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