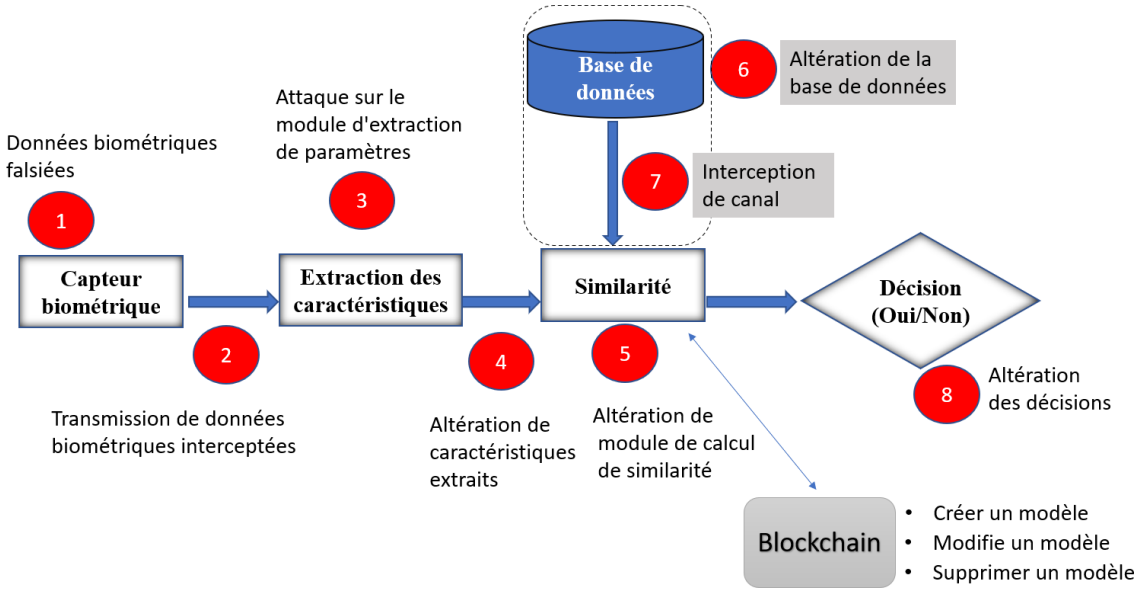

FIGURE 4.1 – Points de compromisiion d'un système biométrique et protection des modèles biométrique basé sur la blockchain

Alors, notre travail consiste à proposer une solution pour sécuriser un système d'authentification biométrique en utilisant la technologie de Blockchain, et en ciblant les deux points d'attaques discutées auparavant (altération de la base de données et l'interception de canal entre la base de données et le module de calcul de similarité).
Afin d'assurer ce but, nous avons adopté deux solutions :

— dans la première solution, nous avons simulé le fonctionnement complet assuré par une blockcahin. Puis, nous avons combiné le fonctionnement d'un système d'au-

thentification biométrique avec celui de la technologie de blockchain, en l'adaptant avec les besoins de sécurisation des modèles biométriques. Cela assurer une solution qui peut être utilisée dans un environnement privé (à l'intérieur d'une entreprise par exemple).

— dans la deuxième solution, nous avons utilisé le concept de contrat intelligent (smart contract en anglais) et la blockcahin Ethereum. Cette solution permet d'avoir un accès public au contrat intelligent, et avoir une solution publique au problème.

2.1 Première solution : implémentation d'une blockchaine privée

Cette solution nous permette de comprendre mieux et de simuler le fonctionnement d'une blockchain et son utilisation pour la manipulation et sauvegarde des données biométriques.
Basant sur le code trouvé dans [68], qui est le code d'une version simplifiée d'une blockchain, nous avons réalisé notre propre solution en :

— intégrant l'utilisation de l'arbre de Merkle.

— adaptant la structure de transition et de bloc pour nos besoins.

— combinant un système biométrique avec la blockchain.

2.1.1 Fonctions assurées par la première solution

Dans cette première solution :

— les fonctionnalités telles que l'ajout, la modification et la suppression des vecteurs (templates) de caractéristiques et l'authentification des agents sont assurés.

— deux types d'utilisateurs du système sont permet : administrateur et agent. L'agent doit s'authentifier afin d'utiliser le système (voir figure 4.2). L'administrateur est responsable d'ajout, de suppression et de modification des templates des agents. Il faut signaler que l'administrateur est avant tout un agent qui doit être s'authentifier avant de pouvoir finaliser leurs tâches (voir figure 4.3).

— les données biométriques (vecteur de caractéristiques extrait d'empreinte digitale) sont hachées par une fonction de hachage, et utilisées avec un identifiant (ID) afin de s'authentifier. Les templates hachées sont sauvegardés dans un arbre de Merkle, dont les feuilles de l'arbre de Merkle présentent les haches des templates.

— toute transaction faite par l'un des deux acteurs (agent et administrateur) est enregistrée sur la blockchain.

