Authentification des documents administratifs à l'aide de la blockchain

RESUME

Les documents administratifs servent entre autres à la traçabilité et constitue un support de décision, de communication et de droit. Ils doivent donc être fiables et d'origine incontestable. Cependant, nous constatons l'évolution inquiétante du phénomène de documents administratifs falsifiés dans cette ère numérique (AI, IOT, Blockchain) en pleine mutation.
Dans ce contexte, nous proposons une application décentralisée (DApp) hybride d'authentification et de sécurisation de documents (PDF, Word) en s'appuyant sur les propriétés de non-répudiation, de transparence et de stockage décentralisé de la blockchain Ethereum 2.0. Nous combinons l'utilisation d'un contrat intelligent, de l'algorithme de hachage SHA-256, de la signature numérique (à l'aide de clés asymétriques ECDSA avec une courbe elliptique secp256r1) et l'horodatage électronique.
Cette solution, en plus de garantir plus de sécurité et d'intégrité des documents administratifs, offre la possibilité de vérifier leur authenticité en temps réel de manière simple.

Mots clés : *authentification, sécurisation, document, blockchain, cryptographie, application décentralisée*

I. INTRODUCTION

La fiabilité de certains documents administratifs est de plus en plus controversée car il est maintenant fréquent de retrouver des documents falsifiés ou d'origine douteuse sur l'espace numérique public, mettant ainsi en déroute, bon nombre de citoyens. Cela pourrait être dû en partie, au développement et à l'exploitation malsaine des multiples outils basés par exemple sur l'Intelligence Artificielle (IA).

En effet, le phénomène de documents falsifiés contribue à ternir l'image de leur légitime auteur qui pourrait être le gouvernement, créant ainsi une crise de confiance entre celui-ci ses usagers-clients. Pour faire face à ce phénomène, des auteurs et destinataires de documents effectuent parfois des opérations d'authentification de ceux-ci, moyennant l'utilisation de temps et de coûts énormes qui pourraient baisser leurs rendements à terme.

La Blockchain est une technologie novatrice en plein essor, qui présente des potentialités pour résoudre efficacement le phénomène de falsification documentaire.

L'objectif de notre travail est de proposer une approche d'authentification de documents à l'aide de la technologie blockchain, et d'implémenter une DApp hybride basée sur cette approche.

II. ÉTAT DE L'ART

La technologie blockchain, propulsée par l'avènement en 2008 de la crypto-monnaie bitcoin de *Satoshi Nakamoto* [1] [10], est en pleine croissance ces dernières décennies. C'est une technologie numérique qui permet de stocker chronologiquement et de

transmettre des informations sous forme de blocs reliés les uns aux autres de manière sécurisée (forte usage de la cryptographie) et sans autorité centrale.

Selon *Imran Bashir* [2] [14], les blockchains de la 3e génération sont applicables, au-delà de l'industrie des services financiers, dans divers domaines sociétaux à usage général tels que les médias, la santé, le gouvernement, etc. Outre Bitcoin, il existe plusieurs blockchains (Solana, Ethereum, Cardano, Avalanche, ...) parmi lesquelles nous adoptons Ethereum pour la présente expérimentation.

1. Blockchain Ethereum

La blockchain publique Ethereum dont le mécanisme de consensus est passé du Proof of Work (PoW) au **Proof of Stake (PoS)** en septembre 2022 [3] [26], a connu plusieurs évolutions après qu'elle ait été annoncé lors de la Conférence nord-américaine sur le Bitcoin à Miami en janvier 2014 puis lancé le 30 juillet 2015 [4] [29]. A travers le livre blanc publié en 2013 [5] [30], *Vitalik Buterin* indiquait que *"L'objectif d'Ethereum est de créer un autre protocole pour développer des applications décentralisées, en offrant un ensemble différent de compromis qui sera, nous le pensons, très utile pour une large gamme d'applications décentralisées. Il sera principalement axé sur les situations dans lesquelles le développement rapide, la sécurité des petites applications rarement utilisées et la possibilité pour les différentes 23 applications d'interagir ensemble de façon très efficace sont importants."*.

