**Définition des mots ou concepts clés**

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.

**Document administratif** : 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*](https://www.csc.bf/index.php/textes-de-reference/lois/item/76-loi-051-portant-sur-l-acces-a-l-information-publique), 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.

**Choix de document administratif pour le taf** :

**Consensus** : selon *Larousse* (<https://www.larousse.fr/dictionnaires/francais/consensus/18357>, consultée le 15-sept-2024), le consensus 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. Dit autrement par *L’internaute* (<https://www.linternaute.fr/dictionnaire/fr/definition/consensus/#faq>, consultée le 15-sept-2024), 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.

**Blockchain** : selon *Wikipédia* (<https://fr.wikipedia.org/wiki/Blockchain>, consultée le 15-sept-2024) c'est une [base de données distribuée](https://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es_distribu%C3%A9e), 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 », lesquels forment ainsi une chaîne de plus en plus longue. L'ensemble est sécurisé par [cryptographie](https://fr.wikipedia.org/wiki/Cryptographie). Par extension, une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements théoriquement protégés contre la [falsification](https://fr.wikipedia.org/wiki/Int%C3%A9grit%C3%A9_(cryptographie)) ou la modification par les [nœuds](https://fr.wikipedia.org/wiki/N%C5%93ud_(r%C3%A9seau)) de stockage ; c'est donc un [registre distribué](https://fr.wikipedia.org/wiki/Registre_distribu%C3%A9) et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti.

**Arbre de Merkle** ou **Arbre de Hachage** : est « une structure de données contenant un résumé d'information d'un volume de données, généralement grand (comme un fichier) » selon *Wikipédia*.

**Hash :** fonction mathématique qui permet d’obtenir une empreinte numérique unique par donnée d’entrée (fichier, texte, …).

**Mineur :** intervenants (ordinateur ou nœud) actifs du réseau qui sélectionnent des transactions et participent à leur validation.

**Travaux existants**

* Au Burkina Faso, le ministère en charge de la fonction publique a procédé, courant juillet 2019, au contrôle de l’authenticité des diplômes des agents publics de l’Etat afin d'identifier les faux diplômes. « *… il s’est agi de mettre en place une équipe d’informaticiens de la fonction publique pour la conception de l’application et de la base de données des diplômes.*», « *Dans un second temps, pour les cas où la vérification ne pouvait pas se faire électroniquement, on a procédé à une vérification physique directement auprès des structures en charge de la délivrance des diplômes. Cela a consisté à mettre en place des équipes de vérificateurs qui, en collaboration avec les services techniques des structures en charge de la délivrance des diplômes procèdent à des vérifications manuelles dans les registres de diplômes.* » ***Source*** *(consultée le 15-sept-2024)* : [*https://www.fonction-publique.gov.bf/accueil/actualites/details?tx\_news\_pi1%5Baction%5D=detail&tx\_news\_pi1%5Bcontroller%5D=News&tx\_news\_pi1%5Bnews%5D=302&cHash=6537be50278b68292c73ccb2aee3a155*](https://www.fonction-publique.gov.bf/accueil/actualites/details?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=302&cHash=6537be50278b68292c73ccb2aee3a155)
* A l’Université Joseph KI-ZERBO du Burkina Faso, l’authentification des diplômes peut être demandée sur le site officiel de l’université à savoir <https://www.ujkz.bf/authentification-de-diplomes/>.

**Eléments de justification :**

* 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*». Link\_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 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 6 Octobre 2023, le Ministère des Affaires Etrangères du Burkina Faso à travers la DRCP/MAECR-BE a publié sur sa page Facebook en ces termes “*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) a 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>.

1. **État de l'art sur la sécurisation des documents administratifs avec la blockchain**

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 de 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.

Mais 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.

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 disparaît progressivement au profit de ce qu’il convient d’appeler « Blockchain ».

Cette section 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 existant sur la sécurisation des documents administratifs avec la blockchain.

* 1. **Les généralités sur la Blockchain**

Dans cette partie, nous faisons l’historique de la technologie blockchain. Nous y donnons des définitions de celle-ci.

* + 1. **Les 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 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], il ressort que selon le chercheur *Ittai Abraham* affirme en ces termes : “*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 ».

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).

Comment peut-on définir formellement la blockchain ?

* + 1. **Les définitions de la 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. Dans notre contexte, l’algorithme de consensus (il en existe plusieurs types) n’est rien d’autre qu’un mécanisme sécurisé par lequel tous les nœuds du réseau blockchain parviennent à un accord unanime sur le contenu des données qui y sont inscrites. 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.

Tous 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].

Après avoir exploré la signification fondamentale de la blockchain, il est essentiel de comprendre les différentes formes qu'elle peut prendre.

* 1. **Les 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 :

* 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 application 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 sont des exemples de blockchains publiques [10].

