MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE ET DE L'INNOVATION
****
SECRÉTARIAT GÉNÉRAL
****
UNIVERSITÉ JOSEPH KI-ZERBO (UJKZ)
****
INSTITUT BURKINABÈ DES ARTS ET MÉTIERS
(IBAM)
****

BURKINA FASO
La Patrie ou la Mort, nous Vaincrons
****

MÉMOIRE POUR L'OBTENTION DU MASTER EN INFORMATIQUE

OPTION : **INGENIERIE DES SYSTEMES D'INFORMATION EN ENTREPRISE**

THÈME :

Authentification de documents administratifs à l'aide de la blockchain

Réalisé par : HIEN Zilèdem Pierre Canisius
Soutenu publiquement le : …/06/2025

Jury de soutenance :
Président :
Directeur de mémoire : M. Yaya TRAORE, *MC en informatique*.
Evaluateur :

Année académique : 2023-2024

DÉDICACE

A ma fille, W. Candice Urielle !

REMERCIEMENTS

Nous tenons tout d'abord à rendre grâce à Dieu Le Tout Puissant, par qui nous vivons.

Au cours de ce cycle de Master, nous avons eu le privilège de collaborer avec des personnes de marques qui nous ont fourni tout le nécessaire afin que nous parvenions à ce résultat. C'est donc le lieu pour nous, à travers ces lignes, de leur traduire notre profonde gratitude.

Nos distincts remerciements vont particulièrement à l'endroit de :

- **Dr. Yaya TRAORE**, notre Directeur de mémoire, qui a bien voulu nous encadrer sans hésitation, et pour sa disponibilité malgré un calendrier chargé. Ses critiques constructives et ses partages d'expériences nous ont été d'une très grande utilité.
- **Pr. Sadouanouan MALO**, pour ses conseils bien avisés, ses multiples encouragements et accompagnements.
- **Monsieur le Directeur de l'IBAM, le corps professoral et tout le personnel de l'IBAM** pour la formation reçue et leur accompagnement.
- **notre famille, nos collègues et camarades** pour leurs soutiens et encouragements.
- **toutes les personnes dont les noms n'ont pu être cités.**

RÉSUMÉ

ABSTRACT

TABLES DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES SIGLES ET ABREVIATIONS

CSS	Cascading Style Sheets ou Feuilles de Style en Cascade
HTML	HyperText Markup Language ou Langage de balises pour l'hypertexte
HTTP	Hypertext Transfer Protocol ou Protocole de Transfert Hypertexte
IBAM	Institut Burkinabè des Arts et Métiers
MC	Maître de conférences
P2P	Peer-to-Peer
PoA	Proof of Autority ou Preuve d'Autorité
PoS	Proof of Stake ou Preuve d'Enjeu
PoW	Proof of Work ou Preuve de Travail
SHA-256	Secure Hash Algorithm (algorithme de hachage sécurisé) 256 bits
UJKZ	Université Joseph KI-ZERBO
IDE	Integrated Development Environment (environnement de développement intégré)
API	Application Programming Interface (interface de programmation d'application)
JSON	JavaScript Object Notation

CHAPITRE 1 :

INTRODUCTION GENERALE

CHAPITRE 1 : INTRODUCTION GENERALE

La pertinence de notre sujet de recherche tient dans un contexte qu'il nous convient de justifier. A l'entame donc de ce mémoire, le présent chapitre est réservé à la définition du cadre de notre projet, à savoir le contexte général dans lequel est né le sujet, et le problème que l'on se propose de résoudre. En plus d'énoncer des hypothèses de recherche, nous y présentons les objectifs et les résultats attendus du projet. Ce chapitre fourni également une vue d'ensemble du déroulement de notre étude.

1.1. Contexte et justification

La fiabilité de certains documents administratifs est de plus en plus controversées ; et ce, avec le développement et l'exploitation fulgurants des multiples outils basés sur l'Intelligence Artificielle (IA). La complexité de ce contexte est caractérisée par le fait que de nombreux cas réels de faux « documents administratifs » ont été retrouvés sur la place publique, mettant en déroute bon nombre de citoyens. Parmi ces cas, la majorité a nécessité des démentis officiels selon des structures étatiques que nous qualifions de « victimes » de faux. En effet, et entre autres éléments, nous faisons observer à titre illustratif que :

- le 16 août 2024, le Ministère de la Fonction Publique, du Travail et de la Protection Sociale publiait un démenti, signé DCRP/MFPTPS, sur sa page Facebook en ces termes « *Une loi portant statut général des agents publics et un projet de loi portant statut général des agents publics circulant sur les réseaux sociaux sont faux. Ces textes ne proviennent pas des services techniques du Ministère de la Fonction Publique, du Travail et de la Protection Sociale, ni du Gouvernement ou de l'Assemblée législative de Transition* ». Source : https://www.facebook.com/share/p/kHPydXy6A1zMniK1/?mibextid=oFDknk.
- le 18 janvier 2024, le Service de Communication et des Relations Publiques de la Direction Générale des Douanes a, de même, publié un démenti sur sa page Facebook comme suit : « *Le Service de Communication et des Relations Publiques de la Direction Générale des Douanes informe le public que les communiqués, ci-dessous, sur une supposée vente aux enchères de véhicules n'émanent nullement des services des Douanes* ». Source : https://www.facebook.com/share/p/15f4cKVZ3P/.
- le 06 octobre 2023, le Ministère des Affaires Etrangères du Burkina Faso, à travers la DRCP/MAECR-BE, avait également publié sur sa page Facebook, ce qui suit : « *Depuis un certains temps un communiqué relatif à une bourse canadienne et impliquant le*

Ministère des Affaires Etrangères du Burkina Faso circule sur les réseaux sociaux. Le Ministère des Affaires Etrangères du Burkina Faso, apporte un démenti à ce communiqué qui est certainement l'œuvre d'individus mal intentionnés. ». Source : https://www.facebook.com/share/p/yqFV712VwsjcHxne/?mibextid=oFDknk.

- le 30 novembre 2021, l'Institut national de la statistique et de la démographie (INSD) avait aussi démenti sur sa page Facebook, un faux recrutement d'étudiants dont il serait l'auteur. Source : https://www.facebook.com/share/p/DYayYQThHP2NLDbF/?mibextid=oFDknk.

Le plus souvent, une copie de chacun de ces documents en question a été marquée d'insigne de faux par les structures « victimes », puis annexée aux différents démentis. De ce fait, ces documents pourraient être classés « administratifs », car par définition, peut être vu comme document administratif, tout acte produit ou reçu, dans le cadre de la mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Il peut s'agir d'un communiqué, un certificat (de prise /cessation de service, administratif, …), un diplôme, un extrait d'acte de naissance, etc.

Ainsi, au regard de la fréquence progressive et élevée de la falsification et/ou fraude de ces types de document, les citoyens, et même des acteurs de l'Administration posent de nombreuses préoccupations sur l'authenticité, ou l'originalité de tel ou tel acte (document) administratif qui se présente à eux.

A l'image de l'IA, la Blockchain est une technologie en plein essor. C'est une technologie de registre numérique distribué qui s'applique dans divers domaines. En outre, la blockchain étant immuable, décentralisée et transparente, pourrait être une alternative aux préoccupations susmentionnées.

C'est pourquoi, dans ce contexte générale, nous nous intéressons donc à l'utilisation de la technologie blockchain, notamment ses protocoles de consensus, de vérification et de validation, pour résoudre la question d'authentification des documents administratifs, afin de réduire les risques de fraudes et de falsifications de ces documents. D'où le thème du présent mémoire « ***Authentification de documents administratifs à l'aide de la blockchain*** » que nous nous proposons d'étudier.

Par ailleurs, la réalisation de cette étude intervient dans le cadre de notre stage de fin de cycle académique de Master à l'Institut Burkinabè des Arts et Métiers (IBAM) qui est l'un des instituts de l'Université Joseph KI-ZERBO (UJKZ) [21] .

