



# MÉMOIRE FIN DE FORMATION POUR L'OBTENTION DU DIPLÔME D'INGÉNIEUR DE CONCEPTION DES TÉLÉCOMMUNICATIONS

SPECIALITE : INGENIERIE DE DONNEES ET INTELLIGENCE ARTIFICIELLE

## THÈME

*Conception d'un système basé sur la technologie blockchain pour la gestion des cas d'homonymies dans le secteur bancaire*

Sous la direction de

M. Moustapha DER

Enseignant - Chercheur

ESMT Dakar

M. Printys Barnard ASSEDE

Chargé des systèmes d'information métier

BCEAO

Présenté et soutenu par

M. Joshua Juste Emmanuel Yun Pei NIKIEMA

Promotion 2021 - 2024

Décembre 2024

## PREAMBULE

Les opinions exprimées dans ce mémoire sont propres à Joshua Juste Emmanuel Yun Pei NIKIEMA et énoncées sous mon entière responsabilité.

## DEDICACES

À mon père Théodore NIKIEMA et ma mère Dorothée Mbilendé NIKIEMA,

Pour votre amour inconditionnel, vos sacrifices et votre soutien constant dans mes études.

Vous êtes mes modèles de persévérance et de réussite.

À ma sœur Myriam Merveille et mes frères Joo Min Magloire et Elithe Yung Myung Lazard,

Pour votre affection et votre présence qui m'ont porté tout au long de ce parcours.

À la mémoire de M. Tiéguélé Abdoul COULIBALY,

Ancien Directeur des Systèmes d'Information de la BCEAO,

Qui nous a quittés prématûrement. Votre vision et votre leadership continueront de nous inspirer.

Ce travail vous est également dédié.

Que ce mémoire soit le témoignage de ma profonde gratitude et de mon affection envers vous tous.

## AVANT-PROPOS

Ce mémoire de fin d'études est l'aboutissement d'un long parcours académique et personnel, jalonné de défis et d'apprentissages enrichissants. Réalisé dans le cadre de ma formation d'ingénieur à l'École Supérieure Multinationale des Télécommunications (ESMT), ce travail est consacré à l'utilisation de la blockchain pour la gestion des identités bancaires dans l'UEMOA. Il m'a permis de relever des défis intellectuels stimulants et de renforcer mes compétences en ingénierie des données et en solutions innovantes pour le secteur bancaire.

En acceptant ce défi de traiter la problématique des homonymies dans le contexte bancaire, mon ambition était de proposer une solution technique répondant à un besoin réel et pressant des institutions financières de la région. Ce mémoire témoigne de mon intérêt pour les technologies émergentes et leur capacité à résoudre des problématiques complexes, tout en promouvant l'innovation et l'intégration régionale.

Ce travail de conception n'aurait pas pu prendre forme sans un cadre académique structurant, des opportunités de recherche enrichissantes et l'accompagnement de professionnels engagés. Je tiens donc à remercier spécialement M. Moustapha DER, enseignant-chercheur à l'ESMT, pour sa disponibilité, ses conseils avisés et son accompagnement rigoureux tout au long de ce projet. Je suis également reconnaissant envers M. Printys Barnard ASSEDE, Chargé des systèmes d'information métier à la BCEAO, pour ses orientations pratiques et sa précieuse expertise qui ont grandement enrichi ma réflexion. À travers ce mémoire, j'espère contribuer modestement à la réflexion et au développement de solutions adaptées aux besoins spécifiques du secteur bancaire en Afrique de l'Ouest.

## REMERCIEMENTS

Nous remercions DIEU le TOUT PUISSANT de nous avoir donné la santé et la volonté d'entamer et d'achever ce mémoire de fin de cycle. C'est LUI la qui fortifie ma foi et me donne le courage d'aller de l'avant.

Ce rapport n'aurait pas été réalisé sans la contribution variée et précieuse de nombreuses personnes, à qui nous adressons notre profonde et sincère reconnaissance. Parmi elles :

- ❖ **Monsieur Jean-Claude Kassi BROU**, Gouverneur de la BCEAO, pour l'opportunité offerte d'effectuer ce stage au sein de cette prestigieuse institution ;
- ❖ **Monsieur Adamou MOUSSA SALEY**, Directeur général de l'ESMT ;
- ❖ **Professeur Ahmed Dooguy KORA**, Directeur de l'Enseignement, de la Formation et de la Recherche ;
- ❖ **Professeur Boudal NIANG**, notre responsable pédagogique, et **Monsieur Hervé OUEDRAOGO**, assistant programme cycle ingénieur, pour leur accompagnement ;
- ❖ À la mémoire de **Monsieur Tiéguélé Abdoul Coulibaly**, ancien Directeur des Systèmes d'Information de la BCEAO, pour sa vision et son leadership ;
- ❖ **Monsieur Moustapha DER**, Enseignant-Chercheur à l'ESMT et directeur de mémoire, qui malgré ses occupations, n'a ménagé aucun effort pour notre encadrement ;
- ❖ **Monsieur Printys Barnard ASSEDE**, Chargé des systèmes d'information métier à la BCEAO et maître de stage, pour son encadrement, sa disponibilité et ses précieux conseils ;
- ❖ **Messieurs Sambo K. SANKARA** Responsable BI à ENI et **Amadou KAMAGATE** Concepteur développeur de logiciel à la BCEAO, pour leurs précieux conseils ;
- ❖ **Tout le corps professoral de l'ESMT**, pour leur disponibilité, leur patience et le savoir qu'ils nous ont inculqué tout au long de notre formation ;
- ❖ **Aux membres du jury**, qu'ils trouvent l'expression de nos remerciements les plus sincères pour l'honneur qu'ils nous font en acceptant d'évaluer ce travail.
- ❖ **L'ensemble du personnel de la Direction des Systèmes d'Information de la BCEAO**, pour leur accueil chaleureux et leur collaboration tout au long de ce stage ;

Enfin, nos sincères remerciements vont à l'endroit de nos amis, de nos camarades de promotion et de tous ceux qui ont contribué d'une manière ou d'une autre, de près ou de loin, à l'élaboration de ce document.

## GLOSSAIRE

1	3DES	Triple Data Encryption Algorithm
2	AES	Advanced Encryption Standard
3	API	Application Programming Interface
4	BCEAO	Banque Centrale des États de l'Afrique de l'Ouest
5	CA	Certificat Authentication
6	CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
7	CEVATEGE	Centre de Valorisation Technologique et de Gouvernance Électronique
8	CNIB	Carte Nationale d'Identité Burkinabè
9	COFEB	Centre Ouest-Africain de Formation et d'Etudes Bancaires
10	CPU	Central Processing Unit
11	CUDA	Compute Unified Device Architecture
12	cURL	client Uniform Resource Locator
13	dApps	decentralized Applications
14	DeFi	Decentralized Finance (finance décentralisée en français)
15	DES	Data Encryption Standard
16	DGICRN	Direction Générale de l'Identification Civile, des Registres et des Notaires
17	DID	Decentralized Identifiers
18	DSI	Direction des Systèmes d'Informations
19	DTCC	Depository Trust & Clearing Corporation
20	ECDSA	Elliptic Curve Digital Signature Algorithm
21	ECC	Elliptic Curve Cryptography
22	EID Togo	electronic-Identification
23	EdDSA	Edwards-curve Digital Signature Algorithm
24	ESMT	École Supérieure Multinationale des Télécommunications
25	EVM	Ethereum Virtual Machine
26	fID	Foundational Digital Identification
27	GPU	Graphics Processing Units
28	HLF	Hyperledger Fabric
29	IBM	International Business Machines corporation
30	IBU	Identifiants Bancaires Uniques
31	ID	Identification
32	IFU	Identifiant Financier Unique
33	InDIA	Ingénierie des Données et Intelligence Artificielle
34	INGC	Ingénieur de Conception
35	KYC	Know Your Customer
36	LCB-FT	Lutte Contre le Blanchiment de capitaux et le Financement du Terrorisme
37	LFW	Labeled Faces in the Wild
38	MNBC	Monnaies Numériques de Banque Centrale
39	MTCNN	Multi-Task Cascaded Convolutional Neural Networks
40	NIF	Numéro d'Identification Fiscal
41	Nina	Numéro d'Identification Nationale
42	NINEA	Numéro d'Identification National des Entreprises et Associations
43	NIU	Numéro d'Identification Unique
44	NTRU	Number Theorists R Us or Native Title Research Unit
45	PaaS	Platform-as-a-Service
46	PoS	Proof of Stake

47	PoW	Proof of Work
48	PNUD	Programme des Nations Unies pour le Développement
49	RCCM	Registre du Commerce et du Crédit Mobilier
50	RNPP	Registre National des Personnes Physiques
51	RSA	Rivest-Shamir-Adleman
52	RUBC	Répertoire Unique des Bénéficiaires de Crédit
53	SDI	Service des Développements Informatiques
54	SHA-256	Secure Hash Algorithm 256
55	UEMOA	Union Economique et Monétaire Ouest Africaine
56	UI	User Interface
57	UML	Unified Modeling Language
58	UMOA	Union Monétaire Ouest Africaine
59	VC	Verifiable Credentials
60	VGGFace2	Visual Geometry Group Face version 2
61	W3C	World Wide Web Consortium
62	WURI	West Africa Unique Identification for Regional Integration and Inclusion
63	YAML	Yet Another Markup Language
64	zk-SNARKs	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
65	zk-STARKs	Zero-Knowledge Scalable Transparent Argument of Knowledge

## LISTE DES FIGURES

Figure I-1 : Organigramme de la BCEAO .....	4
Figure I-2 : Organigramme de la Direction des Systèmes d'Information.....	5
Figure II-1 : Présentation des types de blockchain .....	18
Figure II-2 : Représentation du bloc dans la blockchain.....	19
Figure II-3 : Représentation d'une chaîne de blocs.....	20
Figure II-4 : Schéma du fonctionnement général d'une blockchain .....	21
Figure II-5 : Schéma du chiffrement symétrique .....	22
Figure II-6 : Schéma du chiffrement asymétrique.....	23
Figure II-7 : Un arbre de Merkle binaire .....	24
Figure III-1 : Diagramme permettant de faire le choix du type de blockchain adapté à une problématique .....	37
Figure III-2 : Architecture globale du système basée sur une blockchain en consortium.....	38
Figure III-3 : Diagramme de cas d'utilisation .....	42
Figure III-4 : Diagramme de classe .....	44
Figure III-5 : Diagramme de séquence de la création d'un client .....	45
Figure III-6 : Diagramme d'activité de la création d'un client .....	46
Figure III-7 : Diagramme de déploiement de notre solution .....	48
Figure IV-1 : Logo d'Ethereum .....	51
Figure IV-2 : Logo d'Hyperledger Fabric .....	51
Figure IV-3 : Logo d'Oracle VirtualBox .....	53
Figure IV-4 : Logo de CouchDB.....	53
Figure IV-5 : Logo de Hyperledger Explorer.....	54
Figure IV-6 : Architecture 3 couches de Hyperledger Explorer .....	55
Figure IV-7 : Logo docker .....	55
Figure IV-8 : Logo docker-compose .....	55
Figure IV-9 : Logo de Python .....	56
Figure IV-10 : Logo PyTorch.....	57
Figure IV-11 : Logo de FastAPI .....	57
Figure IV-12 : Logo de JavaScript.....	58
Figure IV-13 : Logo de node.js .....	58
Figure IV-14 : Logo de Express .....	59
Figure IV-15 : Logo de ReactJS .....	59
Figure IV-16 : Logo de tailwindcss.....	60
Figure IV-17 : Logo de Visual Studio code .....	60
Figure IV-18 : Architecture de notre réseau blockchain .....	61
Figure IV-19 : Schéma explicatif des relations possibles entre nœuds, organisations et canal	62
Figure IV-20 : Présentation du Ledger dans Hyperledger Fabric .....	66
Figure IV-21 : Architecture 3-tiers de notre solution.....	71

## LISTE DES TABLEAUX

Tableau I-1 : Effectifs des différents services de la DSI .....	6
Tableau III-1 : Présentations des caractéristiques de chaque type de blockchain.....	36
Tableau III-2 : Présentation du format des données du client.....	40
Tableau IV-1 : Comparaison entre Ethereum et Hyperledger Fabric .....	52
Tableau IV-2 : Résumé des méthodes de la classe ClientManager (notre contrat intelligent) .....	65
Tableau IV-3 : Comparaison entre les modèles MTCNN + InceptionResnetV1 et FaceNet ..	69
Tableau IV-4 : Estimations des coûts de formation et développement des compétences .....	77
Tableau IV-5 : Détail des phases et livrables .....	78
Tableau IV-6 : Estimations des coûts salariaux sur la durée du projet (20 mois).....	78
Tableau IV-7 : Matrice des risques et mesures d'atténuation.....	79

## LISTE DES CAPTURES

Capture III-1 : Légende des éléments de l'architecture .....	38
Capture IV-1 : Partie du script shell start.sh qui configure les variables d'environnement.....	62
Capture IV-2 : Déploiement de Hyperledger Explorer .....	67
Capture IV-3 : Page de connexion à Hyperledger Explorer.....	67
Capture IV-4 : Page d'accueil de Hyperledger Explorer .....	68
Capture IV-5 : Interface documentaire FastAPI de notre API .....	70
Capture IV-6 : Page de connexion à l'application .....	72
Capture IV-7 : Interfaces de visualisation des clients à l'état actif enregistré sur la blockchain .....	73
Capture IV-8 : Interface d'enregistrement d'un client dans la blockchain .....	74
Capture IV-9 : Historique de mise à jour des informations d'un client .....	75
Capture IV-10 : Vue détaillé des informations d'un client .....	76

## SOMMAIRE

INTRODUCTION GENERALE .....	1
Chapitre I : PRESENTATION GENERALE .....	2
Introduction .....	2
I.1    Présentation de la structure.....	2
I.2    Présentation du thème d'étude .....	7
I.3    Contexte .....	12
I.3    Méthodologie et terrain.....	14
Conclusion.....	15
Chapitre II : TECHNOLOGIE BLOCKCHAIN ET GESTION DES IDENTITÉS .....	16
Introduction .....	16
II.1    Fondamentaux de la blockchain .....	16
II.2    Blockchain pour l'identité numérique .....	27
II.3    Applications dans le secteur bancaire .....	28
Conclusion.....	30
Chapitre III : ANALYSE ET CONCEPTION DE LA SOLUTION .....	31
Introduction .....	31
III.1    Périmètre fonctionnel .....	31
III.2    Analyse des besoins .....	33
III.3    Architecture et fonctionnement du système.....	36
III.4    Modélisation du système .....	39
Conclusion.....	49
Chapitre IV : OUTILS D'IMPLEMENTATION, RÉALISATION DE LA SOLUTION ET PLANIFICATION .....	50
Introduction .....	50
IV.1    Outils d'implémentation .....	50
IV.2    Réalisation de la solution .....	61
IV.3    Planification .....	76
Conclusion.....	79
CONCLUSION GÉNÉRALE.....	80

## INTRODUCTION GENERALE

Dans un contexte de transformation numérique accélérée du secteur bancaire en Afrique de l'Ouest, la gestion des identités des clients constitue un enjeu majeur pour les institutions financières de l'UEMOA (Union Économique et Monétaire Ouest Africaine). La problématique des homonymies, particulièrement prégnante dans cette région, pose des défis considérables en termes de sécurité, de conformité réglementaire et de qualité de service.

La BCEAO (Banque Centrale des États de l'Afrique de l'Ouest), en tant que régulateur du système bancaire régional, est confrontée à la nécessité de moderniser les processus d'identification des clients pour prévenir les fraudes, faciliter les transactions transfrontalières et promouvoir l'inclusion financière. L'absence d'un système d'identification unique et harmonisé à l'échelle régionale complexifie la gestion des identités bancaires et augmente les risques opérationnels liés aux homonymies.

Dans ce contexte, la technologie blockchain émerge comme une solution prometteuse pour répondre à ces défis. Ses caractéristiques intrinsèques - décentralisation, immuabilité, traçabilité - en font un outil particulièrement adapté pour la mise en place d'un système d'identification bancaire fiable et sécurisé.

Ce mémoire se propose d'explorer et de concevoir une solution blockchain pour la gestion des homonymies dans le secteur bancaire de l'UEMOA. Notre étude s'articule autour de quatre chapitres principaux :

- Le premier chapitre présente le contexte général du projet, la structure d'accueil et pose la problématique de recherche.
- Le deuxième chapitre explore les fondamentaux de la technologie blockchain et son application dans la gestion des identités numériques.
- Le troisième chapitre détaille l'analyse et la conception de la solution proposée.
- Le quatrième chapitre présente la réalisation technique de la solution et sa planification.

# Chapitre I : PRESENTATION GENERALE

## Introduction

Ce chapitre a pour objectif de poser les bases théoriques et méthodologiques de notre recherche sur l'application de la blockchain à la gestion des homonymies dans le secteur bancaire de l'UEMOA. Nous présenterons d'abord notre structure d'accueil, ensuite nous définirons la problématique et les questions de recherche qui guideront notre étude. Enfin, nous détaillerons la méthodologie adoptée pour mener à bien cette recherche, en précisant les outils de collecte et d'analyse des données.

### I.1 Présentation de la structure

#### I.1.1 Présentation de la structure d'accueil : BCEAO

##### I.1.1.1 Présentation et mission de la BCEAO

La BCEAO, institution publique internationale ayant son siège à Dakar, au Sénégal, a été fondée le 12 mai 1962. A sa création, elle regroupait les Républiques de la Côte d'Ivoire, du Dahomey, de la Haute-Volta, du Mali, de la Mauritanie, du Niger, du Sénégal et du Togo. Actuellement, ses pays membres sont le Bénin, le Burkina Faso, la Côte d'Ivoire, la Guinée-Bissau, le Mali, le Niger, le Sénégal et le Togo. Dans l'espace de l'Union Monétaire Ouest Africaine (UMOA), partageant une monnaie commune qu'est le Franc de la Communauté Financière Africaine (FCFA), la BCEAO est responsable de son émission.

La BCEAO est régie par les textes suivants :

- Le Traité de l'Union Monétaire Ouest Africaine en vigueur depuis le 1er avril 2010 ;
- Les Statuts de la BCEAO qui sont annexés au Traité.
- L'accord de Coopération entre la République Française et les Républiques membres de l'Union Monétaire Ouest Africaine conclu le 4 décembre 1973. Un avenant de cet accord de coopération a été signé entre les pays membres de l'UMOA et la République Française le 29 mai 1984.
- La Convention de compte d'opération le 4 décembre 1973 entre l'UMOA et la République Française.

La Banque Centrale a pour mission :

- Définir et appliquer la politique monétaire de l'UMOA ;
- Assurer la stabilité du système bancaire et financière de l'UMOA ;
- Promouvoir le bon fonctionnement, superviser et sécuriser les systèmes de paiement de l'UMOA ;
- Mettre en œuvre la politique de change de l'UEMOA selon les directives du Conseil des Ministres ;
- Gérer les réserves officielles de change des Etats membres de l'UMOA.

### I.1.1.2 Organisation

La Banque Centrale, d'un point de vue administratif, dispose d'un Siège situé à Dakar, au Sénégal. Dans chacun des États membres de l'UMOA la Banque dispose d'une Direction Nationale constituée d'une Agence Principale et des Agences Auxiliaires.

Les organes institutionnels de la Banque Centrale se composent comme suit :

- Le Gouverneur
- Le Comité de Politique Monétaire
- Le Conseil d'Administration
- Le Comité d'Audit
- Les Conseils Nationaux du Crédit, à raison d'un Conseil dans chacun des États membres de l'UMOA.

L'organisation globale de la Banque Centrale se présente à travers l'organigramme suivant :

## Conception d'un système basé sur la technologie blockchain pour la gestion des cas d'homonymies dans le secteur bancaire

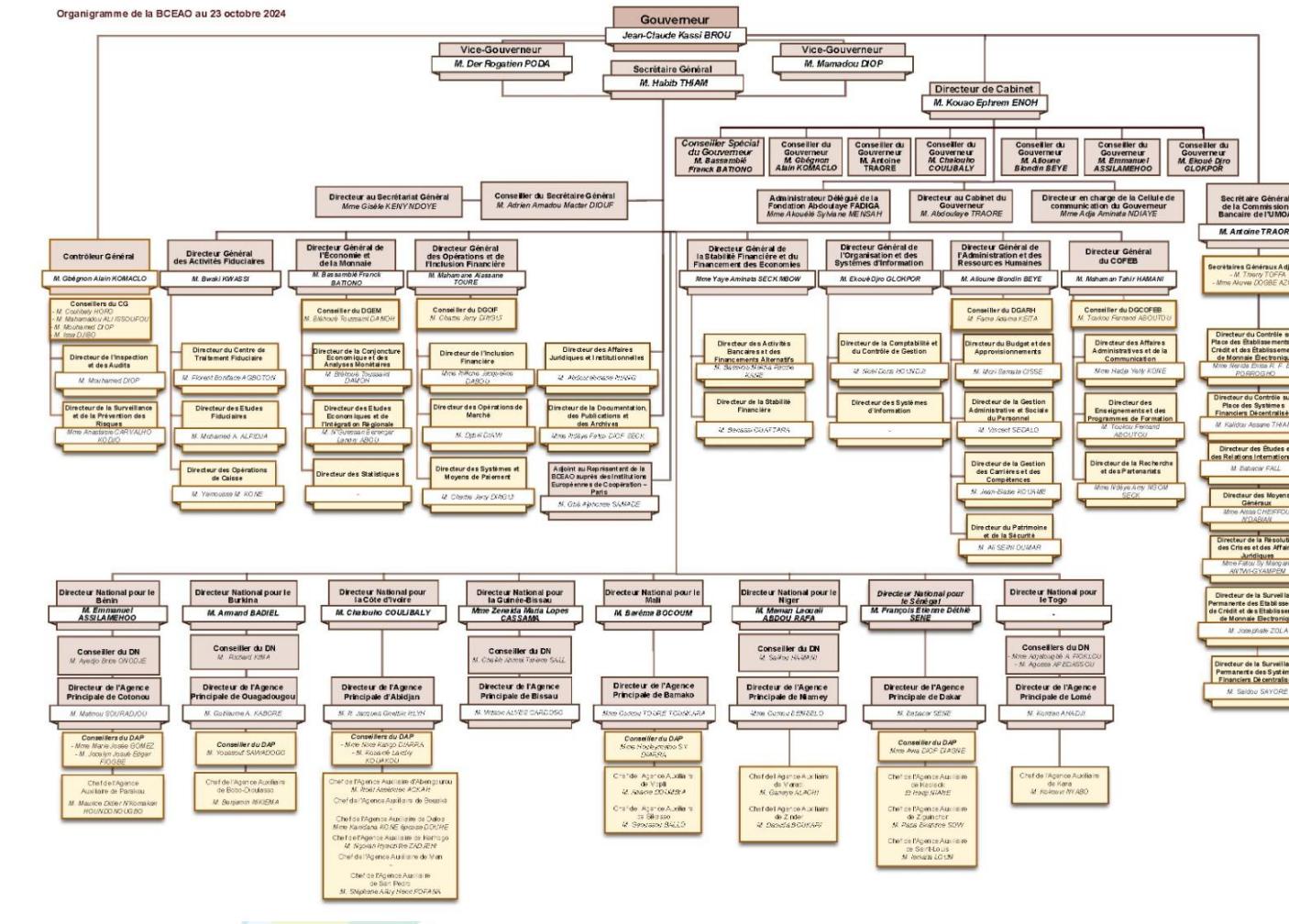


Figure I-1 : Organigramme de la BCEAO

Source : <https://www.bceao.int/fr/content/organigramme-de-la-bceao>

## I.1.2 Présentation de la direction d'accueil : DSİ

La DSİ est structurée en cinq (5) services, énumérés comme suit :

- Le Service de l'Assistance Informatique ;
- Le Service de l'Administration des Réseaux ;
- Le Service de l'Administration des Systèmes Informatiques ;
- Le Service des Développements Informatiques ;
- Le Service Opérationnel de Cybersécurité.

### I.1.2.1 Organigramme et effectifs

Dans la figure ci-dessous nous allons vous présenter l'organigramme de la Direction des Systèmes d'Information.