**Les blockchains privées**

Les blockchains privées ne sont pas ouvertes au public. Elles sont exclusivement accessibles sur invitation. Tous les membres participants de ce réseau blockchain 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. Par exemple, cette approche est plus appropriée lorsque plusieurs succursales d’une même entreprise (organisation) décident de l’utiliser pour se partager directement des informations. Aussi appelées blockchains permissionnées ou blockchains à autorisation, Hyperledger et Ripple sont des exemples de blockchain privée fréquemment cités **Erreur ! Source du renvoi introuvable.**.

**Les blockchains semi-privées**

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

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, 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 permet de garantir la sécurité des transactions restent quasiment les même.

* 1. **La structure et le fonctionnement de la blockchain**
     1. **La 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 en ensemble d’ordinateurs appelés nœuds qui partage 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 1 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 1** : 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*](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] :

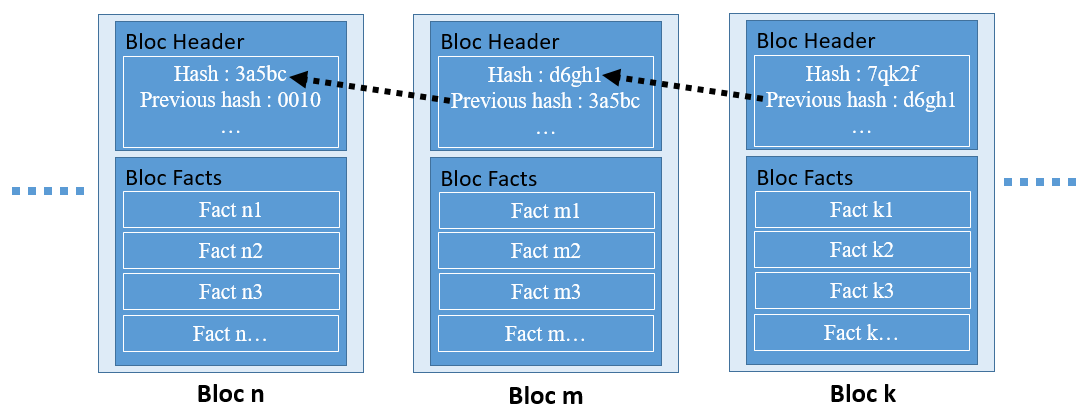
* **la version** qui indique le protocole de validation des règles ;
* **le hash du bloc précédent** qui assure liaison entre les blocs afin de constitué la chaine ;
* **le hash de la racine de Merkle** qui synthétise les informations que renferment toutes les transactions du bloc ;
* **le timestamp (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 2.



**Figure 2** : 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 3 présente un exemple simplifié de blocs.



**Figure 3** : 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 B0, B1, B2 les blocs représentant respectivement les bloc n, bloc m et bloc k de la figure 3, où B0 est le bloc de genèse, B1 le bloc fils de B0 et B2 le petit fils de B0 et fils de B1.

Chaque bloc de la chaine est identifié de manière unique par un hash généré à l’aide d’un algorithme (SHA256, Ethash, ...) de hachage cryptographique. Par exemple, la donnée (ou le texte) α = ***Exemple de hash d'un bloc dans une chaine de blocs*** a comme valeur de hash SHA-256, 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. En effet, le hash de B0 est référencé (ou inscrit comme previous\_hash) dans l’entête de B1 et celui de B1 dans l’entête de B2, 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 B0, cette modification entrainera un changement du hash de B0. Ce changement du hash de B0 nécessitera un changement du pointeur « previous\_hash » dans B1; ce qui entraînera un changement du hash de B1, qui, à son tour changera le hash de B2, 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) devient profond. Ceci explique le caractère immuable de la blockchain.

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

* + 1. **Le 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. En effet, le mécanisme de fonctionnement schématisé sur la figure 4 ci-dessous illustre 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.
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, 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.



**Figure 4** : Mécanisme de fonctionnement global de la blockchain [14]

La figure 1 **circuitTransaction.png** de la section « ANNEXE », permet de suivre l’itinéraire d’une transaction initiée dans un réseau de blockchain.

La technologie blockchain a certainement un potentiel illimité, mais nous essayons de présenter dans la partie suivante, ce à quoi elle pourrait servir.

* 1. **Les domaines d’applications de la blockchain (PAS PERTINENT)**

La blockchain offre beaucoup d’opportunités dans différents domaines d’application.

* 1. **L’application de la blockchain dans les processus d’authentification de documents**

Il existe plusieurs techniques d’utilisation de la blockchain dans les processus de sécurisation et d’authentification de documents électroniques. 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.)***

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 rendre plus modernes et sécurisés les documents électroniques du gouvernement, 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 (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.

**Cas 2 : 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 ;
* 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 avec 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.

**Discussion**

cas 1 :

Oui le problème semble résolu par l’auteur. Mais des questions demeurent :

Comment utiliser un processus de consensus PoA dans une blockchain publique (Etherneum par exemple) sans licence (sans nécessiter d'autorisation) ?

