ENcoinS

October 11, 2021

Contents

Context and goal of the project

Current cryptocurrencies are mainly based on universal consensus which is a slow and costly process. Recently, Rachid Guerraoui and his team [2] proposed a more efficient way of implementing cryptocurrencies based on a weaker consensus named causal order broadcast. The goal of this project is to first implement some primivites which are used in the full consensus protocol proposed by Guerraoui. According to the pace of the students, they may have the time to work on the full protocol. The students can choose the programming language they want to use but coding in Rust is recommended. The project is articulated around differents steps which are described below.

1 Primitives in distributed systems

The idea is to implement some useful primitives in distributed systems that are described in the book [1], starting from basic protocols. The main checkpoints may be implementing :

1. 1 to 1 messaging plain text
2. securisation of the exchanges : encryption for confidentiality and authentifiction (asymetric cryptography)
3. broadcast : sending a message to everyone, develop a distributed architecture
4. reliable broadcast (that works if computers of the system crash)
5. Byzantine reliable broadcast (that works even if there is malicious people too)

To do so, a MPI-like library may be used to simulate a network. According to student's pace, a real network may be used for the application (more information in section 3).

2 Transfert system based on secure broadcast

The second step of this project would be to implement the algorithm described in [2]. It is a new blockchain protocol in which consensus is replaced by a casual broadcast order. More precisely, students will focus on the part with the *1-shared asset transfert* which basically means that we assume that only one person has access to the account and can make payments. In this part, the primitives implemented in section 1 must be widely used.

3 Extra mile

According to student's pace, some improvements can be added to the project.

- Attacks and failures tests are very important to decide wether a scheme is secure. Therefore, implementing crash failures or evil behaviors may be a relevent option.
- Simulating a network thanks to a MPI-like library is good, but testing the protocol on a real network is better. In this context, why not using the machines of the Europe room for a life-size test ?
- The complete protol described in [2] handles shared account (multiple people can pay with same account). To do so, a concensus between these people must be reached and the way to do it has to be designed (or implemented) from scratch. Once this is done, the final protocol may be implemented.

References

[1] Christian Cachin, Rachid Guerraoui, and Lus Rodrigues. *Introduction to Reliable and Secure Distributed Programming*. Springer Publishing Company, Incorporated, 2nd edition, 2011.

[2] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, and Dragos-Adrian Seredinschi. The consensus number of a cryptocurrency (extended version). *CoRR*, abs/1906.05574, 2019.