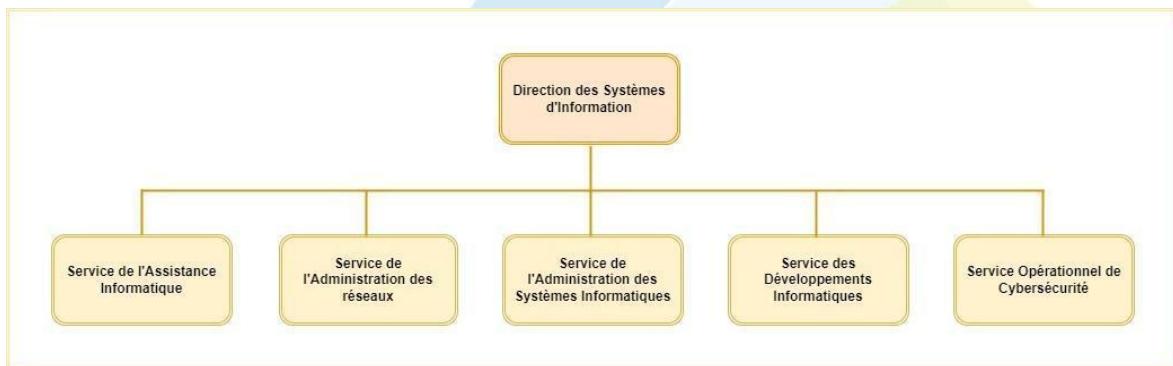


Figure I-2 : Organigramme de la Direction des Systèmes d'Information

Source : Document de la DSİ

Tableau I-1 : Effectifs des différents services de la DSI

Source : Document de la DSI

Service	Effectif
Service de l'Assistance Informatique	9
Service de l'Administration des Réseaux	6
Service de l'Administration Systèmes Informatiques	10
Service des Développements Informatiques	25
Service Opérationnel de Cybersécurité	3

### I.1.2.2 Activités principales

L'une des principales missions de la DSI consiste à mettre en œuvre les directives établies par le CSI. Ce comité est présidé par le Secrétaire Général et ses réunions sont programmées au moins trois fois par an. Les principales tâches exécutées par la DSI incluent entre autres :

- Le support et l'assistance aux utilisateurs des outils informatiques ;
- La conception, la réalisation et la maintenance des applications informatiques et des progiciels ;
- La gestion, l'administration et la sécurisation des données et des serveurs de la Banque Centrale ;
- La supervision des réseaux télécoms/informatiques et la maintenance des équipements.

### I.1.2.3 Enjeux majeurs

Le stage se déroule au sein de la Direction des Systèmes d'Informations (DSI), plus précisément au Service des Développements Informatiques (SDI). Le Service des Développements Informatiques doit relever plusieurs défis majeurs, nécessitant une approche holistique pour garantir le succès des projets.

- **Qualité du logiciel :** Assurer la qualité, la fiabilité et la sécurité des logiciels développés en mettant en œuvre des processus de développement robustes, des tests rigoureux et des normes de qualité élevées.

- **Gestion des ressources :** Optimiser l'utilisation des ressources humaines, matérielles et financières disponibles pour garantir une efficacité et une rentabilité maximales dans le développement des logiciels.
- **Gestion de projet :** Renforcer la planification, la coordination et le suivi des projets de développement informatique aux fins de mieux respecter les délais, les budgets et les exigences des clients tout en minimisant les risques.
- **Sécurité des données :** protéger les données sensibles des utilisateurs et de l'entreprise contre les cybermenaces en mettant en œuvre des mesures de sécurité robustes, des politiques de confidentialité et des pratiques de développement sécurisé.
- **Agilité et flexibilité :** Être capable de s'adapter rapidement aux changements de besoins, de technologies ou de priorités, en adoptant des méthodologies de développement agiles et en favorisant la réactivité et l'adaptabilité de l'équipe.
- **Maintenance et évolutivité :** Assurer la maintenance, le support et l'évolutivité des systèmes logiciels existants tout en répondant aux demandes d'évolution et d'amélioration fonctionnelle.

## I.2 Présentation du thème d'étude

Le secteur bancaire joue un rôle crucial dans le développement économique des pays de l'UEMOA en facilitant les transactions financières, l'épargne et l'octroi de crédits. Cependant, il est confronté à des défis majeurs, notamment celui de la modernisation et de l'intégration technologique pour améliorer l'accessibilité des services financiers à une population en grande partie non bancarisée. Un autre enjeu clé est celui de l'identification unique des clients, essentielle pour prévenir la fraude, se conformer aux réglementations et offrir un service personnalisé.

### I.2.1 Problématique

Les homonymies, c'est-à-dire la présence dans un système des attributs d'identifications identiques ou très similaires de personnes physiques (noms, prénoms, date de naissance, etc.) ou morales (sigle, raison sociale, numéro de registre de commerce, etc.), posent des défis significatifs dans le secteur bancaire. Dans les systèmes traditionnels de gestion des identités,

les homonymies peuvent conduire à des erreurs d'identification, où les transactions et les informations de crédit sont attribuées à la mauvaise personne. Cela peut entraîner des complications telles que des refus de crédit injustifiés, des erreurs dans les relevés de compte et des difficultés pour les clients à accéder à leurs propres informations bancaires.

Dans l'espace régional de l'UEMOA, ces problèmes sont exacerbés par la diversité des systèmes d'identification dans chaque pays membre. L'absence d'un système d'identification unique et harmonisé rend plus difficile la gestion des homonymies à travers les frontières. Par exemple, une personne peut avoir des comptes dans plusieurs banques de différents pays de l'UEMOA, ce qui augmente le risque de confusion et d'erreurs d'identification. Les homonymies compliquent également les processus de vérification des antécédents et de conformité réglementaire. Les banques doivent s'assurer que les personnes qu'elles identifient sont bien celles qu'elles prétendent être, ce qui est particulièrement difficile en cas d'homonymie. Cela peut ralentir les procédures de vérification, augmenter les coûts opérationnels et réduire l'efficacité des services bancaires. Ces difficultés peuvent également être amplifiées par les différences de réglementation et de procédures entre les pays membres.

### **I.2.2 Questionnement sur la gestion des homonymies**

Les homonymies, posent un défi de taille pour l'identification unique des clients dans le secteur bancaire de l'UEMOA. En l'absence d'un système d'identification harmonisé au niveau régional, les banques et de surcroît la BCEAO peine à différencier les individus, ce qui entraîne des erreurs, complique les procédures et augmente les risques de fraude. Notre recherche vise donc à répondre à la question suivante : comment la technologie blockchain peut-elle être utilisée pour résoudre efficacement le problème des homonymies et garantir une identification unique des clients bancaires dans l'espace UEMOA ?

### **I.2.3 Objectif principal**

L'objectif fondamental du projet est de développer un système blockchain décentralisé et sécurisé pour la gestion des identités des clients titulaires de comptes bancaires dans l'espace UEMOA, garantissant que chaque individu ou entité juridique possède un Identifiant Bancaire Unique (IBU).

## I.2.4 Objectifs spécifiques

Pour atteindre l'objectif principal de développer un système blockchain décentralisé et sécurisé pour la gestion des identités bancaires dans l'UEMOA ce qui sera la solution au problème d'homonymie, nous avons défini quatre (04) objectifs spécifiques qui sont :

- **Identifier de manière unique et fiable chaque client bancaire**
  - Développer une infrastructure blockchain capable d'attribuer un Identifiant Bancaire Unique (IBU) à chaque individu ou entité juridique.
  - Concevoir et implémenter des algorithmes robustes pour la détection et la gestion des homonymies.
  - Mettre en place des processus de validation des identités pour garantir l'unicité des IBU à travers toutes les institutions bancaires de l'UEMOA.
- **Assurer la traçabilité et l'immuabilité des données bancaires**
  - Configurer des mécanismes de consensus fiables et sécurisés pour valider toutes les transactions liées à la gestion des identités.
  - Développer des smart contracts pour automatiser les processus de création, mise à jour et audit des identités bancaires.
  - Intégrer des outils permettant une auditabilité complète des données, tout en garantissant leur immutabilité sur la blockchain.
- **Renforcer la sécurité et le contrôle d'accès aux données**
  - Implémenter un système de gestion des identités décentralisé, permettant un contrôle granulaire des accès aux données bancaires sensibles.
  - Configurer des politiques de sécurité avancées, incluant le chiffrement des données (ex. : SHA-256) et l'utilisation de signatures numériques ECDSA (Elliptic Curve Digital Signature Algorithm).
  - Assurer une gestion stricte des droits d'accès, où seules les entités autorisées peuvent interagir avec les données.
- **Garantir l'interopérabilité et l'intégration régionale**
  - Développer des APIs standardisées permettant une interaction fluide entre les systèmes bancaires existants et la blockchain.
  - Concevoir des protocoles d'échange de données interopérables, respectant les normes internationales tout en répondant aux spécificités locales.
  - Mettre en place des canaux de communication sécurisés entre les différentes banques et la BCEAO pour assurer une coopération harmonisée.

Ces objectifs spécifiques couvrent les aspects fonctionnels, techniques et organisationnels nécessaires à la réussite du projet et à l'atteinte de son objectif principal.

### I.2.5 Objectifs de la recherche

L'objectif de cette étude est d'explorer le potentiel de la blockchain comme solution au problème des homonymies dans le secteur bancaire de l'UEMOA. Plus spécifiquement, nous chercherons à :

- Analyser les dispositifs d'identification existants et leurs limites.
- Comprendre le fonctionnement de la blockchain et ses applications pour la gestion des identités.
- Proposer une architecture et une approche basée sur la blockchain et adaptée au contexte de l'UEMOA.
- Évaluer la pertinence et la faisabilité de cette solution innovante.

### I.2.6 Intérêt et pertinence de la thématique

L'étude de l'application de la blockchain à la gestion des identités bancaires dans l'espace UEMOA présente un intérêt scientifique et pratique majeur, au regard des enjeux actuels du secteur financier et des défis de l'intégration régionale.

Sur le plan scientifique, cette recherche s'inscrit dans un champ d'étude émergent et prometteur, au croisement de l'informatique, de la cryptographie et de l'économie. Elle vise à contribuer à une meilleure compréhension des opportunités et des limites de la technologie blockchain pour résoudre des problèmes concrets de gestion des identités dans un contexte spécifique. En analysant les cas d'usage existants et en proposant une architecture adaptée aux besoins de l'UEMOA, cette étude apportera des connaissances nouvelles sur les conditions de mise en œuvre réussie d'une solution blockchain dans un écosystème complexe, impliquant de multiples parties prenantes.

Sur le plan pratique, cette recherche répond à un besoin réel et pressant du secteur bancaire de l'UEMOA, confronté aux défis persistants de l'identification des clients et de la gestion des homonymies. En proposant une solution innovante basée sur la blockchain, cette étude ouvre la voie à une transformation profonde des processus d'identification, vers plus de

sécurité, de fiabilité et d'efficacité. Les résultats de cette recherche pourront être directement exploités par les acteurs du secteur (banques, régulateurs, fournisseurs de solutions) pour guider leurs choix stratégiques et technologiques.

Au-delà du secteur bancaire, cette thématique s'inscrit dans les priorités des politiques publiques de l'UEMOA en matière d'inclusion financière, de transformation digitale et d'intégration régionale. En proposant une solution d'identification interopérable et respectueuse de la vie privée, cette recherche contribue à lever les barrières à l'accès aux services financiers pour les populations les plus vulnérables, tout en favorisant la libre circulation des personnes et des capitaux au sein de l'Union. Elle démontre le potentiel de la blockchain comme technologie de rupture pour relever les défis du développement en Afrique.

Enfin, cette thématique s'inscrit dans les grandes tendances technologiques et sociétales mondiales, marquées par l'essor de l'identité numérique et la quête d'une gouvernance plus décentralisée et inclusive. En explorant une application concrète de la blockchain dans un contexte africain, cette recherche participe au débat global sur les enjeux éthiques, juridiques et sociaux des technologies émergentes, et sur leur rôle dans la construction d'un monde plus juste et durable.

En somme, l'intérêt et la pertinence de cette thématique résident dans sa capacité à articuler des enjeux scientifiques, pratiques et sociétaux, à l'échelle locale et globale. Elle ouvre des perspectives prometteuses pour la recherche, l'innovation et le développement en Afrique, en démontrant comment la technologie blockchain peut être mise au service des besoins spécifiques des populations et des économies de la région.

## I.2.7 Hypothèses de travail

Le sujet d'étude porte sur une implémentation de la gestion des homonymies basée sur la blockchain. L'étude de faisabilité réalisée à cet effet a permis de conclure que l'utilisation de la technologie blockchain ne serait pas appropriée pour gérer les homonymies avec des demandes de fusion de données conduisant à des suppressions ou de désactivations d'informations. L'usage de la technologie blockchain pour adresser stricto sensu cette approche initiale ne serait pas appropriée. La solution à mettre en œuvre consiste à garantir l'unicité recherchée des personnes physiques et morales à travers une gestion de l'identifiant

unique des clients. Cette approche basée sur la blockchain permet d'attribuer un identifiant unique à chaque client bancaire et favorise la résolution du problème des homonymies.

## I.3 Contexte

Pour une compréhension précise du projet, une contextualisation s'impose.

### I.3.1 Environnement bancaire de l'UEMOA

L'Union Économique et Monétaire Ouest Africaine (UEMOA), regroupant huit pays membres (Bénin, Burkina Faso, Côte d'Ivoire, Guinée-Bissau, Mali, Niger, Sénégal et Togo), opère sous une réglementation bancaire harmonisée et une monnaie commune, le Franc CFA. La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO), en tant qu'autorité de régulation, supervise l'ensemble du système bancaire de la zone.

### I.3.2 Cadre réglementaire

#### I.3.2.1 Normes d'identification des clients

La réglementation bancaire de l'UEMOA impose aux banques de mettre en place des procédures robustes d'identification et de vérification de l'identité de leurs clients. Ces procédures doivent être appliquées de manière systématique et constante.

Les banques doivent recueillir et vérifier un ensemble d'informations sur leurs clients, notamment les nom et prénoms, les date et lieu de naissance, la nationalité, l'adresse de résidence, la profession, la pièce d'identité officielle en cours de validité, etc. pour les personnes physiques.

#### I.3.2.2 Exigences en matière de KYC (Know Your Customer)

Au-delà de la simple collecte d'informations, les banques de l'UEMOA sont soumises à des obligations de vigilance renforcée connues sous le nom de "Know Your Customer" (KYC). Les procédures KYC visent à s'assurer que les banques ont une connaissance suffisante de leurs clients pour détecter et prévenir les activités illicites telles que le blanchiment de capitaux, le financement du terrorisme, la fraude ou la corruption. Les banques doivent ainsi mettre en place des dispositifs de surveillance continue des transactions, actualiser

régulièrement les informations sur les clients et signaler aux autorités toute opération suspecte. Le non-respect des obligations KYC expose les banques à des sanctions disciplinaires et pécuniaires de la part des régulateurs.

### I.3.3 État des lieux des systèmes d'identification

#### I.3.3.1 Cartographie des solutions d'identification par pays

La plupart des pays de l'UEMOA ont mis en place ou initié des projets de systèmes d'identification biométrique de leurs citoyens. Ces systèmes reposent généralement sur des cartes d'identité nationale ou des passeports intégrant des données biométriques telles que les empreintes digitales ou la reconnaissance faciale.

Les pays de l'UEMOA présentent donc des niveaux de maturité variables dans leurs systèmes d'identification.

#### I.3.3.2 Limites et insuffisances actuelles

Malgré les progrès réalisés, les systèmes d'identification nationaux des pays de l'UEMOA présentent encore des limites et des insuffisances qui freinent leur utilisation optimale dans le secteur bancaire :

- Absence d'interconnexion et d'interopérabilité entre les systèmes nationaux, qui empêche la reconnaissance mutuelle des identifiants d'un pays à l'autre.
- Qualité et fiabilité variables des données d'identité, avec des risques d'erreurs, de doublons ou de fraude documentaire.
- Accès limité des banques aux registres d'identification nationaux pour des vérifications en temps réel.
- Disparités dans la couverture géographique et démographique des systèmes, avec des populations encore non enregistrées.
- Cadres légaux et réglementaires incomplets ou inadaptés pour l'usage des identifiants dans le secteur financier.

### I.3.4 Besoins et perspectives

Le secteur bancaire de l'UEMOA nécessite la mise en place d'une infrastructure d'identification qui soit :

- Décentralisée et sécurisée
- Interopérable à l'échelle régionale
- Conforme aux normes KYC
- Capable de gérer efficacement les homonymies
- Protectrice des données personnelles

Cette infrastructure devra permettre une identification unique et fiable des clients tout en facilitant les échanges interbancaires au sein de l'espace UEMOA.

Il apparaît donc nécessaire d'explorer des approches innovantes allant au-delà de la simple juxtaposition des systèmes nationaux existants. C'est dans ce contexte que les technologies de type blockchain apparaissent comme une piste prometteuse pour la mise en place d'une infrastructure d'identification décentralisée, sécurisée et interopérable au service de l'inclusion financière dans l'espace UEMOA.

## I.3 Méthodologie et terrain

### I.3.1 Approche méthodologique adoptée

Pour atteindre nos objectifs de recherche, nous avons adopté une approche qualitative et exploratoire. Dans un premier temps, nous avons réalisé une analyse documentaire approfondie pour comprendre les enjeux de l'identification bancaire et le potentiel de la blockchain. Ensuite, nous avons mené des entretiens semi-directifs avec des experts du secteur (responsables conformité, spécialistes blockchain, régulateurs) pour recueillir leurs insights sur la problématique et affiner notre compréhension du sujet.

### I.3.2 Outils et techniques de collecte d'informations

Nous avons utilisé plusieurs outils pour collecter les données nécessaires à notre recherche :

- Analyse documentaire : rapports sectoriels, articles scientifiques surtout issus de recherches du Centre Ouest-Africain de Formation et d'Etudes Bancaires (COFEB), documentations techniques de certaines technologies blockchain, etc.
- Discussions semi-directives avec des experts du domaine bancaire et de la blockchain.

### I.3.3 Limites et contraintes méthodologiques

Notre recherche comporte certaines limites, notamment liées à la nature exploratoire du sujet et à la difficulté d'accéder à certaines données sensibles dans le secteur bancaire. De plus, le caractère novateur de la technologie blockchain implique un recul sur ses applications à long terme. Nous nous sommes efforcés néanmoins de produire une analyse rigoureuse et nuancée.

## Conclusion

Ce premier chapitre nous a permis de poser le cadre théorique et contexte de notre recherche sur l'application de la blockchain à la gestion des homonymies dans le secteur bancaire de l'UEMOA. Après avoir défini la problématique et les questions de recherche, nous avons présenté le contexte dans lequel s'inscrit ce travail, en nous appuyant sur une revue de littérature solide. L'analyse du contexte et des enjeux de l'identification bancaire dans l'UEMOA fait apparaître un écosystème complexe et fragmenté, caractérisé par la coexistence de systèmes nationaux hétérogènes et l'absence d'un identifiant unique communément adopté.

La suite de ce mémoire sera consacrée à une analyse plus détaillée du potentiel de la technologie blockchain pour la gestion des identités bancaires dans l'UEMOA. Nous examinerons les principes de fonctionnement de cette technologie, les cas d'usage pertinents pour le secteur bancaire et les défis à relever pour son déploiement dans le contexte spécifique de la zone UEMOA.

## Chapitre II : TECHNOLOGIE BLOCKCHAIN ET GESTION DES IDENTITÉS

### Introduction

Dans un contexte de transformation numérique et de préoccupations croissantes liées à la protection des données personnelles, la gestion des identités numériques est devenue un enjeu crucial. Face aux limites des systèmes centralisés traditionnels, les solutions décentralisées basées sur la technologie blockchain suscitent un intérêt grandissant. Ce chapitre vise à explorer le potentiel de la blockchain pour la gestion des identités dans le secteur bancaire, en examinant ses fondamentaux techniques, ses cas d'usage et ses perspectives d'évolution.

### II.1 Fondamentaux de la blockchain

#### II.1.1 Définition

Une blockchain est une technologie de stockage et de transmission d'informations transparente, sécurisée et fonctionnant sans organe central de contrôle. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, l'ensemble étant sécurisé par cryptographie, et formant ainsi une chaîne.

Par extension, une blockchain constitue une base de registres distribués et partagés permettant à chaque membre du réseau de vérifier la validité de la chaîne. Son architecture décentralisée élimine le besoin d'une autorité centrale. Chaque bloc contient un ensemble de transactions validées et ajoutées à la chaîne, ainsi qu'une référence (hash) au bloc précédent. La modification d'un bloc nécessite la régénération de tous les blocs suivants, rendant toute manipulation détectable par l'ensemble du réseau. Cette architecture décentralisée élimine le besoin d'une autorité centrale, rendant la blockchain plus sécurisée et transparente. [W6]

## II.1.2 Types de blockchain et cas d'usage

Il existe trois (03) types de blockchain adaptés à différents cas d'usage : [B5] [W5]

- **La blockchain publique**, elle désigne un registre décentralisé qui est la plus répandue et connue dans le monde. Elle fonctionne sur un réseau pair-à-pair, sans organe de contrôle central. Tout le monde peut effectuer des transactions et les vérifier, offrant ainsi un accès libre. Les transactions ne sont pas anonymes mais utilisent des pseudonymes des adresses publiques. Comme exemples de blockchains publiques nous pouvons citer [Bitcoin](#), [Ethereum](#), [Litecoin](#), [Monero](#), [Tezos](#), [Dash](#), [NEO](#), etc.
- **La blockchain privée** encore appelée **blockchain permissionnée**, quant à elle, désigne les registres distribués dont les informations ne sont pas accessibles publiquement. Elle est complètement centralisée et dirigée par un organe central (des acteurs présélectionnés par une autorité dite de confiance), souvent appelé administrateur ou gérant. Ce gérant est responsable de l'ajout des blocs à la chaîne et peut modifier la blockchain à sa guise. Il n'y a pas de lien entre les différents acteurs sans l'autorisation du gérant. Ce type de blockchain est principalement utilisé par des entreprises qui souhaitent garder leurs transactions privées et maintenir un haut niveau de confidentialité, comme les banques. Les cas d'usage de la blockchain privée sont ceux de la [supply chain](#) (ensemble de processus et d'acteurs qui se coordonnent pour transformer des matières premières en produits finis et les livrer aux clients), de la traçabilité ou encore de l'identité décentralisée. Exemples de blockchains privées : [Hyperledger Fabric \(HLF\)](#), [Corda](#), [Blockchain privée d'Uber](#), [Ripple](#), [Tradelens](#), [IBM Food Trust](#), etc.
- **La blockchain de consortium ou hybride** regroupe des acteurs souhaitant collaborer. Dans ce système décentralisé, seuls certains acteurs, généralement les plus importants, peuvent prendre des décisions. Les droits d'écriture peuvent être modifiés, et les décisionnaires choisissent quelles informations seront rendues publiques et quels blocs resteront privés. Ce modèle est souvent utilisé par des organisations qui veulent travailler ensemble tout en maintenant un certain niveau de contrôle et de confidentialité. Dans cette modalité de fonctionnement de la blockchain, chaque transaction est soumise à un vote entre les acteurs du consortium pour valider l'ajout d'un nouveau bloc à la chaîne de blocs.

Le choix d'un type de blockchain dépend donc des exigences en termes de décentralisation, de confidentialité, de performance et de gouvernance.

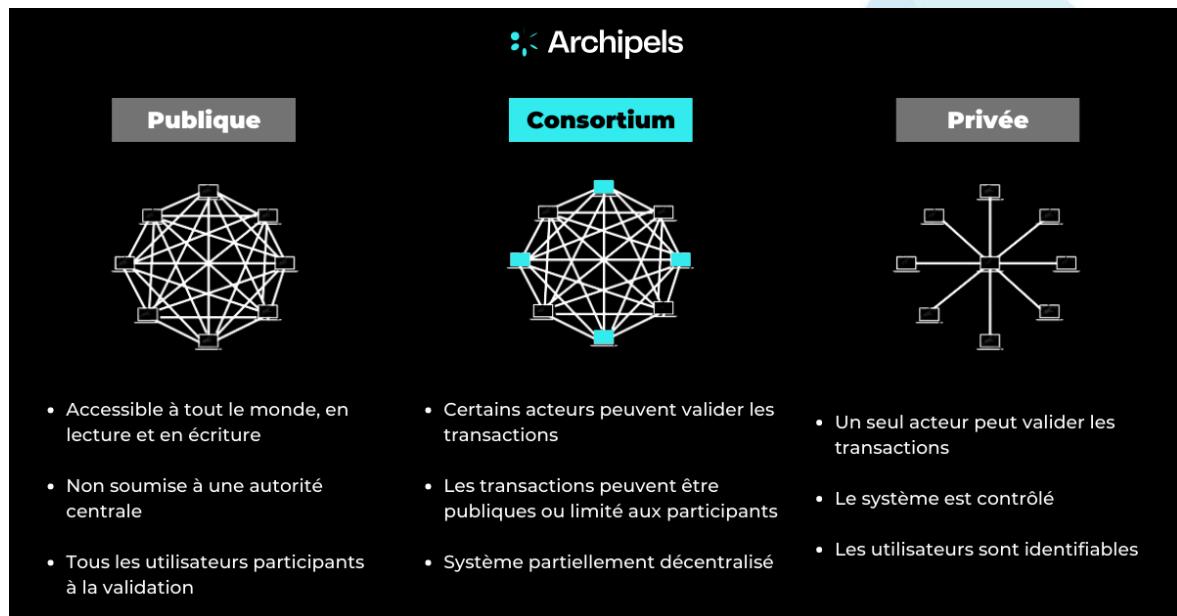


Figure II-1 : Présentation des types de blockchain

Source : <https://www.archipels.io/faq/blockchain-publique-ou-privee-quelle-difference>

### II.1.3 Structure et fonctionnement de la blockchain

La structure de la blockchain repose sur deux éléments fondamentaux : les blocs et la chaîne.