Le PoA repose sur un ensemble restreint de validateurs connus et approuvés, ce qui le rend typiquement adapté aux blockchains privées ou permissionnées. Cependant, il est théoriquement possible d'utiliser un processus de consensus PoA dans une blockchain publique comme Ethereum, sans licence ni permission explicite, en modifiant certains aspects de la gouvernance et de la sélection des validateurs.

Dans « Framework Authentication e-document using Blockchain Technology on the Government system » de Isyak Meirobie et al., laquelle des blockchains publiques a-t-elle été utilisée pour implémenter la solution Go-Chain ?

L'article ne précise pas quelle blockchain publique a été utilisée pour implémenter cette solution.

Comment se fait la transcription du contenu d'un fichier pdf ou word uploadé en un fichier sous forme json ?

Résolu techniquement.

Comment signe-t-on numériquement (signature numérique) un document numérique ?

La signature numérique d'un document numérique repose sur des technologies cryptographiques permettant de garantir l'intégrité, l'authenticité et l'origine du document.

Le contenu du document est passé par une fonction de hachage cryptographique (SHA-256, par exemple), qui génère un "empreinte numérique" unique et fixe. Ensuite, l'empreinte est chiffrée avec la clé privée du signataire, créant la signature numérique qui est rajoutée au document. Donc signature numérique = empreinte numérique chiffré via clé privée = hash chiffré.

Qu'est-ce que signer une transcription numérique ou document numérique en utilisant un Digital Signature Algorithm (DSA) avec Courbe P-256 ? comment le faire ?

La courbe P-256 (**secp256r1**) est une courbe elliptique standard utilisée pour les signatures numériques et la cryptographie à clé publique. Les étapes de signature sont :

1. **Générer une clé privée et publique sur la courbe elliptique P-256**.
2. **Créer un hash du document numérique**.
3. **Signer le hash avec la clé privée**.
4. **Distribuer la clé publique avec la signature**.

Dans le contexte burkinabè, le cadre juridique général permet-il d’exploiter des signatures numériques et/ou électroniques ?

Non pour l’instant à notre connaissance.

Lors du calcul de la racine de Merkle, comment choisir la parité des branches a haché ?

Chaque niveau de l’arbre doit avoir un nombre pair de hash. L’ordre des transactions à apparier dépend de plusieurs critères (frais plus élevé au profit du mineur, efficacité dans l’occupation d’espace du bloc pour améliorer le minage, protocole réseau ou conventions, …). L’horodatage n’est pas fiable pour ordonner les transactions.

Différence entre document numérique et document électronique ?

|  |  |  |
| --- | --- | --- |
| **Critères** | **Document numérique** | **Document électronique** |
| **Origine** | Créé directement au format numérique, sans lien direct avec un support physique. | Peut être créé au format numérique ou converti (numérisé). |
| **Support** | Pas forcément associé à un support particulier (PDF, Word, image, base de données, etc.) | Repose sur un support électronique spécifique(disque, serveur, clé usb, …) |
| **Utilisation courante** | Informatique, multimédia | Administration, archivage, juridique |

Cas 2 :

Est-ce que stoker les infos de l’administration dans la blockchain ne met pas en cause la souveraineté de l’Etat ?

En utilisant la blockchain Ethereum, il y a des coûts connexes liés aux minages (afin d’assurer la sécurité et l’intégrité du réseau). L’administration supportera-t-elle ces coûts de façon pérenne ?