1.2. Problématique et hypothèses

La falsification (ou fraude) documentaire est un problème d'actualité auquel est confrontée particulièrement l'administration publique. Afin de conserver leur image, d'assurer une bonne gouvernance et d'éviter l'usage du faux, les structures publiques et privées s'efforcent de vérifier elles-mêmes, manuellement les dossiers des usagers/clients. A défaut, elles délèguent et suivent une longue procédure de vérifications de ces dossiers par des tiers, moyennant des ressources (financières, humaines, temps, …) considérables. Elles sont également contraintes de rester plus ou moins en veille constante pour démentir d'éventuels faux documents à elles attribués. Cela diminue non seulement le temps consacré aux activités règlementaires des services administratifs, mais augmente les coûts de contrôle et les délais de prestations de services.

De ce fait, quel outil ou quelle technologie peut être mise en œuvre pour faire face à cette situation ? pour nous, la problématique qui se dégage, c'est comment la technologie blockchain peut-elle garantir l'authenticité des documents administratifs de façon plus sécurisée, transparente et efficace ? Autrement dit, comment la blockchain peut-elle aider les administrations à prévenir et/ou à détecter les tentatives de falsification de documents administratifs ? Cette technologie, peut-elle permettre à un service public destinataire d'un document administratif de savoir si oui ou non, il s'agit bien d'un document authentique ?

Pour traiter cette problématique, nous posons les hypothèses suivantes :

Hypothèse 1 : l'intégration de la blockchain dans une solution d'authentification de documents permet de renforcer la sécurité et l'intégrité des documents administratifs en ce sens que ces documents, une fois enregistrés dans une chaîne, ne seront plus modifiables ou supprimables. Ceci se justifie par le fait que la blockchain a un caractère immuable.

Hypothèse 2 : la blockchain permet de vérifier l'authenticité en temps réel des documents sans passer par des procédures manuelles. Ainsi, l'adoption de la blockchain permet une réduction considérable des délais de vérification de documents au profit de l'Administration et des usagers/clients. Et cela pourrait, par ricochet, améliorer la confiance entre les citoyens et les institutions publiques.

Hypothèse 3 : l'utilisation de la blockchain dans le processus d'authentification de documents peut diminuer les cas de falsifications et fraudes des documents administratifs, du fait du caractère transparent des transactions blockchain. Car toute opération d'écriture dans un système de blockchain est traçable.

Pour tester ou mesurer ces hypothèses, nous recourons à des variables tels que le temps moyen de vérification des documents administratifs avant et après l'implémentation de notre solution, et le niveau de satisfaction d'un échantillon de services administratifs. L'on pourra également s'appuyer sur le taux d'incidents de sécurité liés à la manipulation ou à la falsification des documents administratifs sur une période donnée.

1.3. Objectif du projet

Face à la préoccupation évoquée précédemment, notre objectif à travers ce projet est d'explorer l'utilisation de la blockchain dans les processus d'authentification de documents administratifs de manière plus sécurisée, transparente et efficace.

De façon spécifique, il s'agit pour nous, de :

- faire un état de l'art sur la sécurisation et l'authentification des documents avec la blockchain ;
- proposer une approche de résolution en fixant le type de document administratif de base ;
- implémenter la solution (ou l'approche) qui intègre la blockchain et qui offre la possibilité de vérifier l'authenticité de documents administratifs.

1.4. Résultats attendus

Les travaux devront aboutir à des résultats qui présentent la manière dont les structures pourront utiliser la blockchain pour résoudre, entre autres, leurs problèmes de falsification et de fraude documentaire. Concrètement, les résultats suivants sont attendus au terme de notre étude :

- un état de l'art sur la sécurisation et l'authentification des documents administratifs avec la blockchain est fait ;
- une approche de résolution (conception) est proposée ;
- une solution qui intègre la blockchain et qui offre la possibilité de vérifier l'authenticité de documents administratifs est implémentée.

1.5. Organisation du travail

Le présent mémoire est l'aboutissement de plusieurs travaux suivant un projet de chronogramme spécifique illustré par la figure 1 ci-dessous.

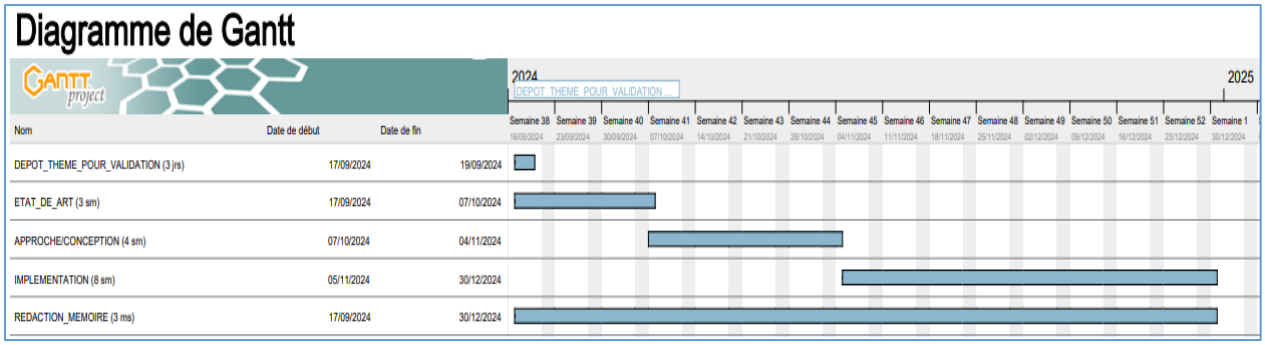


***Figure 1** : Projet de chronogramme des travaux*

Ce mémoire est organisé en cinq (05) principaux chapitres. En dehors de ce présent **chapitre 1**, le reste du présent mémoire est structuré comme suit :

- **le chapitre 2 « concepts de base »** est consacré aux définitions des termes clés utilisés tout au long de nos travaux. Certains concepts dérivés y sont définis et expliqués également.
- **le chapitre 3 « état de l'art »** fait une synthèse des connaissances sur la blockchain et des travaux existants en matière de processus d'authentification et de sécurisation de documents en via la blockchain. Nous menons, à la suite de cette synthèse, une discussion sur les travaux existants.
- **le chapitre 4 « approche »** est dédié à la présentation de notre approche de résolution de la problématique. Nous y listons les étapes à suivre pour la mise en œuvre de notre solution. Nous y fixons aussi le type de document administratif sur lequel nous travaillons.
- **le chapitre 5 « implémentation de l'approche »** est réservé à la mise en œuvre concrète de notre approche. Nous y présentons l'environnement d'implémentation de la solution ainsi que les différents éléments de conception. C'est également le lieu de présenter la solution développée.
- **la conclusion** générale dans laquelle nous dressons un bilan des principales actions réalisées dans le cadre de l'étude. Ce bilan est consolidé de perspectives pour la suite de cette étude.

  Le présent mémoire prend fin avec la présentation des références bibliographiques/webographiques et des annexes.

CHAPITRE 2 :

CONCEPTS DE BASE

CHAPITRE 2 : CONCEPTS DE BASE

Dans le cadre de nos travaux de recherche, nous sommes amenés à appliquer des approches et outils informatiques dans un milieu plus général que celui de l'Informatique. Il convient donc de revenir sur certaines notions et expressions afin d'harmoniser la compréhension pour la suite des travaux. Dans ce chapitre, nous définissons ces concepts clés et quelques-unes de leurs notions sous-jacentes et dérivées.

2.1 Documents administratifs

Dans notre contexte, on entend par **document administratif**, une information conservée sur papier ou sur un support électronique. Outre cette compréhension générale, un cadre juridique donne un contenu plus formel à ce concept.

En effet, au Burkina Faso, selon l'article 4 de la *loi N° 051-2015/CNT du 30 août 2015 portant droit d'accès à l'information publique et aux documents administratifs*, sont considérés comme documents administratifs, les documents produits ou reçus, dans le cadre de la mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission.

Il s'agit par exemple des notes de service, des décisions, des instructions, des circulaires, des directives, des journaux, des délibérations, des rapports, des comptes rendus, des procès-verbaux, des croquis, des plans, des schémas, des avis, des prévisions, des communiqués officiels, des certificats (de prise-reprise-cessation de service, …), des bulletins, des décrets, des arrêtés, etc.