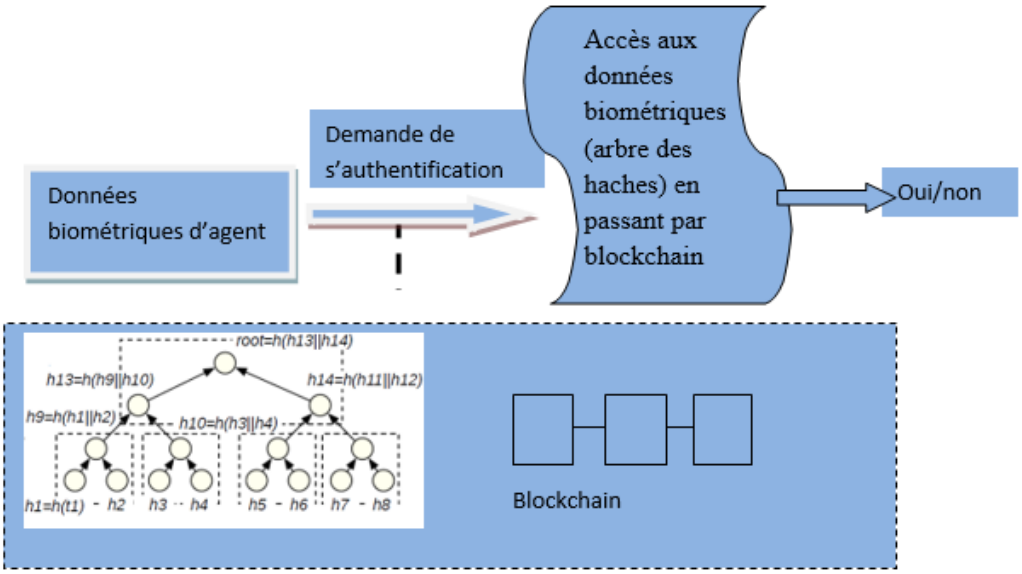

FIGURE 4.2 – Fonctionnalités d'agent

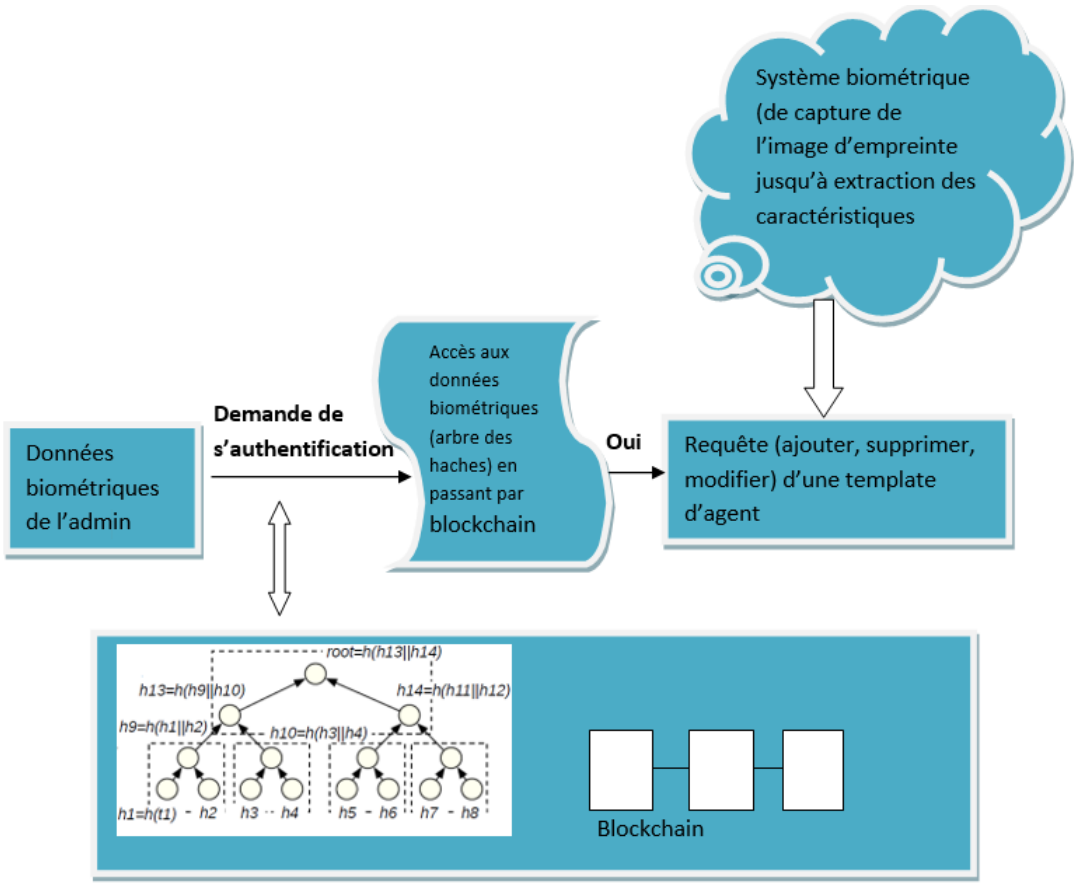

FIGURE 4.3 – Fonctionnalités d'administrateur

2.1.2 Environnement de développement

A) **Langages de programmation**

Dans notre application, nous avons utilisé les langages suivants :

— **Python version 3.7** : Python est un langage de programmation interprété, orienté objet et de haut niveau avec une sémantique dynamique. Ses structures de données intégrées de haut niveau, associées à un typage dynamique et à une liaison dynamique, le rendent très attractif pour le développement rapide d'applications, ainsi que pour une utilisation en tant que langage de script ou de collage pour connecter des composants existants entre eux. La syntaxe simple et facile à apprendre de Python met l'accent sur la lisibilité et réduit donc le coût de la maintenance du programme. Python prend en charge les modules et les packages, ce qui encourage la modularité du programme et la réutilisation du code. L'interpréteur Python et la bibliothèque standard étendue sont disponibles sous forme source ou binaire sans frais pour toutes les principales plates-formes, et peuvent être librement distribués.

— **HTML 5 (HyperText Markup Language 5)** : est une version du HTML (format de données conçu pour représenter les pages web). Cette version a été finalisée le 28 octobre 2014.

— **CSS3** : l'acronyme CSS signifie Feuilles de style en cascade, utilisé pour augmenter la fonctionnalité et la polyvalence, et une performance efficace du contenu du site. Il permet la création des sites Web riches en contenu qui ne nécessitent pas beaucoup de poids ou de codes, cela se traduit par des graphiques et des animations plus interactifs, une interface utilisateur supérieure, une organisation beaucoup plus importante et un temps de téléchargement plus rapide.

— **Flask** : est un Framework d'application Web WSGI (Web Server Gateway Interface) léger. Il est conçu pour faciliter et accélérer la mise en route, avec la possibilité de s'adapter à des applications complexes.

B) **IDE**

Nous avons utilisé jetBrains PyCharm 2020 (développé par l'entreprise tchèque JetBrains), qui est un environnement de développement intégré utilisé pour programmer en Python. Il permet l'analyse de code et contient un débogueur graphique. Il permet également la gestion des tests unitaires, l'intégration de logiciel de gestion de versions, et supporte le développement web avec Flask.

2.1.3 Architecture de blockchaine adaptée

Nous avons proposé une structure de blockcahin adaptée à la manipulation des données biométriques.

a. **Transaction**

Les champs proposés d'une transaction sont :

- Type transaction (ajoute, suppression, modification ou authentification).
- AgentIdentifiant : contient Id + Template haché + Type (administrateur ou agent).
- Template ajoutée : ce champ contient le hache d'une template à ajouter. Il prend la valeur -1 dans le cas d'un agent, et Id + TemplateHaché + Type dans le cas d'un administrateur.
- Adm : pour savoir le type d'un acteur. Il prend la valeur 1 si l'acteur est un administrateur et ou 0 s'il est un agent.
- Timestamp : pour le temps d'une transaction.

b. **Bloc**

Chaque bloc contient les éléments suivants :

- Index de bloc, le premier bloc (genesis bloc a l'index 0).
- Transactions : l'ensemble des transactions qui contient le bloc.
- Timestamp : pour le temps d'un bloc.
- Previous hash : hash de bloc precedent.
- Nonce : initialisé par 0, est incrémenté chaque fois au cours de calcul de hash de bloc jusqu'à l'obtient le hash spécifié.
- Merkle_tree_root_hash : Hash de les transactions de bloc.
- RoutTempTree : Roote de l'arbre de tous les templates hachés (l'arbre de Merkle).

c. **Minage**

Le processus de minage est utilisé à la validation d'un bloc. Cette fonction sert d'interface pour ajouter les transactions en attente à un bloc afin de les ajouter aux blockchains. Cela est réalisé en utilisant l'algorithme de consensus « la preuve de travail » (voir le point suivant). Après l'étape de détermination de la preuve de travail, une vérification de bloc sera appliquée sur le bloc avant son ajout à la blockchain.

La vérification est faite en trois niveaux :

- vérification de la validité de la preuve de travail : on vérifie si la preuve de travail de bloc est valide ou non, plus précisément on vérifier est ce que le hash de bloc commence par deux zéros successive (la difficulté utilisée dans notre algorithme de consensus).
- vérification que la référence vers le bloc précédent dans le bloc et le hash de dernier bloc dans la chaîne correspondent.
- vérification de la validité de la valeur de RoutTempTree par le recalcul de la valeur de hash de la racine de l'arbre de Merkle et son comparaison avec la valeur dans le bloc qui pourrait ajouter dans la chaine.

d. **Consensus**
Dans notre proposition, l'algorithme de consensus utilisé c'est la preuve de travail. Il consiste à trouver un hash pour le bloc commence par un certain nombre de zéros (la difficulté), nous avons utilisé une difficulté égale à 2, ce qui signifie, chaque mineur doit trouver un hash commence par deux zéros par exemple 00a39sd4f54rr7. . . . L'objectif d'utiliser cette simple difficulté pour rendre l'ajoute d'un bloc plus rapide et juste pour mettre les noeuds en d'accord.