- **Bloc**

Un bloc séquentiel de données. Chaque bloc contient un ensemble de transactions ou d'informations groupées à intervalles de temps réguliers ainsi que d'un hachage du bloc précédent dans la chaîne. Ceci relie les blocs ensemble (dans une chaîne), car les hachages sont cryptographiquement dérivés des données des blocs. Cela empêche la fraude, car un changement dans n'importe quel bloc de l'historique invaliderait tous les blocs suivants, puisque tous les hachages ultérieurs changerait et que quiconque exécutant la blockchain le remarquerait.

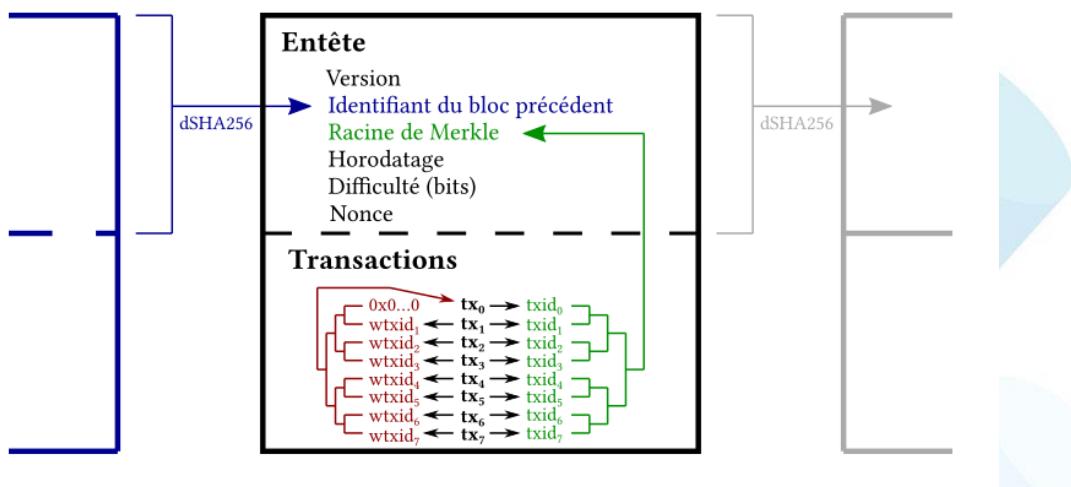


Figure II-2 : Représentation du bloc dans la blockchain

Source : <https://cryptostash.fr/bloc-blockchain-crypto-explication/>

En bleu, on voit l'identifiant du bloc précédent, qui est le résultat de deux hachages successifs par la fonction SHA-256 de l'en-tête de ce bloc. Ce processus relie les blocs entre eux, formant ainsi une chaîne qui constitue la preuve de travail.

En rouge, on observe l'arbre de Merkle des transactions, incluant leurs signatures (ou témoins). Les empreintes de ces transactions forment leur identifiant SegWit (wtxid). La racine de cet arbre de Merkle est inscrite dans la transaction de récompense du bloc (tx0), permettant de relier les signatures aux autres éléments du bloc.

En vert, l'arbre de Merkle représente les transactions sans leurs signatures. Les empreintes de ces transactions forment leur identifiant classique (txid). La racine de cet arbre est inscrite dans l'en-tête du bloc. Puisque tout est interconnecté, toute modification d'une transaction ou de sa signature affecterait l'en-tête, et donc la chaîne de preuve de travail.

- **Chaîne**

La chaîne est une séquence de blocs, chaque bloc étant lié au précédent par un hash cryptographique (empreinte numérique). Ce lien assure l'intégrité des données. Si une donnée dans un bloc est modifiée, le hash du bloc change, rompant ainsi la chaîne et alertant le réseau d'une tentative de falsification. [W7]

Les nœuds du réseau doivent accepter chaque nouveau bloc et valider la chaîne entière pour maintenir la cohérence et la sécurité des données ; on parle de consensus de l'ensemble du réseau.

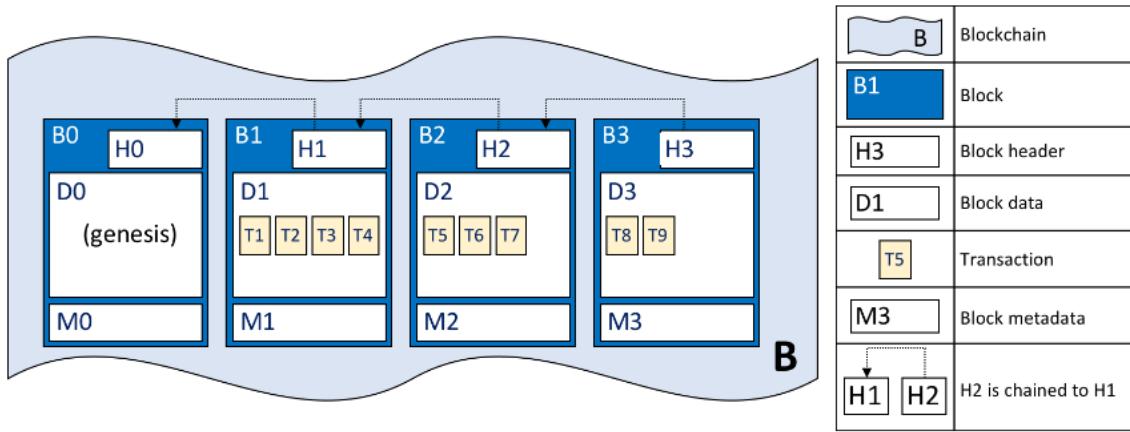


Figure II-3 : Représentation d'une chaîne de blocs

Source : <https://hyperledger-fabric.readthedocs.io/en/release-2.5/ledger/ledger.html>

- **Fonctionnement**

En pratique, une blockchain est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Voici les principales caractéristiques de fonctionnement :

- **Identification cryptographique** : Chaque partie impliquée dans une transaction est identifiée par un procédé cryptographique, assurant la sécurité et l'anonymat.
- **Transmission des transactions** : La transaction est envoyée à un réseau de nœuds de stockage, c'est-à-dire des ordinateurs répartis dans différents espaces géographiques.
- **Stockage distribué** : Chaque nœud du réseau héberge une copie de la base de données contenant l'historique complet des transactions. Cette architecture permet à toutes les parties prenantes d'accéder simultanément aux mêmes informations.
- **Mécanisme de consensus** : La sécurisation des transactions repose sur un mécanisme de consensus entre tous les nœuds. Les données sont déchiffrées et authentifiées par des mineurs ou des centres de données. Une fois validée, la

transaction est ajoutée à la base sous forme d'un bloc de données chiffrées (le « block » dans blockchain).

- **Décentralisation et sécurité :** La gestion décentralisée de la sécurité empêche la falsification des transactions. Chaque nouveau bloc ajouté à la chaîne est lié au précédent et une copie est transmise à tous les nœuds du réseau. Cette intégration est chronologique, indélébile et infalsifiable.

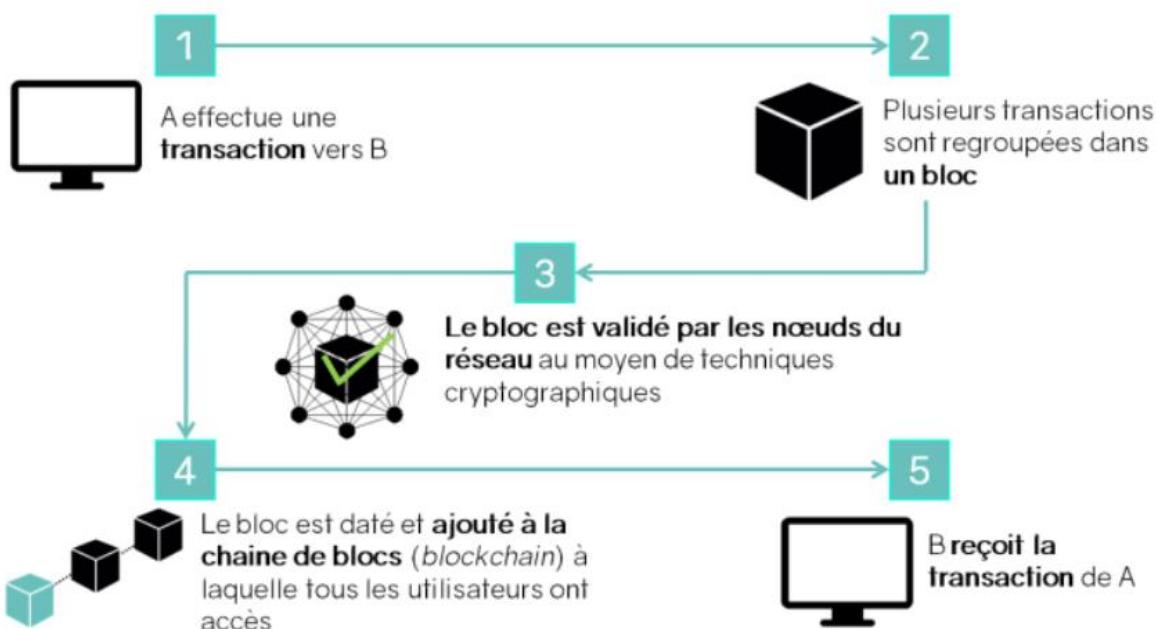


Figure II-4 : Schéma du fonctionnement général d'une blockchain

Source : <https://blog.ippon.fr/2018/01/08/fonctionnement-dune-blockchain/>

## II.1.4 Mécanismes de consensus et sécurité

La sécurité de la blockchain repose sur les mécanismes cryptographiques et des protocoles de consensus :

### II.1.4.1 Cryptographie : un pilier de la sécurité de la blockchain

La cryptographie joue un rôle essentiel dans la sécurité et le fonctionnement des systèmes basés sur la blockchain. Elle permet de garantir la confidentialité, l'intégrité et l'authenticité des données et des transactions, en les protégeant contre les accès non autorisés et les manipulations malveillantes. Cette partie vise à introduire les principaux concepts et techniques cryptographiques utilisés dans le contexte de la blockchain. [B2]

### II.1.4.1.1 Rappels sur la cryptographie

- **Définition et objectifs**

La cryptographie est la science de la protection de l'information. Elle consiste à transformer un message en clair en un message chiffré, de manière à ce qu'il ne soit lisible que par les personnes autorisées. Les principaux objectifs de la cryptographie sont de garantir :

- La confidentialité : seules les parties autorisées peuvent accéder à l'information
- L'intégrité : l'information ne peut pas être modifiée de manière indétectable
- L'authenticité : l'origine de l'information peut être vérifiée de manière fiable

- **Types de cryptographie**

Il existe deux grandes familles de cryptographie :

- La cryptographie symétrique : elle utilise la même clé pour chiffrer et déchiffrer les données. Les algorithmes les plus courants sont AES, DES, 3DES.

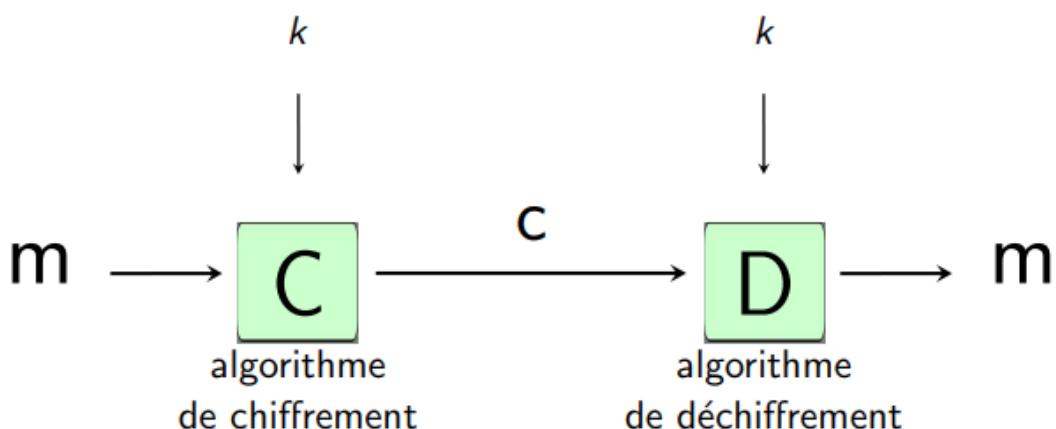


Figure II-5 : Schéma du chiffrement symétrique

Source : <https://repository.root-me.org/Cryptographie/Sym%C3%A9trique/FR%20-%20Chiffrement%20sym%C3%A9trique.pdf>

- La cryptographie asymétrique : elle utilise une paire de clés, une clé publique pour chiffrer et une clé privée pour déchiffrer. Les algorithmes les plus courants sont RSA, ECC.

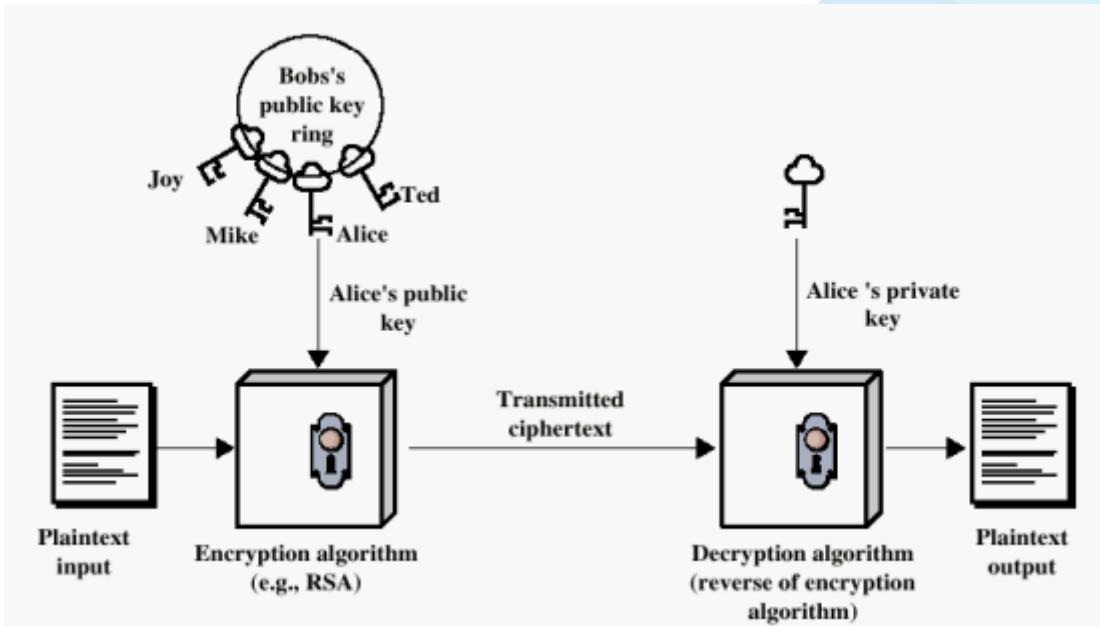


Figure II-6 : Schéma du chiffrement asymétrique

Source : <https://people.irisa.fr/Bernard.Cousin/Cours/2-Clef%20publique.2P.pdf>

#### II.1.4.1.2 Cryptographie et blockchain

- **Hachage cryptographique**

Le hachage est une fonction qui transforme une donnée de taille arbitraire en une empreinte de taille fixe. En blockchain, le hachage est utilisé pour :

- Identifier de manière unique les blocs et les transactions
- Vérifier l'intégrité des données (toute modification change l'empreinte)
- Lier les blocs entre eux (chaque bloc inclut le hash du bloc précédent) Les algorithmes de hachage les plus utilisés en blockchain sont SHA-256 et Keccak-256.

- **Signatures numériques**

Les signatures numériques permettent de prouver l'authenticité et la non-répudiation d'une transaction blockchain. Elles reposent sur la cryptographie asymétrique :

- L'émetteur signe la transaction avec sa clé privée
- Le destinataire vérifie la signature avec la clé publique de l'émetteur Les algorithmes de signature les plus courants sont ECDSA et EdDSA (Edwards-curve Digital Signature Algorithm).

- **Arbres de Merkle**

Les arbres de Merkle sont des structures de données utilisées en blockchain pour vérifier efficacement la présence et l'intégrité d'une transaction dans un bloc. Il s'agit d'un arbre binaire dont :

- Les feuilles sont les transactions du bloc
- Chaque nœud est le hash de la concaténation de ses deux nœuds fils
- La racine (Merkle root) est incluse dans l'en-tête du bloc Pour prouver l'inclusion d'une transaction, il suffit de fournir le chemin de Merkle (les nœuds frères) jusqu'à la racine.

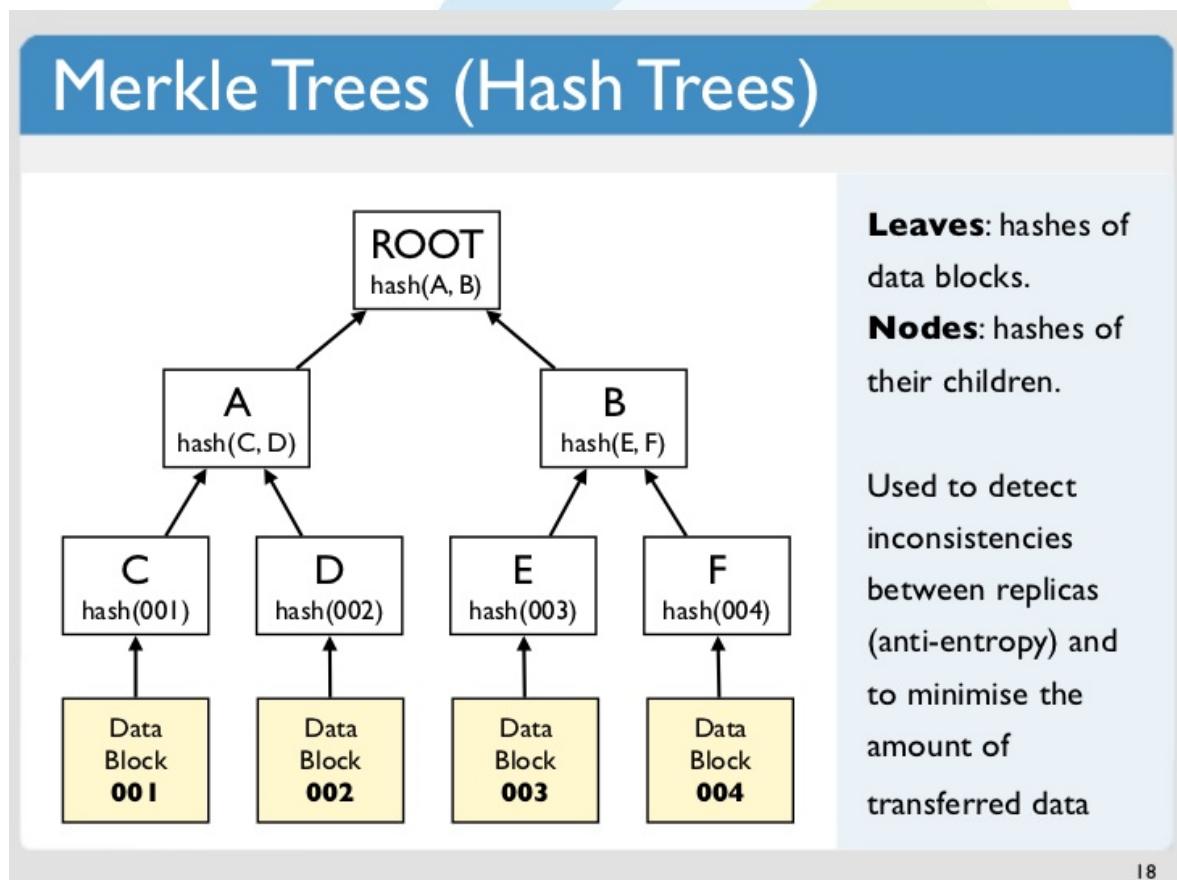


Figure II-7 : Un arbre de Merkle binaire

Source : <https://tryalgo.org/fr/2016/12/10/arbres-de-merkle/>

### II.1.4.1.3 Perspectives et défis

- **Cryptographie post-quantique**

L'avènement des ordinateurs quantiques représente une menace potentielle pour la sécurité des systèmes cryptographiques actuels, notamment ceux basés sur la factorisation (RSA (Rivest-Shamir-Adleman)) ou les logarithmes discrets (ECC (Elliptic Curve Cryptography)). La recherche en cryptographie post-quantique vise à développer des algorithmes résistants aux attaques quantiques, tels que :

- Les codes correcteurs d'erreurs (McEliece, NTRU)
- Les réseaux euclidiens (CRYSTALS-KYBER, SABER)
- Les fonctions de hachage (SPHINCS+)

- **Cryptographie pour la confidentialité**

La transparence des blockchains publiques peut être un frein à l'adoption pour certains cas d'usage nécessitant une confidentialité renforcée. Plusieurs techniques cryptographiques sont étudiées pour concilier transparence et confidentialité :

- Les transactions confidentielles (Confidential Transactions, bulletproofs...)
- Les preuves à divulgation nulle de connaissance (zk-SNARKs, zk-STARKs)
- Le chiffrement homomorphe (qui permet de calculer sur des données chiffrées)

La cryptographie est un élément central de la sécurité et de la confiance dans les systèmes blockchain. Les techniques de hachage, de signature numérique et les arbres de Merkle permettent de garantir l'intégrité, l'authenticité et l'efficacité des transactions. Les défis à venir, tels que la menace quantique ou les exigences de confidentialité, nécessiteront de nouvelles avancées cryptographiques pour assurer la pérennité et l'adaptabilité de la technologie blockchain.

### II.1.4.2 Protocoles de consensus

L'ajout dans la chaîne ou la modification d'un bloc nécessite une validation des nœuds du réseau via une gestion de consensus. Les blockchains, en fonction de leur type, utilisent différents mécanismes de preuve pour valider les transactions et ajouter de nouveaux blocs. Le consensus (ou mécanisme de consensus) est un ensemble de protocoles et de règles qui

permettent aux nœuds du réseau (ou nodes) de s'entendre sur l'état actuel de la blockchain, garantissant ainsi la sécurité, la stabilité et la décentralisation du système. Le consensus est atteint lorsque tous les nœuds du réseau sont d'accord sur l'ensemble des transactions validées et stockées dans la blockchain. Pour y arriver, les nœuds utilisent des algorithmes de consensus qui vérifient et valident les transactions, créant ainsi un consensus sur l'état de la blockchain. Voici les principaux types : [W8] [B3]

- **Preuve de travail (Proof of Work – PoW)**

La preuve de travail est couramment utilisée dans les blockchains publiques comme Bitcoin et Ethereum. Ce mécanisme repose sur la résolution d'un problème cryptographique complexe, que les mineurs doivent résoudre pour valider un bloc. La résolution nécessite une puissance de calcul importante, impliquant un coût énergétique significatif. La difficulté du problème augmente progressivement. Le processus est asymétrique : il est difficile à résoudre, mais facile à vérifier. Le premier mineur à trouver la solution voit son bloc validé par le réseau avant d'être ajouté à la chaîne.

- **Preuve d'autorité (Proof of Authority - PoA)**

La preuve d'autorité, quant à elle, est adaptée aux blockchains privées et se base sur la réputation et la confiance. Seul un nombre limité de nœuds de confiance ont le droit de valider les blocs, ces nœuds étant généralement désignés par un administrateur. Ce système, bien que plus centralisé, offre une meilleure performance et scalabilité, ce qui peut être avantageux pour certaines applications.

- **Preuve d'enjeu (Proof of Stake - PoS)**

La preuve d'enjeu est souvent utilisée dans les blockchains de consortium et repose sur la participation des utilisateurs. Les validateurs doivent prouver qu'ils possèdent une certaine quantité de crypto-monnaies pour être sélectionnés. La sélection des validateurs est aléatoire, mais pondérée par leur participation. Ce mécanisme réduit la consommation d'énergie par rapport à la preuve de travail et évite la centralisation en empêchant les plus riches utilisateurs d'avoir un avantage systématique.