Le problème de décentralisation des données …

**METHODES D’AUTHENTIFICATION DE DOCUMENTS**

|  |  |  |
| --- | --- | --- |
| **Méthodes et principes** | **Technologies & Protocoles** | **Références** |
| **Signature numérique** (Digital Signature)  Une signature numérique est générée en appliquant un **algorithme cryptographique** (ex : RSA, ECDSA) sur l’empreinte (hash) du document à l’aide d’une **clé privée**. Le destinataire peut ensuite vérifier l’authenticité du document en **décryptant** la signature avec la **clé publique** de l’émetteur.  **Bon pour un document juridique ou administratif** | * **PKI (Infrastructure à Clé Publique)** : Utilise des certificats numériques (X.509). * **Algorithmes :** RSA, DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), EdDSA. * **Formats supportés :** PDF (Adobe Sign), Word (Office Digital Signature).   **Exemple d’outils :**   * OpenSSL * Adobe Acrobat * Microsoft Office * Let's Encrypt | <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>  <https://helpx.adobe.com/fr/acrobat/using/validating-digital-signatures.html>  <https://fr.wikipedia.org/wiki/Signature_num%C3%A9rique>  **La signature numérique** (ou signature électronique) est un moyen sécurisé qui permet d'authentifier l'auteur d'un document électronique et de garantir l'intégrité dudit document [45]. Elle permet ainsi d'assurer la non-répudiation c’est à dire, la quasi impossibilité de remettre en cause le document. De façon opérationnelle, l'émetteur (ou auteur), à l'aide de sa clé privée, génère d’abord la signature en appliquant l'algorithme cryptographique à clé publique (RSA, ECDSA, etc.) sur l'empreinte du document. L’empreinte signée est ensuite envoyée avec les données originales au destinataire. Ainsi, le destinataire peut vérifier l’authenticité du document en décryptant les données signées avec la clé publique de l’émetteur et en les comparant à la valeur de hachage des données originales (en utilisant le même algorithme de hachage). Pour ce faire, une PKI (Infrastructure à Clé Publique) est aussi souvent utilisée pour la gestion des certificats numériques. [46] Une signature numérique doit nécessairement remplir les conditions suivantes :   * authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine ; * infalsifiable : une personne ne peut pas se faire passer pour un autre. La signature ne peut pas être falsifiée ; * non réutilisable : la signature fait partie du document signé et ne peut être déplacée sur un autre document ; * inaltérable : une fois que le document est signé, on ne peut plus le modifier ; * irrévocable : la personne qui a signé ne peut le contester.   La technique de signature numérique est bien adaptée pour signer rapidement et facilement les documents électroniques administratifs et juridiques depuis n’importe où |
| **Hachage & Empreinte numérique** (Document Hashing)  Un algorithme de hachage (ex : SHA-256, SHA-3) est appliqué sur un document pour générer une **empreinte unique**. Toute modification du document entraîne un changement de cette empreinte, permettant de vérifier son intégrité. | 🔹 **Limite :**   * Ne prouve pas l’identité de l’auteur, mais seulement l’intégrité du document. * Utilisé en complément avec une signature numérique.   🔹 **Exemple d’outils :**   * OpenSSL (openssl dgst -sha256 fichier.pdf) * SHA256sum (sha256sum fichier.pdf) | <https://www.ionos.fr/digitalguide/sites-internet/developpement-web/hachage/>  <https://www.cnil.fr/fr/securite-chiffrement-hachage-signature>  <https://fr.wikipedia.org/wiki/Fonction_de_hachage_cryptographique> |
| **Horodatage électronique** (Timestamping)  Un **tiers de confiance (TSA - Time Stamping Authority)** applique une signature horodatée sur l’empreinte du document. Cela permet de **prouver qu’un document existait à une date donnée** et qu’il n’a pas été modifié.  **Bon pour un document juridique ou administratif** |  RFC 3161 (protocole standard d’horodatage).   Services d’horodatage qualifiés (ex : DigiCert, GlobalSign).   Blockchain (voir section 5).  **Exemple d’outils :**   * OpenTSA * Adobe Timestamp Server * Chronos (service d’horodatage basé sur Ethereum) | <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>  <https://www.docusign.com/fr-fr/blog/authentification-et-verification-de-la-signature-electronique> |
| **Filigrane numérique et tatouage électronique** (Digital Watermarking)   Ajout d’un **filigrane visible ou invisible** pour identifier l’auteur et protéger le document contre la falsification.   Utilisé pour **les images, vidéos et documents PDF**.  **Bon pour protéger un contenu multimédia** |  **Watermarking** invisible avec encodage dans les métadonnées du fichier.   **Tatouage numérique** (ex : utilisé pour lutter contre la fraude documentaire).  **Exemple d’outils :**   * Digimarc * iText (ajout de filigrane sur PDF avec Java). | <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>  <https://helpx.adobe.com/fr/acrobat/using/validating-digital-signatures.html> |
| **Blockchain & Preuve d’existence**  Les empreintes numériques des documents peuvent être stockées **dans une blockchain** pour assurer une authentification **décentralisée et inaltérable**.  **Bon pour un document dont l’intégrité doit être vérifiable publiquement** | **Avantages :**  ✅ Preuve immuable et horodatée. ✅ Vérification publique sans autorité centrale.  **Exemples de plateformes :**   * **Ethereum & Smart Contracts** (Stocker un hash de document avec une signature). * **Bitcoin OP\_RETURN** (Inscription d’un hash de document dans la blockchain). * **Services dédiés :**   + **Stampd.io**   + **OriginStamp**   + **Blockcerts (pour certificats numériques de diplômes)** | <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>  <https://www.docusign.com/fr-fr/blog/authentification-et-verification-de-la-signature-electronique> |
| **RFID & Codes QR pour authentification physique**  Les documents imprimés peuvent contenir :   * Un **QR Code** renvoyant vers une base de données pour vérifier l’authenticité. * Une **puce RFID/NFC** intégrée avec des informations cryptées.   **Bon** **pour un document papier nécessitant une vérification rapide** | QR Code + Base de données sécurisée  **Exemples d’application :**   * Passeports électroniques (e-Passports). * Certificats officiels avec QR Codes. * Factures électroniques sécurisées.   L'intégration de puces RFID ou de codes QR dans des documents physiques permet une vérification rapide et fiable de leur authenticité. | <https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature>  <https://helpx.adobe.com/fr/acrobat/using/validating-digital-signatures.html> |