2.2 Sécurisation et authentification

La sécurisation et l'authentification sont intrinsèquement liés et indissociables à la limite.

La sécurisation (d'un document) c'est l'ensemble de mesures à prendre et à mettre en œuvre pour garantir la traçabilité liée aux accès, et la protection des informations sensibles (électroniques ou physiques). Elle vise à empêcher que les données soient manipulées ou reproduites de manière illicite ou non autorisée.

L'authentification quant à elle, est un processus, par lequel un système informatique ou un humain prouve ou certifie qu'un document est authentique. Un document est dit authentique s'il s'agit de l'original, d'une copie conforme à l'original ou de l'original après *vérification* et *validation* par un sujet habilité ou compétent. Le sujet étant jusque-là un Officier de l'Etat Civil, un Officier de Police

judiciaire, l'Autorité ayant délivré le document, le Greffe des cours et tribunaux, le Notaire pour le cas du Burkina Faso.

2.3 Consensus

Dans le contexte de blockchain, le concept de consensus indispensable. C'est une procédure qui consiste à dégager un accord sans procéder à un vote formel, ce qui évite de faire apparaître les objections et les abstentions [17] . Dit autrement par [20] , le consensus désigne toute situation où plusieurs parties se mettent d'accord, sans possibilité d'opposition et sans que les intérêts de l'une ou l'autre des différentes parties ne se trouvent lésés. Le consensus s'établit généralement à l'unanimité, ou tout du moins à la majorité. Le consensus est indissociable du mot voisin « consentement » : il ne revêt pas un caractère irréfutable, il s'agit de quelque chose que l'on admet, sur laquelle on s'accorde, et que l'on accepte comme une vérité ou comme une solution, en réponse à une question ou à un problème donné. Appliqué à la Blockchain, le consensus (il en existe plusieurs types) est un processus sécurisé par lequel un groupe de pairs (ou nœuds) sur un réseau de blockchain parviennent à un accord unanime pour déterminer quelles transactions de la blockchain sont valides et lesquelles ne le sont pas. On parle alors de mécanisme de consensus ou d'algorithme de consensus [18] . D'une blockchain à une autre, ces méthodes utilisées pour parvenir à cet accord sont appelées Proof of Work (PoW), Proof of Stake (PoS), Proof of Autority (PoA), etc.

La Preuve de travail (Proof of Work – PoW) est le premier algorithme de consensus implémenté dans une cryptomonnaie et utilisé par Bitcoin. Ce mécanisme nécessite une puissance de calcul considérable pour résoudre les problèmes mathématiques complexes et valider un bloc. La PoW est efficace en terme de sécurité. Mais sa limite est le fait qu'elle exige une quantité importante d'électricité et de ressources matérielles (Application-Specific Integrated Circuits, Graphics Processing Units, Serveurs puissants, Equipements de data center, ...) pour fonctionner.

La preuve d'enjeu (Proof of Snake – PoS), contrairement à la PoW, ne requiert pas une puissance de calcul pour valider les transactions et créer de nouveaux blocs. Dans ce mécanisme, les nœuds validateurs sont sélectionnés en fonction de la quantité de monnaie qu'ils sont prêts à mettre en jeu comme garantie. Ainsi, les nœuds détenteurs de monnaie sont encouragés à agir honnêtement et à sécuriser le réseau de la blockchain au risque de perdre leur mise.

La preuve d'autorité (Proof of Authority – PoA) quant à elle, est un algorithme de consensus approprié pour les blockchains d'entreprise du fait de sa faible consommation en énergie. Elle fait tout de même l'objet de critiques car elle fonctionne sur le principe de centralisation de droits de validation sur la base de confiance.

2.4 Blockchain

La blockchain se définit de plusieurs manières.

De manière basique, la blockchain est une technologie numérique de stockage chronologique et de transmission d'informations sous forme de blocs reliés les uns aux autres de manière sécurisée et sans autorité centrale. En termes plus simple, le Mathématicien *Jean-Paul Delahaye*, la définit comme étant : « *un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible* ».

De manière technique, la blockchain est assimilable à une base de données distribuée, dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés, puis groupés à intervalles de temps réguliers en blocs. L'ensemble de ces blocs est sécurisé par cryptographie et forme ainsi une chaîne de plus en plus longue. Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements théoriquement protégés contre la falsification ou la modification par les nœuds de stockage ; c'est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis la création de la transaction initiale [8] .

On peut donc comprendre que cette technologie est basée sur le concept de grand livre distribué ou de base de données partagée. Cela implique que dans le réseau blockchain, chaque participant (nœud) au réseau a sa propre copie de la base de données. Pour y parvenir, un **algorithme de consensus** est utilisé. En effet, l'algorithme de consensus est essentiellement caractérisé par :

- **un accord unanime sur le contenu des données**, afin de permettre à tous les nœuds (ou du moins la majorité des participants) du réseau de valider et de s'accorder sur quelles données doivent être inscrites dans la blockchain, du fait de la présence de données contradictoires. La cryptographie est utilisée lors de la validation des transactions.
- **une conformité des copies des données convenues,** afin de s'assurer que toutes les transactions ajoutées à la blockchain sont les mêmes pour chaque utilisateur.

- **une absence de tricherie par altérations des données ou tentative de fraude**, qui est garanti grâce à des mécanismes cryptographiques qui rendent toute tentative de modification ultérieure des données pratiquement impossible. En effet, dans une chaîne de blocs, les transactions sont horodatées en permanence. Cette sorte d'archivage empêche la suppression ou l'inversion des transactions une fois ajoutées à la chaîne de blocks, et dès que d'autres blocs ont été ajoutés à la suite.

Tout se passe dans un réseau distribué de sorte à ce que si un nœud tombe en panne, les autres peuvent continuer à fonctionner de façon transparente ; ce qui garantit la disponibilité et la fiabilité dans les transactions. On parle précisément de système distribué décentralisé. Dans ce système, chaque participant peut vérifier les informations de manière indépendante car les processus de vérification ne dépendent d'aucune autorité centralisée [1] .

Il semble indispensable de revenir sur les termes arbre/racine de Merkle, hash, et mineur qui sont des composants fondamentaux de la technologie blockchain.

L'arbre de Merkle ou arbre de Hash (ou hachage) est une structure d'arbre binaire où chaque nœud de l'arbre est le résultat d'une fonction de hachage appliquée aux données des nœuds enfants. En effet, chaque nœud est identifié avec un identifiant unique (hachage). Ces nœuds initiaux (nœuds enfants ou feuilles), sont ensuite associés à un nœud supérieur appelé nœud parent. Le nœud parent a, à son tour, un identifiant unique résultant du hachage de ses nœuds enfants. Cette structure est répétée jusqu'au nœud racine ou racine Merkle (racine Merkle), dont l'empreinte est associée à tous les nœuds de l'arbre. Crée en 1979 par le cryptographe informaticien *Ralph Merkle*, il est utilisé dans la blockchain et la cryptographie [19] . L'annexe 1 présente une illustration de l'arbre de Merkle où les hash sont nécessairement couplés par paire de nœud – le nœud EF y étant seul et différent de la racine, a été dupliqué et couplé avec lui-même.

Un hash est le résultat d'une fonction mathématique qui permet d'obtenir une empreinte numérique unique de taille fixe par donnée d'entrée (fichier, texte, …) de taille non bornée. Cette empreinte numérique est difficilement (voir impossible) devinable par un humain. Par exemple, l'algorithme SHA-256 (32 octets) produit toujours une valeur de sortie hexadécimale de 64 caractères.

Un mineur est un intervenant (ordinateur ou nœud) actifs du réseau de blockchain qui sélectionne des transactions et participe à leur validation.

Dans ce chapitre, nous avons présenté et défini les concepts de base et notions tels que le document administratif, l'authentification et la sécurisation, le consensus et la blockchain. Certains composants fondamentaux de la blockchain ont été également abordés.

