NFB: protocole de Notarisation des Documents dans la Blockchain

Haikel Megrahi *, Nouha Omrane **
Rakia Jaziri***

* Etudiant en Big data - Université Paris 8
haikel.magrahi@etud.univ-paris8.fr
** Expert R&D - Docapost DPS, France
nouha.omrane@docapost.fr
*** Maître de conférences, LIASD
rjaziri@ai.univ-paris8.fr

1 Introduction

Les blockchains comme Bitcoin(Nakamoto, 2008) et Ethereum (Foundation, 1990) et leurs réseaux respectifs pair à pair ont connu une évolution significative dans de nombreux secteurs au cours des dernières années. De nombreux systèmes et protocoles de stockage ont émergé pour permettre le stockage de données distribuées associées aux transactions. Aucun de ces outils n'a proposé l'archivage des documents à valeur probatoire.
Dans cet article, nous décrivons un nouveau protocole appelé NFB (protocole de notarisation des documents dans la Blockchain. Ce protocole assure la communication entre deux systèmes : une blockchain et un système de gestion de documents centralisé. La méthode décrite est utilisée pour permettre aux utilisateurs d'archiver, contrôler, analyser, auditer et valider leurs données dans une solution sécurisée sur des fournisseurs de données tiers.

2 Architecture du protocole NFB

NFB est un protocole qui assure la communication entre deux écosystèmes différents, d'une part, la blockchain qui est un réseau P2P décentralisé où les participants partagent un ledger distribué (registre), non falsifiable et transparent, et d'autre part un système d'archivage des documents à valeur probatoire. Ce protocole repose sur une architecture de microservices, basé sur la couche Blockchain, la couche DMS et la couche de coordination. La couche Blockchain permet de s'interfacer avec la blockchain. Ce microservice met à disposition plusieurs fonctionnalités notamment l'historisation des transactions (Muneeb Ali, 2017), le déploiement de smartcontrats et la récupération des blocs et des transactions (Shawn Wilkinson, 2016). NFB se base sur la Blockchain Quorum (Morgan, 2016) qui est un "fork" de la blockchain publique Ethereum (Foundation, 1990). Il s'agit d'une blockchain permissive et privée, où tous les noeuds qui se connectent au réseau sont connus et chacun a un rôle qui lui est associé. La couche DMS contient l'ensemble des services Web qui gèrent l'archivage électronique des

documents dans une solution centralisée. Ce service implémente trois fonctionnalités de base notamment l'archivage des documents, l'indexation des métadonnées associés à un document et la récupération d'un document physique. La couche de coordination implémente le patron gateway et assure une communication entre les deux couches Blockchain et DMS. Elle permet d'orchestrer les tâches et les actions entre les différents acteurs. Cette couche offre des endpoints REST pour l'utilisation "as a service" .

3 Notarisation des documents

Le protocole NFB propose trois fonctionnalités majeures pour la notarisation des documents en utilisant la blockchain notamment l'archivage des documents, la récupération des documents et la preuve de l'existence des documents. La couche de coordination établit une demande de connexion à la couche DMS, et en même temps une demande d'ouverture d'un flux pour tracer les transactions, grâce à la couche Blockchain. L'utilisateur sélectionne le document à archiver et saisit un ensemble défini de métadonnées associées au document. Ensuite, la couche de coordination envoie une requête d'archivage à la couche DMS. Puis, une deuxième requête pour tracer une transaction contenant les informations du document. Lorsqu'un utilisateur souhaite récupérer ou rechercher un document, Il saisit un ou plusieurs mots clé à rechercher. Une demande de récupération du document est envoyée vers la couche DMS. Cette dernière, retourne un ensemble de document qui matchent avec la requête. Ensuite, l'utilisateur choisit le document en question. Lorsqu'il clique sur le document, la couche de coordination envoie une transaction à la blockchain contenant les informations de l'action et du document. Après la récupération du document, la couche de coordination envoie à la couche Blockchain une autre transaction qui contient la réponse de cette action et qui traduit que l'utilisateur a bien récupéré le document.

4 Conclusion

Cette approche met l'accent sur l'un des avantages de l'utilisation de la blockchain : celui qui permet d'apporter des éléments de preuve de l'existence d'informations pendant une période donnée. Elle propose également à des utilisateurs de faire un audit pour prouver, ou vérifier, l'existence des documents grâce à l'utilisation d'un système d'archivage des documents à valeur probatoire. Il permet aussi d'examiner les transactions, en relation avec ce document, tracées dans le ledger de la Blockchain grâce à un identifiant unique.

Références

Foundation, L. (1990). Ethereum. *https ://github.com/ethereum/wiki/wiki/White-Paper*.

Morgan, J. (2016). *Quorum: Whitepaper*. https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum-Whitepaper-20v0.1.pdf.

Muneeb Ali, R. S. (2017). Blockstack: A new decentralized internet. *http://blockstack.org*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Shawn Wilkinson, T. B. (2016). Storj: A peer-to-peer cloud storage network.