## II.2 Blockchain pour l'identité numérique

### II.2.1 Concepts d'identité décentralisée

La gestion des identités numériques est un cas d'usage prometteur de la technologie blockchain. Le concept d'identité décentralisée ou auto-souveraine vise à redonner aux individus le contrôle de tout et d'une partie de leurs données d'identité.

Dans un modèle d'identité décentralisée, les utilisateurs créent et gèrent leurs propres identifiants vérifiables sur une blockchain sans dépendre d'une autorité centrale. Ils peuvent sélectivement partager ces identifiants avec des tiers pour accéder à des services, tout en conservant la maîtrise de leurs données personnelles.

La blockchain, par ses propriétés de décentralisation, d'immuabilité et de transparence, offre une infrastructure adaptée pour l'émission, le stockage et la vérification d'identités numériques de manière sécurisée et respectueuse de la vie privée.

### II.2.2 Smart contract ou contrat intelligent et gestion des identités

Un contrat intelligent est un protocole ou un programme informatique irrévocable, le plus souvent déployé sur la blockchain qui exécute un ensemble d'instructions prédéfinies. L'idée derrière ce concept de smart contracts est de garantir la force obligatoire des contrats non plus par le droit, mais directement par le code informatique : « [Code is law](#) », pour reprendre la célèbre formule de Lawrence Lessing. La meilleure façon d'envisager un contrat intelligent est de penser à un distributeur automatique : lorsque vous insérez la bonne somme d'argent et appuyez sur le bouton d'un article, le programme (le contrat intelligent) active la machine pour distribuer l'article que vous avez choisi. Les blockchains programmables comme Ethereum ont introduit le concept de contrat intelligent (smart contract), qui est un programme autonome dont l'exécution est déclenchée par des transactions sur la blockchain. Les smart contracts jouent un rôle clé dans la gestion décentralisée des identités en permettant l'automatisation de processus tels que :

- L'émission et la révocation d'identifiants vérifiables
- La vérification de l'authenticité des attestations
- La gestion du consentement et des autorisations d'accès
- L'application de politiques de confidentialité

L'utilisation de smart contracts renforce la sécurité et l'efficacité des systèmes d'identité décentralisée en réduisant les risques d'erreur humaine et en garantissant l'application impartiale des règles.

### II.2.3 Standards et protocoles

L'adoption à grande échelle de solutions d'identité numérique basées sur la blockchain nécessite l'émergence de standards et de protocoles interopérables. Plusieurs initiatives visent à développer des cadres techniques et des bonnes pratiques pour la gestion décentralisée des identités, notamment :

- Les spécifications du World Wide Web Consortium (W3C) Decentralized Identifiers (DID) et Verifiable Credentials (VC) qui définissent des formats standardisés pour les identifiants décentralisés et les attestations vérifiables.
- Le protocole d'identité décentralisée de Sovrin, qui s'appuie sur une blockchain permissionnée et une gouvernance distribuée.
- Le réseau d'identité décentralisée d'Hyperledger Indy, qui fournit des outils et des bibliothèques pour la création de solutions d'identité souveraine.

L'adoption de standards ouverts est essentielle pour garantir la portabilité et l'interopérabilité des identités numériques à travers différents domaines et juridictions.

## II.3 Applications dans le secteur bancaire

### II.3.1 Cas d'usage existants

La technologie blockchain trouve de nombreuses applications dans le domaine de l'identification bancaire, en particulier dans des contextes où la gestion des homonymies et la lutte contre la fraude identitaire constituent des enjeux majeurs. Plusieurs initiatives ont été lancées pour tirer parti de la blockchain dans la gestion des identités bancaires :

- **Le projet Hades de Africa BIoT Labs**, un système d'identité décentralisé basé sur la blockchain Near, qui vise à fournir une infrastructure KYC fiable et transparente pour les applications bancaires en Afrique.

- **La plateforme d'identité numérique décentralisée** développée par Kiva en partenariat avec la Sierra Leone, qui permet aux citoyens non bancarisés d'accéder à des services financiers grâce à une identité vérifiable sur blockchain. [W2]
- **Kenya** : Le Kenya avait prévu de lancer en décembre 2023 un système d'identification numérique national utilisant la blockchain, baptisé « Maisha Namba ». Ce projet s'inscrit dans une initiative plus large visant à intégrer des solutions basées sur la blockchain pour améliorer l'identification des citoyens et faciliter l'accès aux services gouvernementaux et financiers. Le système fournira à chaque Kényan un numéro d'identification unique qui deviendra son numéro d'identité personnel à vie, de la naissance à la mort. La carte d'identité biométrique associée, appelée « Carte Maisha », remplacera l'actuelle carte d'identité de deuxième génération et sera utilisée pour la vérification hors ligne. Le gouvernement kényan s'est associé au PNUD (Programme des Nations Unies pour le Développement) pour mobiliser les ressources nécessaires au développement et à la mise en œuvre de ce système. [W3]
- **Ethiopie** : Cardano, la plateforme blockchain, s'associe au gouvernement éthiopien pour révolutionner le système éducatif. Grâce à Atala PRISM, une solution d'identification native, 5 millions d'étudiants et 750 000 professeurs bénéficieront d'un système de suivi numérique sécurisé. Cette initiative, s'inscrivant dans le cadre du programme Digital Éthiopie 2025, permettra de vérifier les notes, de lutter contre la fraude aux diplômes et de favoriser l'accès à l'emploi. Ce projet illustre le potentiel de la blockchain pour numériser les services publics dans les pays en développement. [W4]

Ces cas d'usage montrent comment la blockchain peut être utilisée pour créer des systèmes d'identification bancaire plus inclusifs, plus sécurisés et plus respectueux de la vie privée.

### II.3.2 Perspectives d'évolution

Au-delà de la gestion des identités, la blockchain ouvre de nouvelles perspectives pour la transformation numérique du secteur bancaire. Parmi les pistes d'évolution prometteuses :

- L'automatisation des processus de conformité (KYC, LCB-FT signifiant Lutte Contre le Blanchiment de capitaux et le Financement du Terrorisme) grâce à des smart contracts appliquant les règles de vérification et de surveillance des transactions.

- Le développement de nouvelles formes de monnaies numériques de banque centrale (MNBC) adossées à des registres distribués, permettant des paiements transfrontaliers plus rapides et moins coûteux.
- L'émergence de modèles de finance décentralisée (DeFi) basés sur des protocoles blockchain ouverts et interopérables, offrant de nouveaux services financiers sans intermédiaires.
- L'intégration des solutions d'identité blockchain avec les technologies d'intelligence artificielle et d'apprentissage automatique pour une évaluation en temps réel des risques.

Ces évolutions nécessiteront une adaptation des cadres réglementaires et une collaboration étroite entre régulateurs, institutions financières et acteurs technologiques pour créer un écosystème d'identité numérique de confiance. [B4]

## Conclusion

Ce chapitre a permis d'explorer le potentiel de la technologie blockchain pour la gestion des identités dans le secteur bancaire. Après avoir présenté les fondamentaux techniques de la blockchain et ses différents types, nous avons examiné les concepts clés de l'identité décentralisée et le rôle des smart contracts dans l'automatisation des processus d'identification. L'analyse des cas d'usage existants a mis en lumière les opportunités offertes par la blockchain pour créer des systèmes d'identification plus sécurisés, plus inclusifs et respectueux de la vie privée. Elle a également souligné les défis à relever en termes de gouvernance, d'interopérabilité et d'expérience utilisateur. Enfin, nous avons esquissé quelques perspectives d'évolution liées à l'application de la blockchain dans le secteur bancaire, au-delà de la seule gestion des identités. Ces pistes ouvrent la voie à une réflexion plus large sur la transformation numérique du secteur et le rôle que pourrait y jouer la technologie blockchain.

Le prochain chapitre sera consacré à la conception d'une solution d'identification bancaire basée sur la blockchain, adaptée au contexte spécifique de l'UEMOA qui permettra de résoudre le problème des homonymies. Nous détaillerons l'architecture fonctionnelle et technique envisagée, ainsi que les choix de mise en œuvre retenus pour répondre aux enjeux identifiés.

## Chapitre III : ANALYSE ET CONCEPTION DE LA SOLUTION

### Introduction

La gestion des homonymies dans le secteur bancaire de l'UEMOA constitue un défi majeur pour la sécurité et l'efficacité des opérations financières. Cette section présente l'analyse détaillée et la conception d'une solution blockchain pour résoudre ce problème. La solution proposée vise à créer un système d'identification unique, sécurisé et interopérable, permettant aux institutions bancaires de l'UEMOA de gérer efficacement les identités de leurs clients tout en garantissant la protection des données personnelles. Par conséquent résolvant le problème d'homonymie.

### III.1 Périmètre fonctionnel

Le périmètre fonctionnel définit l'ensemble des fonctionnalités, acteurs et interactions du système de gestion des identités bancaires visant à résoudre la problématique des homonymies dans l'espace UEMOA. Il établit les limites précises du système et spécifie les capacités fonctionnelles requises pour atteindre les objectifs fixés. Dans la mise en place de notre solution, les informations adressées portent sur les personnes physiques exclusivement.

#### III.1.1 Objectifs du système

Le système vise trois objectifs fondamentaux qui constituent le socle de notre solution pour une identification bancaire fiable dans l'espace UEMOA.

- Création et gestion d'identifiants bancaires uniques (IBU)
- Résolution des cas d'homonymies
- Partage sécurisé des données clients entre institutions

### III.1.2 Fonctionnalités principales

Ces fonctionnalités représentent les capacités essentielles du système, structurées en trois axes majeurs pour répondre aux besoins opérationnels des institutions bancaires.

- **Gestion des Identités**

- Création et attribution des IBU
- Détection et gestion des homonymies
- Mise à jour des informations clients
- Gestion des documents d'identité

- **Administration et Sécurité**

- Configuration des accès utilisateurs
- Traçabilité des opérations
- Contrôle des habilitations

- **Fonctionnalités de Recherche**

- Recherche multicritères (nom, prénoms)
- Reconnaissance faciale
- Consultation des historiques

### III.1.3 Acteurs du système

Les acteurs du système sont les parties prenantes qui interagissent avec le réseau Blockchain. Ils constituent l'écosystème complet du système, chacun ayant un rôle spécifique dans le processus d'identification bancaire. Ils sont classifiés comme suit :

- **BCEAO (Banque Centrale des États de l'Afrique de l'Ouest) :** Superviseur du réseau blockchain. Elle gère la gouvernance, la validation des transactions et l'ajout de nouvelles institutions au réseau. La BCEAO est garante de la conformité et de la sécurité des opérations.
- **Banques et institutions financières :** Chaque banque est membre du réseau blockchain et possède un nœud lui permettant d'interagir avec le système. Les banques peuvent vérifier l'existence des clients, créer de nouveaux clients et ajouter des comptes bancaires associés.

- **Clients :** Les clients sont les entités dont les informations sont enregistrées dans la blockchain. Ils peuvent être des individus ou des entreprises, et chaque client est identifié par un IBU unique. Il n'est pas un acteur participant au ré

## III.2 Analyse des besoins

L'analyse des besoins définit les exigences fonctionnelles et non-fonctionnelles nécessaires pour un système d'identification bancaire efficace et sécurisé.

### III.2.1 Besoins fonctionnels

Cette section détaille l'ensemble des fonctionnalités requises pour que le système remplisse sa mission principale de gestion des identités bancaires. Ces besoins définissent les capacités attendues du système pour résoudre efficacement la problématique des homonymies dans l'espace UEMOA, en assurant une identification unique et fiable des clients bancaires.

#### III.2.1.1 Gestion des identités

Ce module constitue le cœur du système, assurant une identification unique et fiable des clients bancaires.

- **Création d'IBU (Identifiant Bancaire Unique)**
  - Génération automatique d'identifiants uniques pour chaque client
  - Validation des informations d'identité à l'entrée
  - Association des données biométriques à l'IBU
  - Vérification de l'unicité de l'identifiant
- **Détection des Homonymies**
  - Algorithmes de comparaison des noms et prénoms
  - Analyse des données biométriques
  - Vérification des documents d'identité
  - Système de scoring pour évaluer la probabilité d'homonymie
- **Gestion des Informations Clients**
  - Mise à jour des données personnelles
  - Ajout/suppression de comptes bancaires
  - Modification du statut client
  - Gestion des documents justificatifs

- **Recherche par Critères**

- Recherche exacte par IBU
- Recherche approximative par nom/prénom
- Filtres par données démographiques
- Historique des recherches

- **Reconnaissance Faciale**

- Capture d'image en temps réel
- Comparaison avec la base de données biométriques
- Détection des tentatives de fraude
- Gestion des faux positifs

### III.2.1.2      **Gestion des accès**

Cette composante implémente les mécanismes de sécurité essentiels pour protéger l'intégrité du système.

- **Authentification**

- Authentification multi facteur pour les utilisateurs bancaires
- Gestion des certificats numériques
- Contrôle d'accès basé sur les rôles
- Sessions sécurisées avec timeout automatique

- **Droits d'Accès**

- Définition des profils utilisateurs
- Attribution des permissions par fonction
- Gestion des habilitations temporaires
- Restriction géographique des accès

- **Traçabilité**

- Journalisation des consultations
- Enregistrement des modifications
- Horodatage des opérations
- Rapports d'audit

### III.2.2 Besoins non-fonctionnels

Au-delà des fonctionnalités, le système doit répondre à des exigences essentielles de qualité de service. Ces besoins non-fonctionnels couvrent la sécurité, la performance et la conformité réglementaire, aspects critiques pour un système d'identification bancaire opérant dans un environnement aussi sensible que celui de l'UEMOA.

#### III.2.2.1 Sécurité

La protection des données constitue une exigence fondamentale du système.

- **Chiffrement**

- Chiffrement des données sensibles au repos.
- Chiffrement des communications.
- Gestion des clés cryptographiques.
- Protection contre les attaques.

- **Contrôle d'Accès**

- Authentification forte
- Autorisation basée sur les rôles
- Ségrégation des données
- Prévention des fuites de données

#### III.2.2.2 Performance

Les critères de performance définissent les standards opérationnels du système.

- **Temps de Réponse**

- Recherche instantanée
- Création d'IBU en temps réel
- Synchronisation rapide entre nœuds
- Optimisation des requêtes

- **Scalabilité**

- Support de millions de clients
- Gestion de pics de charge
- Extensibilité horizontale
- Répartition de charge

### III.2.2.3 Conformité

L'adhésion aux normes garantit la légitimité du système. Pour cela certains aspects doivent être atteints dans notre système.

- Respect des dispositions réglementaires de la BCEAO en matière de déclaration de données
- Conformité sur la protection des données
- KYC

## III.3 Architecture et fonctionnement du système

### III.3.1 Choix du type de blockchain

Tableau III-1 : Présentations des caractéristiques de chaque type de blockchain

Source : Personnelle

Caractéristiques	Blockchain Publique	Blockchain Privée	Blockchain Consortium
Accès	Ouvert à tous	Restreint à un groupe sélectionné	Restreint à un consortium
Décentralisation	Entièrement décentralisée	Entièrement centralisée	Semi-décentralisée
Transparence	Très élevée	Faible	Moyenne
Sécurité	Très élevée grâce à la décentralisation	Peut-être élevée mais dépend du contrôle central	Élevée grâce à la collaboration du consortium
Confidentialité	Faible	Élevée	Moyenne
Scalabilité	Faible	Élevée	Élevée
Performance	Moyenne	Élevée	Élevée
Gouvernance	Décentralisée	Centralisée	Consortium

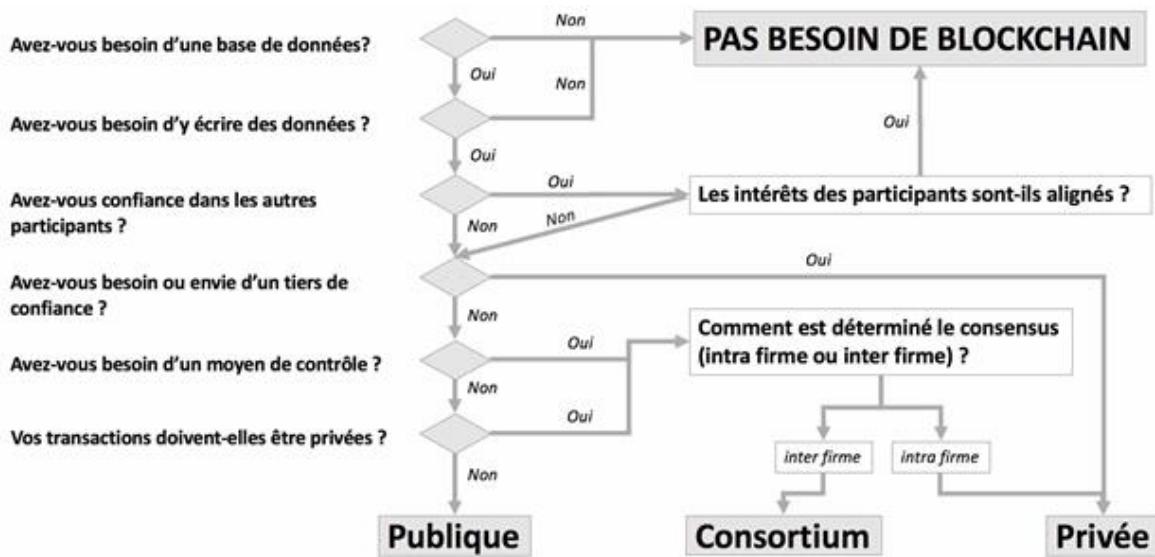


Figure III-1 : Diagramme permettant de faire le choix du type de blockchain adapté à une problématique

Source : <https://www.week-lab.com/les-differents-types-de-blockchain/>

Une blockchain de consortium est recommandée pour le système d'identification bancaire unique de l'UEMOA pour plusieurs raisons :

- Confidentialité et sécurité :** les données sensibles peuvent être partagées de manière sécurisée entre les banques participantes tout en préservant la confidentialité.
- Contrôle et gouvernance :** les institutions financières de l'UEMOA et la BCEAO peuvent collaborer pour gérer et maintenir le réseau, assurant une gouvernance équilibrée.
- Décentralisation et confiance :** Bien que contrôlée, la nature semi-décentralisée du consortium renforce la confiance entre les participants en répartissant le contrôle.
- Scalabilité et performance :** Permet une gestion efficace des transactions et des identifiants, crucial pour un système utilisé à grande échelle.

### III.3.2 Architecture globale du système

Le système de gestion des identités bancaires repose sur une architecture blockchain permissionnée et décentralisée en consortium. Cette architecture permet à chaque institution bancaire de l'UEMOA et à la BCEAO d'agir en tant qu'organisation du réseau. Les nœuds partagent un accès aux transactions enregistrées sur la blockchain, garantissant ainsi la sécurité, la transparence et l'intégrité des données relatives aux identités bancaires.

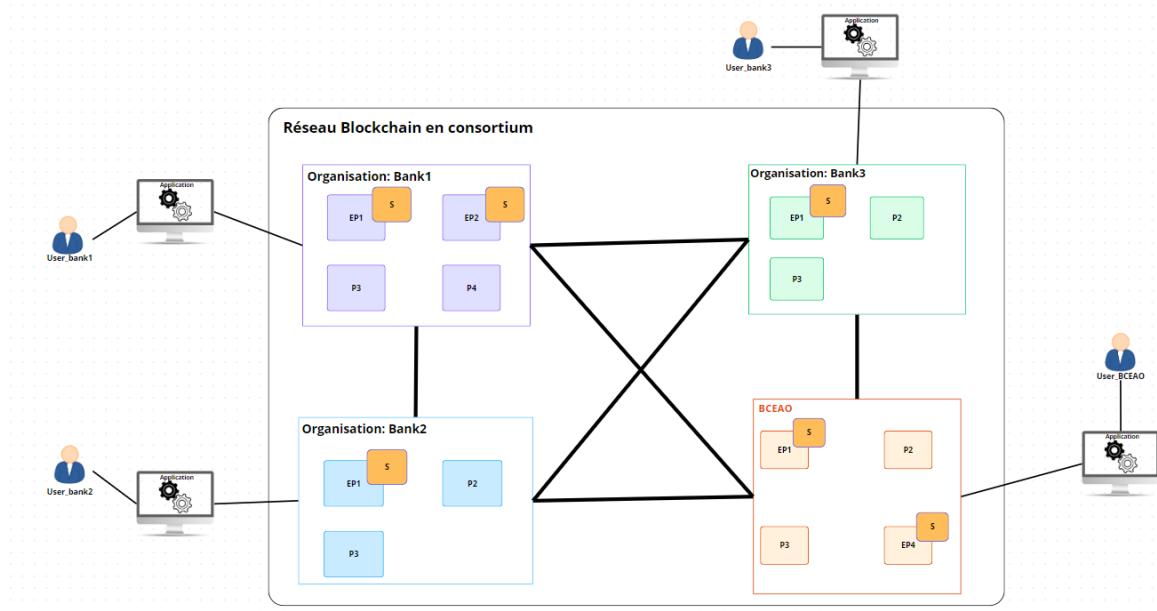


Figure III-2 : Architecture globale du système basée sur une blockchain en consortium

Source : Personnelle

<b>EP</b>	Endorser Peer
<b>P</b>	Peer
<b>S</b>	Chaincode

Capture III-1 : Légende des éléments de l'architecture

Source : Personnelle

L'architecture proposée pour le système de gestion des IBU est illustrée par le schéma ci-dessus. Elle repose sur une blockchain de consortium où la BCEAO joue un rôle central de

régulateur et de superviseur, tandis que les institutions bancaires sont les participants actifs du réseau. L'architecture proposée comprend trois composantes principales :

- **Infrastructure blockchain**

- Un réseau de consortium incluant la BCEAO et les banques
- Chaque participant dispose de ses propres nœuds
- Protection des données par cryptographie avancée

- **Rôles des participants**

- BCEAO : supervision, gouvernance et conformité réglementaire
- Banques : vérification et attribution des IBU via leurs nœuds
- Application décentralisée pour l'interaction avec le réseau

- **Fonctionnement**

- Smart contracts pour l'automatisation des processus
- Vérification et attribution des IBU par consensus
- Sécurisation des données clients

Cette architecture assure une gestion décentralisée et sécurisée des identifiants bancaires uniques dans l'espace UEMOA.

### III.4 Modélisation du système

La modélisation du système constitue une étape fondamentale dans la conception de notre solution blockchain pour la gestion des identités bancaires. Pour représenter efficacement l'architecture et le fonctionnement du système, nous utilisons le langage de modélisation UML (Unified Modeling Language), un standard graphique qui permet de visualiser, spécifier et documenter les différents aspects d'un système d'information. À travers les diagrammes UML tels que les cas d'utilisation, les diagrammes de séquence et les diagrammes de classes, nous pouvons décrire de manière claire et précise la structure des données, les interactions entre les composants et les règles métier qui gouvernent notre solution. Cette modélisation nous permettra d'assurer une implémentation cohérente et efficace du système.

### III.4.1 Modèle de données

Pour garantir une gestion efficace et cohérente des informations dans notre système blockchain, il est essentiel de définir un modèle de données. Ce modèle spécifie la manière dont les données des clients bancaires, leurs identifiants uniques et les transactions sont organisés et stockés dans le réseau. Il prend en compte les exigences de sécurité, de traçabilité et d'interopérabilité propres au secteur bancaire de l'UEMOA. Les informations relatives aux clients constituent les actifs stockés de manière immuable sur la blockchain.

Ces données sont constituées comme suit :

Tableau III-2 : Présentation du format des données du client

Source : Personnelle

Champs	Description	Obligatoire	Type de données	Nom du champ JSON
IBU	Identifiant bancaire unique du client	Oui	String	IBU
Prénom	Prénom du client	Oui	String	firstName
Nom	Nom de famille du client	Oui	String	lastName
Date de naissance	Date de naissance du client (format : YYYY-MM-DD)	Oui	Date	dateOfBirth
Sexe	Genre du client	Oui	String	gender
Email	Adresse email du client	Oui	String	email
Nationalité(s)	Liste des nationalités du client	Oui	Array of Objects	nationality
Liste des comptes	Liste des comptes du client	Oui	Array of Objects	accountList
Statut	Statut actif ou non	Oui	Boolean	isActive
Document	Informations relatives	Oui	Object	documentIdentification
Face ID	Image faciale du client	Oui	Binary	imageFace

### III.4.2 Diagrammes UML

#### III.4.2.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation met en évidence les interactions possibles entre les acteurs externes (utilisateurs ou systèmes) et le système étudié. Pour notre projet, il s'agit de modéliser les fonctionnalités principales offertes par la solution blockchain pour la gestion des identités bancaires.