CHOIX TYPE DOCUMENT

|  |  |  |
| --- | --- | --- |
| **Type** | **Portée** | **Méthode appropriée** |
| notes de service | Admin to admin\_empl |  |
| décisions | Admin to admin\_empl |  |
| instructions | Admin to admin\_empl |  |
| circulaires | Admin to admin\_empl |  |
| directives | Admin to admin\_empl |  |
| journaux | Admin to public |  |
| délibérations | Admin to admin\_empl  Admin to public |  |
| rapports | Admin to admin |  |
| comptes rendus | Admin to admin  Admin to public (ex : conseil des ministres) |  |
| procès-verbaux | Admin to admin |  |
| croquis | Admin to public |  |
| plans | Admin to public |  |
| schémas | Admin to public |  |
| communiqués officiels | Admin to public |  |
| certificats (de prise-reprise-cessation de service, …) | Admin to admin |  |
| bulletins | Admin to admin |  |
| décrets | Admin to public |  |
| arrêtés | Admin to public |  |

Â, Ê, Î, Ô, Û, Ä, Ë, Ï, Ö, Ü, À, Æ, æ, Ç, É, È, Œ, œ, Ù

# **CHAPITRE 4 : APPROCHE**

**Deux (02) options de procédé :**

* **OPTION 1 :** utilisation d’algorithmes de hachage simple + blockchain
* **OPTION 2 :** utilisation d’algorithmes de hachage + signature numérique + blockchain
* **Chaque option est constituée de deux (02) phases (voir figure 5 ci-dessous) :** 
  + **Phase 1 :** Enregistrement de documents administratifs dans la blockchain
  + **Phase 2 :** Vérification/authentification de documents administratifs via la blockchain

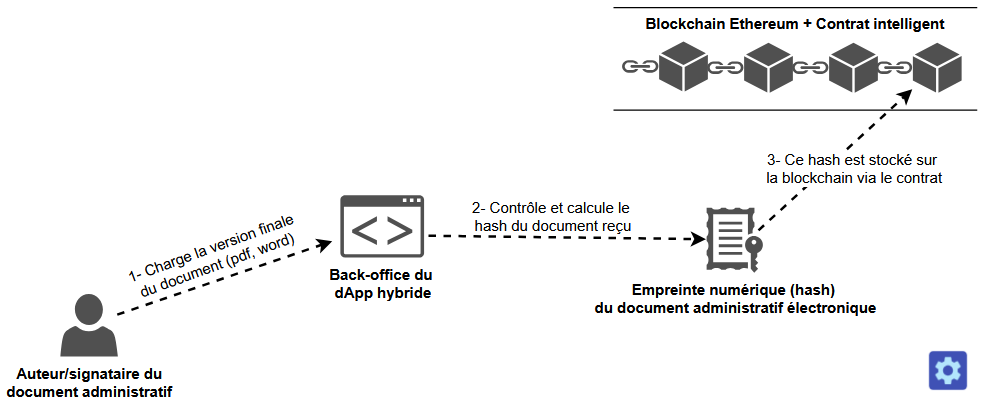
****

**Figure 5** : Différentes phases de l'approche d'authentification de documents administratifs à l'aide de la blockchain

# **OPTION 1 (PHASE 1) : ALGORITHMES DE HACHAGE SIMPLE + BLOCKCHAIN**

**DESCRIPTION DES ETAPES DE LA PHASE 1 (voir figure 6 ci-dessous)**

1. L’auteur upload (via le frontend) la version finale du document PDF ou Word. Le frontend transmet ces données au backend.
2. Le backend calcule un hash SHA-256 du document uploadé.
3. Le backend transfère le hash brut au contrat intelligent qui le stocke sur la blockchain. Une notification est retournée au frontend depuis la blockchain en passant par le backend.

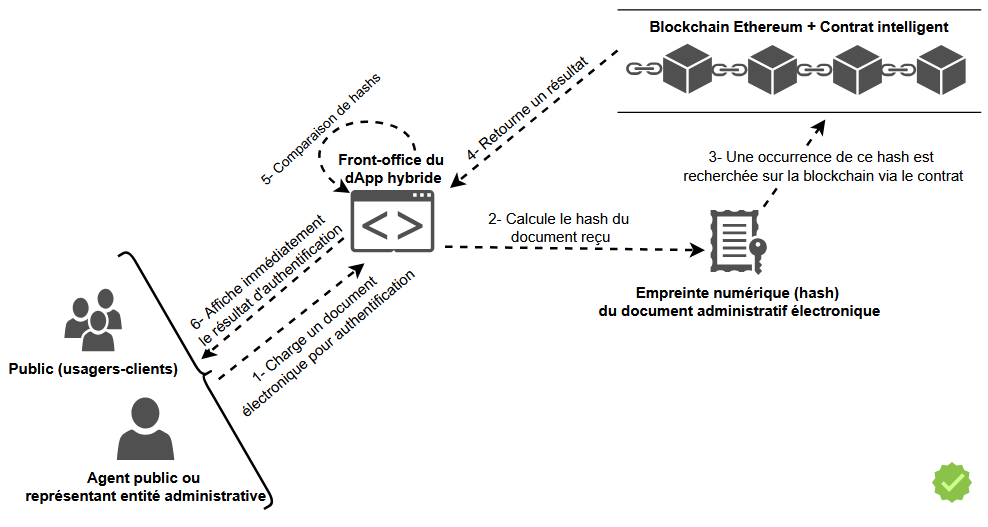


**Figure 6** : Etapes d'enregistrement de document dans la blockchain en utilisant le hachage simple + blockchain (OPTION1-PHASE1)

