University of Bern
Institute of Computer Science
Cryptology and Data Security

Analysis and Documentation of the Snowman Consensus Protocol

BSc, MSc Thesis

Project Description

Avalanche has become one of the leading protocols for implementing distributed ledgers, like a block chain, and the market capitalization of its associated cryptocurrency AVAX ranks in the top 20. The Avalanche protocol combines several techniques to addresses the problem of any data structure that is distributed among several parties: forming consensus about the current state of the data structure among the participating honest parties, even if some are Byzantine (i.e., behave in unintended or even malicious ways), while maintaining security, low latency and high throughput.

A whitepaper from 2019 (first source below) proposed a blockchain, called X-Chain, for a decentralized currency. The whitepaper introduces the Chain based on the UTXO model, which can be seen as directed graph where the nodes are called transactions (tx) that represent a transfer of currency between users. Each such tx consumes outputs of other tx, which is denoted with directed edges in the graph, and produces output itself. The current state of the UTXO graph indicates current and historic ownership. The whitepaper continues to build a protocol where that UTXO graph forms a DAG (directed acyclic graph). It then uses an intricate protocol to keep this data structure consistent among all parties that is built upon on a randomised self-stabilizing protocol that solves a simpler case of binary consensus, called “Snow” consensus protocols.

However, since the publication of this whitepaper the implementation of the Avalanche consensus protocol has evolved significantly. For example, the X-Chain has since moved to a classic chain structure instead of a DAG with associated changes in the associated consensus mechanism that has been dubbed the “Snowman” protocol. While the initial consensus mechanism has been reasonably well documented (see second source), understanding of the consensus mechanism of the latest iteration of the Avalanche consensus protocol is still lacking. The focus of the proposed thesis is to fill this knowledge gap by analyzing the open source code of the current implementation of the Avalanche protocol that uses the Snowman consensus mechanism. The goal is to give an abstract, well documented description of the current protocol via pseudo-code. The findings should be well visualized and presented in a written part.

Recommended Reading

- Yin et al., Scalable and Probabilistic Leaderless BFT Consensus through Metastability
- Amores-Sesar at al., When is Spring coming? A Security Analysis of Avalanche Consensus, OPODIS ’22

Requirements

- Decent skills in programming and code analysis
- Theory: 40% Systems: 60%

Contact

- **Philipp Schneider**, philipp.schneider2@unibe.ch