Voici les principaux cas d'utilisation identifiés :

- **Connection à la plateforme :** L'employé de banque doit se connecter avant d'effectuer d'autres actions.
- **Enregistrement d'un client :** Un employé de banque peut enregistrer un nouveau client en ajoutant ses informations personnelles, ses documents d'identification et ses nationalités.
- **Mise à jour des informations client :** Un employé peut :
  - Ajouter ou supprimer un compte bancaire pour un client.
  - Ajouter ou supprimer une nationalité associée au client.
- **Consultation des informations client :** Un employé peut visualiser les données d'un client, notamment ses informations personnelles, ses comptes bancaires ouverts dans ses livres et ses documents d'identification.
- **Consulter l'historique des mises à jour d'un client :** Un employé peut consulter toutes les modifications effectuées sur les informations d'un client, comme l'ajout ou la suppression d'un compte ou d'une nationalité.
- **Désactivation ou réactivation d'un client :** Un employé peut demander au régulateur (BCEAO) de désactiver ou de réactiver un client selon des critères spécifiques.
- **Recherche de clients :** Un employé peut :
  - Rechercher un client par reconnaissance faciale.
  - Rechercher un client à l'aide de son nom et prénom.
- **Validation des transactions :** La BCEAO valide toutes les transactions impliquant la désactivation ou la réactivation d'un client. Toutes les autres transactions relatives à l'ajout ou la mise à jour sont validées automatiquement.

Les acteurs principaux sont :

- **Employé de banque** : Responsable de la gestion des données client.
- **BCEAO** : Superviseur du réseau et valideur des transactions.

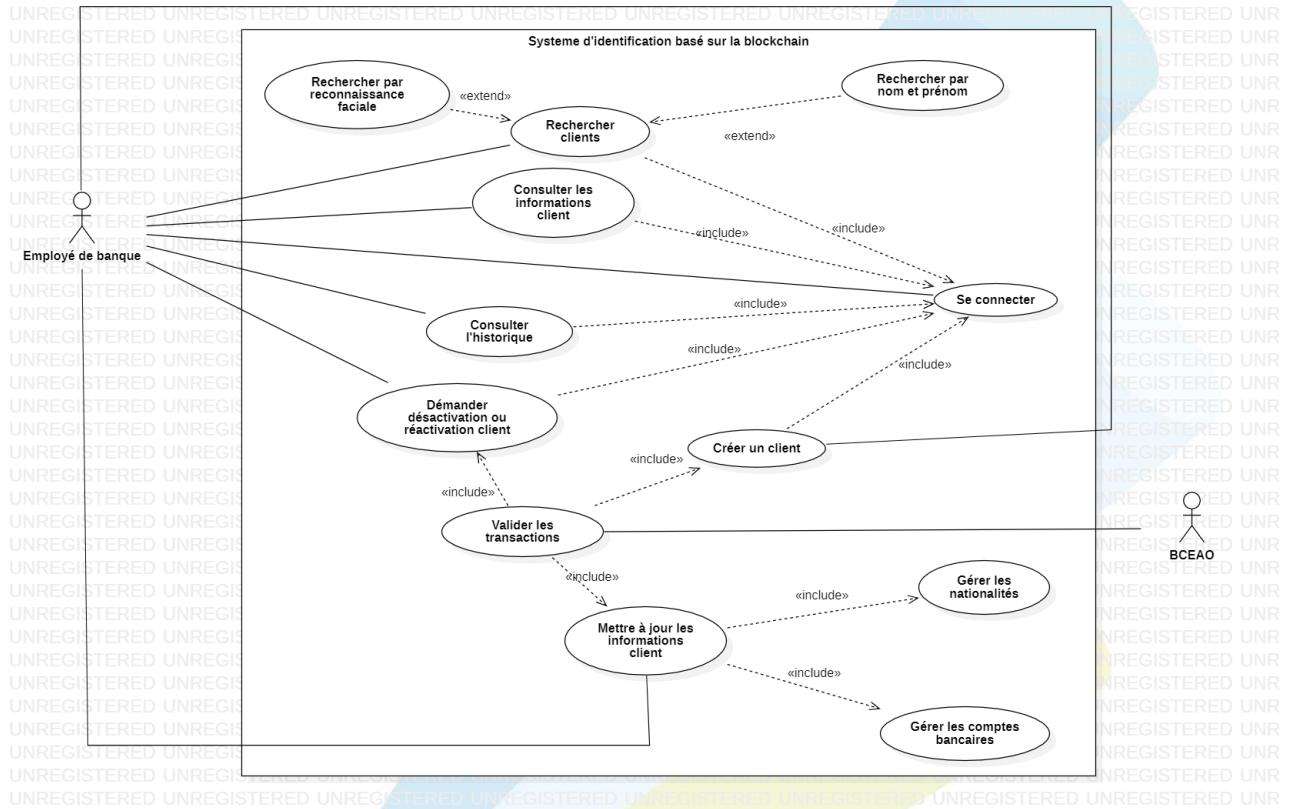


Figure III-3 : Diagramme de cas d'utilisation

Source : Personnelle

### III.4.2.2 Diagramme de classe

Le diagramme de classe est utilisé pour représenter la structure statique du système en mettant en évidence les classes, leurs attributs, leurs méthodes, ainsi que les relations entre elles. Ce diagramme constitue la base pour la conception et l'implémentation du système.

Dans le contexte de notre solution blockchain pour la gestion des identités bancaires, le diagramme de classe inclut les éléments suivants :

- **Client** : Représente les informations personnelles des clients, telles que leur prénom, nom, date de naissance, sexe, email, image faciale (biométrie) et leur IBU (Identifiant Bancaire Unique).

- **Account** : Définit les comptes associés à chaque client, avec des attributs comme le numéro de compte, le type de compte et son statut.
- **Bank** : Modélise les banques du réseau, responsables de la gestion des clients et des transactions.
- **Document** : Stocke les informations relatives aux documents d'identification du client, y compris le type de document, le numéro, les dates de délivrance et d'expiration, et une image du document.
- **Imageface** : Définit l'image du client.
- **Nationality** : Indique-la ou les nationalités d'un client.
- **Transaction Blockchain** : Enregistre les opérations effectuées dans le réseau, comme l'enregistrement ou la mise à jour des informations client. Chaque transaction est associée à un type (inscription, mise à jour ou consultation).
- **BCEAO** : Représente la banque centrale, qui joue un rôle clé dans l'audit et la validation des transactions dans le réseau blockchain.

#### Relations entre les classes

- Un Client peut être associé à plusieurs comptes bancaires (Account), documents (Document) et nationalités (Nationality).
- Un client est associé à une image faciale.
- Bank est liée à plusieurs comptes et transactions.
- Les Transactions sont également validées et supervisées par la BCEAO.
- La relation entre Document et Nationality est une relation "1 à 1..\*" pour identifier l'origine nationale du document.

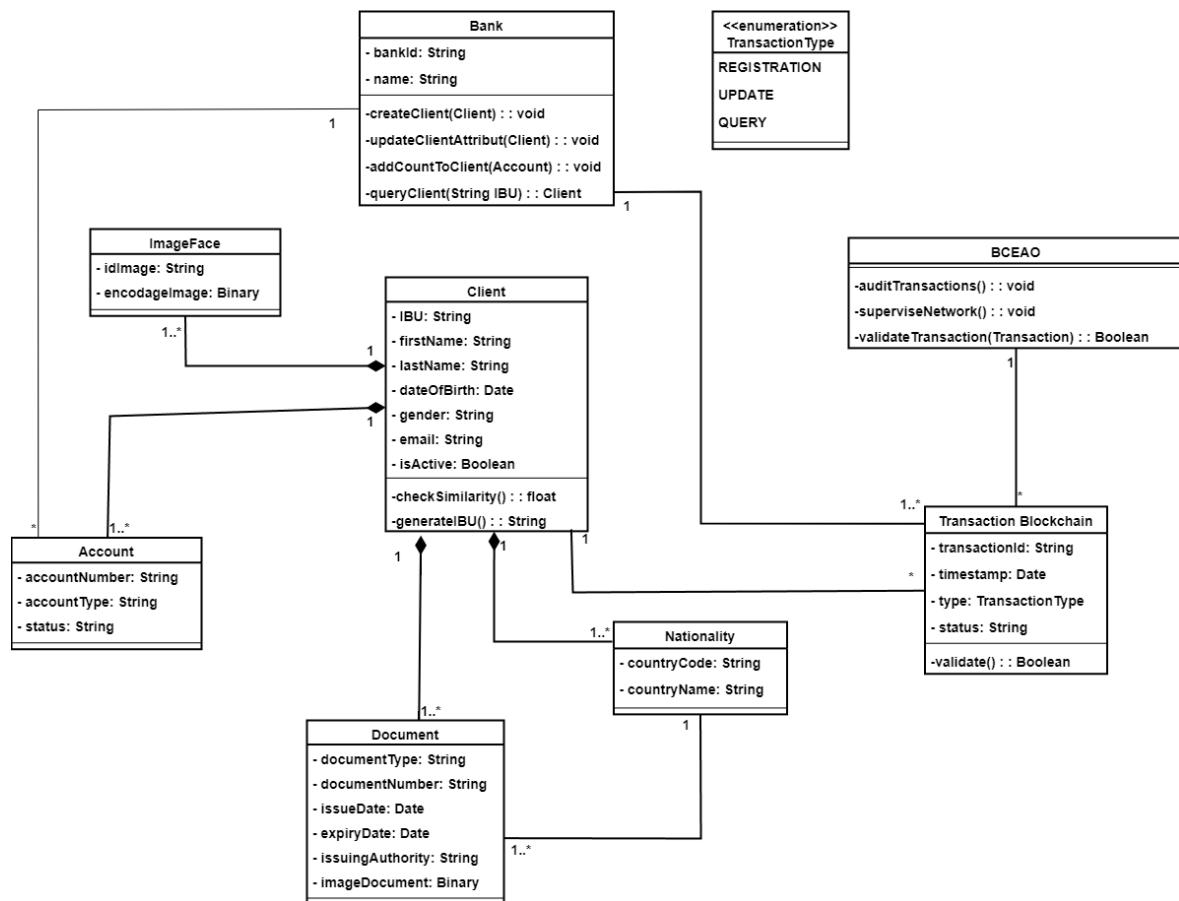


Figure III-4 : Diagramme de classe

Source : Personnelle

### III.4.2.3 Diagramme de séquence

Le diagramme de séquence est la représentation graphique des interactions entre les acteurs et le système, selon un ordre chronologique dans la formulation UML. On montre ses interactions dans le cadre d'un scénario du diagramme de cas d'utilisation.

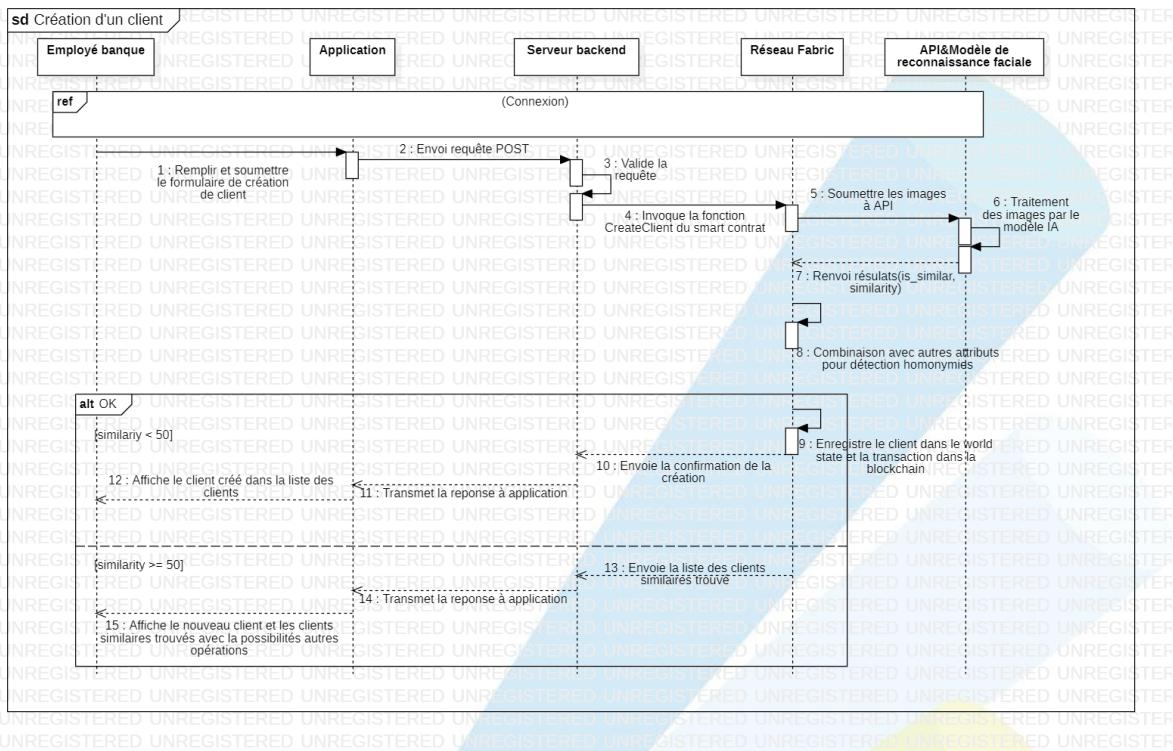


Figure III-5 : Diagramme de séquence de la création d'un client

Source : Personnelle

- **Employé banque :** Représente l'agent bancaire qui initie le processus de création d'un nouveau client. Il est responsable de la saisie des informations via le formulaire.
- **Application :** Interface utilisateur qui permet à l'employé d'interagir avec le système. Elle sert de point d'entrée pour la saisie des données et l'affichage des résultats.
- **Serveur backend :** Composant central qui gère la logique métier, valide les requêtes et coordonne les interactions entre les différents composants du système. Il est responsable de l'invocation du smart contract.
- **Réseau Fabric :** Représente l'infrastructure blockchain Hyperledger Fabric qui gère les transactions et le stockage permanent des données clients. Il assure l'intégrité et la traçabilité des informations.
- **API/Module de reconnaissance faciale :** Composant spécialisé qui traite les images fournies pour la détection des homonymies basée sur la reconnaissance faciale. Il renvoie un score de similarité qui est utilisé dans le processus de détection des doublons.

Le diagramme montre clairement la séquence d'interactions entre ces acteurs, depuis la saisie initiale des informations jusqu'à l'enregistrement final dans la blockchain, en passant par les vérifications d'homonymie.

### III.4.2.4 Diagramme d'activité

Dans le contexte de notre application blockchain pour la gestion des homonymies bancaires, le diagramme d'activité représente graphiquement le flux de travail du processus d'authentification et de création d'un nouveau client. Il modélise la séquence des actions et les points de décision depuis la connexion de l'agent bancaire jusqu'à l'enregistrement final du client dans la blockchain.

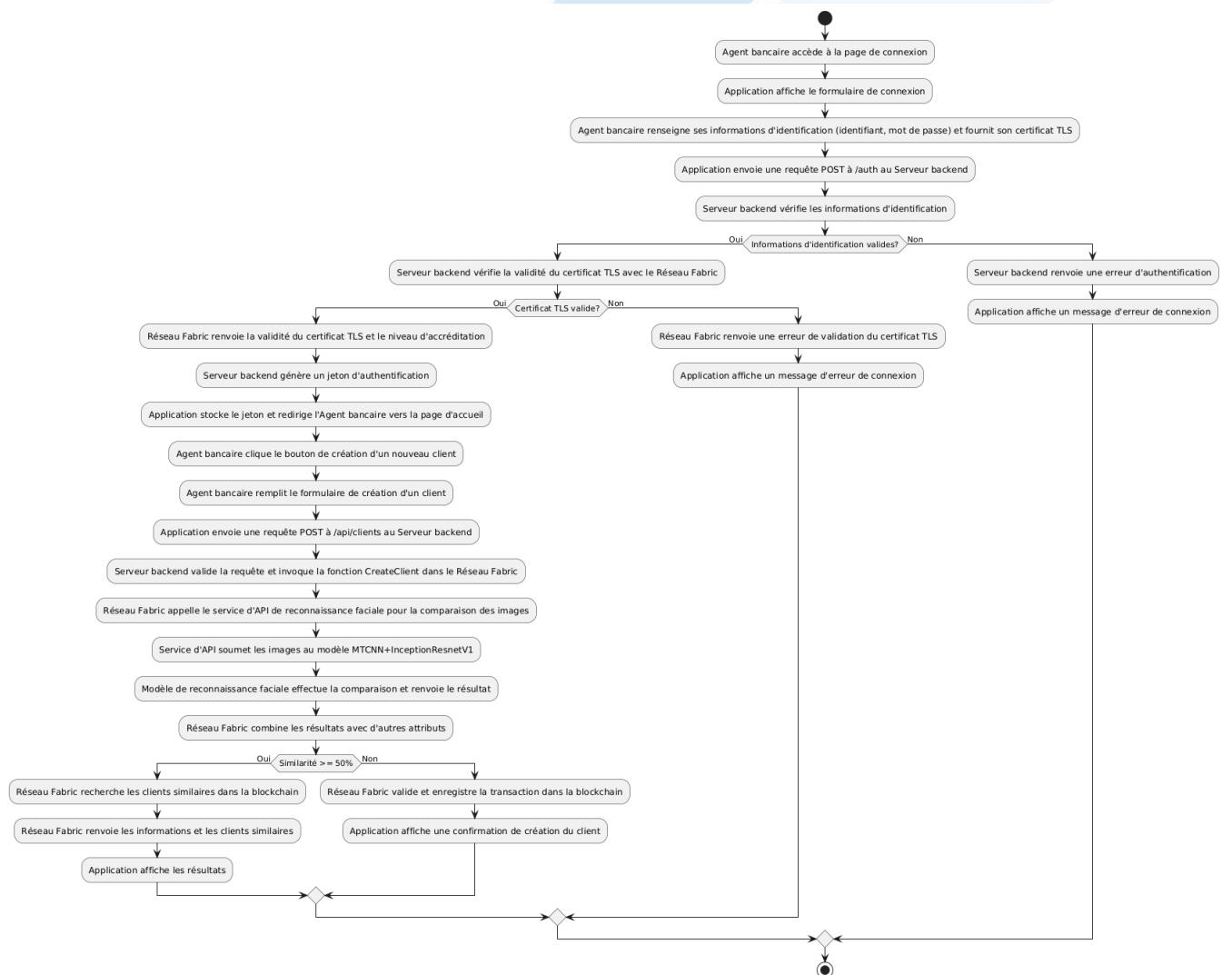


Figure III-6 : Diagramme d'activité de la création d'un client

Source : Personnelle

Le diagramme illustre trois processus principaux :

- **Processus d'authentification**

- L'agent bancaire accède à la page de connexion
- Saisie des informations d'identification et du certificat TLS
- Vérification des crédenciales et du certificat
- Redirection vers la page d'accueil en cas de succès

- **Processus de saisie client**

- Accès au formulaire de création
- Saisie des informations du client
- Transmission des données au serveur backend

- **Processus de vérification et enregistrement**

- Analyse biométrique via le service de reconnaissance faciale
- Vérification des similarités avec la base existante
- Enregistrement dans la blockchain ou affichage des cas similaires

Les points de décision clés sont :

- La validation des informations d'identification
- La validité du certificat TLS
- Le score de similarité (seuil de 50% retenu) pour la détection d'homonymies

Ce diagramme d'activité permet de visualiser clairement le flux complet du processus métier et les différentes branches conditionnelles qui peuvent être suivies selon les résultats des vérifications.

### **III.4.2.5 Diagramme de déploiement**

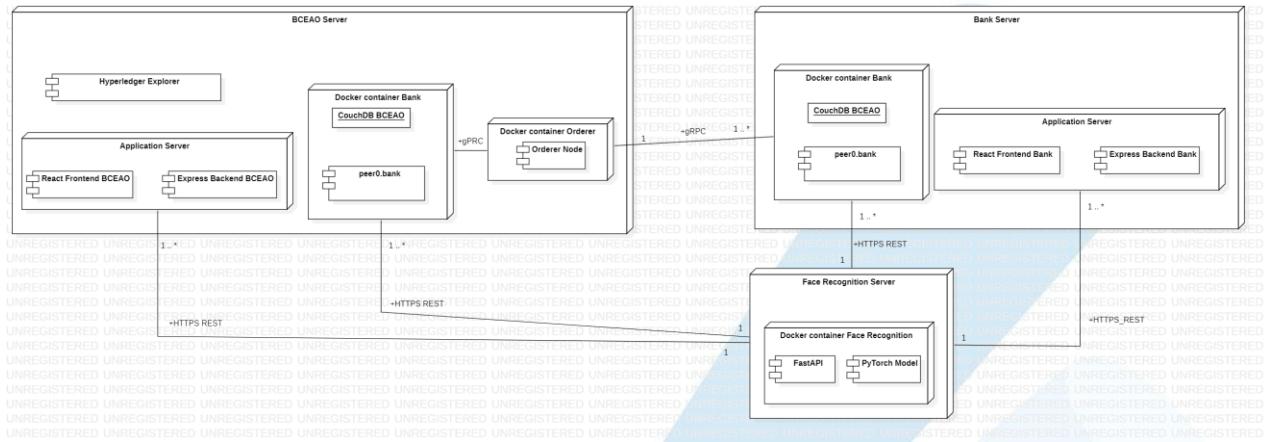


Figure III-7 : Diagramme de déploiement de notre solution

Source : Personnelle

Le diagramme de déploiement illustre l'architecture physique de notre système de gestion des homonymies bancaires. Il met en évidence la distribution des différents composants sur les serveurs et leurs interactions. L'architecture se compose de trois serveurs principaux :

## Le serveur de Reconnaissance Faciale

- Héberge un conteneur Docker avec l'API FastAPI et le modèle PyTorch
  - Fournit les services de reconnaissance faciale à l'ensemble du système
  - Accessible via HTTP/REST par les nœuds blockchain et les applications

## Le serveur BCEAO

- Contient l'ordonnanceur (Orderer Node) dans un conteneur Docker dédié
  - Héberge un nœud pair (Peer) avec sa base de données CouchDB
  - Dispose d'une application web complète (Frontend React et Backend Express)
  - Intègre Hyperledger Explorer pour le monitoring du réseau

### **Le serveur Bancaire** (réplifiable pour chaque banque)

- Héberge un nœud pair avec sa base de données CouchDB
  - Dispose de sa propre application web (Frontend React et Backend Express)
  - Interagit avec l'ensemble du réseau via le nœud ordonnanceur

Les communications entre ces composants s'effectuent via trois protocoles principaux :

- gRPC pour les communications blockchain entre les nœuds pairs et l'ordonnanceur
- HTTPs/REST pour les appels API vers le service de reconnaissance faciale
- Fabric SDK pour l'interaction entre les applications et leurs nœuds blockchain respectifs

Cette architecture assure une séparation claire des responsabilités tout en maintenant une forte interopérabilité entre les composants. Elle permet une scalabilité horizontale par l'ajout de nouveaux serveurs bancaires tout en conservant la centralisation nécessaire au niveau de la BCEAO.

## Conclusion

Ce chapitre a permis de définir l'architecture détaillée d'une solution blockchain pour la gestion des identités bancaires dans l'espace UEMOA. L'analyse approfondie des besoins fonctionnels et non-fonctionnels a mis en évidence la nécessité d'un système robuste, sécurisé et interopérable, capable de répondre aux exigences spécifiques du secteur bancaire régional. Le choix d'une blockchain de consortium, avec la BCEAO comme superviseur et les banques comme participants actifs, offre un équilibre optimal entre décentralisation et contrôle. Cette architecture permet d'assurer la confidentialité des données tout en garantissant la transparence nécessaire aux opérations bancaires. La modélisation du système à travers les diagrammes UML a permis de formaliser la structure des données et les interactions entre les différents composants. Cette phase d'analyse et de conception constitue ainsi une base solide pour le développement d'une solution qui permettra de résoudre efficacement la problématique des homonymies dans le secteur bancaire de l'UEMOA.

## **Chapitre IV : OUTILS RÉALISATION DE LA PLANIFICATION D'IMPLEMENTATION, LA SOLUTION ET**

### **Introduction**

La mise en œuvre pratique d'une solution blockchain pour la gestion des identités bancaires nécessite une sélection rigoureuse d'outils et de technologies adaptés aux exigences du projet. Ce chapitre présente les différents outils choisis pour l'implémentation de notre solution, détaille le processus de réalisation et établit un planning de déploiement. Nous commencerons par présenter les technologies blockchain sélectionnées et les outils nécessaires à leur utilisation. Ensuite, nous aborderons les technologies utilisées pour le développement du modèle de reconnaissance faciale, du backend et du frontend de notre application. La phase de réalisation sera détaillée à travers la description de l'architecture technique, le déploiement du réseau blockchain et l'implémentation des différentes composantes de la solution. Enfin, nous présenterons une planification détaillée du projet, incluant les aspects financiers et les perspectives d'évolution.

