Système de vote pour le contrôle d'accès, basé sur la technologie Blockchain

Encadrantes : Maryline Laurent et Nesrine Kaaniche

Binôme requis

La Blockchain est une technologie inventée à la fin des années 2000. C'est le projet Bitcoin d'échange de cryptomonnaie (des Bitcoins) [1, 2] sur Internet qui l'a rendue populaire et a permis de démontrer sa grande fiabilité. En 2014, la fondation à but non lucratif Ethereum dirigée par Vitalik Buterin [3, 4] lance l'idée d'étendre le principe de la Blockchain à une Blockchain programmable, ouvrant ainsi le champ à tout type de transactions (smart contracts) et à pléthore de nouveaux services. Avec la première version du code source d'Ethereum mise à la disposition du grand public en 2015 [4], de nombreux industriels et développeurs indépendants se lancent alors dans la course pour proposer de nouvelles innovations. La Blockchain [1, 2, 3, 4] est très souvent assimilée à un gros livre de comptes publiquement accessibles et auditables. Ses membres peuvent y ajouter des écritures, mais cette opération nécessite une validation par plusieurs membres du groupe (appelés nœuds mineurs), voire la majorité du groupe.

Ce projet consiste à mettre en place un système de vote pour la validation des actions faites sur un document, en se basant sur la technologie Blockchain [5]. En effet, avant de partager un document au sein d'un groupe d'utilisateurs, le client créera deux « *smart contracts* ». Le premier contrat précisera les différentes actions autorisées sur le document et les ensembles des utilisateurs autorisés. Le deuxième contrat précisera l'ensemble des votants autorisés et le protocole de vote. Ce deuxième contrat met en œuvre le principe de vote à la majorité. L'initiateur soumet le type de l'action prévue avec l'identifiant du document au contrat de vote. Le contrat de vote reçoit la modification et, après vérification, lance la phase de vote pour la modification. Les détails du processus du vote peuvent être trouvés dans cet article [5].

Quand un utilisateur veut modifier un document, il doit tout d'abord interagir avec le premier smart contract. A son tour, ce dernier interagit avec le deuxième smart contract, pour établir une session de vote afin de valider (ou non) la demande de l'utilisateur. Le résultat du vote sera enregistré dans une transaction dans le Blockchain.

Livrables :

- Maquette : code source, démonstration et guide d'installation
- Rapport du projet et présentation

Références

[1] « Comprendre la Blockchain, anticiper le potentiel de disruption de la Blockchain sur les organisations », Livre blanc, Editeur U, janvier 2016.
[2] https://bitcoin.org/
[3] Interview de Vitalik Buterin, https://www.ethereum-france.com/interview-de-vitalik-buterin-createur-dethereum-et-president-de-la-fondation-partie-1-sur-2/, 2016

[4] https://www.ethereum-france.com/
[5] Ramachandran, A. and Kantarcioglu, M., 2018, March. SmartProvenance: A Distributed, Blockchain Based Data Provenance System. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy* (pp. 35-42). ACM.