2.1.4 Comment les données biométriques sont sécurisées dans notre proposition ?

Les données biométriques sont sécurisées dans notre solution comme suit

— **L'arbre des haches des templates** : dans notre proposition, la base de données des modèles biométriques est remplacé par un arbre de Merkle sauvegardé sur le réseau. La première étape sert à calculer les haches des vecteurs extraits à partir des empreintes digitales. Les feuilles de l'arbre de Merkle contiennent ces haches des données biométriques, puis de concaténer les haches résultantes deux à deux et de les hacher, et ainsi de suite jusqu'à l'obtient d'un seul hash qui s'appelle Racine de Merkle (Merkle root) qui est nommé RoutTempTree dans notre application. La valeur de RoutTempTree est calculée à chaque fois un bloc sera ajouté aux blockchains. Dans l'état normal de fonctionnement de notre système, quand une opération d'écriture (ajoute, suppression ou modification) dans la blockchain, la valeur de RoutTempTree sera changée. Contrairement dans les opérations de lecture (authentification ou recherche), la valeur reste la même. Dans ce dernier cas, si elle est changée on détecte qu'il y a une altération illégale dans le système et on détecte au niveau de quel bloc.

— **La blockchain** : utilisée pour enregistrer tout accès à la l'arbre des haches des templates, d'où chaque opération sera enregistrée dans l'historique de la blockchain. Ce fonctionnement d'une blockchain permet de résoudre le problème de canal entre la base de données et le module de calcul de similarité.

Comme la montre dans la figure 4.4, la valeur de l'arbre de hashes des templates biométriques dans le premier bloc (root_temp_tree) est : '59c39247d3a96bb85ce79be371f0cfe2b704b15fe6bff5714ac915b693717bc2' (point A dans la figure 4.4), après une opération de lecture (transaction sur la blockchain de type recherche) la valeur de hash de l'arbre de Merkle des templates reste la même (point C dans la figure 4.4). Après une opération d'écriture (transaction sur la blockchain de type ajoute), la valeur de root_temp_tree été changé et devenue : '6e0fecf98de367884a41938c99c5b5fef644f9eeb3ca05a2a0b2fc7d1ed34426' (point E dans la figure 4.4).
Si la valeur de root_temp_tree changé illégalement, elle sera détectée et dans quel

FIGURE 4.4 – Valeur de root_temp_tree dans différents blocs après différents opérations (transactions)

bloc. D'une autre cotée chaque accès à l'arbre de haches de templates sera détecté et enregistré dans les transactions dans la blockchain, alors les problèmes d'altération des bases de données des modèles biométriques et l'interception de canal seront résolus. seront résolus.

2.1.5 Les interfaces de l'application BioBlockchain_Application

L'utilisation de notre application BioBlockchain_Application se fait à travers une page d'authentification appelé « authentifacation.html » qui offre 2 liens vers d'autres pages « agent.html » et « admin.html ».

A) **Page authentifacation.html** : dans cette page, l'utilisateur doit s'authentifier pour accéder au système, elle contient les éléments suivants :

- type d'accès au système, il existe deux options « Agent » et « Admin » dont l'utilisateur doit sélectionner son type d'accès au système.
- User id : ou l'utilisateur doit entrer son id pour l'authentification.
- un champ pour sélectionner l'image d'empreinte d'utilisateur.
- Login : bouton pour valider les informations remplis. Si les informations sont correctes, une autre page sera affichée selon le type d'utilisateur (page admin si l'utilisateur est un admin ou page agent si l'utilisateur est un agent).
- Reset : pour effacer les informations remplies et reremplir à nouveau.

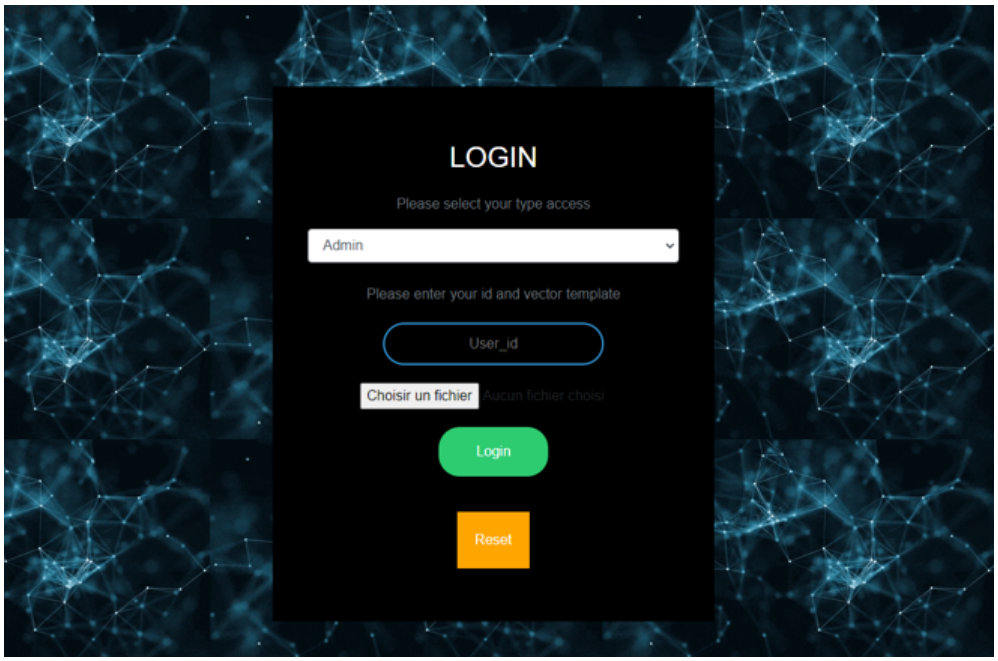

FIGURE 4.5 – Page authentification.html)

B) **Page agent.html**

Dans cette page, on affiche une page pour informer l'agent qu'il est authentifié, et peut accéder au système.

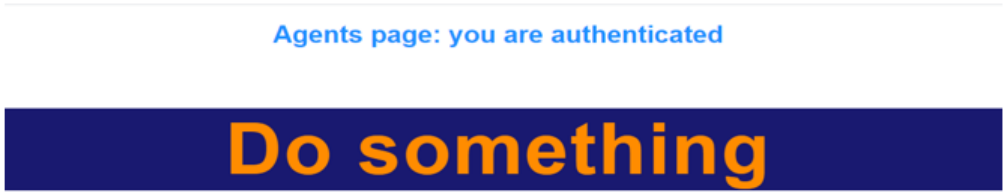

FIGURE 4.6 – Page agent.html)

C) **Page admin.html**

La page admin est la page la plus importante dans notre application, car la gestion de système se fait dans cette page, elle se compose de 4 options :

— **ajouter un utilisateur** : dans cette partie, l'admin peut ajouter des utilisateurs au système, l'ajoute se fait après l'insertion de l'id de l'utilisateur

et son type avec son empreinte digitale et le clic sur le bouton « Add ».

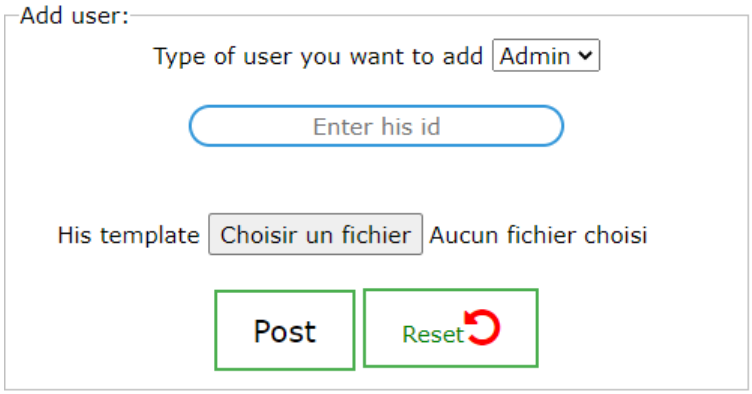

FIGURE 4.7 – Ajouter un utilisateur

— **Effacer un utilisateur** : l'effacement d'un utilisateur se fait après l'insertion de l'id de l'utilisateur et son hash et le clic sur le bouton « Delete ».