### **IV.1 Outils d'implémentation**

#### **IV.1.1 Technologie blockchain utilisée**

Pour la mise en place pratique du réseau blockchain pour la gestion des identifiants bancaires uniques (IBU) au sein de l'espace UEMOA, plusieurs plateformes s'offrent à nous, mais notre choix s'est porté sur deux d'entre elles : Ethereum et Hyperledger Fabric. Ces deux outils présentent des caractéristiques distinctes qui influencent leur adéquation pour un projet de cette envergure.

### Ethereum

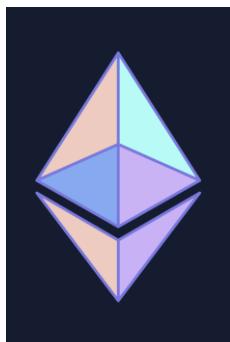


Figure IV-1 : Logo d'Ethereum

Source : <https://ethereum.org/fr/>

Ethereum est une plateforme blockchain publique, open source et décentralisée qui permet la création et l'exécution de smart contracts. Développée par Vitalik Buterin en 2015, Ethereum est l'une des premières blockchains à introduire la possibilité de programmer des applications décentralisées, en anglais : decentralized Applications (dApps) au-dessus de sa chaîne principale, avec une machine virtuelle : Ethereum Virtual Machine (EVM) qui exécute les contrats intelligents. [W9]

### Hyperledger Fabric



Figure IV-2 : Logo d'Hyperledger Fabric

Source : <https://www.lfdecentralizedtrust.org/projects/fabric>

Hyperledger Fabric est une plateforme blockchain de type consortium, spécialement conçue pour les environnements d'entreprise. Développée par la Fondation Linux, Fabric est

modulaire et permet la création de réseaux blockchain privés et permissionnés, où l'accès est contrôlé et les participants sont des entités préautorisées.

Tableau IV-1 : Comparaison entre Ethereum et Hyperledger Fabric

Source : Personnelle

Critère	Ethereum	Hyperledger Fabric
Type de réseau	Public	Privé (permissionné)
Décentralisation	Haute	Faible à moyen (Accès contrôlé)
Frais de transaction	Élevés (Gas fees)	Faibles à inexistant
Confidentialité	Faible (Transactions publiques)	Élevée (canaux privés)
Performance/Scalabilité	Limitée	Élevée (optimisée pour les entreprises)
Modularité	Moins modulaire	Très modulaire
Écosystème	Riche (nombreuses dApps et outils disponibles)	Moins mature (Moins de dApps et d'outils)
Gouvernance	Décentralisée, mais moins de contrôle sur le réseau	Centralisée, adaptée aux entreprises

Pour un projet visant la gestion des IBU dans l'espace UEMOA, Hyperledger Fabric semble être l'outil le plus approprié. Son architecture permissionnée et ses capacités de confidentialité des transactions répondent mieux aux exigences du secteur bancaire en matière de sécurité et de conformité réglementaire. Cependant, Ethereum pourrait être envisagé si une plus grande flexibilité des smart contracts et un écosystème riche sont jugés plus critiques que les considérations de confidentialité et de coût transactionnel. Le choix final dépendra des priorités stratégiques de la BCEAO, notamment en matière de gouvernance, de sécurité et de coûts opérationnels. Dans le cadre de ce mémoire, nous explorerons la technologie Hyperledger Fabric pour développer notre solution.

## IV.1.2 Outils nécessaires pour l'utilisation de Hyperledger Fabric

### IV.1.2.1 VirtualBox

Oracle VM VirtualBox est un logiciel de virtualisation open-source qui permet de créer et de gérer des machines virtuelles sur un ordinateur physique. Il offre la possibilité d'exécuter plusieurs systèmes d'exploitation simultanément sur une même machine physique.



Figure IV-3 : Logo d'Oracle VirtualBox

Source :

<https://virtualisation.developpez.com/tutoriels/virtualbox/utilisation/images/fetch.png>

VirtualBox est très important car l'utilisation HLF nécessite un système d'exploitation Linux. Et avec VirtualBox nous créerons une machine virtuelle sur laquelle nous installerons un système d'exploitation Linux précisément Ubuntu.

### IV.1.2.2 CouchDB



Figure IV-4 : Logo de CouchDB

Source : <https://couchdb.apache.org/>

Apache CouchDB est un système de gestion de base de données orienté documents, écrit en langage Erlang et distribué sous licence Apache.

Conçu pour le Web, il fait partie de la mouvance NoSQL, et a été conçu pour pouvoir être réparti sur une grappe de serveurs. Ainsi pour la mise en place de la blockchain à l'aide d'Hyperledger Fabric, CouchDB est utilisé comme système de gestion de base de données qui est associé à chaque nœud du réseau.

#### IV.1.2.4 Hyperledger Explorer



Figure IV-5 : Logo de Hyperledger Explorer

Source : <https://wiki.hyperledger.org/display/explorer/Hyperledger+Explorer>

Hyperledger Explorer est un outil de visualisation spécialement conçu pour les blockchains Hyperledger Fabric, développé conjointement par DTCC, Intel et IBM. Il se distingue comme le premier explorateur dédié aux blockchains privées, offrant une interface web intuitive construite avec ReactJS et Material UI. L'outil permet de visualiser et d'interroger les opérations blockchain, d'explorer les registres distribués tout en maintenant la confidentialité des données grâce à son architecture en trois couches. Cette solution facilite l'extraction de valeur commerciale des données blockchain tout en respectant les exigences de sécurité. Il suit une architecture logicielle à 3 couches.

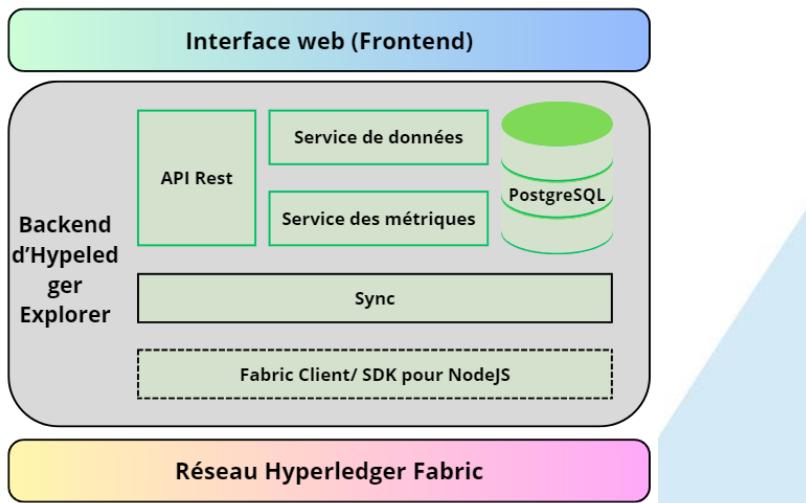


Figure IV-6 : Architecture 3 couches de Hyperledger Explorer

Source : Personnelle

#### IV.1.2.4 Docker et Docker-compose



Figure IV-7 : Logo docker

Source : <https://www.stickpng.com/img/icons-logos-emojis/tech-companies/docker-full-logo>



Figure IV-8 : Logo docker-compose

Source : <https://github.com/docker/compose?tab=readme-ov-file>

Docker et Docker Compose sont des outils complémentaires de conteneurisation. Docker permet d'encapsuler une application et ses dépendances dans un conteneur isolé, offrant une exécution cohérente sur différentes plateformes sans nécessiter de machine virtuelle complète. Utilisant le format de conteneur Linux LXC et une API de haut niveau, cette approche de conteneurisation est plus légère que la virtualisation traditionnelle. Docker Compose vient compléter cette technologie en permettant la gestion d'applications multi-conteneurs via un fichier de configuration YAML (Yet Another Markup Language) unique, simplifiant ainsi le déploiement et l'orchestration des services, réseaux et volumes. L'ensemble fonctionne dans tous les environnements (production, développement, tests) et est particulièrement efficace pour le déploiement de systèmes distribués, offrant une solution proche d'une plateforme en tant que service (PaaS).

#### **IV.1.3 Outils utilisés pour l'utilisation du modèle de reconnaissance faciale**

##### **IV.1.3.1 Python**



Figure IV-9 : Logo de Python

Source : <https://www.python.org/>

Python est un langage de programmation open source, multi paradigme et multi-plateforme créé par Guido van Rossum en 1991. Il est conçu pour être facile à apprendre et à utiliser, avec une syntaxe simple et lisible. C'est le langage de programmation que nous utiliserons pour l'implémentation de notre modèle de reconnaissance faciale et l'API REST permettant de consommer le modèle.

#### IV.1.3.2 PyTorch



Figure IV-10 : Logo PyTorch

Source : <https://pytorch.org/>

PyTorch est une bibliothèque logicielle Python open source d'apprentissage automatique qui s'appuie sur Torch. Elle permet d'effectuer les calculs tensoriels nécessaires notamment pour l'apprentissage profond (Deep Learning). Ces calculs sont optimisés et effectués soit par le processeur (CPU signifiant Central Processing Unit) soit, lorsque c'est possible, par un processeur graphique (GPU signifiant Graphics Processing Units) supportant CUDA (Compute Unified Device Architecture).

#### IV.1.3.3 FastAPI



Figure IV-11 : Logo de FastAPI

Source : <https://fastapi.tiangolo.com/>

FastAPI est un framework Python moderne pour créer des API REST. Il est rapide, facile à utiliser et offre de nombreuses fonctionnalités avancées. Grâce à FastAPI nous développerons l'API REST que nous intégrerons dans notre chaincode (contrat intelligent) et dans notre application web.

#### IV.1.4 Outils utilisés pour le développement du backend

##### IV.1.4.1 JavaScript

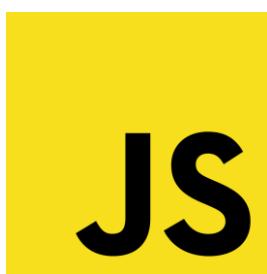


Figure IV-12 : Logo de JavaScript

Source : <https://www.javascript.com/>

JavaScript est un langage de programmation informatique qui permet de créer du contenu dynamique sur les pages web. Il est exécuté au sein du navigateur du client, en mode local, c'est-à-dire sur l'ordinateur même de l'utilisateur qui visite le site web. JavaScript est souvent utilisé pour ajouter des interactions et des effets visuels à un site web, tels que des animations, des menus déroulants, des formulaires validés en temps réel, etc. C'est le langage que nous utiliserons au niveau de notre backend, frontend et le développement de notre contrat intelligence.

##### IV.1.4.2 Node.js



Figure IV-13 : Logo de node.js

Source : <https://nodejs.org/en/>

Node.js est une plateforme logicielle libre et open-source qui permet d'exécuter du code JavaScript côté serveur, en utilisant le moteur JavaScript V8 de Google. Elle a été créée en 2009 par Ryan Dahl et les développeurs de Node.js. Node.js est conçu pour être un

environnement d'exécution JavaScript léger et performant, capable de gérer des applications réseau évènementielles hautement concurrentes. Il utilise une architecture basée sur un événementiel single-threaded (un seul thread d'exécution), ce qui signifie qu'il peut gérer plusieurs requêtes de manière simultanée et non bloquante.

#### IV.1.4.3 Express



Figure IV-14 : Logo de Express

Source : <https://expressjs.com/>

Express.js est un framework minimaliste et léger pour les applications web Node.js, conçu pour faciliter la création de serveurs web et d'applications web évolutives. Il est considéré comme le framework standard pour le développement de serveurs en Node.js.

### IV.1.5 Outils utilisés pour le développement du frontend

#### IV.1.5.1 ReactJS

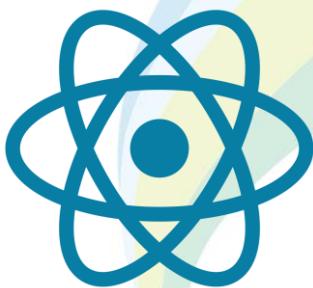


Figure IV-15 : Logo de ReactJS

Source : <https://react.dev/>

ReactJS est une bibliothèque open source JavaScript pour créer des interfaces utilisateurs. Elle est maintenue par Meta (anciennement Facebook) ainsi que par une communauté de développeurs individuels et d'entreprises depuis 2013.

#### IV.1.5.2 Tailwind CSS



Figure IV-16 : Logo de tailwindcss

Source : <https://tailwindcss.com/>

Tailwind CSS (Cascading Style Sheets) est un framework CSS open source. La fonctionnalité principale de cette bibliothèque est, contrairement à d'autres frameworks CSS comme Bootstrap, qu'elle ne procure pas une série de classes prédéfinies pour des éléments tels que des boutons ou des tables. À la place, Tailwind crée une liste de classes CSS « utilitaires » pouvant être utilisés pour ajouter un style à chaque élément en les mélangeant et en les agençant.

#### IV.1.6 Visual Studio code



Figure IV-17 : Logo de Visual Studio code

Source : [https://fr.wikipedia.org/wiki/Visual\\_Studio\\_Code](https://fr.wikipedia.org/wiki/Visual_Studio_Code)

Visual Studio Code est un éditeur de code extensible développé par Microsoft pour Windows, Linux et MacOs. Donc pour l'édition de tous nos codes nous utiliserons Visual studio code.

## IV.2 Réalisation de la solution

### IV.2.1 Topologie de notre blockchain

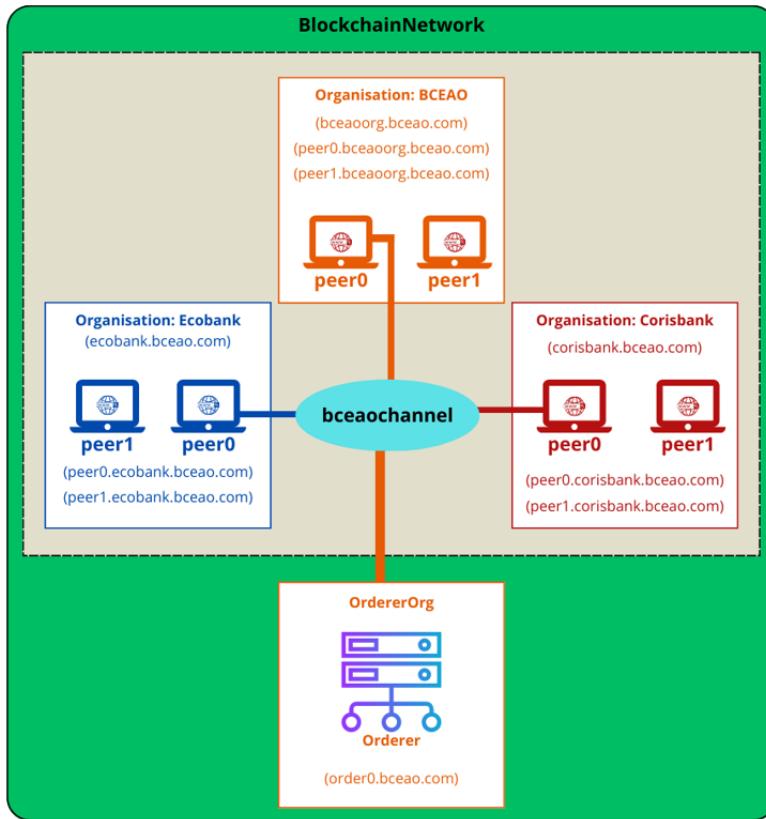


Figure IV-18 : Architecture de notre réseau blockchain

Source : Personnelle

Nous utiliserons pour notre projet de mémoire la dernière version d'HLF qui est le v2.5.9. Notre réseau est composé de trois (03) organisations nommées **BCEAO** **Ecobank** et **Corisbank** ayant chacune **2 nœuds** (peer0 et peer1) et d'un ordonnateur nommé **OrdererOrg**. Elles sont jointes à un canal par un de leurs nœuds. Le canal permet d'envoyer des transactions entre ces deux organisations et porte le nom **bceaochannel**. Le réseau et le canal sont pris en charge par une organisation de commande nommée **OrdererOrg** qui fournit le service de commande de transactions avec un seul nœud de commande : **orderer0.bceao.com**.

Chaque organisation peut en réalité fonctionner avec un seul nœud mis en place. Toutefois, un ou plusieurs nœuds peuvent être configurés pour une organisation et fonctionner via un nœud principal ou être directement reliés au canal au même titre que le nœud principal.

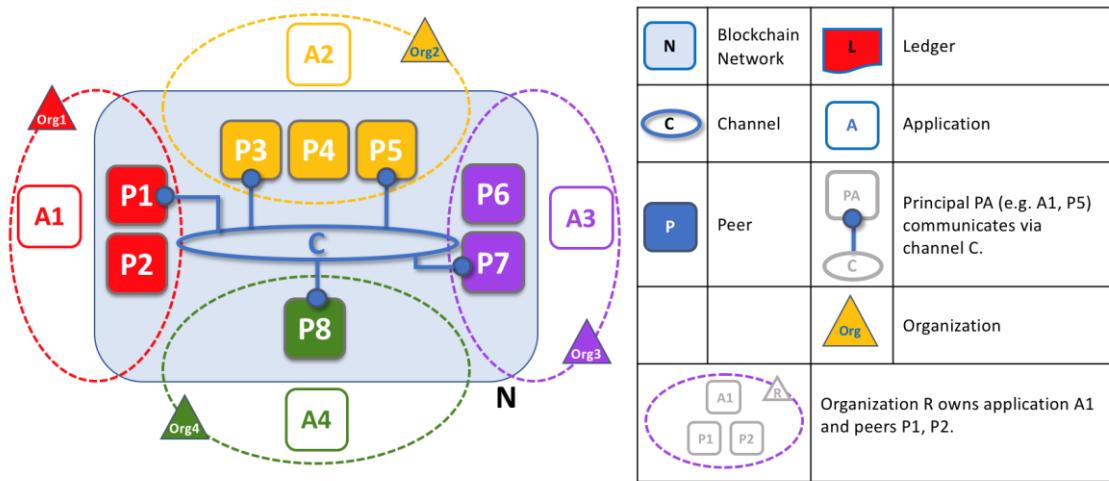


Figure IV-19 : Schéma explicatif des relations possibles entre nœuds, organisations et canal

Source : <https://hyperledger-fabric.readthedocs.io/en/release-2.5/peers/peers.html>

## IV.2.2 Réalisation

### IV.2.2.1 Déploiement de la blockchain et du chaincode

- Pour le réseau blockchain**

Le lancement de notre réseau Hyperledger Fabric est orchestré par le script **start.sh**, qui s'appuie sur des fonctions utilitaires définies dans **utils.sh**. Ce processus se déroule en plusieurs étapes clés :

- Préparation de l'environnement**

```
# Configuration des variables d'environnement
# Ajout du chemin vers les binaires Fabric
export PATH=${PWD}/../fabric-samples/bin:${PATH}
# Définition du chemin de configuration Fabric
export FABRIC_CFG_PATH=${PWD}/config
# Version des images Docker à utiliser
export IMAGE_TAG=latest
```

Capture IV-1 : Partie du script shell start.sh qui configure les variables d'environnement

Source : Personnelle

Cette étape configure les variables d'environnement nécessaires pour les outils Fabric et Docker.

- **Génération du matériel cryptographique**

Cette étape génère les certificats et clés pour chaque organisation (BCEAO, Ecobank, Corisbank et l'Orderer).

- **Configuration du réseau**

- Création du bloc genesis pour initialiser le réseau
- Démarrage des conteneurs Docker pour tous les composants
- Création du canal de communication bceaochannel
- Configuration des nœuds ancrés pour chaque organisation

- **Configuration des organisations bancaires**

Pour chaque banque (Ecobank et Corisbank) :

- Configuration des nœuds principaux (peer0) et secondaires (peer1)
- Intégration au canal
- Mise à jour des nœuds ancrés

La fonction **switchIdentity** de utils.sh joue un rôle crucial en permettant de :

- Basculer entre les identités des différentes organisations
- Configurer les certificats TLS appropriés
- Définir les points d'accès aux pairs

- **Distribution du matériel cryptographique**

Enfin, le script :

- Configure les permissions appropriées
- Copie le matériel cryptographique vers les applications connexes (explorer et application principale)

Ce processus automatisé garantit un déploiement cohérent et sécurisé de notre réseau blockchain.

- **Pour le chaincode**

Notre chaincode est implémenté en JavaScript et structuré de la manière suivante :

- **index.js** : Point d'entrée du chaincode qui exporte le contrat ClientManager.
- **lib/clientManager.js** : Implémentation du contrat gérant les clients, avec les méthodes pour créer, lire, mettre à jour et supprimer des clients, ainsi que des requêtes avancées.
- **utils/clientUtils.js** : Contient des fonctions utilitaires pour générer des UBI uniques, vérifier les doublons, calculer la similarité des noms, etc.
- **utils/imageUtils.js** : Contient des fonctions pour gérer le stockage des images dans la blockchain de chaque nœud.

Le contrat principal **ClientManager** est défini dans lib/clientManager.js. Il hérite de la classe Contract fournie par le SDK Fabric et implémente les méthodes suivantes :

Tableau IV-2 : Résumé des méthodes de la classe ClientManager (notre contrat intelligent)

Source : Personnelle

Méthode	Description
InitLedger	Initialise la blockchain avec des données de test
CreateClient	Créer un nouveau client avec un UBI unique
ReadClient	Récupère les détails d'un client par son UBI
UpdateClient	Met à jour les détails d'un client existant
UpdateClientAttributes	Met à jour des attributs spécifiques d'un client
DeactivateClient	Désactive un client
ActivateClient	Réactive un client
AddAccount	Ajouter un compte bancaire pour un client
RemoveAccount	Supprime un compte bancaire pour un client
AddNationality	Ajoute une nationalité pour un client
RemoveNationality	Supprime une nationalité pour un client
GetAllClients	Récupère tous les clients
GetActiveClients	Récupère uniquement les clients actifs
GetClientHistory	Récupère l'historique complet des modifications d'un client
GetClientHistoryByDateRange	Récupère l'historique des modifications d'un client sur une plage de dates
GetClientAttributeHistory	Récupère l'historique des modifications d'un attribut spécifique d'un client
GetClientHistorySummary	Récupère un résumé de l'historique des modifications d'un client (nombre, types, auteurs...)

Chaque méthode effectue les validations nécessaires sur les entrées, vérifie les autorisations basées sur l'identité de l'appelant, puis interagit avec le **ledger** en utilisant l'API **ctx.stub de Fabric**.

Les données sont **stockées dans le world state du ledger de chaque nœud sous forme de paires clé-valeur**, où la clé est l'UBI du client et la valeur est un objet JSON représentant l'état complet du client, y compris son historique de modifications. Des fonctions utilitaires dans **utils/clientUtils.js** sont utilisées pour des tâches comme la génération d'UBI uniques, la détection de doublons, le calcul de similarité des noms, la validation des nationalités, etc.

Les **transactions sont stockées dans la Blockchain**.

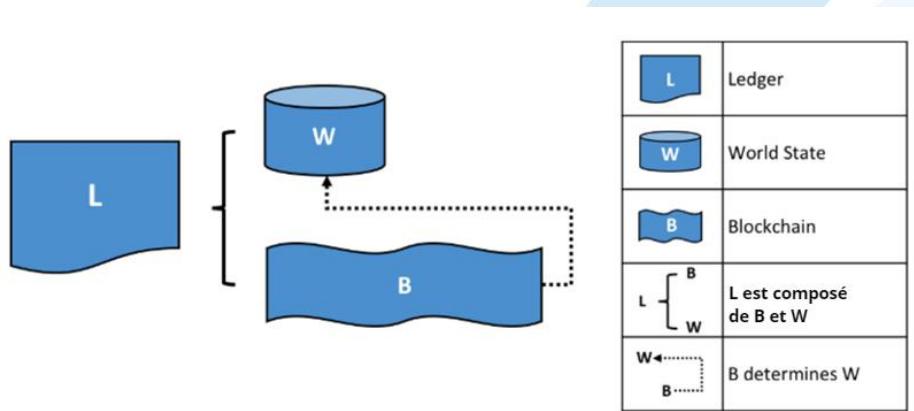


Figure IV-20 : Présentation du Ledger dans Hyperledger Fabric

Source : <https://hyperledger-fabric.readthedocs.io/en/release-2.5/ledger/ledger.html>

Un **Ledger L** comprend la **blockchain B** et le **world state W**, où la blockchain B détermine le **world state W**. Nous pouvons aussi dire que le **world state W** est dérivé de la blockchain B.

