Instituto Superior Técnico, Universidade de Lisboa
Master of Science in Computer Science and Engineering
Highly Dependable Systems

HDS Serenity Ledger: Developing a High-Dependability Blockchain System

1st Stage

André Jesus (110860) André Páscoa (110817) Nyckollas Brandão (110893)

October, 2023

1 Introduction

In this initial stage, our primary objectives were to finalize the implementation of the Istanbul BFT Consensus Algorithm (IBFT) [1] consensus algorithm, incorporating the round change mechanism. Additionally, we aimed to ensure integrity and authenticity guarantees in message exchange using a Public Key Infrastructure (PKI). Furthermore, the development of a client library and clients, along with rigorous testing and evaluation of the system, were key focus areas.

2 Design Explanation and Justification

2.1 System Architecture

Our system is composed of multiple nodes responsible for maintaining the blockchain, which communicate with each other using the IBFT. Clients interact with these nodes through a client library, functioning as an API for executing operations on the blockchain. Currently, the client application offers two operational modes: when provided with a script as an argument, it executes commands read from the script; alternatively, without a script argument, it operates as a command-line interface, allowing users to directly input and execute commands.

2.2 Communication

Communication between all entities is facilitated through Authenticated Perfect Links. We utilize the perfect link implementation provided by the professor, that works over UDP, and then employed a digital signature algorithm to guarantee authentication, integrity and non-repudiation. This involves each sent message being signed with the sender's private key and subsequently verified by the receiver using the sender's public key. We opted for digital signatures

over Message Authentication Codes (MAC) due to the absence of infrastructure for symmetric key sharing necessary for MAC usage. Additionally, digital signatures offer enhanced security by guaranteeing non-repudiation.

Furthermore, to enable secure communication, all entities possess access to the public keys of the other nodes beforehand, retrieved from configuration files.

2.3 Consensus Algorithm

The majority of the consensus algorithm was already implemented, and we focused on implementing the round change mechanism according to the paper.

In our system, the different nodes of the blockchain communicate with each other through authenticated perfect links. Each node is listening on two ports: one to receive messages from other nodes of the blockchain and another to listen for client messages.

3 Testing Approach and Dependability Guarantees

To verify the behavior, correctness and robustness of the system under various fault models, including crash fault and arbitrary fault scenarios, we have enhanced the configuration of individual nodes. These properties classify nodes as exhibiting normal behavior or simulating specific "bad" behaviors, such as:

- **Non-Leader Consensus Initiation**: Initiating a consensus without being the leader to test if the system can handle unexpected actions.
- **Leader Impersonation**: Simulating being the leader (or other node), causing other nodes to fail signature verification, testing resilience against malicious actors.
- **Corrupt Broadcasting**: Broadcasting different values to different nodes to assess the consistency and fault tolerance of the system.
- **Corrupt Leader**: Leader sends different messages to different nodes.
- **Crash**: Simulating crash failures by abruptly terminating node processes after a fixed duration of operation.

In the next stage of our testing approach, we aim to incorporate additional scenarios to further enhance the resilience and dependability of our system.

Since the algorithm is well-implemented and there is always a quorum of correct nodes, our system is prepared for these situations. All tests ran without problems, proving that our system provides safety, integrity, authenticity, reliability, and availability.

4 Conclusion

We conclude that we have successfully achieved all objectives outlined in the first part of the project. Moving forward, we propose the following improvements:

- Enhance the connection between clients and nodes; currently, they broadcast messages to all nodes, which may not be the most efficient method.
- Implement a mechanism to exclude Byzantine nodes from the system when detected, enhancing overall system reliability and security.

References

[1] H. Moniz. The istanbul bft consensus algorithm. *arXiv preprint arXiv:2002.03613*, 2020.