Avec cette harmonisation de la compréhension de ces concepts, nous proposons dans le chapitre suivant, un état des connaissances sur la technologie blockchain et surtout l'application de celle-ci dans les processus d'authentification de documents.

CHAPITRE 3 :

ÉTAT DE L'ART

CHAPITRE 3 : ÉTAT DE L'ART

On ne peut parler de Blockchain sans aborder la notion de **transaction**. La transaction est une opération d'échange qui implique plusieurs parties [2] . Dans ce sens, l'opération peut être commerciale ou boursière, un contrat ou accord, etc. Parmi les parties impliquées dans une transaction, occupe en bonne position un tiers de confiance qui permet d'une part de sécuriser la transaction et d'autre part de certifier la validité de ladite transaction. En effet, le tiers de confiance est une entité neutre et indépendante telle qu'une institution financière ou un notaire.

La mondialisation de ce système de transaction à partir des années 1960 a conduit à l'augmentation fulgurante du nombre de transactions ; entrainant ainsi l'accroissement des risques liés à l'authenticité des transactions, qui, jusque-là étaient transcrites dans des registres (document) physiques. Mais grâce à l'avènement et à l'évolution rapide de la Technologie, notamment dans les domaines du web et de la cryptographie, le principe du tiers de confiance disparait progressivement au profit de ce qu'il convient d'appeler « Blockchain ».

Ce chapitre du présent mémoire a pour but de présenter la technologie blockchain tout en rappelant son historique. Nous y abordons la classification de la blockchain, sa structure ainsi que son fonctionnement. Aussi, on y retrouve particulièrement une présentation des travaux existants sur la sécurisation et l'authentification des documents avec la blockchain.

3.1 Généralités sur la Blockchain

3.1.1. Origines de la blockchain

Dès les années 1990, la perspective de digitalisation des documents sous format numérique soulevait déjà la question de savoir comment certifier la date à laquelle un document a été créé ou modifié pour la dernière fois. Comment faire en sorte qu'un utilisateur ne puisse pas antidater ou modifier la date d'un document mis sur support numérique ? dans [3] , *Stuart Haber et W. Scott Stornetta* ont proposé dans ce sens, des procédures informatiques pratiques pour l'horodatage numérique de documents sous forme numérique. Leurs réflexions sur entre autres le hachage, et les signatures numériques, les ont permis d'incorporer, en 1992, le concept d'arbre de Merkle au système d'horodatage de documents avec le concours de *Dave Bayer*. Cette innovation a amélioré l'efficacité du système en permettant à plusieurs documents d'être regroupés en un seul bloc [4] .

Dans [5] , le chercheur *Ittai Abraham* a affirmé : "*The longest running blockchain started in 1995 and is still running strong today. (...)*" ; ceci pour indiquer que le premier système de certification

décentralisé est celui de la société Surety, qui publie chaque semaine depuis 1995 un certificat cryptographique de sa base de données dans la rubrique « Annonces et objets trouvés » du « New York Times ». Pour en venir, le concept de Blockchain en lui-même, basé sur la cryptographie, a été évoqué pour la première fois au début des années 1980. Mais de nos jours, il est impossible de dissocier les concepts de blockchain et de crypto-monnaies car elles constituent le point essentiel d'émergence de la blockchain. En effet, la crypto-monnaie est une monnaie virtuelle dont l'implémentation repose sur des algorithmes cryptographiques permettant de générer de la monnaie et de faire des transactions anonymes entre des paires sur internet. Dans ce sens, le bitcoin, une crypto-monnaie qui s'est rapidement imposée de manière non triviale, a été annoncé en 2008 par son mystérieux – mystérieux, car « Satoshi Nakamoto » est largement considéré comme un pseudonyme, et la véritable identité de l'inventeur du bitcoin reste un inconnue – développeur, **Satoshi Nakamoto** [6] . Le bitcoin, selon *S. Nakamoto* dans [7] (plus détaillé par *G. Ferréol et R. Romain* dans [2]), repose sur trois fondamentaux à savoir : le réseau pair-à-pair sans autorité centrale, les transactions et le triple protocole de vérification-consensus-validation. Ces éléments constituent une chaîne de blocs (ou blockchain en anglais).

La technologie blockchain, dans son évolution, se distingue en différentes formes que nous trouvons essentiel de présenter.

3.1.2. Types de blockchain

La classification de la technologie blockchain est possible du fait de son évolution générationnelle. Dans [9] , *Imran Bashir* discute de quatre (04) générations (ou niveaux) de la blockchain. Il s'agit de la :

- Blockchain 1.0 : cette génération ne concernait que les crypto-monnaies car elle a été introduite avec l'invention du Bitcoin. Elle inclut donc les applications de base telles que les paiements et les applications servant à effectuer de simples transferts de valeurs.
- Blockchain 2.0 : elle est une évolution de la première génération à travers l'intégration des contrats intelligents et autres applications dérivées des services financiers.
- Blockchain 3.0 : les blockchains de la troisième génération ont permis d'envisager, au-delà de l'industrie des services financiers, de nombreuses autres applications à usage général telles que les médias, la santé, le gouvernement, etc.

- Blockchain X : la génération X permet de se projeter dans une vision où la blockchain va fournir des services dans tous les domaines de la société.

En se basant sur cette évolution générationnelle, nous présentons dans cette section, une classification de la blockchain selon différents attributs qui pourraient se chevauchés.

Les blockchains publiques

Ces blockchains sont également appelés « blockchains sans permission ». C'est des blockchains qui sont ouvertes au public – donc accessibles à tous, au point de ne requérir aucune permission spécifique à l'entrée, ni au moment de réaliser une transaction – et chaque utilisateur peut conserver sans autorisation préalable, une copie du registre sur son nœud local. Les blockchains publiques sont aussi caractérisées par le fait que toute personne, en tant que nœud du réseau distribué, peut participer au processus de prise de décision. La prise de décision sur l'état de ce type de blockchain nécessite l'utilisation d'un mécanisme de consensus distribué. Il peut arriver qu'un nœud participant soit récompensé pour sa participation. Ce type de blockchain est en général open source. Ethereum et Bitcoin[1] sont des exemples de blockchains publiques [10] .

Les blockchains privées

Les blockchains privées ne sont pas ouvertes au public. Elles sont accessibles uniquement sur invitation et tous les membres participants se connaissent et se font confiance. Les membres participants peuvent être un groupe d'individus ou d'organisations qui ont décidé de partager le registre entre eux. Dans ce type de blockchain, un mécanisme de consensus est utilisé pour valider l'écriture des données parmi ses participants privilégiés. Cette approche est très utile lorsque la blockchain est utilisée entre des entreprises appartenant à la même industrie par exemple. Aussi appelées blockchains permissionnées ou blockchains à autorisation, Hyperledger et Ripple sont des exemples de blockchain privée fréquemment cités [10] .

Les blockchains semi-privées

Encore appelé blockchain de consortium, ce type de blockchain constitue un hybride entre la blockchain publique et la blockchain privée.

[1] Détails sur : https://www.blockchain.com/fr/explorer

Dans ce type de blockchain, seuls quelques nœuds sélectionnés sont prédéterminés à se partager la responsabilité de la maintenance et de la sécurisation du réseau blockchain. Ils ont la responsabilité de déterminer les droits d'accès aux données. Les nœuds participants, eux, sont invités. Les décisions sont prises par la majorité des acteurs présélectionnés. Cela signifie qu'en dehors des données spécifiques stockées, le reste des données sont accessibles au public. Ainsi, des membres publics peuvent vérifier (à l'aide de contrats intelligents) si les transactions privées ont été effectuées. Le fait d'avoir des droits de lecture pouvant être publics ou limités aux participants permet de préserver la confidentialité des données, comme dans les blockchains privées. BigchainDB, EEA et R3 sont des exemples de blockchain de consortium [11] .

Outre ces trois (03) principaux types de blockchain selon les attributs réseau, il existe des blockchains dérivées telles que les sidechains (chaines secondaires ou chaîne de transactions gérée par une sous-communauté) [12] , les grands livres autorisés, les grands livres distribués, les grands livres partagés, les blockchains entièrement privées et propriétaires, les blockchains à jetons, les blockchains sans jetons, etc. [9] . Nous nous intéressons aux grands livres autorisés et aux blockchains entièrement privées et propriétaires.