# **OPTION 1 (PHASE 2) : ALGORITHMES DE HACHAGE SIMPLE + BLOCKCHAIN**

**DESCRIPTION DES ETAPES DE LA PHASE 2 (voir figure 7 ci-dessous)**

1. L’utilisateur (public ou agent public) upload le document PDF ou Word (via le frontend). Le frontend transmet ces données au backend.
2. Le backend calcule le hash du document soumis à l’authentification.
3. Le backend utilise cet hash et interroge la blockchain via le contrat intelligent pour récupérer une occurrence du hash (empreinte numérique) auparavant stocké dans la blockchain.
4. La blockchain retourne une réponse au backend via le contrat intelligent.
5. Le backend compare le hash recalculé avec celui stocké sur la blockchain. Si les hashs ne sont pas identiques, alors le document soumis à authentification a été modifié et n’est donc pas authentique (vérification de l’intégrité du document). S’ils correspondent, on conclut que le document est authentique.
6. Après comparaisons, une notification est faite par le backend à l’utilisateur via le frontend.

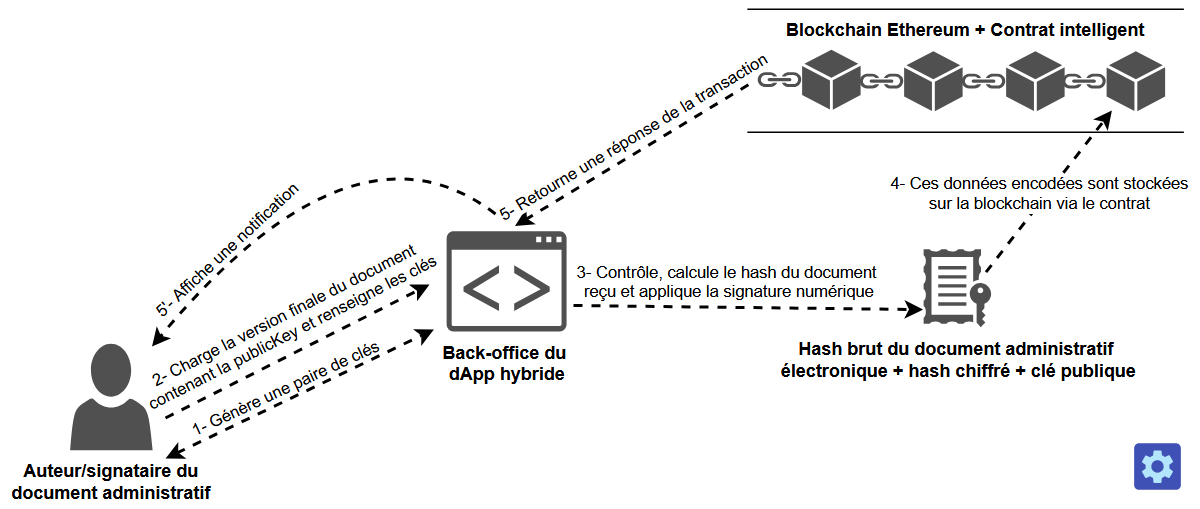


**Figure 7** : Etapes de vérification/authentification de documents via la blockchain (OPTION1-PHASE2)

# **OPTION 2 (PHASE 1) : ALGORITHMES DE HACHAGE + SIGNATURE NUMERIQUE + BLOCKCHAIN**

**DESCRIPTION DES ETAPES DE LA PHASE 1 – SIGNATURE NUMERIQUE BASEE SUR SHA256WITHECDSA (P-256) (voir figure 8 ci-dessous).** Pour la signature numérique, on génère les clés ECDSA [[1]](#footnote-1)en utilisant **la courbe elliptique secp256r1** (aussi appelée P-256) qui est compatible avec Ethereum et NIST**.**

1. L’auteur génère une paire de clés (via le backend en passant par le frontend). Ces clés ne doivent pas être perdues et la clé privée doit être soigneusement conservée.
2. L’auteur intègre la clé publique dans le document de sorte à ce qu’elle soit visible.
3. L’auteur upload (via le frontend) la version finale PDF ou Word du document contenant sa clé publique. Lors de l’upload, il renseigne la paire de clés. Le frontend transmet ces données au backend.
4. Le backend calcule un hash SHA-256 du document uploadé. Le backend chiffre le hash calculé avec la clé privée de l’auteur (on obtient donc un hash signé – c’est la signature numérique).
5. Le backend transfère le hash brut, le hash signé et la clé publique (le tout encodé) au contrat intelligent qui les stocke sur la blockchain. Ainsi, lorsqu’un utilisateur veut vérifier l’authenticité, la clé publique correspondante est utilisée pour déchiffrer et vérifier la signature.
6. Une notification est retournée au frontend depuis la blockchain en passant par le backend.