La possibilité de produire des applications décentralisées basées sur Ethereum – fonctionnant sur un **réseau Peer to Peer** – s'appui considérablement sur l'utilisation de contrats intelligents. Et cela fait d'Ethereum une blockchain Turing Complete [6] [31], contrairement au réseau Bitcoin. Dans certains cas d'usage d'Ethereum comme le nôtre, nous utilisons impérativement deux (02) comptes. Le premier est un **compte de propriété externe (EOA)** contrôlé par une clé privée cryptographique, disposant de plusieurs centaines d'ETH et identifiable par une adresse (hash de 42 caractères hexadécimaux préfixé de ***0x***). Tandis que le second est un **compte de contrat (CA)** dont l'adresse est obtenu après déploiement (utilisant ≈782016 Gas) de notre contrat intelligent.

Techniquement, un **contrat intelligent** désigne un programme informatique implémenté dans un langage de programmation de haut niveau tel que Solidity, Vyper, etc. et dont le code compilé en bytecode est déployé sur notamment une version spécifique de la machine virtuelle de blockchain – l'EVM, s'agissant d'Ethereum. Il est ainsi destiné à s'y exécuter de façon autonome lorsque certains critères sont remplis. Outre leurs avantages en termes de rapidité, d'exactitude, de transparence et de sécurité, les contrats intelligents constituent selon [2] [14], une caractéristique révolutionnaire de la blockchain pour le fait qu'ils permettent une flexibilité, une autonomisation et un contrôle très souhaitable des actions voulues par les utilisateurs.

2. Authentification et sécurisation de documents

En convenant que le **document** désigne une information conservée sur papier ou sur un support électronique, l'**authentification** d'un document est un processus par lequel un système informatique ou un humain

prouve ou certifie qu'un document est authentique. En générale, pour l'humain habilité – officier de l'État civil, officier de Police, autorité officielle ayant délivré le document, etc. –, le processus consiste à s'assurer que les signature et cachet visibles sur le document (original, copie conforme à/de l'original) émanent d'une autorité officielle et que la date de signature ou délivrance, le nom et la fonction du signataire sont aussi lisibles.

Dans tous les cas, l'authentification est un composant de la sécurisation qui, elle-même, est un 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).

3. Méthodes existantes d'authentification de documents

Plusieurs méthodes d'authentification de documents numériques existent.

- **Technique de signature numérique**

Ce moyen sécurisé permet de prouver l'identité de l'auteur d'un document électronique et de garantir l'intégrité dudit document à l'aide de la cryptographie à clé publique. Elle permet ainsi de garantir la non-répudiation, c'est à dire la quasi impossibilité de remettre en cause ou de rénier le document. Une signature numérique doit nécessairement être authentique, infalsifiable, non réutilisable, inaltérable et irrévocable [7] [44].

- **Technique de hachage ou empreinte numérique**

Cette technique consiste à appliquer un algorithme (SHA-2, SHA-3, etc.) à sens unique sur le document pour générer une empreinte numérique unique. Cette technique ne prouve pas l'identité de l'auteur, mais uniquement l'intégrité du document.

- **Technique d'horodatage électronique**

Le plus souvent basée sur la signature numérique et le hachage, cette technique sert à prouver qu'un document existait à une date donnée.

- **Technique des RFID et codes QR**

L'identification par radiofréquence (RFID – Radio Frequency Identification) et le code à réponse rapide (QR Code – quick response code) sont utilisés dans de nombreux secteurs d'activités (commerce, administration, santé, ...) pour suivre certains biens ou vérifier l'authenticité de des documents notamment physiques.

- **Technique Blockchain**

Isyak Meirobie et al. [8] [49] ont mis en place un cadre d'authentification des documents électroniques à l'aide de la technologie Blockchain pour le système gouvernemental d'Indonésie. Go-Chain stocke sur une blockchain publique, la signature (DSA à courbe P-256) haché (en SHA256) de la transcrition numérique du document. Cette transcription est également distribuée au public sous format json. Aussi, *Ana BAKHOUM* [9] [37] a proposé un système décentralisé de sauvegarde et sécurisation des E-livrets scolaires (SDSEL) dans la blockchain Ethereum via un contrat intelligent. Cela vise à assurer la fiabilité, l'authenticité, la transparence et la sécurité des E-livrets. Notre solution innove avec l'intégration de l'horodatage électronique et la non manipulation directe des clés cryptographiques par les acteurs grand public. Elle offre la possibilité de vérifier l'authenticité de documents en temps réels, de manière sécurisée, transparente et sans passer par une autorité centrale de vérification.