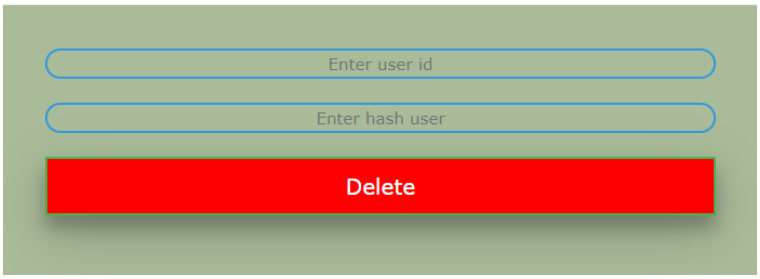

FIGURE 4.8 – Effacer un utilisateur

— **Modifier un utilisateur** : pour modifier un utilisateur, l'admin doit entrer l'id de l'utilisateur ainsi que leur hash, puis entrer les nouvelles valeurs, et cliquer sur le bouton modifier.

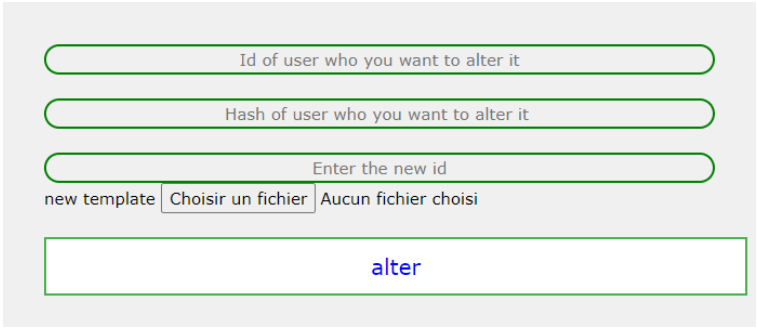

FIGURE 4.9 – modifier un utilisateu

— **Chercher un utilisateur** : cette opération a le rôle de tester l'appartient d'un utilisateur ou non dans notre système. Les étapes suivies pour chercher

un utilisateur dans notre système sont : l'insertion de son id et son hash, puis le clic sur le bouton « Search ».

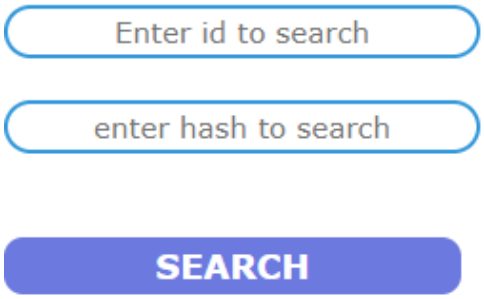

FIGURE 4.10 – Chercher un utilisateu

Avec les options expliquées (ajout, suppression, modification et la recherche), il existe aussi 2 boutons dans la page admin sont :

— **bouton request to mine** : ce bouton sert à faire la dernière étape de l'ajout des blocs dans la Blockchain. En cliquant sur ce bouton request to mine, toutes les transactions en attente (non confirmées) seront ajoutées à la blockchain en les ajoutant au bloc et en déterminant la preuve de travail.

— **bouton Historique** : ce bouton permet d'afficher tous les détails de toutes les opérations (transactions) effectuées dans notre application.

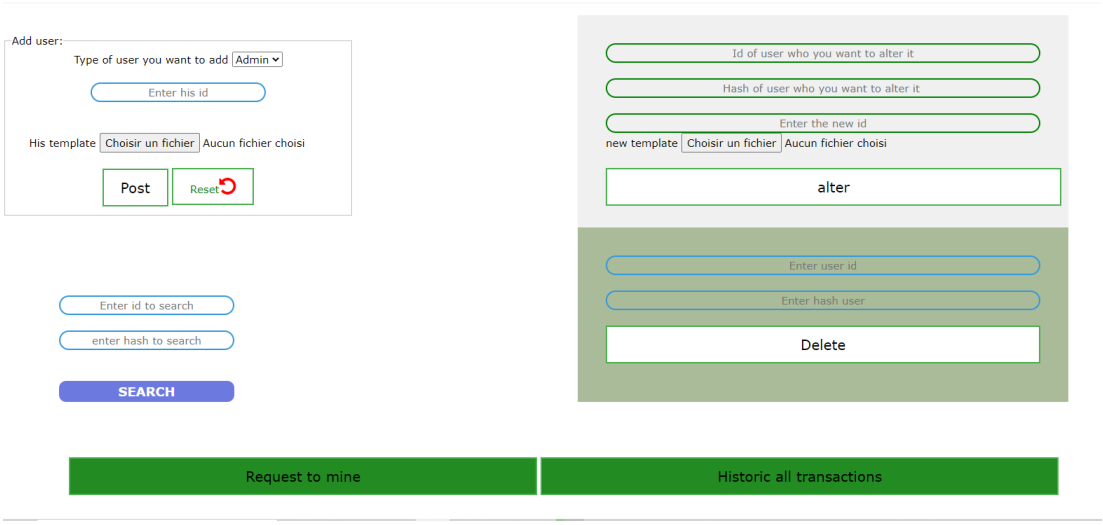

FIGURE 4.11 – Page admin

2.2 Deuxième solution : Utilisation de blockchain Ethereum

L'architecture utilisée dans cette partie remplace la base de données de modèles habituels d'un système biométrique par une blockchain, en ajoutant des opérations de base (c'est-à-dire, la création, la modification et la suppression de modèles) grâce à l'utilisation de **smart contract**. Cette conception offre certains avantages :

— les modifications apportées aux architectures biométriques existantes sont minimes, de sorte que les techniques et algorithmes biométriques habituels (par exemple, l'extraction et l'appariement de caractéristiques) peuvent être utilisés normalement.

— pas besoin d'utiliser des smart contracts complexes, ce qui facilite le développement et réduit les coûts d'exécution. Les contrats intelligents n'implémentent pas de «logique» biométrique, mais seulement les fonctions minimales nécessaires pour gérer le stockage des modèles.

2.2.1 Réseau utilisé

Comme nous avons vu dans le chapitre 2 section 4.2, Ethereum est une plate-forme informatique conçue pour faciliter les contrats intelligents dans lesquels Ether est la crypto-monnaie utilisée. Nous avons utilisé le réseau Ethereum « Test Net » car les transactions et l'écriture dans le Réseau principal Ethereum coutent du gas qui coute aussi de l'éther. Contrairement au réseau Test Net qui ne contient que des faux éthers gratuits et faciles à collecter.

Test Net : réseau utilisé pour tester les contrat intelligents (Smart contract) et les DApp (Decentralised application) avant d'être déployée dans le réseau principale ethereum. Actuellement, il existe 4 types de réseau test Ethereum différent selon le mécanisme de consensus utilisé. Ces quatre types sont expliqués comme suit :

— Réseau de test Ropsten : un réseau de test Proof-of-Work pour Ethereum. Pour acquérir l'ETH sur Ropsten, on peut miner sur le réseau.