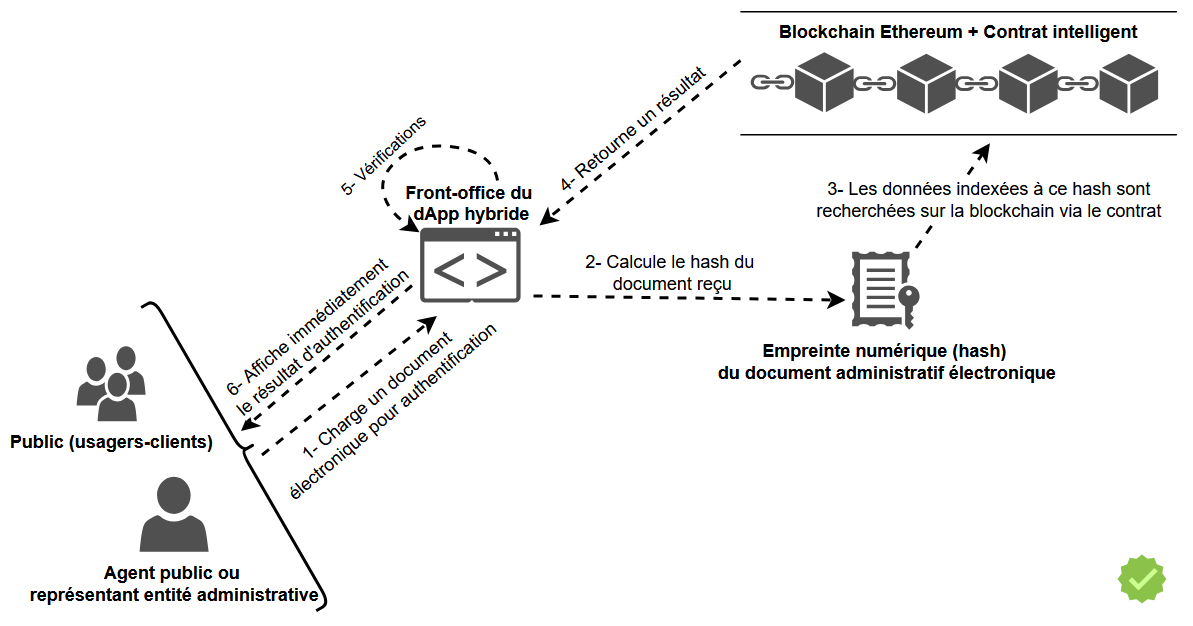


**Figure 8** : Etapes d'enregistrement de document dans la blockchain en utilisant le hachage + signature numérique + blockchain (OPTION2-PHASE1)

# **OPTION 2 (PHASE 2) : ALGORITHMES DE HACHAGE + SIGNATURE NUMERIQUE + BLOCKCHAIN**

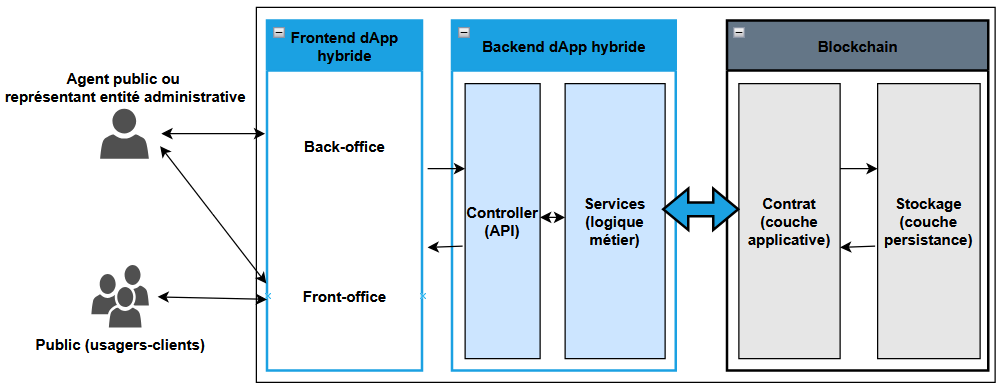
**DESCRIPTION DES ETAPES DE LA PHASE 2 (voir figure 9 ci-dessous)**

1. L’utilisateur (public ou agent public) upload le document PDF ou Word (via le frontend). Le frontend transmet ces données au backend.
2. Le backend calcule le hash du document soumis à l’authentification.
3. Le backend utilise cet hash et interroge la blockchain via le contrat intelligent pour récupérer l’empreinte numérique brute, la signature numérique et la clé publique auparavant stockées dans la blockchain.
4. La blockchain retourne une réponse au backend via le contrat intelligent.
5. Le backend décode les données reçues de la blockchain et effectue 2 vérifications :
   1. Il compare le hash recalculé avec celui stocké. Si les hashs ne sont pas identiques, alors le document a été modifié et n’est donc pas authentique (c’est la vérification de l’intégrité du document). S’ils correspondent, on passe à la seconde vérification (b).
   2. Il vérifie la signature numérique avec la clé publique stockée. Si cette vérification échoue, alors la signature ne provient pas du bon signataire, c’est-à-dire de l’auteur ayant validé la version finale du document (c’est la vérification de l’authenticité du document). Si la signature est valide, alors on déclare que le document est authentifié et authentique.
6. Après vérifications, une notification est faite par le backend à l’utilisateur via le frontend.



