Highly Dependable Systems

João Furtado 99095

Guilherme Carabalone 99078

João Bettencourt 96880

SEC Group 29

March 8, 2024

Abstract

This report outlines the enhancements made by SEC Group 29 to a blockchain system. Our objectives were: improving channel authentication, developing a client library, implementing round change functionality, and conducting comprehensive testing.

Contents

1 Introduction

This stage of the project aimed to complete the initial channel implementation, create a library for the client to append blocks to the blockchain, implement the missing round change component of the IBTF algorithm and test the system behaviour.

Not all of these objectives were met, namely the tests and details of the round change protocol.

2 Implementation Details

2.1 Channels

After analysing the given channel implementation, it was concluded that the abstraction provided were Perfect Links.

With that in mind, the next step was to authenticate the channels using a Public Key Infrastructure (PKI), thereby guaranteeing Authenticated Perfect Links. In the beginning of the system's execution, both clients and nodes know everyone's public key. Therefore, every message is signed with a digital signature (DS) before being sent over the Links, and whoever receives it only accepts the message if the signature is valid.

2.2 Client Library

Each client has access to a library instance, which is utilized to communicate with the server nodes.

When a client wants to make an append request, it sends a broadcast to the server nodes and waits until consensus is reached.

Instead of employing a broadcast mechanism, we explored the possibility of multicasting the request to a subset of f + 1 nodes. This approach was considered more efficient due to the reduced message overhead. However, we opted for the former method in our early implementation to ensure that the leader reliably received the client requests. If the client were to multicast the request and the leader node did not belong to the subset of nodes, additional processes would be required to forward the request to the leader. This step would be necessary for the leader to initiate the broadcasting of Pre-Prepare messages to commence the consensus process.

2.3 Round change

Initially, our approach involved implementing the pseudocode algorithm outlined in Dr. Henrique Moniz's paper. Regrettably, we encountered delays in the implementation process. Despite our efforts, we proceeded with the full implementation of the pseudocode without incorporating message justifications. As a result, our current implementation is far from perfect. Notably, while we can advance to new rounds, certain events such as commit still accept messages from previous rounds and make decisions based on outdated values. Unfortunately, these issues hindered our progress to address the justifications for our implementation. Due to time constraints, we were unable to debug the current round change implementation. We aim to complete this implementation before transitioning to the second stage of the project.

2.4 Tests

Similar to our challenges with implementing round changes, time constraints limited our ability to conduct thorough testing. We managed to execute only one test by running:

```
python3 puppet_master 3
```

This test delays messages for half of the server nodes, triggering the round change process. However, although the round change occurs, the server nodes still base their decisions on values from the previous round. This highlights the importance of testing for validating implementation functionality. Unfortunately, due to time limitations, we were unable to conduct further tests or address the observed issues before proceeding to the next project stage.

2.5 Future Improvements

To enhance the system's functionality and reliability, several areas warrant attention:

- Fix round change functionality.
- Provide justifications for round changes.
- Conduct thorough testing.
- Implement multicasting to a subset of f+1 nodes instead of broadcasting.

3 Conclusion

In summary, while the implementation of channels and the client library proved successful, the same cannot be said for round changes and testing. Before advancing to stage two, we will address these aspects to ensure the completeness and reliability of our blockchain system.