— Réseau de test kovan : un réseau de test de preuve d'autorité (proof of authority) pour Ethereum. Pour acquérir l'ETH sur Kovan, on peut le demander à un robinet (des sites web qui offrent aux visiteurs ETH gratuitement en échange de l'exécution de plusieurs tâches).

— Réseau de test Rinkeby : un réseau de test de preuve d'autorité pour Ethereum. Pour acquérir l'ETH sur Rinkeby, on peut le demander à un robinet.

— Réseau de test Goerli : un réseau de test Proof-of-Authority pour Ethereum. Pour acquérir l'ETH sur Görli, on peut utiliser le pont à étranglement unidirectionnel de l'un des trois autres réseaux de test (Ropsten, Kovan, rinkeby)

Nous avons utilisé le réseau de test **Ropsten**.

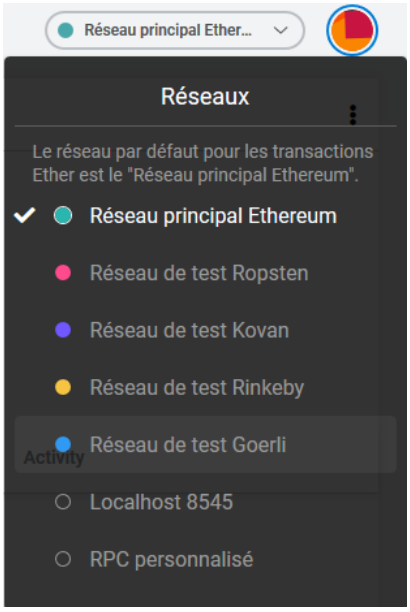

FIGURE 4.12 – Types de réseau ethereum

2.2.2 Environnement de développement

a. **Langage de programmation**

Le langage le plus connu et le plus répandu pour les smart contract, et que nous avons utilisé dans notre programmation de smart contract, est le langage de programmation **solidity**. Ce langage est un langage de haut niveau orienté objet pour la mise en œuvre de contrats intelligents. Ce langage est devenu presque un standard pour la rédaction des smart contract. Solidity est de type statique, prend en charge l'héritage, les bibliothèques et les types complexes définis par l'utilisateur, entre autres fonctionnalités.

b. **IDE**

Remix IDE permet de développer, déployer et administrer des contrats intelligents pour Ethereum comme des blockchains. Il peut également être utilisé comme plateforme d'apprentissage.

2.2.3 Développement et déploiement de smart contract sur le réseau test Net

Dans cette partie nous expliquons les étapes suivies dans notre développement et déploiement de smart contract.

a. **Création d'un compte (portefeuille) dans le réseau**

Nous avons créé un compte sur le réseau à l'aide de **MetaMask** (extension ajoutée au navigateur pour le transformer à un navigateur Blockchain car la plupart des navigateurs web ne se connectent pas aux réseaux décentralisés). Ce compte contient notre adresse ainsi que l'ether utilisé dans Ethereum.

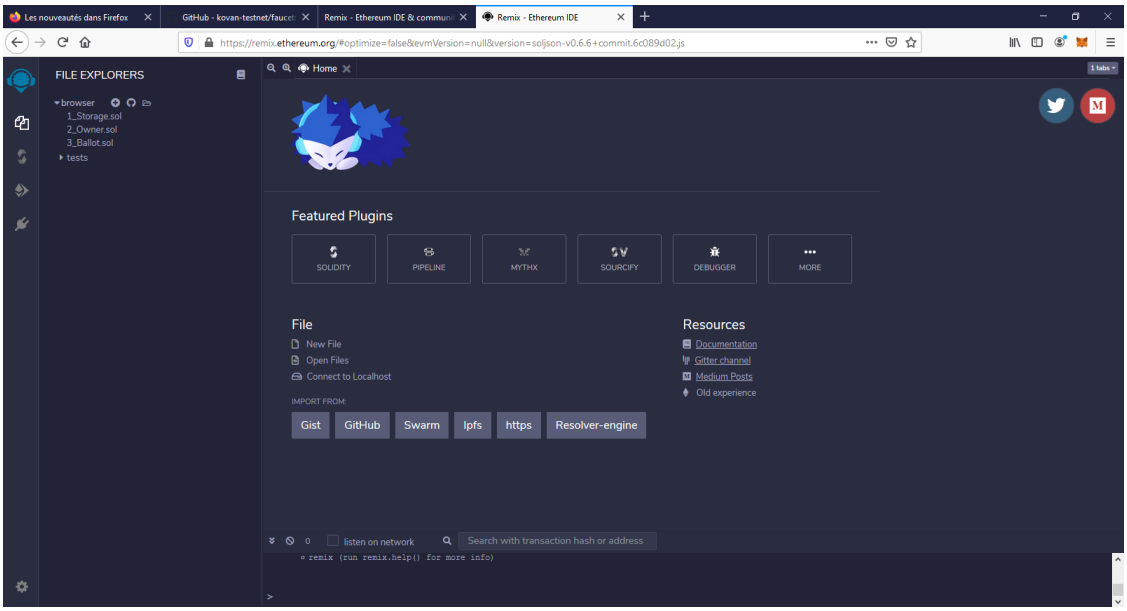

FIGURE 4.13 – Interface de remix IDE

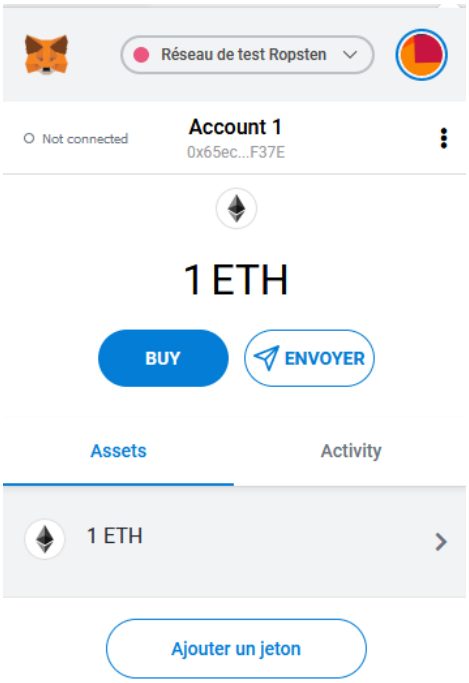

FIGURE 4.14 – Notre propre portfeuille

b. **Récolter ethers**

Nous avons récolté des faux éthers par la demande sur des sites appelés faucet, ces derniers nous envoie d'éther quand on entre notre adresse et cliquer sur obtenir de l'éther.

c. **Création de notre smart contract**

Basant sur le code trouvé dans [56], on a créé une smart contract nommé « smart.sol » dont l'extension .sol réfère aux silodity (langange de programmation

utilisé lors de création de smart contract). Nous avons utilisé le réseau test de Ropsten. Premièrement on a testé le code dans notre propre machine par la sélection d'environnement d'exécution JavaScript VM comme le montre dans la Figure 4.15 Après le déploiement de notre smart contract localement, le résultat

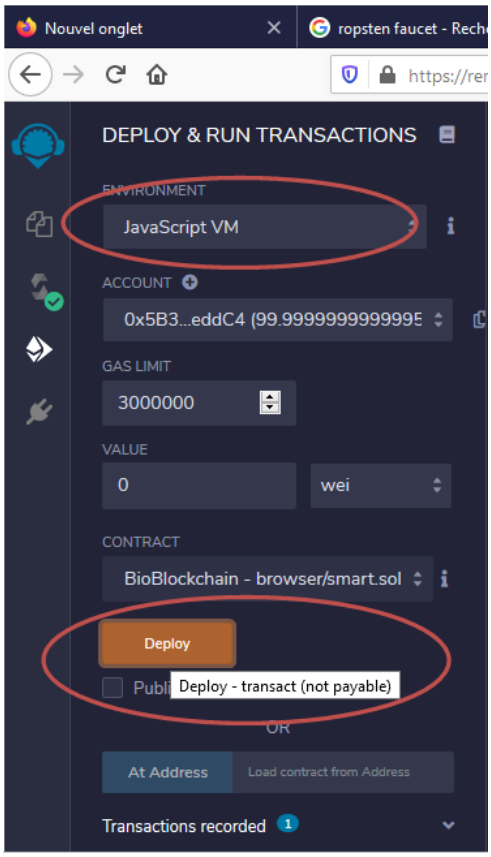

FIGURE 4.15 – Environnement d'exécution de smart contract localement

d'exécution est apparu, dans notre programme (smart contract), on a 4 opérations :

— **createNewTemplate** : pour stocker un nouveau modèle biométrique.