**Figure 9** : Etapes de vérification/authentification de documents via la blockchain (OPTION2-PHASE2)

# **ARCHITECTURE EN COUCHE DE L’APPROCHE**



**Figure 10** : Architecture en couches de l'approche

# **Technologies cibles à utiliser :**

* **Ethereum Mainnet** (coûteux en frais de gaz, mais sécurisé) comme réseau public
* **Truffle** et **Ganache pour déployer et tester la solution localement**
* **Contrat intelligent en Solidity**
* **Frameworks Spring Boot et Angular**
* **Algorithme de hachage SHA-256, chiffrement/déchiffrement avec ECDSA (courbe P-256)**
* **Librairie Web3j, API JSON RPC**
* **IDEs IntelliJ IDEA 2024.1.4, Visual Studio Code 1.96.2, Remix-Ethereum IDE**

# **Mémo d’implémentation de l’approche :**

1. Créer le hash du document via un backend Spring Boot. Ce code reçoit en entrée, le document PDF ou WORD et calcule son hash en utilisant **SHA-256**. Le hachage de PDF textuel et de WORD peut se faire sans inquiétude. Par contre, pour les scans images dans un fichier PDF, on peut premièrement extraire le texte du fichier via un système **OCR** (Reconnaissance Optique de Caractères) et calculer le hash de ce texte uniquement. Deuxièmement, on peut hacher directement l’image (le fichier binaire complet). Cependant pour ce deuxième cas, si par exemple, je scanne deux fois le même document papier en PDF avec des imprimantes différentes, les fichiers auront-ils le même hash ? **NON**: car les images scannées ont des variations en terme de résolution, d'alignement, de luminosité, de compressions, etc. et contiennent des métadonnées (date de création, logiciel utilisé, etc.) différentes. Dans tous les cas, nous sommes certains qu'un hash demeure identique tant que le texte extrait est strictement le même.

**S’il y avait la possibilité d’avoir une paire de clés, l’administration pourrait joindre la clé publique afin que celle-ci plus le document soient hachés. Ainsi, l’administration marquerait cette clé publique visiblement sur le document à l’endroit des usagers.**

1. Créer un smart contract en **Solidity** qui permet d’enregistrer un hash sur la blockchain et de vérifier son existence et sa validité.
2. Utiliser **Web3j** pour faire interagir le backend Spring Boot avec la blockchain. En effet, Web3j permet d'envoyer des transactions vers Ethereum, de déployer et appeler des contrats intelligents et de gérer les clés privées/publics pour signer des transactions. Ainsi, le hash du document calculé par le backend sera directement enregistré sur la blockchain en renseignant l’adresse du compte contrat, l’url **RPC** pour Ganache et la clé privée de test (par exemple). De même, pour la vérification, il suffira que le backend recalcule le hash du document qu’il va passer en paramètre à l’appel de la méthode de vérification du contrat qui est sur la blockchain.
3. Créer un frontend Angular qui se chargera d’envoyer le document au backend. Il aura aussi la charge de recevoir la réponse de vérification venant du backend qu’il va afficher.
4. On peut dire que **notre solution est une dApp hybride** (de rigueur) car le backend sert uniquement de passerelle vers la blockchain et ne stocke aucune donnée dans une base de données classique. Si on veut une dApp pure, il faut rendre le backend plus léger et utiliser Metamask / WalletConnect dans le frontend Angular pour interagir directement avec Ethereum. *NB : Une application est dite dApp, si elle repose uniquement (sans backend classique) sur Ethereum (contrat intelligent) pour la logique métier et la persistance*.
5. Déploiement :

**Déploiement du Smart Contract Ethereum** : le faire sur un réseau public pour être conforme au choix de Ethereum Mainnet. Cela garantira que la solution soit totalement décentralisée. Pour les besoins de tests en réseau, on pourra utilise Testnets(Goerli, Sepolia, ou autre) : idéal pour tester avant d’aller sur mainnet.

**Déploiement du Backend (Spring Boot)** : Le backend doit être accessible au frontend et pouvoir interagir avec la blockchain. Option Cloud (AWS) ou Serveur dédié virtuel (VPS – vitual private server) Linux avec Docker.

**Déploiement du Frontend (Angular)** : L’application frontend doit être accessible aux utilisateurs finaux. Option Cloud AWS ouServeur Nginx.

1. ECDSA = Elliptic Curve Digital Signature Algorithm [↑](#footnote-ref-1)