Sujet TER 2022-2023

Corentin Travers
corentin.travers@univ-amu.fr
Arnaud Labourel
arnaud.labourel@univ-amu.fr

Contexte

Une *blockchain* est un registre distribué qui trace la propriété de *jetons* qui peuvent être fongibles (comme les crypto-monnaies) ou non-fongible (comme un ticket de cinéma.). Par contraste avec une base de données, les utilisateurs sont non-authentifiés et potentiellement malveillant. Il s'agit de systèmes *sans permission* (permissionless en anglais). La blockchain elle-même peut être implémentée au dessus d'un réseau pair-à-pair dont certains nœuds sont aussi possiblement malhonnêtes.

Une problématique est l'échange de jetons entre deux ou plusieurs blockchain. Des attaques spectaculaires sur des blockchains ces dernières années exploitent des faiblesses dans l'implémentation ou la conception des protocoles d'échange [3, 4, 5]

L'objectif de ce ter est de dresser un panorama des protocoles d'échange de jetons entre entre blockchains ainsi que de leurs différentes faiblesses.

Travail à faire

Il s'agit de produire un état l'art sur les protocoles d'échanges de jetons entre blockchains.

- On pourra dans un premier temps s'intéresser aux systèmes centralisés, qui nécessitent une plateforme tiers pour réaliser l'échange. Pour en appréhender les principes, on pourra commencer par étudier les analyses d'attaques sur les plateformes [3, 4, 5].
- Ensuite, avec comme point de départ les articles [1, 2] on s'intéressera aux protocoles d'échange centralisés. En fonction du temps restant, le groupe pourra implémenter un ou plusiers protocoles proposés dans [1, 2] ou d'autres découverts au cours de l'étude.

Références

[1] Maurice Herlihy : Atomic Cross-Chain Swaps. PODC 2018 : 245-254 https://arxiv.org/abs/1801.09515

[2] Maurice Herlihy, Liuba Shrira, Barbara Liskov : Cross-chain Deals and Adversarial Commerce. Proc. VLDB Endow. 13(2) : 100-113 (2019) https://vldb.org/pvldb/vol13/p100-herlihy.pdf

[3] Nomad Bridge Hack : Root Cause Analysis https://medium.com/nomad-xyz-blog/nomad-bridge-hack-root-cause-analysis-875ad2e5aacd voir aussi cette discussion sur twitter https://twitter.com/samczsun/status/1578167198203289600

[4] Cross-chain bridge vulnerability summary https://medium.com/coinmonks/cross-chain-bridge-vulnerability-summary-f16b7747f364

[5] Solana's Wormhole Hack Post-Mortem Analysis https://extropy-io.medium.com/solanas-wormhole-hack-post-mortem-analysis-3b68b9e88e13