Projet IFT785
Simulateur de typage de blocs pour DLT

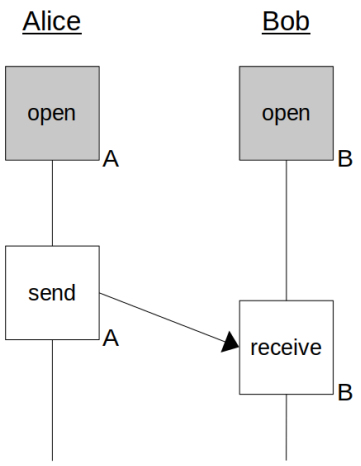
Prérequis

- Maitriser les concepts de base de chaine de bloc : hashage, signature, type de preuve…
- Programmation Python

Présentation

Les *Distributed Ledger Technologies* sont des outils de partage de données décentralisés destinés à des groupes d'utilisateur.rice.s non synchronisé.e.s et non hiérarchisé.e.s, ne se faisant a priori pas confiance. Pour assurer la sécurité et la cohérence des données, plusieurs implémentations des DLT ont été envisagées. Par exemple, *Bitcoin*[1] utilise un principe de minage par preuve de travail pour forcer les utilisateur.rice.s à engager leur matériel et leur énergie lors de la publication de donnée. Également parmi les plus populaires, *Ethereum*[2] utilise une technique par preuve d'enjeu, où les plus doté.e.s ont intérêt à assurer la sécurité du réseau, c'est dernier.e.s ayant majoritairement droit à la publication.

Une autre solution est celle proposée par *Nano*[3]. Elle aborde les questions de sécurité en divisant la responsabilité de publication sur chaque membre. Un.e utilisateur.rice n'a uniquement le droit de publier des informations le/la concernant (chacun.e étant alors responsable de sa propre chaine de blocs). Ainsi, pour effectuer une transaction d'Alice vers Bob, Alice devra publier une "émission" à destination de Bob, et Bob devra publier une "réception" liée à l'émission d'Alice. Deux blocs sont alors nécessaires, chacun respectivement publié sur les chaines d'Alice et de Bob, et ils sont de deux types différents. Sur le schéma ci-contre, Alice émet le bloc *send*, puis quelque temps plus tard, Bob émet le bloc *receive* associé au bloc d'Alice. Les blocs typés *open* représentent les blocs genesis de chaque chaine, et les lettres associées représentent l'émetteur.rice de la signature.



Dans ce projet, on s'intéressera au typage des blocs et aux possibilités qu'ils offrent pour mettre en œuvre des interactions complexes entre les membres. On s'affranchira de toutes les contraintes de communication associées à un réseau pairs-a-pairs, et on simulera le comportement des chaines de blocs sur un unique ordinateur via une interface simple en ligne de commande.

Projet IFT785 - Beltzer Baptiste
baptiste.beltzer@usherbrooke.ca

Objectif

L'objectif du projet est de concevoir un système de blocs typés pour généraliser l'approche proposé par *Nano*. On souhaite construire un objet générique de type "bloc" possédant les propriétés communes à tous les blocs (header, timestamp, hash, ...), puis proposer un système basé sur les DSL (*Domain-specific language*[4]) permettant de décrire de nouveaux types de bloc (dérivant du bloc générique), ainsi que leurs interactions possibles. Un ensemble de règles décrivant des types de bloc, des interactions et des contraintes de validité sera appelé un scénario.

Le projet commencera par la conception et l'implémentation des éléments de base permettant la manipulation des chaines de bloc ainsi que les publications et validations de blocs génériques. Puis, le projet évoluera avec l'introduction de différents scenarii permettant une évolution graduelle de la complexité. Voici un exemple de premiers scenarii qui pourront être introduits.

1. Gestion d'une devise avec le scénario d'échange de tokens tel que présenté ci-dessus, la création de tokens, la destruction, la mise en gage...
2. Généralisation des scénarii précédent avec la création/destruction de nouvelles devises.
3. Scénario de procuration : autoriser quelqu'un d'autre à publier sur sa chaine.
4. Scénario de partage de matériel cryptographique : protocole d'échange de clés Diffie-Hellman.
5. Scénario d'engagement et de preuve de connaissance.

Bibliography

[1] Satoshi Nakamoto, "Blockchain Powered Platform for Consolidated, Shared and Trusted". [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform". [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[3] Colin LeMahieu, "Nano: A Feeless Distributed Cryptocurrency Network". [Online]. Available: https://content.nano.org/whitepaper/Nano_Whitepaper_en.pdf

[4] "Domain-specific language on Wikipedia". [Online]. Available: https://en.wikipedia.org/wiki/Domain-specific_language

Projet IFT785 - Beltzer Baptiste
baptiste.beltzer@usherbrooke.ca