Un grand livre autorisé est une blockchain dans laquelle l'utilisation d'un mécanisme de consensus distribué n'est pas nécessaire car les utilisateurs sont connus et se font confiance. Les participants au réseau du grand livre autorisé peuvent utiliser un protocole d'accord pour maintenir une version partagée de la vérité sur l'état des enregistrements dans la blockchain. Dans ce cas, il n'est pas nécessaire que le grand livre autorisé soit privée, car elle peut être publique avec un contrôle d'accès réglementé. Les grands livres autorisés sont aussi appelés blockchains ou registres avec permission.

Comme leur nom l'indique, les blockchains entièrement privées et propriétaires ne sont pas ouverte au grand public. Mais, dans des contextes privés spécifiques au sein d'une organisation, il pourrait être nécessaire de partager des données et de fournir un certain niveau de garantie quant à l'authenticité des données. Ces blockchains pourraient être utiles, par exemple, pour la collaboration et le partage de données entre différents départements gouvernementaux [9] .

Bien qu'il y ait plusieurs types de blockchains, dans la technologie blockchain, la structure et le mode fonctionnement qui permettent de garantir la sécurité des transactions restent quasiment les même.

3.1.3. Structure et fonctionnement de la blockchain

3.1.3.1. Structure de la blockchain

La blockchain, comme son nom l'indique, est une chaine ou liste chainée reliant des **blocs en retour** et hébergée dans des nœuds en réseau. Les blocs se définissent comme des groupements de transactions.

En effet, la structure de la blockchain repose sur l'architecture réseau distribué Peer to Peer (P2P) – aussi appelé pair-à-pair en français – qui est un réseau d'égal à égal. Ce type de réseau regroupe un ensemble d'ordinateurs appelés nœuds qui partagent les informations ou fichiers entre eux de manière directe, rapide et abordable. Ces nœuds contiennent donc une copie de la blockchain et fournissent un consensus sur l'état de celle-ci à tout moment. La figure 2 ci-dessous présente un schéma de réseau décentralisé P2P où chaque utilisateur ou nœud possède à la fois le rôle de serveur et de client ; ce qui est différent pour les réseaux classiques.

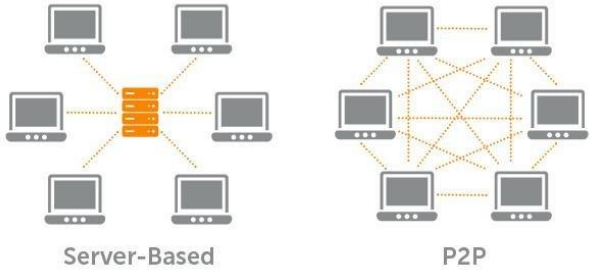


***Figure 2** : Réseau basé sur les Serveurs vs Réseau P2P*

Source figure : *https://www.researchgate.net/figure/Reseau-base-sur-les-Serveurs-vs-Reseau-P2P_fig5_335174496*

Les blocs quant à eux, sont plus ou moins importants en fonction du nombre de données qu'ils renferment. Ils se distinguent les uns des autres grâce à un identifiant, un code unique appelé "hash". En effet, chaque bloc contient deux (02) parties à savoir l'entête (header) et le corps (facts) du bloc.

Le header contient plusieurs informations clés telles que [13] :

- **la version** qui indique le protocole de validation des règles ;
- **le hash du bloc précédent** qui assure liaison entre les blocs afin de constituer la chaine ;
- **le hash de la racine de Merkle** qui synthétise les informations que renferment toutes les transactions du bloc ;
- **le timestamp (date et heure de création)** pour l'horodatage du bloc qui précise le temps de minage ;
- **les bits** qui indique la valeur actuelle de la difficulté de minage ;
- **le nonce** qui est un numéro aléatoire utilisé lors du minage pour trouver un hash valide.

En pseudo-code, une entête d'un bloc peut ressembler au contenu de la figure 3 ci-dessous.

```
BlocHeader: {
    Version: 1,
    PreviousBlockHash: "00000000000004X8G...",
    MerkleRoot: "3a5bc234ad...",
    Time: 1234567890,
    Bits: 1703ddf8c3,
    Nonce: 2085406893
}
```

***Figure 3** : Exemple d'entête d'un bloc*

Le corps du bloc contient les transactions qui doivent être stockés dans les bases de données. Ces transactions sont appelées « facts » ou « faits ». La transaction est l'élément de base de la blockchain Bitcoin (primitive des autres blockchains). La figure 4 ci-dessous présente un exemple simplifié chaîne de blocs.

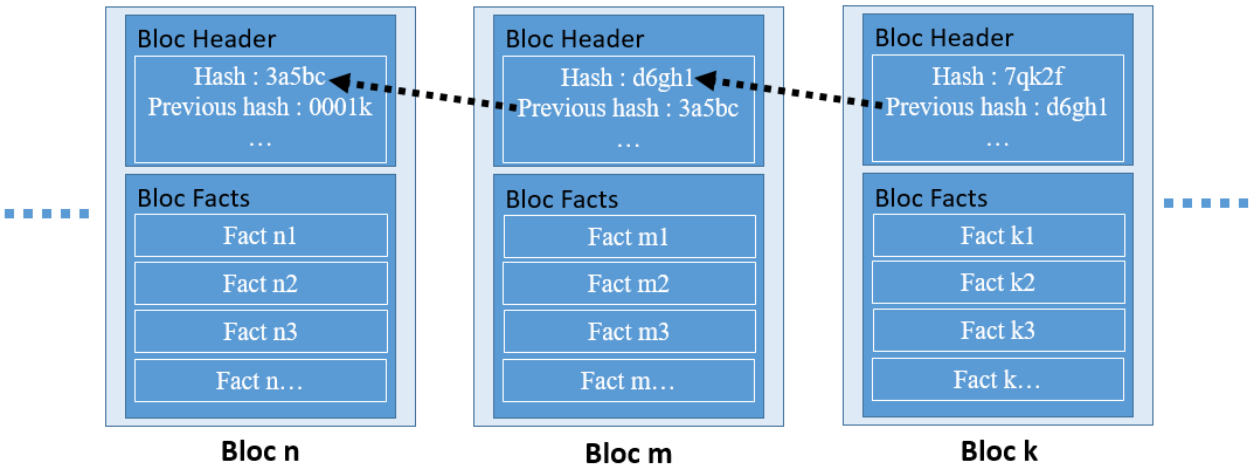


***Figure 4** : Schéma simplifié d'une chaîne de blocs*

Dans ce schéma, nous pouvons constater que ***bloc_m.previous_hash = bloc_n.hash*** *et* ***bloc_k.previous_hash = bloc_m.hash*** ; ce qui justifie la notion de blocs chaînés « en retour ». Mais il peut arriver qu'il y ait des chaînes de blocs orphelines (chaînes secondaires). Dans ce cas, la chaîne principale est composée de la plus longue suite de blocs après le bloc initial (ou bloc de genèse).

En générale, les facts sont organisés de manière séquentielle, de la plus ancienne à la plus récente, et peuvent être des transactions monétaires, des données médicales, des informations industrielles, des logs systèmes, etc. [14] .

La logique de chaînage des blocs peut être décrite comme suit :

Soient B_0, B_1, B_2, les blocs représentant respectivement les bloc n, bloc m et bloc k de la figure 4 ci-dessus ; où B_0 est supposé bloc de genèse, B_1 le bloc fils de B_0 et B_2 le petit fils de B_0 et fils de B_1.