— **deleteTemplate** : pour supprimer un modèle.

— **modifyTemplate** : pour modifier un modèle.

— **getTemplate** : pour chercher un modèle s'il existe ou non.

Après l'exécution dans notre propre machine sans aucun problème, la dernière étape est le déploiement sur le réseau TestNet, cette étape est validée par la sélection d'environnement Injected web3 et clique sur « deploy ». Puisque cette opération consomme une somme d'ethers, une fenêtre de confirmation de l'opération est affichée, alors la transaction est confirmée et ajoutée à un block, ce dernier est ajouté dans la blockchain.

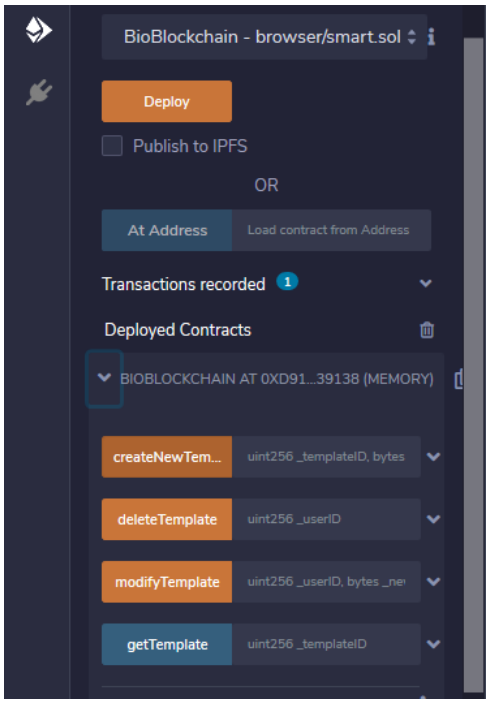

FIGURE 4.16 – Résultat de smart contract

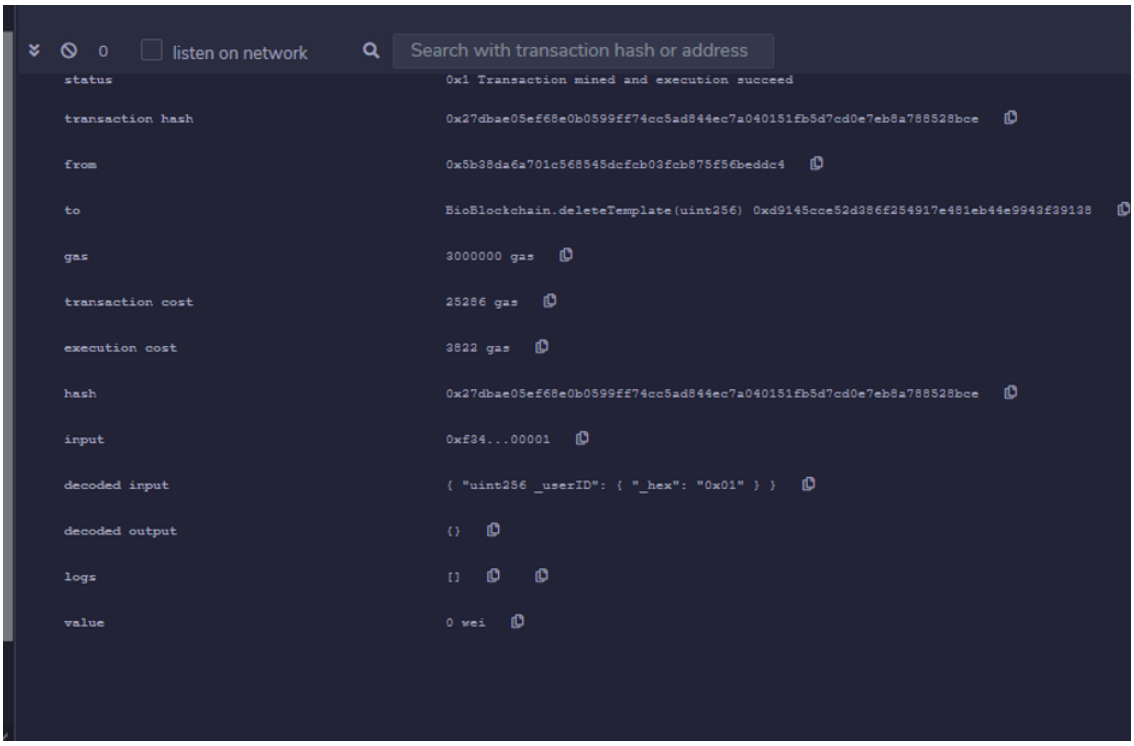

FIGURE 4.17 – Résultat d'une suppression (deleteTemplate)

2.2.4 Comment les données sont sécurisées dans cette solution ?

La sécurisation est assurée par le principe de fonctionnement d'une blockchain et un smart contract.

FIGURE 4.18 – Fenêtre de confirmation de transaction

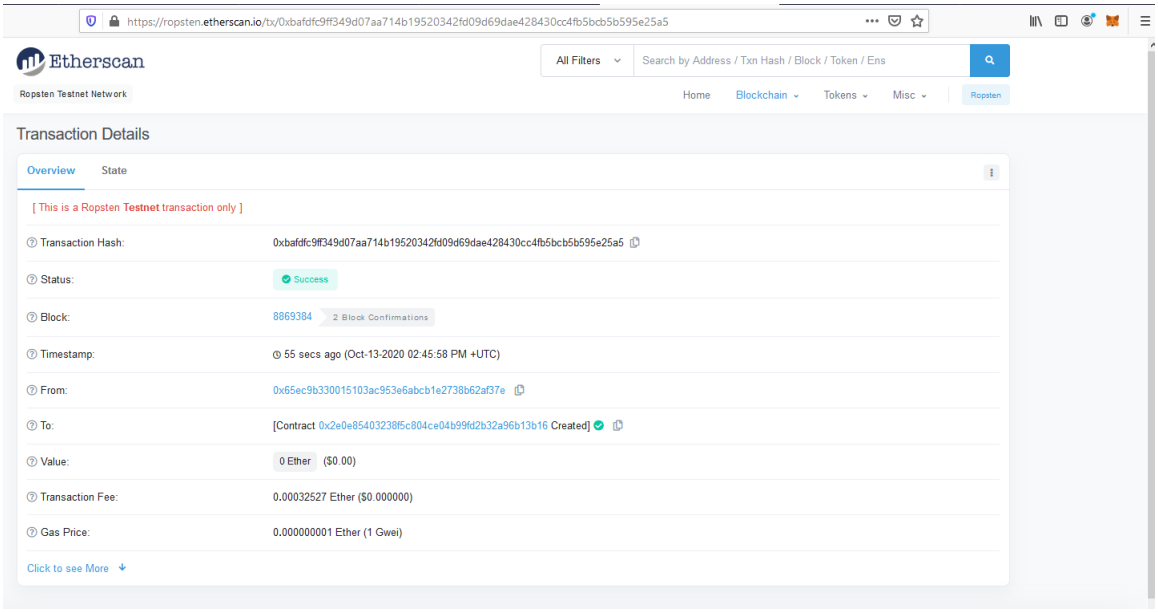

FIGURE 4.19 – Confirmation de transaction et validation de bloc

— Un compte est créé pour chaque smart contrat dans la blockchain Ethereum, dont peut y accéder via son adresse.