#### IV.2.2.3 Déploiement de l'application de monitoring de la blockchain : Hyperledger Explorer

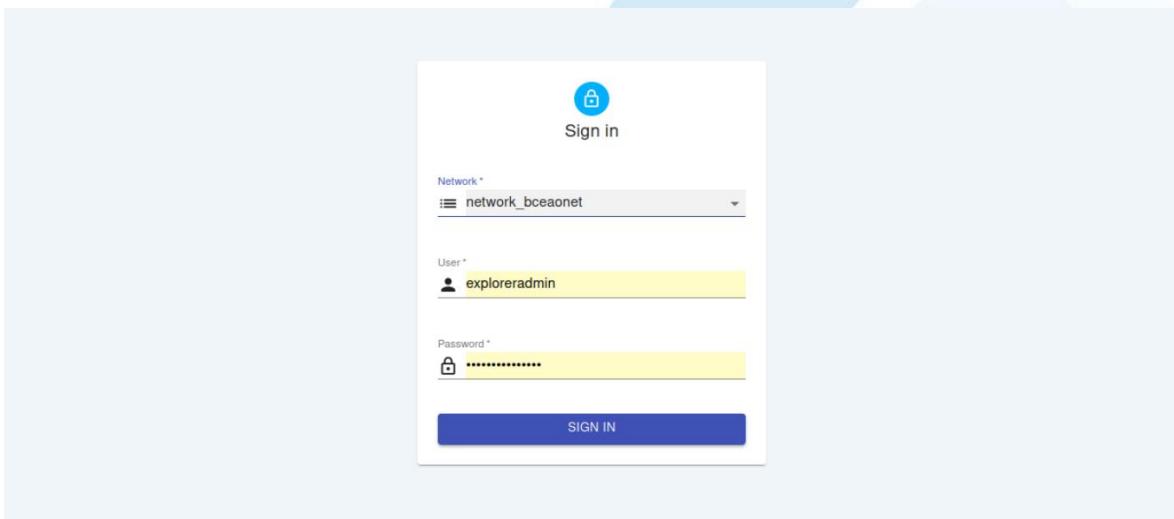
Explorer permet de visualiser en temps réel l'état de la blockchain, les transactions, les blocs, les données de chaincode et les informations de réseau de façon intuitive. Hyperledger explorer est construit sous forme d'image docker.

```
hlfuser@hlfuser-VirtualBox:~/Bureau/HLF_project_jyen/explorer$ docker-compose up
Creating volume "explorer_pgdata" with default driver
Creating volume "explorer_walletstore" with default driver
  Firefox explorerdb.mynetwork.com ... done
Creating explorer.mynetwork.com ... done
```

Capture IV-2 : Déploiement de Hyperledger Explorer

Source : Personnelle

- Page de connexion

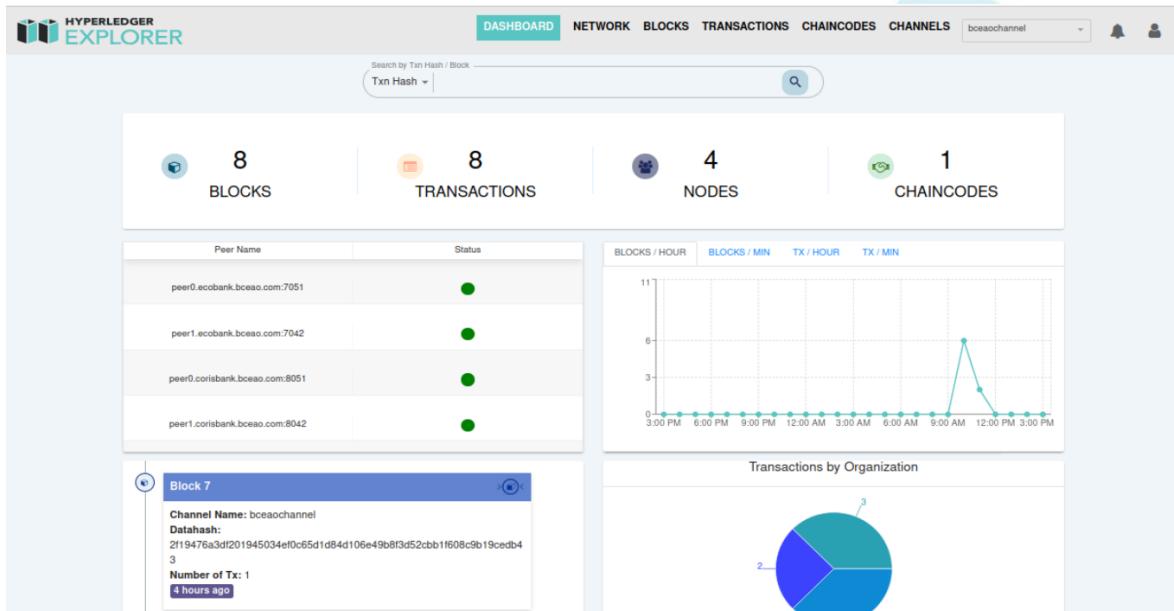


Capture IV-3 : Page de connexion à Hyperledger Explorer

Source : Personnelle

Elle comporte 3 champs à remplir. Le premier champ permet de choisir le réseau blockchain parmi ceux que Hyperledger Explorer a détecté. Le deuxième est le nom d'utilisateur et le troisième son mot de passe.

- Page d'accueil



Capture IV-4 : Page d'accueil de Hyperledger Explorer

Source : Personnelle

Ce logiciel propose différentes fonctionnalités pratiques, telles que l'obtention des derniers statuts des blocs, du réseau et des chaincodes, la visualisation des blocs et des transactions, la mesure des blocs et des transactions en heures et minutes, la recherche et le filtrage des blocs et des transactions par plage de dates et canaux, la découverte dynamique de nouveaux canaux et le changement de présentation des données par canaux, ainsi que la réception de notifications en temps réel pour les nouveaux blocs.

#### IV.2.2.4 Déploiement de l'API de reconnaissance faciale

Nous avons développé une API de reconnaissance faciale basée sur le modèle MTCCN (Multi-Task Cascaded Convolutional Neural Networks) + InceptionResnetV1 pré-entraîné sur le dataset VGGFace2, intégré dans notre chaincode afin de s'assurer de l'unicité du client lors de sa création ainsi que permettant d'identifier les clients à partir de leurs photos de manière rapide et précise.

Tableau IV-3 : Comparaison entre les modèles MTCNN + InceptionResnetV1 et FaceNet

Source : Personnelle

Critères	MTCNN + InceptionResnetV1	FaceNet (dlib)
Précision (LFW Dataset)	99.65%	99.63%
Temps de traitement (CPU)	~450 ms/image	~300 ms/image
Temps de traitement (GPU)	~70 ms/image	~50 ms/image
Taille du modèle	~90 Mégabit	~67 Mégabit
Sensibilité au bruit	Faible (grâce à l'alignement automatique de MTCNN)	Moyenne (moins robuste aux visages inclinés)
Nombre d'étapes	Deux étapes : détection (MTCNN) et embedding (InceptionResnetV1)	Deux étapes : détection et embedding avec dlib
Capacité multi-visages	Peut gérer plusieurs visages dans une image	Gère plusieurs visages, mais légèrement moins rapide
Comparaison à grande échelle	Optimisé pour des bases de données importantes (~millions d'entrées)	Performant, mais moins rapide sur de très grandes bases de données
Performance sur des images bruitées	Très robuste (grâce à MTCNN)	Moyennement robuste

La combinaison **MTCNN + InceptionResnetV1** a été choisie pour notre API de reconnaissance faciale en raison de sa précision supérieure 99.65% sur le jeu de données LFW (Labeled Faces in the Wild) par rapport à **FaceNet/dlib**. Malgré un temps de traitement CPU légèrement plus long 450 ms contre 300 ms et une taille plus importante, elle offre un traitement GPU rapide (70 ms/image), un alignement automatique des visages, une

robustesse au bruit, et une excellente capacité à gérer les bases de données volumineuses et la détection multi-visages. Ces caractéristiques en font la solution idéale pour notre système qui requiert haute précision et évolutivité. L'API expose deux Endpoint :

- "/" : Retourne un message de bienvenue
- "/api/face-recognition" : Compare deux images de visages et retourne leur score de similarité cosinus. Un seuil de 0.8 est utilisé pour déterminer si les visages sont similaires.

Le code utilise la bibliothèque **facenet\_pytorch** pour la détection (**MTCNN**) et l'extraction d'**embeddings** (**InceptionResnetV1**). Les images uploadées sont d'abord converties en tenseurs, puis passées dans le modèle pour obtenir les **embeddings**. Notre contrat intelligent consomme cette API lors de la création d'un client. L'application cliente la consomme également pour effectuer des recherches de clients à partir de leur photo. Cela permet une identification rapide et pratique dans l'interface utilisateur.

The screenshot shows the FastAPI documentation interface. At the top, it says "FastAPI 0.1.0 (GAS3) /openapi.json". Below this, there's a "default" section with two entries: a POST endpoint for "/api/face-recognition" labeled "Face Recognition" and a GET endpoint for "/" labeled "Root". Underneath, there's a "Schemas" section containing three JSON schema definitions:

```
Body_face_recognition_api_face_recognition_post <-
  image1*           Image1 > [...]
  image2*           Image2 > [...]
}

HTTPValidationError <-
  detail
    Detail > [...]
}

ValidationError <-
  loc*
    Location > [...]
  msg*
    Message > [...]
  type*
    Error Type > [...]
}
```

Capture IV-5 : Interface documentaire FastAPI de notre API

Source : Personnelle

### IV.2.3     Architecture logiciel de notre application

Notre application adopte une architecture N-tiers, plus précisément une architecture 3-tiers, qui sépare l'application en trois couches distinctes et indépendantes. Cette architecture permet une meilleure maintenabilité, scalabilité et séparation des responsabilités.

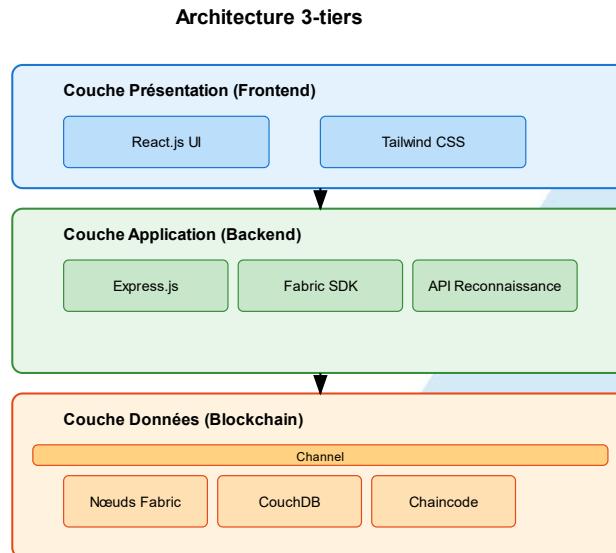


Figure IV-21 : Architecture 3-tiers de notre solution

Source : Personnelle

Cette architecture 3-tiers montre la séparation claire des composants de l'application avec :

- **Couche Présentation (Frontend)**
  - Interface utilisateur développée avec React.js et Tailwind CSS
  - Permet aux utilisateurs d'interagir avec le système
  - Communique avec le backend via des requêtes http
- **Couche Application (Backend)**
  - Serveur Express.js exposant une API REST
  - Gère la logique métier et les interactions avec le réseau blockchain
  - Intègre la communication avec l'API de reconnaissance faciale
  - Utilise le SDK Fabric pour interagir avec le réseau blockchain
- **Couche Données (Blockchain)**
  - Réseau Hyperledger Fabric avec ses différents nœuds
  - CouchDB comme système de gestion de base de données pour chaque nœud

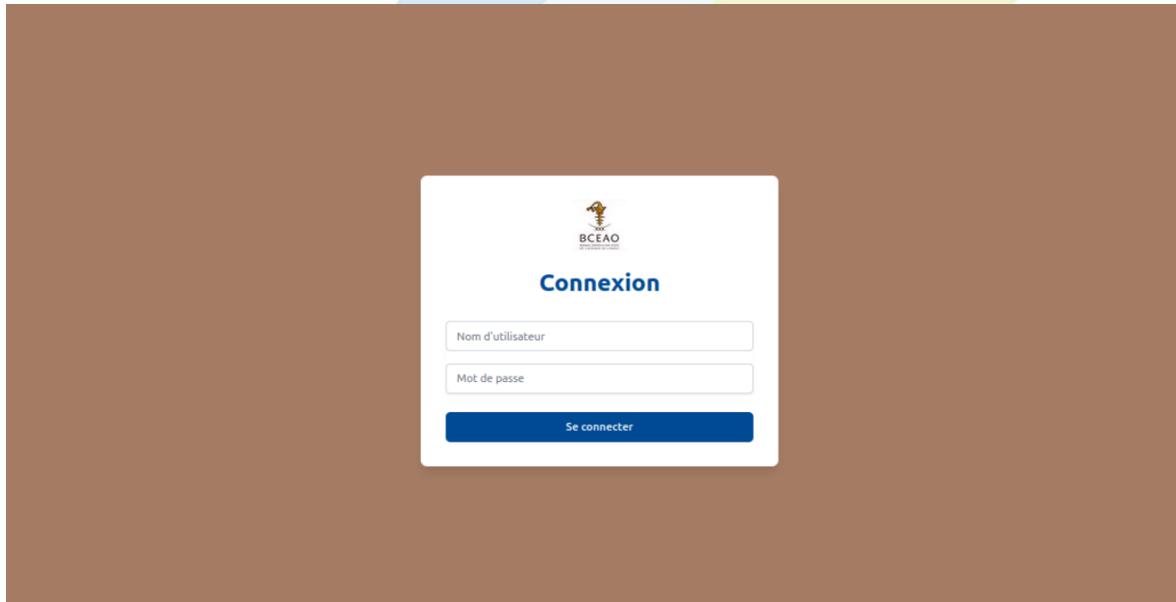
- Chaincode (smart contract) implémentant la logique métier et intégrant la reconnaissance faciale
- Canal (channel) pour la communication entre les organisations

Cette architecture permet une séparation claire des responsabilités, facilitant la maintenance et l'évolution du système. Chaque couche peut être mise à jour ou modifiée indépendamment des autres, tant que les interfaces entre les couches restent stables.

#### IV.2.4 Résultats obtenus

Cette section présente les résultats concrets de notre implémentation, à travers les interfaces et fonctionnalités développées pour le système de gestion des identifiants bancaires uniques (IBU). Les captures d'écran et descriptions qui suivent illustreront comment notre solution répond aux objectifs initiaux de sécurité, de traçabilité et d'unicité des identités bancaires.

- **Page de connexion**



Capture IV-6 : Page de connexion à l'application

Source : Personnelle

- **Page de gestion des clients des banques actifs**

Après connexion à l'application, l'agent de banque accède directement à la liste des clients ayant un compte bancaire dans au moins l'une des banques de l'espace UEMOA qui ont un état actif. L'agent de banque peut ainsi effectuer plusieurs actions (appelées transactions) sur la blockchain.

The screenshot shows the BCEAO Blockchain application interface. At the top, there is a header bar with the BCEAO logo, the text "BCEAO Blockchain", and navigation links for "Clients Actifs", "Tous les clients", "Nouveau Client", "admin\_ecobank", and "Déconnexion". Below the header, there is a search bar with fields for "Rechercher par image" (with a "Parcourir..." button), "Nom" (with a "Nom de Famille" input field), and "Prénom" (with a "Prénom" input field). A "Réinitialiser la recherche" button is also present. The main area is titled "Clients Actifs" and displays a table of active clients. The table has columns: PHOTO, UBI, NOM, PRÉNOM, EMAIL, STATUT CLIENT, ACTIONS, and STATUT DEMANDE. There are four rows of data:

PHOTO	UBI	NOM	PRÉNOM	EMAIL	STATUT CLIENT	ACTIONS	STATUT DEMANDE
	UEMOA-2024-000002	Cissé Alice	Abdoulaye	abdoulaye.cisse6@email.com	Actif	Voir Modifier Historique	TRAITE
	UEMOA-2024-000003	Cissé	Fatoumata	fatoumata.cisse657@email.com	Actif	Voir Modifier Historique	TRAITE
	UEMOA-2024-000005	Sissoko	Abdoulaye	abdoulaye.sissoko267@email.com	Actif	Voir Modifier Historique	TRAITE
	UEMOA-2024-000006	Koné	Aïssata	aïssata.koné949@email.com	Actif	Voir Modifier Historique	TRAITE

Capture IV-7 : Interfaces de visualisation des clients à l'état actif enregistré sur la blockchain

Source : Personnelle

- **Page d'enregistrement d'un client dans la blockchain**

L'action principale est l'enregistrement d'un client sur la blockchain s'il n'existe pas déjà dans l'optique d'obtenir un identifiant bancaire unique dans tout l'espace UEMOA.

The screenshot shows the 'Nouveau Client' (New Client) form. At the top, there are tabs for 'Clients Actifs' (Active Clients), 'Tous les clients' (All Clients), 'Nouveau Client' (New Client) (which is selected and highlighted in yellow), 'admin\_ecobank' (Ecobank Admin), and 'Déconnexion' (Logout). The main form fields include:

- Face ID: A placeholder 'Parcourir...' with a file path 'photoidentity.jpg'.
- Prénom: Joshua Juste.
- Image: A small thumbnail of a person's face.
- Text: 'Format acceptés: JPEG, PNG, JPG. Taille maximale: 2MB'.
- Nom: NIKIEMA.
- Email: joshua.nikiema24@gmail.com.
- Date de Naissance: 01/01/2000.
- Genre: Masculin.
- Nationalité et Document d'identité:
  - Burkina Faso
  - Passeport - N°A223301
  - Document fourni: An image of a passport.
  - Modifier button.
- Compte Bancaire:
  - Ecobank (ECO0011121552)
  - Supprimer button.

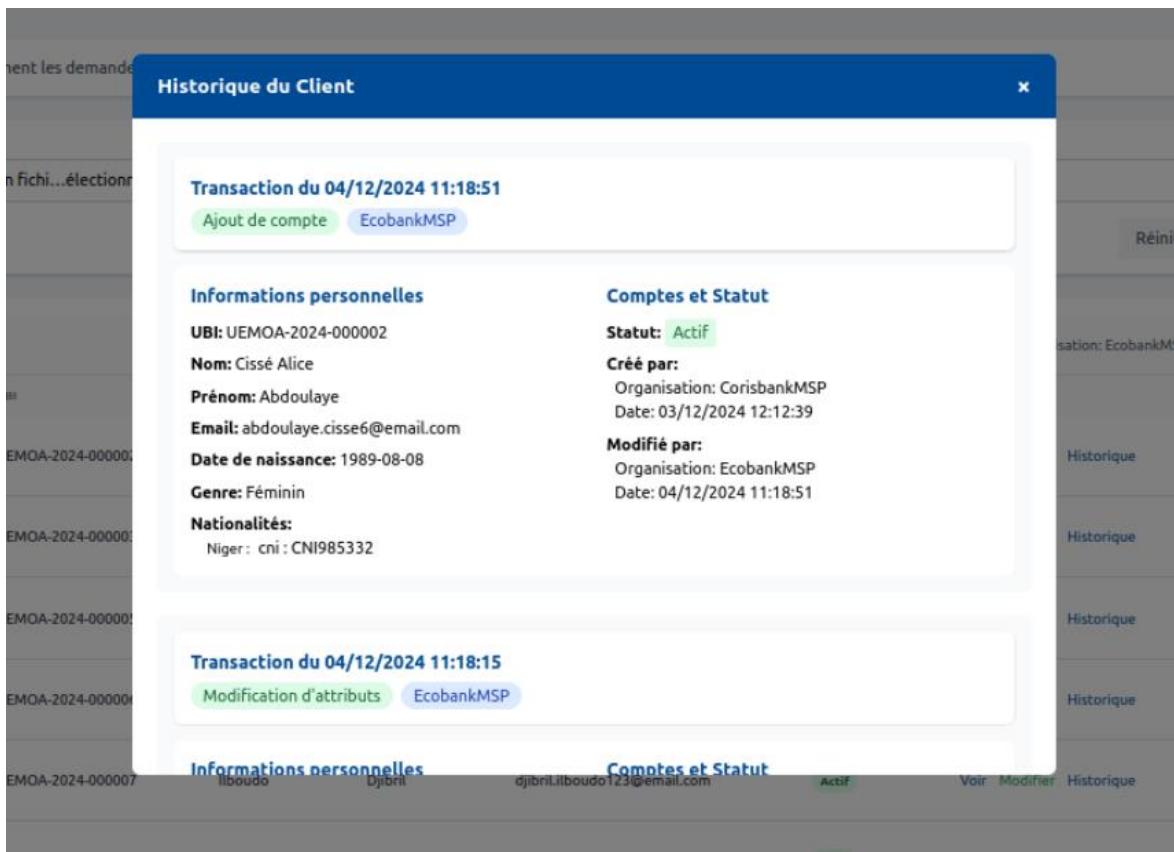
At the bottom right are 'Annuler' (Cancel) and 'Enregistrer' (Register) buttons.

Capture IV-8 : Interface d'enregistrement d'un client dans la blockchain

Source : Personnelle

- **Page de consultation de l'historique de mise à jour des clients**

La blockchain ayant comme valeur intrinsèque la traçabilité, on a vu sur tous les changements d'informations opérés sur un client tel que qui est-ce qui l'a effectué et quand.



Capture IV-9 : Historique de mise à jour des informations d'un client

Source : Personnelle

- **Page de consultation des informations d'un client**

Sur un client spécifique déjà enregistré sur la blockchain, l'agent de banque peut consulter toutes les informations du client dont il a l'autorisation et aussi lui joindre un compte bancaire ou mettre à jour ses documents d'identités en fonction de son degré d'accréditation.

The screenshot shows a client detail page titled "Détails du Client". It displays the following information:

- IBI: UEMOA-2024-000002
- Statut: Actif
- Photo du Client: A small portrait photo of a man.
- Nom: Cissé Alice
- Prenom: Abdoulaye
- Email: abdoulaye.cisse6@email.com
- Date de naissance: 1989-08-08
- Genre: Féminin

Below this, there's a section for "Gestion des Identités" (Identity Management) with a note indicating 1 nationalité(s) enregistrée(s). It shows a document upload area for a "Niger" passport (CN 985332) and a "Identity Card" document from "indya".

There's also a section for adding new nationalities, with fields for "Pays" (Country), "Type de document" (Document Type), and "Numéro du document" (Document Number). A "Ajouter la nationalité" (Add Nationality) button is at the bottom.

Capture IV-10 : Vue détaillé des informations d'un client

Source : Personnelle

## IV.3 Planification

La mise en œuvre d'un système blockchain pour la gestion des homonymies bancaires dans l'espace UEMOA nécessite une planification rigoureuse. Cette planification englobe la gestion des ressources humaines, l'établissement d'un calendrier précis et l'anticipation des risques potentiels. En tant que projet stratégique pour le secteur bancaire de l'UEMOA, il est crucial d'adopter une approche méthodique qui prend en compte les spécificités de l'environnement local et les contraintes organisationnelles de la BCEAO.

### IV.3.1 Coûts des ressources humaines

La stratégie de ressources humaines pour ce projet s'appuie largement sur les compétences existantes au sein de la BCEAO, complétées par des formations spécifiques en technologie blockchain. Cette approche vise à développer une expertise interne durable tout en optimisant les coûts de mise en œuvre.

Tableau IV-4 : Estimations des coûts de formation et développement des compétences

Source : Personnelle

Profil	Statut	Type de formation	Coût unitaire	Nombre	Coût total (FCFA)
Chef de projet IT	À recruter	Formation blockchain avancée	2500000	1	2500000
Développeurs existants	À recruter	Formation développement	1500000	2	3000000
Expert sécurité	À recruter	Sécurité blockchain	1500000	1	3000000
Testeurs QA	À recruter	Tests applications blockchain	1500000	2	3000000
Architectes blockchain	À recruter	Certification avancée	2500000	2	5000000
<b>Total Formation</b>					<b>16500000</b>

### IV.3.2 Planning et phases du projet

Le déploiement du système est planifié selon une approche progressive, permettant de valider chaque étape avant de passer à la suivante. Cette méthodologie est particulièrement importante compte tenu de la nature critique du système pour le secteur bancaire.