Chaque bloc de la chaine est identifié de manière unique par un hash généré à l'aide d'un algorithme (SHA-256, Ethash, ...) de hachage cryptographique. Par exemple, la donnée (ou le texte) d'entrée α = ***Exemple de hash d'un bloc dans une chaine de blocs*** a comme valeur de hash SHA-256, la sortie β = ***9bd4e3e89d144d8b8849736a6e5c60e1ec122da45d55bc5eaebdb2e8edf2f20c***. Et la moindre modification de α engendre obligatoirement un changement de β. Chaque bloc fait référence au bloc précédant à travers le hash de celui-ci. En effet, le hash de B_0 est référencé (ou inscrit comme previous_hash) dans l'entête de B_1 et celui de B_1 dans l'entête de B_2, formant ainsi une chaîne.

Dans une chaîne donnée, si l'identité du bloc de genèse ou d'un bloc parent change, l'identité des blocs enfants changera obligatoirement. Autrement dit, si un utilisateur modifie B_0, cette modification entrainera un changement du hash de B_0. Ce changement du hash de B_0 imposera un changement du pointeur « previous_hash » dans B_1 ; ce qui entraînera un changement du hash de B_1, qui, à son tour changera le hash de B_2, et ainsi de suite. De ce fait, cette opération de cascade implique le recalcul des hash de tous les blocs suivants dès qu'un bloc parent (ayant plusieurs descendants) viendrait à être modifier. Et plus la chaîne de blocs est longue, plus le recalcul devient énorme et coûteux, et plus l'historique (horodatage via la clé **timestamp** ou **time** du header) devient profond. Ceci explique le caractère immuable de la blockchain.

En sus de cette structuration, comment fonctionne la technologie blockchain ?

3.1.3.2. Fonctionnement de la blockchain

Le mécanisme global de fonctionnement de la blockchain passe par l'initiation d'une transaction, la validation de bloc via un consensus, et l'ajout du bloc validé à la chaîne précédente. Dans [14] , *Oussama* fait une présentation de ce mécanisme sur laquelle nous nous appuyons ici à travers la figure 5 ci-dessous.

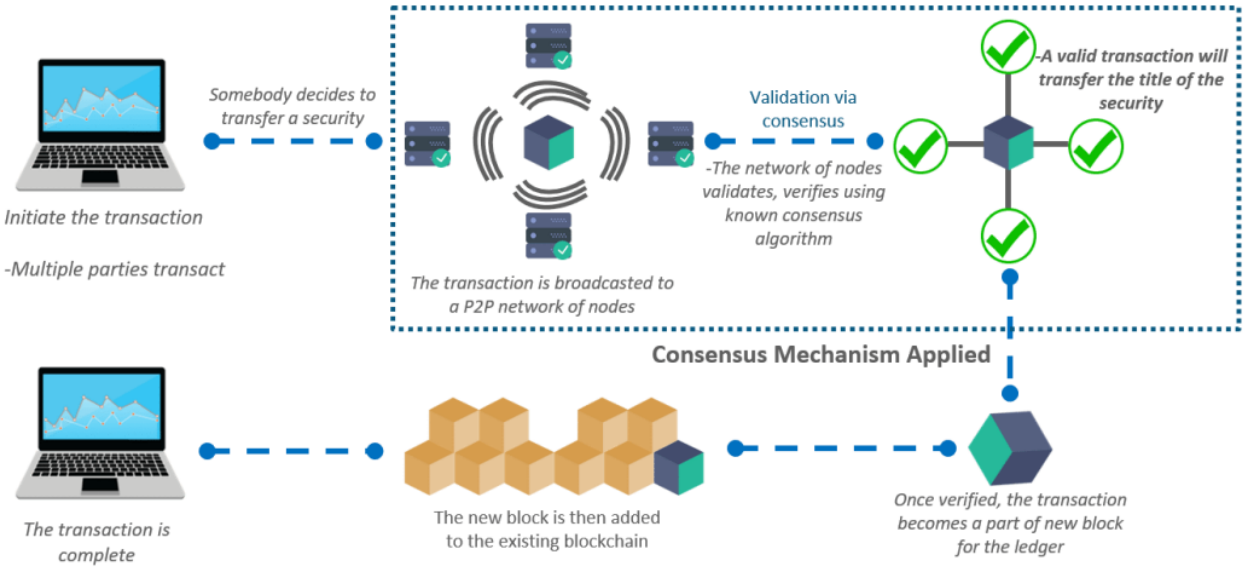


Figure 5 : *Mécanisme de fonctionnement global de la blockchain [14]*

En effet, le mécanisme de fonctionnement est résumé en six (6) étapes à savoir :

1- Un utilisateur de la blockchain initie une transaction ***Tx***.

2- *Tx* est publiée (ou diffusée) sur le réseau de blockchain.

3- Les mineurs (ordinateur doté de grosses capacités de traitement ou intervenants actifs du réseau) entrent en compétition et valident *Tx*. Dans ce cas, une empreinte digitale appelée « hash » est générée par application d'une fonction irréversible (ou algorithmes) de hachage.

4- Si *Tx* est validée, elle est vérifiée puis ajoutée à d'autres transactions dans un bloc en construction. Ce processus permet de garantir que toutes les transactions sont légitimes. Légitimes pour indiquer que les transactions sont authentiques, valides (respect des tailles du bloc), non falsifiées, et acceptées par le réseau

5- Après ce mécanisme de consensus, le bloc, désormais construit, est ajouté à la chaîne de blocs précédents (blockchain existante). Avant qu'un bloc ne soit ajouté à la chaîne existante, il est diffusé à tous les nœuds du réseau blockchain, suivi de l'acceptation de sa validité par ceux-ci. Ce bloc devient alors sécurisé et inaltérable. Cependant, si un bloc n'est pas entièrement validé, il ne peut pas être ajouté à la chaîne. Concernant les mécanismes de consensus, les plus populaires et les plus utilisés sont le Proof of Work (PoW) ou le Proof of Stake (PoS) [13] .

6- Ainsi, *Tx* est confirmée et considérée comme effectuée avec succès.

La figure présentée dans la section « ANNEXE 2 », permet de suivre l'itinéraire d'une transaction initiée dans un réseau de blockchain.

La technologie blockchain a assurément un potentiel considérable, mais il convient de se questionner sur les cas d'utilisation et les méthodes d'application de cette technologie en matière d'authentification et/ou de sécurisation de documents.

2.1 Blockchain et authentification de documents : travaux existants

Il existe plusieurs techniques d'utilisation de la blockchain dans les processus de sécurisation et d'authentification de documents numériques. Dans cette partie du présent mémoire, nous présentons quelques travaux existants y relatifs.

Cas 1 : Cadre d'authentification des documents électroniques à l'aide de la technologie Blockchain dans le système gouvernemental (*Isyak Meirobie et al.)*

Titre d'origine : *« Framework Authentication e-document using Blockchain Technology on the Government system ».*

Dans [15], *Isyak Meirobie et al.* ont présenté le résultat de leurs recherches qui ont conduit à la mise en place d'une plateforme d'authentification des documents électroniques à l'aide de la technologie Blockchain dans le système gouvernemental d'Indonésie. Les problèmes ayant suscités ces recherches sont le manque de sécurité dans le stockage de toutes les données des documents, les redondances profondes de données et la présence de tierces parties qui interfèrent dans les transmissions de documents. Afin de minimiser la falsification des documents et de maximiser les documents électroniques du gouvernement d'une manière moderne et sécurisée, la méthode a été de combiner la blockchain, des smarts contracts (contrats intelligents) et des Decentralized Autonomous Organization (DAO ou type de plus complexe des smarts contracts).

En effet, les gouvernements pourraient charger un ensemble de données et de documents sur une blockchain publique (sans nécessiter d'autorisation) et utiliser des signatures pour signer les transactions. Les signatures sont librement accessibles via le site web de l'institut. Et chaque gouvernement qui souhaite confirmer l'authenticité d'un document via la blockchain peut s'en assurer grâce à sa transcription numérique, tout en vérifiant que la transaction qui l'intègre à la blockchain est signée par le gouvernement lui-même. Au lieu de stocker toutes les données complètes sur la blockchain, seul le hachage de la signature SHA256 des données est stocké. Cela élimine la nécessité d'un stockage massif tout en garantissant l'intégrité et la vérification de toutes les données. La blockchain publique utilisée est sans licence, basée le processus de consensus PoA.