— La structure de données utilisée dans le smart contract proposé est l'arbre des haches. Les données biométriques sont sauvegardées comme des données hachées dans un arbre de Merkle. Ce dernier est sauvegardé d'une façon sécurisée dans le

blockchaine.

— Toute transaction effectuée dans la blockchain ne peut pas être supprimée et une trace de son exécution est sauvegardée pour toujours.

3 Conclusion

Ce chapitre contient notre proposition pour sécuriser un système d'authentification biométrique en basant sur la technologie de blockchain. Nous avons utilisé l'empreinte digitale comme modalité. Nous avons ciblé deux problèmes de sécurisation des systèmes biométriques : l'attaque d'altération des templates, et l'attaque de canal entre la base de données et le module de calcul de similarité. Pour atteindre ce but, nous avons proposé deux solutions : la première proposition est d'implémenter une blockchain et l'adapter pour sécuriser un système d'authentification biométrique, et la deuxième proposition est basée sur l'utilisation d'une smart contract sur le réseau test net d'Ethereum. Nous avons expliqué aussi comment la sécurisation de tel système est assurée par nos propositions.

CONCLUSION GÉNÉRALE

Le but de ce mémoire était d'étudier l'applicabilité de la technologie Blockchain dans le contexte de la gestion des identités, plus précisément pour la sécurisation du système biométrique dans les deux niveaux : base des templates et le canal entre cette dernière et le module de calcul de similarité. Pour ce faire, nous avons proposé deux solutions basées sur la Blockchain pour améliorer l'efficacité et la sécurité du système biométrique.

Dans la première proposition, nous avons développé notre application BioBlockchain_Application, dont le backend est une blockchain, et le frontend est une application web dédié à être utilisé par les administrateurs du système biométrique ainsi que les agents. Après l'utilisation de l'application BioBlockchain_Application, le système biométrique était devenu plus sécurisé car, la blockchain a remplacé la base de données de manière fiable et plus sécurisée. La deuxième proposition, sert à l'utilisation d'un smart contract sur le réseau Blockchain Ethereum. La manipulation de cette blockchain Ethereum via des smart contract est sécurisée, et son utilisation pour sécuriser une base de données d'un système biométrique est une bonne solution, dont les données sont non altérables et infalsifiables sur cette Blockchain.

Au cours de la réalisation de ce projet, nous avons découvert la technologie blockchain et son fonctionnement et conception plus près. Nous avons traité cette nouvelle technologie, ce qui nous a rendus plus expérimentés et mieux informés dans le domaine, ce qui nous a permis d'approfondir nos connaissances. Cependant, nous pensons n'avoir fait qu'un pas dans ce vaste domaine parce que, nous avons répondu sur une seule question et en avons eu beaucoup d'autres. Nous proposons comme des travaux futurs les points suivants :

— Utilisation de la blockchain pour une sécurité complète du système biométrique ou d'autres points de compromissions.

— L'application de la blockchain dans d'autres systèmes.

— Utiliser un smart contract dans autres plateformes Hyperledger Fabric par exemple.

BIBLIOGRAPHIE

[1] Khellat-Kihel Souad. *Identification biométrique par fusion multimodale de l'empreinte d'articulation, l'empreinte digitale et l'empreinte veineuse du doigt.* Thèse de doctorat, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2017.

[2] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition.* Springer, 2005.

[3] Florent Perronnin and Jean-Luc Dugelay. Introduction à la biométrie-authentification des individus par traitement audio-vidéo. *Traitement du signal*, 19(4), 2002.

[4] Benabdi Mouad. *Identification des personnes par les empreintes d'articulation des doigts et le deep learning.* Thèse de doctorat, Universite mohamed boudiaf-m'sila, 2019.

[5] Khellat-Kihel Badra. Sécurisation des réseaux wifi par authentification biométrique par empreinte digitale. Mémoire d'ingéniorat en informatique, université Mohamed Boudiaf - m'sila, 6 2009.

[6] Khellat-Kihel Souad. Reconnaissance des individus par leurs réseaux veineux. Mémoire de master en informatique, 6 2012.

[7] Mourad Chaa. *Système de reconnaissance de personne par des techniques biométriques.* Thèse de doctorat, Université Ferhat Abbas – Sétif, 1 2017.

[8] Dib Soumeya. Identification des individus par les techniques multimodales : application sur les images du visage. Mémoire de master, Université Dr. Tahar Moulay saida, 6 2015.

[9] Messaoudi Fatima. Identification des individus par la biométrie multimodale. Mémoire de master, Université des Sciences et de la Technologie d'Oran USTO-MB, 2012.

[10] Nicolas Morizet. *Reconnaissance biométrique par fusion multimodale du visage et de l'iris*. Thèse de doctorat, Télécom ParisTech, 3 2009.

[11] Belghechi Rima. Contribution à la reconnaissance d'empreintes digitales par une approche hybride. Mémoire de master, Institut National de formation en Informatique (I.N.I), 2006.

[12] Mohamad El-Abed. *Évaluation de système biométrique*. Thèse de doctorat, Université de Caen, 2011.

[13] Rouigheb Abdenebi. Etude et élaboration de méthodes de détection multimodales appliquées à la reconnaissance biométrique. Mémoire de master, Université des sciences et de la technologie d'Oran USTO-MB, 2008.

[14] S. Benkhaira. Systèmes multimodaux pour l'identification et l'authentification biométrique. Mémoire de master, Université du 20 Août 1955 de Skikda, 2014.

[15] Bruce Schneier. The uses and abuses of biometrics. *Communications of the ACM*, 42(8) :136–136, 1999.

[16] data protection working party 2003, working document on biometrics 12168/ 02. *Tech rep*, (29), 2003.

[17] Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Davide Maltoni, and Julian Fierrez. Fake fingertip generation from a minutiae template. In *2008 19th International Conference on Pattern Recognition*, pages 1–4. IEEE, 2008.

[18] Estelle Cherrier, Patrick Lacharme, and Christophe Rosenberger. La biométrie révocable : principes et limites. In *Atelier de Protection de la Vie Privée (APVP 2012)*, page 6 p., Ile de Groix, France, 2012.

[19] Nalini K. Ratha, Jonathan H. Connell, and Ruud M Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3) :614–634, 2001.

[20] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies. *Curso elaborado pela*, 2019.

[21] David Grellety. La signature électronique avec .net, 27 février 2009 - Mis à jour le 9 mai 2010,.

[22] Guilieb. Illustration de signature et vérification d'un message. 16 December 2015.

[23] Ralph C Merkle. A digital signature based on a conventional encryption function. In *Conference on the theory and application of cryptographic techniques*, pages 369–378. Springer, 1987.