III. METHODOLOGIE

Décrite ci-dessous, elle est constituée de sept (7) étapes clés illustrées par la figure 2.

a. Compréhension du concept et définition du projet

Nous déterminons et modélisons les acteurs destinataires de la solution et leurs rôles. Après exploration des travaux existants en la matière, nous choisissons la blockchain appropriée sur la base de plusieurs critères dont le protocole de consensus et les technologies d'implémentation requises. Dans cette étude, l'entité administrative (ou son mandataire) est la première catégorie d'acteurs qui ont la possibilité de générer des paires de clés asymétriques, d'enregistrer des documents sur Ethereum et de vérifier l'authenticité de ceux-ci depuis ladite blockchain. La seconde catégorie est représentée par le grand public qui peut vérifier l'authenticité de documents à travers la blockchain.

b. Définition du design de l'expérience utilisateur (UX) et de l'interface (UI)

Nous avons opté pour un design fortement basé sur les principes de simplicité, de clarté et de feedback utilisateur car cela déterminent l'adoption et l'efficacité de la DApp auprès des utilisateurs finaux.

c. Développement du contrat intelligent

Il est essentiel de choisir le langage de programmation et les outils de développement. Une fois implémenté, nous avons itéré le 3-uplet {compilation, déploiement, test} du contrat intelligent sur un réseau de test en local et en ligne afin d'ajuster les fonctionnalités et l'utilisation des frais de gas pour les transactions.

d. Intégration aux frontend et backend

L'intégration du contrat intelligent dans une application classique permet d'interagir avec la blockchain. Pour une intégration réussie, nous avons adopté une architecture claire de la DApp (figure 1) où les responsabilités de chaque composant sont bien définies.

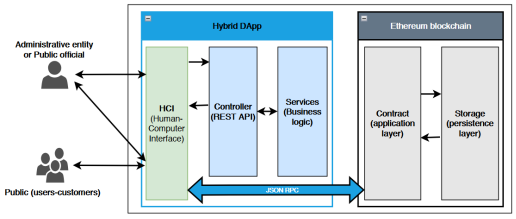

Figure 1: Architecture simplifiée en couches de la solution

e. Tests et validations

Pour s'assurer du bon fonctionnement et de la performance de la solution, nous avons effectué essentiellement des tests unitaires, des tests d'intégration et des tests d'acceptation.

f. Déploiement et mise en production

Il s'agit de préparer une stratégie de déploiement progressif avec une prévision de rollback en cas d'urgence. Cette stratégie doit prendre en compte la surveillance constante suivi de mises à jour.

g. Suivi et évolution

Cette étape consiste à surveiller les performances d'exécution de la DApp telles que les temps de réponse, les taux d'erreur, le coût de gas, etc. Cela peut faire l'objet de planification des améliorations et de nouvelles fonctionnalités de la DApp y compris le contrat intelligent.

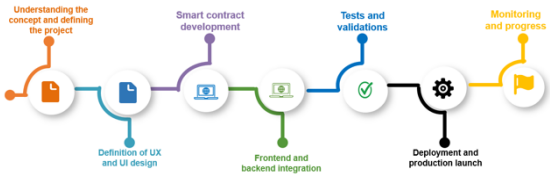

Figure 2 : Méthodologie de réalisation de la DApp

IV. EXPERIMENTATION DE LA SOLUTION

1. Outils

L'implémentation requière au moins un ordinateur ayant un processeur Core i7, 16

Go de RAM et 128 Go SSD de stockage, sans exigence de système d'exploitation. PowerDesigner 16.5.0.3982 et draw.io (en ligne) ont servi à la modélisation des spécifications techniques et fonctionnelles. Les parties backend et frontend (communiquant par API REST) de la DApp ont été implémentées avec Visual Studio Code 1.96.2 en utilisant les frameworks Spring-boot 3.4.1 (Maven 3.8.1 + Java 17) et Angular 15 (HTML5, TypeScript/ JavaScript, SCSS/CSS3).