Concrètement, les auteurs de cette étude ont mis en place une interface utilisateur simple dénommé Go-Chain (Government Blockchain). Go-Chain est construit en 3 couches essentielles à savoir la couche de vérification, la couche des services de logique métier, et la couche d'accès/persistance de données. En amont, les documents (pdf ou word) gouvernementaux peuvent être téléversés, signés (via clé privée), transcrits numériquement en json et stockés (après calcul de la racine de Merkle) sur la blockchain. La transcription sous forme json peut être distribué au public. En retour, le public peut présenter le document haché à toute entreprise ou institution comme preuve valable. Mais, pour tout de même vérifier la validité ou l'authenticité d'un document via la blockchain, le public peut téléverser le document numérique gouvernemental dans Go-Chain, en y saisissant une clé privée. Après recalcule de la racine de Merkle, le cadre compare cette racine recalculée avec la racine de Merkle auparavant stockée sur la blockchain et signale si elle a été signée par une institution légitime. Pour la signature, l'auteur a utilisé un Digital Signature Algorithm (DSA) avec une courbe P-256. Et lorsque le document chargé par le public est valide, la clé publique, l'empreinte digitale SHA265 et d'autres données apparaissent sur l'écran de vérification Go-Chain.

En termes d'outils et de technologies, les auteurs ont utilisé HTML5, CSS3, JavaScript (ES6), Python 3, le microframework Flask et des serveurs HTTP.

<u>Cas 2</u> : La Blockchain pour la Sécurisation des E-livrets scolaires (*Ana BAKHOUM*)

Ana BAKHOUM [1] a proposé, au profit du système d'enseignement moyen et secondaire du Sénégal, la dématérialisation du livret scolaire (d'où le E-livret). Le livret scolaire est un document administratif au format papier qui permet de répertorier les notes des élèves de la classe de sixième à la classe de terminal. Le même livret scolaire est transféré dans chaque établissement d'enseignements fréquenté par l'élève. Cette dématérialisation a constitué à la mise en place d'un système de recueil et de stockage (dans une base de données relationnelle MySQL hébergée par un serveur) des informations qui étaient dans le livret en papier. Dans cette dynamique, la problématique majeure traitée par l'auteur est comment assurer la fiabilité, l'authenticité, la transparence et la sécurité des E-livrets ? quelle architecture idéale, quel type de stockage utilisé ?

Dans ses travaux en lien avec cette problématique, l'auteur a fait une revue de littérature sur la technologie blockchain en générale et la blockchain Ethereum en particulier. Il a aussi passé en revue, la question de la sécurité informatique et celle notamment appliquée à la technologie

blockchain. De ce qui est de la sécurité informatique en générale, il s'agit des obligations d'authentification, d'intégrité, de confidentialité, de disponibilité et de non-répudiation. Celle-ci pourrait faire face partiellement aux vulnérabilités, menaces, risques et attaques dans la blockchain. Car dans la pratique, il existe de multiples attaques qui manipulent directement ou indirectement le mécanisme de récompense (des mineurs), donnant ainsi d'injustes avantages aux mineurs de plus grandes tailles aux détriment des petits mineurs.

Selon les standards de la norme ISO/TC 307 [16], plusieurs propriétés de sécurité sont intégrées dans la blockchain, notamment dans les applications basées sur les Distributed Ledger Technologies (DLT). Ce sont entre autres les propriétés :

- d'intégrité qui assure la protection de données contre toute modification après création ;
- d'authenticité qui permet de vérifier, qui enregistre une transaction dans le registre ;
- de confidentialité qui garantit que le registre est uniquement consultable par ceux qui y sont autorisés ;
- de disponibilité qui permet d'assurer la disponibilité à tout moment de toute transaction déjà enregistrée ;
- d'ordonnancement des événements rendant impossible le changement d'ordre des enregistrements dans le registre avec l'horodatage ;
- de « trusted-server less » permettant à la blockchain de toujours fonctionner malgré l'absence de serveur de confiance ;
- etc.

Dans la même logique, des mécanismes de sécurité ont été intégrés dans la blockchain tels que la cryptographie (surtout asymétrique), la signature numérique, le hachage.

L'étude a, à terme, permis de mettre en place un système décentralisé de sécurisation des E-livrets scolaires (SDSEL) en s'appuyant sur la technologie Blockchain, particulièrement sur Ethereum. Outre leur sécurisation, le SDSEL permet de valider ou de vérifier les E-livrets scolaires des élèves. La démarche a été de :

- développer le système (déjà existant et utilisé dans l'étude) de gestion des livrets électroniques (SGLE) qui permet de saisir et traiter, des informations des livrets scolaires à savoir les établissements, les élèves, les notes, les appréciations du conseil, etc.

- développer l'application décentralisée (Dapp) dénommé « SDSEL » pour la sauvegarde des E-livrets dans la blockchain ;
- importer les informations des E-livrets depuis la base de données du SGLE vers la Blockchain des E-livrets ;
- consulter les listes et statistiques des élèves et leur livret ; cela permet de vérifier la conformité avec le livret généré par le SGLE ;
- développer (en perspective de l'étude) les contrats qui permettront à l'office du bac de générer automatiquement la liste des élèves inscrits en terminale qui servira à l'organisation de l'examen de baccalauréat ;
- déployer (en perspective de l'étude) le SDSEL dans la blockchain publique Ethereum afin qu'elle soit accessible par tous les établissements d'enseignements.

En termes d'outils et de technologies pour la mise en place du Dapp SDSEL, l'auteur a utilisé l'API JavaScript Web3, l'API JSON RPC, le langage de programmation Solidity, l'IDE Remix-IDE, le framework Truffle Framework qui intègre GANACHE, les frameworks Angular et Spring.

En s'appuyant sur ces études précédentes et en tenant compte des différents contextes, voyons si la blockchain est-elle plus indiquée pour résoudre la problématique de sécurisation et d'authentification de documents administratifs.

2.2 Discussion

Après analyse de la synthèse des travaux réalisés par *Ana BAKHOUM* et les co-auteurs *Isyak Meirobie et al.*, nous décelons quelques points communs.

En effet, ces auteurs ont utilisé une **blockchain publique** dans le cadre de leurs travaux. Par ailleurs, si *Isyak Meirobie et al.* n'ont pas, dans leur synthèse, mentionné explicitement laquelle des blockchains publiques qu'ils ont expérimenté, *Ana BAKHOUM* a, quant à elle, utilisé Ethereum.

Aussi, les deux (02) acteurs ont utilisé la notion de **contrat intelligent**. Des contrats intelligents ont été développés afin d'automatiser des traitements sur la blockchain. Il s'agit par exemple de :

- la transcription numérique de documents, le hachage, la signature numérique et le stockage des données dans la blockchain ;
- l'importation et le stockage des E-livrets dans la blockchain ;

- la vérification de l'authenticité des E-livrets et documents gouvernementaux depuis la blockchain ;
- etc.

Cela dénote de l'utilisation des propriétés de stockage décentralisé et de transparence (fiabilité) et d'intégrité de la technologie blockchain.

De plus, [1] et [15] ont travaillé sur des **documents électroniques,** même s'il s'agit de différents types de documents. Ramenant à notre sujet du présent mémoire, cela pourrait être intéressant dans la mesure où l'Administration utilise couramment des documents électroniques ; sachant qu'un document est dit électronique, s'il est créé directement au format numérique (sans lien direct avec un support physique) ou converti (numérisé).

En outre, dans les différentes solutions mises en place, toutes les données sujettes à authentification et devant être sécurisées **ne sont pas entièrement stockées** sur la blockchain, évitant ainsi les stockages massifs.

Hormis ces points communs, quelques applications suscitent des réflexions d'ordre technique et juridique. En effet, comment opérer le choix du processus de consensus qui puisse cadrer avec le type de blockchain adopté ([15] a utilisé le PoA) ? relativement au contexte de notre présent projet, le cadre juridique national permet-il d'exploiter des signatures numériques et/ou électroniques de documents administratifs ? stocker des informations issues de documents administratifs dans la blockchain (même hachées et/ou cryptées) ne met-il pas en cause la souveraineté de l'Etat ? afin d'assurer la sécurité et l'intégrité du réseau de blockchain, il y a des coûts connexes liés entre autres aux minages des transactions blockchain. En adoptant une blockchain publique pour solutionner la sécurisation et l'authentification de documents administratifs, l'Administration supportera-t-elle ces coûts de façon pérenne ?

