Title
Subtitle

Guilherme João Bidarra Breia Lopes

Master's disseration planning
Engenharia Informática
(2nd degree cycle)

Supervisor: Prof. Doctor Simão Melo de Sousa

janeiro de 2023

Palavras-chave

Inserir palavras-chave

Contents

Acronymms

NFT	Non-fungible token

Chapter 1

Introduction

1.1 Intoduction

Blockchains have gained significant attention in recent years for their potential to revolutionize various industries by providing a secure and transparent method for storing and transferring information and assets. At their core, blockchains are decentralized and permissionless ledger systems that leverage cryptography, consensus algorithms and State Machine Replication to maintain a shared history of all transactions on the network.

The increasing popularity of blockchains can be attributed to the growing demand for secure and transparent systems in various industries, particularly finance, supply chain management, digital identity and recently digital assets with the use of Non-fungible tokens.

In addition, the distributed nature of blockchains enables them to operate in a trustless environment, reducing the risk of single point of failure and ensuring the integrity of data stored on the network.

Consensus algorithms play a crucial role in the functioning of blockchains, as they determine the process by which transactions are validated, new blocks are added to the chain, and other details such as the selection of the next block producer.

Different consensus algorithms offer varying levels of security, scalability, and decentralization, and choosing the right algorithm for a specific use case is critical for the success of a blockchain network.

The main objectives of this dissertation are to compare different consensus algorithms for blockchains, evaluate the trade-offs between security, scalability, decentralization, and explore the potential for consensus algorithms to be plugged and changed on demand. Additionally, the dissertation will cover the implementation and testing of a blockchain network with a pluggable consensus algorithm and a thorough examination of the Tezos(REFERENCIA) blockchain as a testbed for consensus algorithms.

This dissertation will provide valuable insights into the field of blockchains and consensus algorithms, contributing to the development of more secure, scalable, and efficient blockchain systems, such as tools and methods to test consensus algorithms, to develop algoritms and to include them in already developed blockchain nodes.

1.2 Motivation

Despite the growing popularity of blockchains, there is currently a lack of tools and methods for easily swapping and testing different consensus algorithms in a live environment. This makes it difficult to determine which algorithm is best suited for a specific use case, particularly in the context of the blockchain trilemma, where it is challenging to achieve optimal

balance between scalability, security, and decentralization.

Additionally, developing consensus algorithms can be a complex and time-consuming task, and there is currently no standardized method for describing and implementing them. This presents a significant barrier to the adoption and evolution of blockchains, as it limits the ability of developers to experiment with new and innovative consensus algorithms. Also, the decentralization being one of the strenghts points of blockchain networks falls in the hands of a few selected developers.

This dissertation aims to address these challenges by providing a comprehensive analysis of different consensus algorithms for blockchains, and exploring the potential for consensus algorithms to be plugged and changed on demand. The results of this study will serve as valuable feedback for the development of a domain-specific language for describing consensus algorithms, and will provide insights into the most effective methods for testing consensus algorithms in a live environment.

The importance of this research cannot be overstated, as the ability to easily swap and test consensus algorithms is critical for the continued growth and evolution of blockchains. This will not only benefit the academic community but also industry stakeholders, who will be able to make informed decisions about which consensus algorithm is best suited for their specific use case.

In conclusion, this dissertation is motivated by the growing need for a comprehensive analysis of consensus algorithms for blockchains, and the desire to explore new and innovative methods for swapping and testing consensus algorithms in a live environment. The objective of this study is to contribute to the development of a standardized method for describing and testing consensus algorithms, ultimately advancing the field of blockchains and improving the security, scalability, and decentralization of blockchain networks.

1.3 Problem Statement

(REFERENCIA) (TODO: REMOVER REPETIÇÃO DAS COISAS) Consensus algorithms, being a fundamental aspect of blockchain technology, are subject to a range of emerging problems. Hardforks, network Denials of Service attacks, centralization of networks, and other relevant issues are challenging the stability and security of these systems. The choice between scalability, security, and decentralization, as described by the Blockchain Trilema, can lead to trade-offs in the design of consensus algorithms.

One of the challenges of consensus algorithms is the difficulty of changing the rules of the game after a blockchain network has been established. The hard forks of the Bitcoin, Bitcoin Cash, and Bitcoin SV networks have highlighted this issue. Similarly, the Ethereum network has also undergone several hard forks, leading to a split in its community.

Scalability issues are another challenge faced by some blockchain networks, including Bitcoin and Ethereum, which have struggled to accommodate increasing demand. In addition, some networks, such as Solana, have experienced outages, further highlighting the need for a more robust and reliable consensus system.

This dissertation aims to address these challenges by exploring the development of con-

sensus algorithms and ways to test them. The Tezos blockchain provides a suitable platform for this work, as it has a pluggable consensus system and allows for the implementation of different consensus algorithms. The goal is to learn how to develop consensus protocols in Tezos, develop the main entry points for a possible connection with a Domain Specific Language, and develop ways to test consensus algorithms. The first subject of such tests will be a proof-of-work consensus algorithm.

The question we want to answer in this dissertation is the following: How can we make a blockchain network that is flexible in terms of consensus algorithm selection and provides a platform for testing and comparison of different consensus algorithms? By addressing this question, we aim to provide a solution that will allow blockchain networks to be more scalable, secure, and decentralized, thereby addressing the challenges posed by the trilema. Additionally, this dissertation will serve as input/feedback for later work on a Domain Specific Language that will be used to describe consensus algorithms, making it easier to develop and test consensus algorithms in the future.

1.4 Document Organization

Bibliography