Le contrat intelligent a été implémenté et testé en Solidity ^0.8.28 sur Remix-Ethereum IDE (en ligne). Le portefeuille de crypto-monnaie MetaMask v2.132.0 a été intégré pour les demandes et signatures des transactions blockchain qui se font par le protocole JSON Remote Procedure Call auprès de Angular via l'Application Binary Interface. En terme de technologies fondamentales, nous avons expérimenté le framework Hardhat ^2.24.0 et la librairie Ethers.js ^6.14.0 pour configurer le réseau blockchain de test (network Localhost), compiler et déployer notre contrat. Afin de générer les paires de clés cryptographiques ECDSA (Elliptic Curve Digital Signature Algorithm), nous utilisons la dépendance Maven bouncycastle ; ce qui nous permet d'exploiter la courbe elliptique secp256r1 (P-256) pour les signatures numériques des empreintes numériques calculées à travers l'algorithme SHA-256. P-256 étant compatible avec ethereum et les normes du National Institute of Standards and Technology (NIST) [10] [51] [11] [52].

2. Simulations

Notre approche d'authentification est constituée de deux (02) phases ordonnées et complémentaires, illustrées par les figures 3 et 4. Ces opérations sont instantanées sur le réseau local de test.

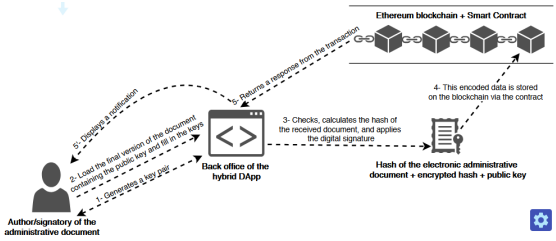

Figure 3: PHASE 1 - Enregistrement de document administratif dans la blockchain Ethereum

Le paiement de frais de Gas est obligatoire ici. Selon nos expérimentations sur les communiqués officiels, le stockage d'un fichier d'environ 500 Ko nécessite en moyenne 322200 Gas, soit 389212,119378 GWei (0,000389212119378 ETH, sachant que 1 ETH = 10^9 Gwei = 10^{18} Wei).

Dans cette phase 1, l'auteur génère une paire de clés asymétriques via la DApp. Il intègre (facultatif) sa clé publique dans le document de sorte à ce qu'elle soit visible, puis upload la version finale en PDF ou Word du document dans la DApp en renseignant la paire de clés. La DApp extrait le contenu (textuel) du fichier uploadé, calcule le hash de ce contenu et le chiffre avec la clé privée de l'auteur. On obtient ainsi un hash signé – c'est la signature numérique du document. Ces données obtenues (hash brut, hash signé et clé publique de l'auteur) sont encodées et stockées dans Ethereum par appel de la méthode *storeAdministrativeDocument()* du contrat intelligent. L'horodatage est calculé et joint aux données stockées.

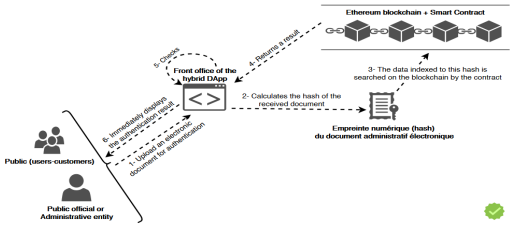

Figure 4: PHASE 2 - Vérification ou authentification de documents administratif sur la

Cette phase 2 permet à l'utilisateur d'uploader simplement le document PDF

ou Word dans la DApp et de soumettre le formulaire de demande d'authentication. La DApp extrait le contenu (textuel) du fichier uploadé et calcule son hash. La méthode *getAdministrativeDocument()* du contrat intelligent est ensuite utilisée pour rechercher l'occurrence de ce hash dans Ethereum. Si occurrence trouvée (document potentiellement intègre), la DApp vérifie la signature numérique associée à cette occurrence via la clé publique auparavant stockée. C'est la vérification de l'authenticité du document. Si la signature est valide, alors la DApp notifie que le document est authentifié et authentique. En revanche, le document est déclaré non authentique en cas d'absence d'occurrence ou de signature invalide. C'est-à-dire que la signature ne provient pas du bon signataire – ayant validé la version finale du document.