En tout état de cause, l'adoption de la blockchain nous semble appropriée pour la résolution de notre problématique. Dans le chapitre suivant, nous présentons, en tenant compte de ce qui précède, notre approche qui permet d'authentifier un type spécifique de document administratif.

CHAPITRE 4 :

APPROCHE

CHAPITRE 4 : APPROCHE

Je liste les étapes (peut-être en sous points) pour la réalisation. Là je fixe le type de document administratif sur lequel nous travaillons.

CHAPITRE 5 :

IMPLÉMENTATION DE L'APPROCHE

CHAPITRE 5 : IMPLÉMENTATION DE L'APPROCHE

5.1 Environnement de développement

5.2 Déroulement de notre approche

Je présente les éléments de conception, et liste les étapes de l'approche suivies.

5.3 Présentation de l'outil

CONCLUSION ET PERSPECTIVES

CONCLUSION ET PERSPECTIVES

RÉFÉRENCES

[1] Ana BAKHOUM, "*La Blockchain pour la Sécurisation des E-livrets scolaires.*", *2019.* Disponible sur https://rivieresdusud.uasz.sn/handle/123456789/1803. [Consulté le : 10-sept-2024].

[2] GODEBARGE Ferréol, ROSSAT Romain, "*Principes clés d'une application blockchain*", *2016.*

[3] Stuart Haber et W. Scott Stornetta, "*How To Time-Stamp a Digital Document", 1990.* Disponible sur https://link.springer.com/article/10.1007/BF00196791. [Consulté le : 17-sept-2024].

[4] Dave Bayer, Stuart Haber et W. Scott Stornetta, "*Improving the Efficiency and Reliability of Digital Time-Stamping*", *1992.* Disponible sur https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24. [Consulté le : 17-sept-2024].

[5] Le Monde.fr, "*La première blockchain de l'histoire date de 1995, et elle est imprimée sur papier*", *1er sept.2018.* Disponible sur https://archive.wikiwix.com/cache/index2.php?url=https%3A%2F%2Fwww.lemonde.fr%2Fbig-browser%2Farticle%2F2018%2F09%2F01%2Fla-premiere-blockchain-de-l-histoire-date-de-1995-et-elle-est-imprimee-sur-papier_5349082_4832693.html#federation=archive.wikiwix.com&tab=url. [Consulté le : 17-sept-2024].

[6] Ramesh Subramanian et Theo Chino, "*The State of Cryptocurrencies, Their Issues and Policy Interactions*", Journal of International Technology and Information Management: Vol. 24: N°3, Article 2, *2015*. Disponible sur https://scholarworks.lib.csusb.edu/jitim/vol24/iss3/2/. [Consulté le : 18-sept-2024].

[7] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", p. 9. Disponible sur https://bitcoin.org/bitcoin.pdf. [Consulté le : 19-sept-2024].

[8] Wikipédia, "*Blockchain*", *22 août 2024.* Disponible sur https://fr.wikipedia.org/wiki/Blockchain#Histoire. [Consulté le : 19-sept-2024].

[9] Imran Bashir, "*Mastering Blockchain*", *mars 2017.* Disponible sur https://books.google.bf/books?hl=fr&lr&id=urkrDwAAQBAJ&oi=fnd&pg=PP1&dq=blockchain&ots=Ixal3edv1P&sig=Wvsy1GIGQmEXu1191tT78WpzlP8&redir_esc=y&pli=1#v=onepage&q=blockchain&f=false. [Consulté le : 28-sept-2024].

[10] Cryptoast.fr, "*Blockchain publique et blockchain privée : quelles différences ?* ", *juin 2023.* Disponible sur https://cryptoast.fr/differences-blockchain-publique-blockchain-privee/. [Consulté le : 29-sept-2024].

[11] 101Blockchains, "*Blockchain Consortium: Top 20 Consortia You Should Check Out*", *février 2021*. Disponible sur https://101blockchains.com/blockchain-consortium/. [Consulté le : 02-oct-2024].

[12] Adam Back et al., "*Enabling Blockchain Innovations with Pegged Sidechains*", *octobre 2014, 25 pages*. Disponible sur https://blockstream.com/sidechains.pdf. [Consulté le : 02-oct-2024].

[13] W3R.ONE MAGAZINE, "*Éléments Fondamentaux d'un Bloc dans la Blockchain*", *09 février 2024*. Disponible sur https://w3r.one/fr/blog/blockchain-web3/architecture-blockchain/conception-de-blocs/elements-fondamentaux-bloc-blockchain. [Consulté le : 21-oct-2024].

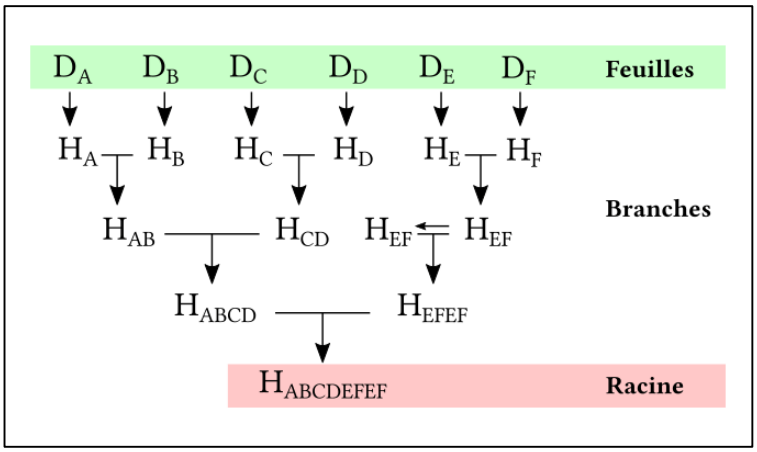
[14] Oussama Abderraouf Ayadi, "*CHAPITRE III : État de l'art de la Blockchain*", *juillet 2019, 45 pages*. Disponible sur https://www.researchgate.net/publication/335174496_CHAPITRE_III_Etat_de_l%27art_de_la_Blockchain. [Consulté le : 21-oct-2024].

[15] Isyak Meirobie et al., "*Framework Authentication e-document using Blockchain Technology on the Government system*", International Journal of Artificial Intelegence Research, Vol 6, N° 2,

Décembre 2022, 12 pages. Disponible sur http://ijair.id/index.php/ijair/article/view/294/pdf. [Consulté le : 31-oct-2024].
[16] ISO, "*Standards by ISO/TC 307 Blockchain and distributed ledger technologies*". Disponible sur https://www.iso.org/committee/6266604/x/catalogue/p/1/u/1/w/0/d/0.
[17] Larousse, "*Concensus*" sur https://www.larousse.fr/dictionnaires/francais/consensus/18357. [Consulté le : 15-sept-2024].
[18] crypto.com | university, "*Qu'est-ce que le consensus ? Guide du débutant*". Disponible sur https://crypto.com/fr/university/consensus-mechanisms-explained. [Consulté le : 15-sept-2024].
[19] Bit2Me Academy, "*Qu'est-ce qu'un arbre Merkle ?",* avril 2023. Disponible sur https://academy.bit2me.com/fr/que-es-un-arbol-merkle/. [Consulté le : 18-dec-2024].
[20] L'internaute, "*Concensus*". Disponible sur https://www.linternaute.fr/dictionnaire/fr/definition/consensus/#faq. [Consulté le : 15-sept-2024].
[21] Université Joseph KI-ZERBO, https://www.ujkz.bf/.

ANNEXES

Annexe 1 : exemple d'arbre de Merkle dans Bitcoin



Source : https://cryptoast.fr/wp-content/uploads/2020/08/merkle-tree-general.png

Annexe 2 : circuit d'une transaction