[24] Rima Ouidad Belguechi. *Sécurité des systèmes biométriques : révocabilité et protection de la vie privée*. Thèse de doctorat, Ecole Nationale Supérieure d'Informatique, 6 2015.

[25] Ying Luo, S Cheung Sen-ching, and Shuiming Ye. Anonymous biometric access control based on homomorphic encryption. In *2009 IEEE International Conference on Multimedia and Expo*, page 34. IEEE, 2009.

[26] Berkay Topcu, Hakan Erdogan, Cagatay Karabat, and Berrin Yanikoglu. Biohashing with fingerprint spectral minutiae. In *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, pages 1–12. IEEE, 2013.

[27] Rima Belguechi, Vincent Alimi, Estelle Cherrier, Patrick Lacharme, Christophe Rosenberger, et al. An overview on privacy preserving biometrics. *Recent Application in Biometrics*, pages 65–84, 2011.

[28] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system (white paper). *URL : https ://bitcoin. org/bitcoin. pdf (accessed : 18.07. 2019)*, 2008.

[29] Nik Roby Dylan Yaga, Peter Mell and Karen Scarfone. Blockchain technology overview. *URL : https ://bitcoin. org/bitcoin. pdf (accédé : 18.05. 2020)*, octobre 2018.

[30] Nicolae Sfetcu. La technologie blockchain. 04 2019.

[31] L. Leloup and W. Mougayar. *Blockchain : la révolution de la confiance*. Eyrolles, 2017.

[32] Blockchain France. La blockchain décryptée. *Les clefs d'une révolution. Paris, Netexplo*, 2016.

[33] Rui Zhang, Rui Xue, and Ling Liu. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3) :1–34, 2019.

[34] Florian Haffke. Technical analysis of established blockchain systems. *Thèse de master. Université technique de Munich, SW Engineering for Business Informatics*, 2017.

[35] Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan. Threshold-optimal dsa/ecdsa signatures and an application to bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security*, pages 156–174. Springer, 2016.

[36] Olivier Desplebin, Gulliver Lux, and Nicolas Petit. Comprendre la blockchain : quels impacts pour la comptabilité et ses métiers ? *ACCRA*, (2) :5–23, 2019.

[37] Jan Rüth, Torsten Zimmermann, Konrad Wolsing, and Oliver Hohlfeld. Digging into browser-based crypto mining. In *Proceedings of the Internet Measurement Conference 2018*, pages 70–76, 2018.

[38] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology : Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[39] Imran Bashir. *Mastering blockchain*. Packt Publishing Ltd, 2017.

[40] Guillaume Chanut. Tout savoir sur les nœuds bitcoin. en lignel. `https://cryptoast.fr/bitcoin/`. Page consultée le 6 février 2020, mis à jour le 12 septembre 2020l 2020.

[41] Jean-Guillaume Dumas and Pascal Lafourcade. 4. les crypto-monnaies, une réalité virtuelle ?

[42] Dejan Vujičić, Dijana Jagodić, and Siniša Ranđić. Blockchain technology, bitcoin, and ethereum : A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*, pages 1–6. IEEE, 2018.

[43] Jonatan Bergquist. Blockchain technology and smart contracts : Privacy-preserving tools, 2017.

[44] Sigrid Seibold and George Samman. Consensus : Immutable agreement for the internet of value. *KPMG< https ://assets. kpmg. com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism. pdf*, 2016.

[45] Fan Yang, Wei Zhou, QingQing Wu, Rui Long, Neal N Xiong, and Meiqi Zhou. Delegated proof of stake with downgrade : A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7 :118541–118555, 2019.

[46] T Laurence. *Introduction to Blockchain Technology*. Van Haren Publishing, 2019.

[47] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency : the Works of Leslie Lamport*, pages 203–226. 2019.

[48] Xin Lil Hao Xu, Muyun Chen. Practical byzantine fault tolerance consensus and a simple distributed ledger application.

[49] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology : Beyond bitcoin. *Applied Innovation*, 2(6-10) :71, 2016.

[50] Bennanni Sid Ahmed. Implémentation d'un smart contract sous la plateforme ethereum : vote électronique. Mémoire de master, Université du Sad Dahlab de Blida 1, Juillet 2019.

[51] Toby Gibbs and Suwaree Yordchim. Thai perception on litecoin value. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 8(8) :2613–5, 2014.

[52] Wenbin Zhang, Yuan Yuan, Yanyan Hu, Karthik Nandakumar, Anuj Chopra, Sam Sim, and Angelo De Caro. Blockchain-based distributed compliance in multinational corporations' cross-border intercompany transactions. In *Future of Information and Communication Conference*, pages 304–320. Springer, 2018.

[53] Karthik Nandakumar and Anil K Jain. Biometric template protection : Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5) :88–100, 2015.

[54] Julien Bringer, Hervé Chabanne, and Alain Patey. Privacy-preserving biometric identification using secure multiparty computation : An overview and recent trends. *IEEE Signal Processing Magazine*, 30(2) :42–52, 2013.

[55] Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana, and Ruben Vera-Rodriguez. Blockchain and biometrics : A first look into opportunities and challenges. In *International Congress on Blockchain and Applications*, pages 169–177. Springer, 2019.

[56] Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana, and Ruben Vera-Rodriguez. Biometric template storage with blockchain : A first look into cost and performance tradeoffs. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 0–0, 2019.

[57] Ronald L Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–565. Springer, 2001.

[58] Emeline Hufschmitt. *Signatures pour l'anonymat fondées sur les couplages et applications*. Thèse de doctorat, Université de Caen, Novembre 2007.

[59] Julian Fierrez, Aythami Morales, Ruben Vera-Rodriguez, and David Camacho. Multiple classifiers in biometrics. part 2 : Trends and challenges. *Information Fusion*, 44 :103–112, 2018.

[60] Jean-Pierre Flori. Sécurité et insécurité de la blockchain et des smart contracts. In *Annales des Mines-Realites industrielles*, number 3, pages 98–101. FFE, 2017.

[61] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust*, pages 164–186. Springer, 2017.

[62] Kyriakos Mouratidis, Dimitris Sacharidis, and Hweehwa Pang. Partially materialized digest scheme : an efficient verification method for outsourced databases. *The VLDB Journal*, 18(1) :363–381, 2009.

[63] Heverson B Ribeiro and Emmanuelle Anceaume. Datacube : A p2p persistent data storage architecture based on hybrid redundancy schema. In *2010 18th Euromicro Conference on Parallel, Distributed and Network-based Processing*, pages 302–306. IEEE, 2010.

[64] Mehmet Aydar, Salih Cemil Cetin, Serkan Ayvaz, and Betul Aygun. Private key encryption and recovery in blockchain. *arXiv preprint arXiv :1907.04156*, 2019.

[65] Oscar Delgado-Mohatar, Julian Fierrez, Ruben Tolosana, and Ruben Vera-Rodriguez. Blockchain meets biometrics : Concepts, application to template protection, and trends. *arXiv preprint arXiv :2003.09262*, 2020.

[66] Rafael Páez, Manuel Pérez, Gustavo Ramírez, Juan Montes, and Lucas Bouvarel. An architecture for biometric electronic identification document system based on blockchain. *Future Internet*, 12(1) :10, 2020.

[67] Vanga Odelu. Imbua : identity management on blockchain for biometrics-based user authentication. In *International Congress on Blockchain and Applications*, pages 1–10. Springer, 2019.

[68] Code python disponible sur. en lignel. `https://github.com/satwikkansal/python_blockchain_app/tree/ibm_blockchain_post`. Page consultée le 6 septembre 2020.