CONCLUSION

Face à l'essor du phénomène de falsification documentaire, il est crucial de mettre à profit les avancées et inovations technologiques, pour repenser les méthodes d'authentification et de sécurisation des documents numériques. Pour ce faire, nous avons proposé une application décentralisée hybride qui interagi avec la blockchain Ethereum à l'aide d'un contrat intelligent. Dans cette solution, nous avons intégré l'utilisation de l'horodatage électronique, de la signature numérique basé sur les clés asymétiques et de la technique de hachage à travers l'algorithme SHA-256.

Les résultats issus de nos expérimentations confirment que la technologie blockchain est prometteuse pour garantir l'authenticité et la sécurisation des documents administratifs. Cependant, il conviendrait d'approfondir les reflexions sur la souveraineté des données numériques, et l'intégration d'autres pipelines pour prendre en charge les documents électroniques aux contenus non textuels.

REFERENCES

[1] R. Subramanian et T. Chino, « The State of Cryptocurrencies, Their Issues and Policy Interactions », *J. Int. Technol. Inf. Manag.*, vol. 24, nº 3, p. 40, janv. 2015, doi: 10.58729/1941-6679.1045.

[2] I. Bashir, *Mastering Blockchain*. Packt Publishing Ltd, 2017.

[3] « Qu'est-ce que le consensus ? Guide du débutant », *Qu'est-ce que le consensus ? Guide du débutant*, 13 mai 2022. Consulté le: 15 septembre 2024. [En ligne]. Disponible sur: https://crypto.com/fr/university/consensus-mechanisms-explained

[4] « Ethereum », *Wikipédia*. 22 janvier 2025. Consulté le: 10 février 2025. [En ligne]. Disponible sur: https://fr.wikipedia.org/wiki/Ethereum

[5] T. Bourbotte, « C'est quoi Ethereum ? Nos explications pour tout savoir sur cette blockchain et sa cryptomonnaie ETH », *Cryptoast*, 20 décembre 2024. Consulté le: 10 février 2025. [En ligne]. Disponible sur: https://cryptoast.fr/fiche-ethereum/

[6] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, et H.-N. Lee, « Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract », *IEEE Access*, vol. 10, p. 6605-6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[7] F. Num, « La signature électronique : un outil devenu incontournable - francenum.gouv.fr », Direction générale des entreprises, 7 décembre 2020. Consulté le: 21 février 2025. [En ligne]. Disponible sur: https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature

[8] I. Meirobie, A. P. Irawan, H. T. Sukmana, D. P. Lazirkha, et N. P. L. Santoso, « Framework Authentication e-document using Blockchain Technology on the Government system », *Int. J. Artif. Intell. Res.*, vol. 6, nº 2, Art. nº 2, déc. 2022, doi: 10.29099/ijair.v6i2.294.

[9] A. Bakhoum, « La Blockchain pour la Sécurisation des E-livrets scolaires », 2019. Consulté le: 10 septembre 2024. [En ligne]. Disponible sur: http://rivieresdusud.uasz.sn/xmlui/handle/123456789/1803

[10] É. (gapz) Gaspar, « Standardisation des courbes elliptiques : à qui faire confiance ? | Connect - Editions Diamond », avril 2016. Consulté le: 18 avril 2025. [En ligne]. Disponible sur: https://connect.ed-diamond.com/MISC/mischs-013/standardisation-des-courbes-elliptiques-a-qui-faire-confiance

[11] C. de la sécurité des télécommunications Canada, « Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) », *Centre canadien pour la cybersécurité*, 15 octobre 2020. Consulté le: 18 avril 2025. [En ligne]. Disponible sur: https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062