Tableau IV-5 : Détail des phases et livrables

Source : Personnelle

Phase	Durée	Ressources clés	Livrables	Jalons
Initialisation	2 mois	- Chef de projet BCEAO	- Cahier des charges - Plan projet	M2 : Validation du cadrage
Formation	2 mois	- Équipe BCEAO	- Certification blockchain - Compétences validées	M4 : Équipe formée
Conception	3 mois	- Architectes - Expert	- Architecture technique - Design smart contracts	M7 : Validation architecture
Développement	2 mois	- Développeurs - Architectes	- Code source - Documentation	M9 : Code complet
Tests	2 mois	- Testeurs - Développeurs	- Tests internes - Tests avec banques	M11 : Validation tests
Déploiement pilote	3 mois	- Toute l'équipe	- Déploiement banques pilotes	M14 : Validation pilote
Déploiement général	6 mois	- Toute l'équipe	- Déploiement progressif - Formation utilisateurs	M20 : Go-live complet

Tableau IV-6 : Estimations des coûts salariaux sur la durée du projet (20 mois)

Source : Personnelle

Profil	Statut	Rémunération mensuelle (FCFA)	Durée (mois)	Nombre	Coût total (FCFA)
Chef de projet IT	Existant BCEAO	2500000	20	1	50000000
Développeurs	Existant BCEAO	1500000	18	2	54000000
Expert sécurité	Existant BCEAO	2000000	20	1	40000000
Testeurs QA	Existant BCEAO	1500000	12	2	36000000
Architectes blockchain	À recruter	2000000	18	2	72000000
<b>Total Salaires</b>					<b>252000000</b>

### IV.3.3 Gestion des risques

L'identification et la gestion des risques sont essentielles pour garantir le succès du projet. Une analyse approfondie a permis d'identifier les principaux risques techniques, organisationnels et opérationnels, ainsi que les stratégies d'atténuation correspondantes.

Tableau IV-7 : Matrice des risques et mesures d'atténuation

Source : Personnelle

Catégorie	Risque	Probabilité	Impact	Mesures d'atténuation	Responsable
Technique	Performance réseau	Moyenne	Élevé	- Tests de charge - Architecture	Architecte
Sécurité	Failles de sécurité	Faible	Critique	- Audits réguliers - Tests	Expert sécurité
Organisation	Résistance au changement	Élevée	Moyen	- Formation - Communication	Chef de projet
Réglementaire	Non-conformité	Faible	Élevé	- Validation BCEAO	Chef de projet

## Conclusion

Ce chapitre a permis d'exposer les aspects pratiques de la mise en œuvre de notre solution blockchain pour la gestion des identités bancaires dans l'espace UEMOA. L'utilisation d'outils modernes et éprouvés, tant pour la partie blockchain que pour le développement des applications associées, garantit la robustesse et la pérennité du système.

La réalisation concrète du projet, structurée en plusieurs phases distinctes et s'appuyant sur une architecture distribuée, démontre la faisabilité technique de la solution proposée. L'estimation financière et le planning de réalisation fournissent un cadre réaliste pour le déploiement du système, tout en identifiant les opportunités d'évolution future. Cette mise en œuvre constitue ainsi une première étape vers la modernisation des processus d'identification bancaire dans l'espace UEMOA.

## CONCLUSION GÉNÉRALE

Au terme de cette étude, nous avons démontré la pertinence et la faisabilité d'une solution blockchain pour la gestion des homonymies dans le secteur bancaire de l'UEMOA. Notre recherche a permis de développer une architecture technique robuste, basée sur Hyperledger Fabric, capable de répondre aux exigences spécifiques du contexte régional.

La solution proposée, articulée autour d'un Identifiant Bancaire Unique (IBU), offre plusieurs avantages significatifs :

- Une identification unique et fiable des clients à l'échelle régionale
- Une gestion sécurisée et transparente des données d'identité
- Une interopérabilité accrue entre les institutions bancaires
- Une conformité renforcée aux exigences réglementaires

L'implémentation réussie de notre prototype ouvre la voie à plusieurs cas d'usage innovants :

- Un KYC mutualisé permettant le partage sécurisé des informations de conformité
- Un système de scoring crédit partagé offrant une vision consolidée de l'historique client
- Un registre unique des garanties bancaires assurant la traçabilité des engagements

De plus, cette architecture pourrait servir de socle technologique pour le développement d'une MNBC, facilitant l'émission d'un e-FCFA et l'optimisation des paiements transfrontaliers.

Les axes d'amélioration envisagés comprennent :

- L'intégration avec les systèmes d'identification nationaux existants
- L'extension des fonctionnalités pour inclure d'autres cas d'usage bancaire
- L'optimisation des performances pour un passage à l'échelle régionale

Cette étude ouvre ainsi la voie à une transformation profonde des processus bancaires dans l'espace UEMOA, contribuant à la modernisation du secteur financier régional et à l'amélioration de l'inclusion financière.

## BIBLIOGRAPHIE

- [B1] : Tao Hai (2022), BVFLEMR : an integrated federated learning and blockchain technology for cloud-based medical records recommendation system.
- [B2] : Imran Bashir (2018), Mastering Blockchain, Second Edition, Birmingham, pp.112-158.
- [B3] : Imran Bashir (2018), Mastering Blockchain, Second Edition, Birmingham, pp.72-79.
- [B4] : Agossou Jacques GANSINHOUNDE (2023), Opportunités et Défis de la Blockchain pour les Economies de l'espace CEDEAO, les précis du COFEB N°23, pp.17-38
- [B5] : Agossou Jacques GANSINHOUNDE (2023), Opportunités et Défis de la Blockchain pour les Economies de l'espace CEDEAO, les précis du COFEB N°23, pp.15-16
- [B6] : Robin GUYOMAR (2020), TPE : Programmation d'une Blockchain à l'aide de la plateforme Hyperledger.
- [B7] : Christian E. Pulmano (2023), Towards the Development of a Blockchain-based Decentralized Digital Credential System using Hyperledger Fabric for Participatory Governance, Procedia Computer Science, N°219, pp.99-106.

## WEBOGRAPHIE

[W1] : Application de la blockchain au Nigéria <https://cointelegraph.com/learn/nigeria-enaira-cbdc> (Consulté le 26 juillet 2024)

[W2] : Projet Blockchain en Sierra Leone : <https://www.devex.com/news/in-sierra-leone-new-kiva-protocol-uses-blockchain-to-benefit-unbanked-95490> (Consulté le 26 juillet 2024)

[W3] : Projet Blockchain au Kenya <https://www.wearetech.africa/fr/fils/actualites/gestion-publique/kenya-le-gouvernement-s-associe-au-pnud-pour-lancer-un-systeme-d-identite-numerique> (Consulté le 26 juillet 2024)

[W4] : Projet Blockchain en Ethiopie <https://www.wearetech.africa/fr/fils/actualites/tech/ethiopie-cardano-entamera-le-projet-d-identification-numerique-des-eleves-par-la-blockchain-dans-deux-mois> (Consulté le 26 juillet 2024)

[W5] : Ethereum vs Hyperledger Fabric <https://chainhero.io/fr/2018/07/ethereum-vs-hyperledger-fabric-2/> (Consulté le 01 aout 2024)

[W6] : Cours sur la blockchain par Ethereum <https://ethereum.org/fr/developers/docs/intro-to-ethereum/> (Consulté le 01 aout 2024)

[W7] : Hyperledger Fabric documentation <https://hyperledger-fabric.readthedocs.io/en/release-2.5/ledger/ledger.html> (Consulté le 05 aout 2024)

[W8] : Hyperledger Fabric documentation [https://hyperledger-fabric.readthedocs.io/en/release-2.5/fabric\\_model.html](https://hyperledger-fabric.readthedocs.io/en/release-2.5/fabric_model.html) (Consulté le 05 aout 2024)

[W9] : Hyperledger documentation <https://hyperledger-fabric.readthedocs.io/en/release-2.5/index.html> (Consulté le 05 aout 2024)

## ANNEXES

Annexe 1: Fichier de configuration de détaillé de la structure et des politiques de règles de la blockchain écrit en YAML

```
> config > ! configtx.yaml
# Configuration du réseau Hyperledger Fabric pour le système bancaire UEMOA

# Définition des organisations participantes au réseau
Organizations:

    # Configuration de l'organisation Orderer (service de commande)
    - &[REDACTED]
        Name: [REDACTED]                                # Nom de l'organisation Orderer
        ID: [REDACTED]                                   # Identifiant MSP (Membership Service Provider)
        MSPDir: [REDACTED]                               # Chemin vers les
        # Définition des politiques d'accès pour l'Orderer
        Policies:
            Readers:                                     # Politique de lecture
                Type: [REDACTED]
                Rule: "[REDACTED]"
            Writers:                                     # Politique d'écriture
                Type: [REDACTED]
                Rule: "[REDACTED]"
            Admins:                                       # Politique d'administration
                Type: [REDACTED]
                Rule: "[REDACTED]"
        # Point de terminaison du service Orderer
        OrdererEndpoints:
            - [REDACTED]

    # Configuration de la banque Ecobank
    - &[REDACTED]
        Name: [REDACTED]
        ID: [REDACTED]
        MSPDir: [REDACTED]
        # Politiques spécifiques à Ecobank
        Policies:
```

Annexe 2 : Fichier docker compose pour la configuration d'un conteneur docker représentant un nœud membre de la blockchain

```
> docker > docker-compose-bceaoorg.yaml
version: '3'

volumes:
  peer0 [REDACTED]:
  peer1 [REDACTED]

networks:
  [REDACTED]

services:
  couchdb [REDACTED]
    container_name: [REDACTED]
    image: hyperledger/fabric-couchdb
    environment:
      - COUCHDB_USER=[REDACTED]
      - COUCHDB_PASSWORD=[REDACTED]
    ports:
      - [REDACTED]
    networks:
      - [REDACTED]

  peer0 [REDACTED]:
    networks:
      - [REDACTED]
    container_name: [REDACTED]
    image: hyperledger/fabric-peer:${IMAGE_TAG}
    environment:
      - CORE_VM_ENDPOINT=unix:///host/var/run/docker.sock
      # Generic peer variables
      - CORE_PEER_TLS_ENABLED=true
      - CORE_PEER_TLS_CERT_FILE=[REDACTED]
      - CORE_PEER_TLS_KEY_FILE=[REDACTED]
      - CORE_PEER_TLS_ROOTCERT_FILE=[REDACTED]
      # Specific peer variables
      - CORE_PEER_ID=[REDACTED]
      - CORE_PEER_ADDRESS=[REDACTED]
      - CORE_PEER_LISTENADDRESS=[REDACTED]
      # chaincode variables
```

Annexe 3 : Fichier de configuration de base spécifique à un organisation pour pouvoir générer ses certificats d'authentification

```
> cryptogen-input > ! crypto-config-ecobank.yaml
# Configuration des organisations Peer pour Ecobank
PeerOrgs:
  # Définition de l'organisation Ecobank
  - Name: [REDACTED] # Nom de l'organisation
    Domain: [REDACTED] # Domaine utilisé pour générer les certificats

  # Configuration du template pour les peers
  Template:
    Count: [REDACTED] # Nombre de peers à créer pour cette organisation (peer0 et peer1)
    SANs: [REDACTED] # Subject Alternative Names pour les certificats TLS
    | - [REDACTED] # Permet l'accès local aux peers pendant le développement
```

Annexe 4 : Fichier docker compose pour le déploiement de l'application de monitoring Hyperledger Explorer

```
> docker-compose.yaml

# SPDX-License-Identifier: Apache-2.0
version: '3'

volumes:
  pgdata:
  walletstore:

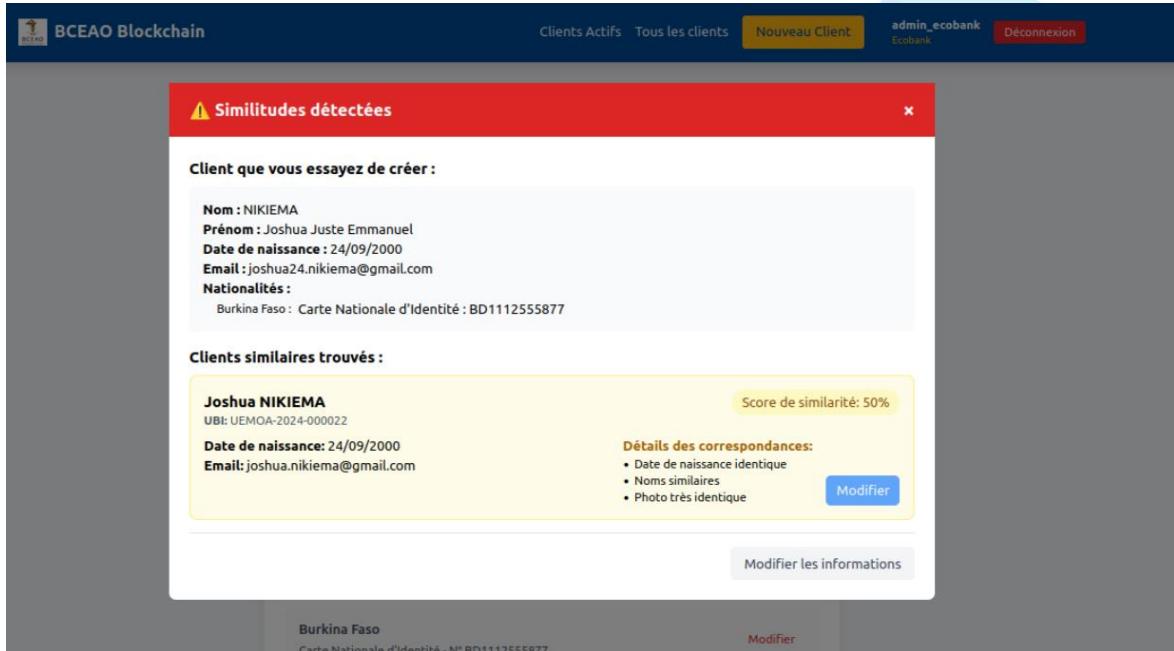
networks:
  mynetwork.com:
    external:
      name: [REDACTED]

services:

explorerdb.mynetwork.com:
  image: ghcr.io/hyperledger-labs/explorer-db:latest
  container_name: [REDACTED]
  hostname: [REDACTED]
  environment:
    - DATABASE_DATABASE=[REDACTED]
    - DATABASE_USERNAME=[REDACTED]
    - DATABASE_PASSWORD=[REDACTED]
  healthcheck:
    test: "pg_isready -h localhost -p 5432 -q -U postgres"
    interval: 30s
    timeout: 10s
    retries: 5
  volumes:
    - pgdata:/var/lib/postgresql/data
  networks:
    - [REDACTED]

explorer.mynetwork.com:
  image: ghcr.io/hyperledger-labs/explorer:latest
  container_name: [REDACTED]
  hostname: [REDACTED]
  environment:
    - DATABASE_HOST=[REDACTED]
```

## Annexe 5 : Détection d'un cas de similitude lors de l'enregistrement d'un client dans la blockchain



## TABLE DES MATIÈRES

PREAMBULE.....	i
DEDICACES .....	ii
AVANT-PROPOS .....	iii
REMERCIEMENTS .....	iv
GLOSSAIRE.....	v
LISTE DES FIGURES .....	vii
LISTE DES TABLEAUX.....	viii
LISTE DES CAPTURES.....	ix
INTRODUCTION GENERALE .....	1
Chapitre I : PRESENTATION GENERALE.....	2
Introduction .....	2
I.1    Présentation de la structure .....	2
I.1.1 Présentation de la structure d'accueil : BCEAO .....	2
I.1.1.1 Présentation et mission de la BCEAO .....	2
I.1.1.2 Organisation.....	3
I.1.2 Présentation de la direction d'accueil : DSI .....	5
I.1.2.1    Organigramme et effectifs.....	5
I.1.2.2    Activités principales .....	6
I.1.2.3    Enjeux majeurs .....	6
I.2    Présentation du thème d'étude.....	7
I.2.1    Problématique.....	7
I.2.2    Questionnement sur la gestion des homonymies .....	8
I.2.3    Objectif principal .....	8
I.2.4    Objectifs spécifiques.....	9
I.2.5    Objectifs de la recherche .....	10
I.2.6    Intérêt et pertinence de la thématique.....	10
I.2.7    Hypothèses de travail.....	11
I.3    Contexte .....	12
I.3.1    Environnement bancaire de l'UEMOA.....	12
I.3.2    Cadre réglementaire.....	12
I.3.2.1    Normes d'identification des clients .....	12
I.3.2.2    Exigences en matière de KYC (Know Your Customer) .....	12
I.3.3    État des lieux des systèmes d'identification .....	13
I.3.3.1    Cartographie des solutions d'identification par pays.....	13
I.3.3.2    Limites et insuffisances actuelles .....	13

I.3.4 Besoins et perspectives .....	14
I.3 Méthodologie et terrain .....	14
I.3.1 Approche méthodologique adoptée .....	14
I.3.2 Outils et techniques de collecte d'informations .....	15
I.3.3 Limites et contraintes méthodologiques .....	15
Conclusion .....	15
Chapitre II : TECHNOLOGIE BLOCKCHAIN ET GESTION DES IDENTITÉS .....	16
Introduction .....	16
II.1 Fondamentaux de la blockchain.....	16
II.1.1 Définition.....	16
II.1.2 Types de blockchain et cas d'usage.....	17
II.1.3 Structure et fonctionnement de la blockchain .....	18
II.1.4 Mécanismes de consensus et sécurité.....	21
II.1.4.1 Cryptographie : un pilier de la sécurité de la blockchain.....	21
II.1.4.2 Protocoles de consensus .....	25
II.2 Blockchain pour l'identité numérique .....	27
II.2.1 Concepts d'identité décentralisée.....	27
II.2.2 Smart contract ou contrat intelligent et gestion des identités.....	27
II.2.3 Standards et protocoles .....	28
II.3 Applications dans le secteur bancaire .....	28
II.3.1 Cas d'usage existants .....	28
II.3.2 Perspectives d'évolution.....	29
Conclusion .....	30
Chapitre III : ANALYSE ET CONCEPTION DE LA SOLUTION .....	31
Introduction .....	31
III.1 Périmètre fonctionnel.....	31
III.1.1 Objectifs du système.....	31
III.1.2 Fonctionnalités principales.....	32
III.1.3 Acteurs du système .....	32
III.2 Analyse des besoins .....	33
III.2.1 Besoins fonctionnels.....	33
III.2.1.1 Gestion des identités .....	33
III.2.1.2 Gestion des accès .....	34
III.2.2 Besoins non-fonctionnels .....	35
III.2.2.1 Sécurité .....	35
III.2.2.2 Performance.....	35
III.2.2.3 Conformité .....	36

---

III.3	Architecture et fonctionnement du système .....	36
III.3.1	Choix du type de blockchain .....	36
III.3.2	Architecture globale du système .....	38
III.4	Modélisation du système .....	39
III.4.1	Modèle de données.....	40
III.4.2	Diagrammes UML .....	41
III.4.2.1	Diagramme de cas d'utilisation .....	41
III.4.2.2	Diagramme de classe .....	42
III.4.2.3	Diagramme de séquence.....	44
III.4.2.4	Diagramme d'activité .....	46
III.4.2.5	Diagramme de déploiement.....	48
	Conclusion .....	49
	<b>Chapitre IV : OUTILS D'IMPLEMENTATION, RÉALISATION DE LA SOLUTION ET PLANIFICATION .....</b>	<b>50</b>
	Introduction .....	50
IV.1	Outils d'implémentation.....	50
IV.1.1	Technologie blockchain utilisée .....	50
IV.1.2	Outils nécessaires pour l'utilisation de Hyperledger Fabric .....	53
IV.1.2.1	VirtualBox.....	53
IV.1.2.2	CouchDB.....	53
IV.1.2.4	Hyperledger Explorer .....	54
IV.1.2.4	Docker et Docker-compose.....	55
IV.1.3	Outils utilisés pour l'utilisation du modèle de reconnaissance faciale .....	56
IV.1.3.1	Python .....	56
IV.1.3.2	PyTorch.....	57
IV.1.3.3	FastAPI .....	57
IV.1.4	Outils utilisés pour le développement du backend .....	58
IV.1.4.1	JavaScript .....	58
IV.1.4.2	Node.js .....	58
IV.1.4.3	Express.....	59
IV.1.5	Outils utilisés pour le développement du frontend .....	59
IV.1.5.1	ReactJS.....	59
IV.1.5.2	Tailwind CSS .....	60
IV.1.6	Visual Studio code .....	60
IV.2	Réalisation de la solution.....	61
IV.2.1	Topologie de notre blockchain .....	61

IV.2.2 Réalisation .....	62
IV.2.2.1 Déploiement de la blockchain et du chaincode.....	62
IV.2.2.3 Déploiement de l'application de monitoring de la blockchain : Hyperledger Explorer .....	66
IV.2.2.4 Déploiement de l'API de reconnaissance faciale .....	68
IV.2.3 Architecture logiciel de notre application .....	71
IV.2.4 Résultats obtenus .....	72
IV.3 Planification.....	76
IV.3.1 Coûts des ressources humaines .....	76
IV.3.2 Planning et phases du projet.....	77
IV.3.3 Gestion des risques.....	79
Conclusion .....	79
CONCLUSION GÉNÉRALE .....	80
BIBLIOGRAPHIE .....	I
WEBOGRAPHIE .....	II
ANNEXES.....	III
TABLE DES MATIÈRES .....	VII



## MÉMOIRE FIN DE FORMATION POUR L'OBTENTION DU DIPLÔME D'INGÉNIEUR DE CONCEPTION DES TÉLÉCOMMUNICATIONS

**Spécialité : INGENIERIE DE DONNEES ET INTELLIGENCE ARTIFICIELLE**

**Auteur :** M. Joshua Juste Emmanuel Yun Pei NIKIEMA

**Titre du mémoire :** Conception d'un système basé sur la technologie blockchain pour la gestion des cas d'homonymies dans le secteur bancaire

**Sous la direction de :** M. Moustapha DER, Enseignant/chercheur à l'ESMT

M. Printys Barnard ASSEDE, Chargé des systèmes d'information métier à la BCEAO

### RESUME

La gestion des homonymies représente un défi crucial pour les institutions bancaires de l'UEMOA, impactant l'identification unique des clients et augmentant les risques d'erreurs et de fraude. Ce mémoire explore l'application de la blockchain comme solution innovante à cette problématique, dans un contexte d'intégration régionale et de transformation numérique.

Menée au sein de la Direction des Systèmes d'Information de la BCEAO, cette recherche s'est appuyée sur une analyse des systèmes d'identification existants dans les huit pays membres, complétée par des entretiens avec des experts et le développement d'un prototype fonctionnel. La solution s'est fondée sur une blockchain de consortium utilisant Hyperledger Fabric, où la BCEAO a joué le rôle de superviseur et les banques celui de participants actifs. L'architecture inclut des mécanismes de reconnaissance faciale, des algorithmes de similarités et des smart contracts pour gérer les Identifiants Bancaires Uniques (IBU), assurant une identification fiable à l'échelle régionale. Les résultats démontrent la faisabilité technique de cette solution et ouvrent des perspectives pour des applications telles que le KYC mutualisé ou un système de scoring crédit partagé, contribuant ainsi à moderniser le secteur bancaire de l'UEMOA.

Cette étude illustre le potentiel des technologies émergentes pour renforcer l'intégration financière en Afrique de l'Ouest, tout en répondant aux exigences de sécurité et de conformité réglementaire.

**Mots clés :** Homonymie, Blockchain, Espace UEMOA, BCEAO, Consortium, Hyperledger Fabric, Hyperledger Explorer, Chaincode, Contrat Intelligent, Reconnaissance Faciale.



## MÉMOIRE FIN DE FORMATION POUR L'OBTENTION DU DIPLÔME D'INGÉNIEUR DE CONCEPTION DES TÉLÉCOMMUNICATIONS

**SPECIALTY:** DATA ENGINEERING AND ARTIFICIAL INTELLIGENCE

**Author:** Mr. Joshua Juste Emmanuel Yun Pei NIKIEMA

**Title of thesis:** Design of a system based on blockchain technology for managing cases of homonyms in the banking sector

**Under the supervision of:** Mr. Moustapha DER, Teacher/researcher at ESMT

Mr. Printys Barnard ASSEDE, Business Information System Manager at BCEAO

### ABSTRACT

The management of homonyms represents a crucial challenge for banking institutions in the UEMOA, impacting the unique identification of customers and increasing the risk of errors and fraud. This thesis explores the application of blockchain as an innovative solution to this problem, in a context of regional integration and digital transformation.

Conducted within BCEAO's Information Systems Department, this research was based on an analysis of existing identification systems in the eight member countries, supplemented by interviews with experts and the development of a functional prototype. The solution was based on a consortium blockchain using Hyperledger Fabric, with BCEAO acting as supervisor and the banks as active participants. The architecture includes facial recognition mechanisms, similarity algorithms and smart contracts to manage Unique Bank Identifiers (UBIs), ensuring reliable identification on a regional scale. The results demonstrate the technical feasibility of this solution and open up prospects for applications such as pooled KYC or a shared credit scoring system, thereby helping to modernize the UEMOA banking sector.

This study illustrates the potential of emerging technologies to strengthen financial integration in West Africa, while meeting security and regulatory compliance requirements.

**Keywords:** Homonymy, Blockchain, UEMOA, BCEAO, Consortium, Hyperledger Fabric, Hyperledger Explorer, Chaincode, Smart Contract, Facial Recognition.