RESEARCH

A Study of Blockchain Consensus Mechanisms with Emphasis on Proof-of-Reputation

Yidi XING[1*]
, Omar HASAN[1]
, Sonia BEN MOKHTAR[1]
, Tarek AWWAD[1]
, Lionel BRUNIE[1]
and Harald KOSCH[2]

Correspondence:
idi.xing@insa-lyon.fr
LIRIS Laboratory, National
nstitute of Applied Sciences of
yon, 20 avenue Albert Einstein,
9100 Villeurbanne, FR
ull list of author information is
vailable at the end of the article

Abstract

- What is blo

- The emergence of blockchain technology enables people to build a distributed, decentralized and tamper-proof account book through a trust free P2P network. This technology has broad application prospects in the fields of digital assets, remittances, online payment and other financial services. Sytems based on blockchain technologies combined the application of P2P network, public key cryptography, hash pointer and cryptographic hash function to ensure the decentralization, persistence, tamper resistance, forgery resistance and auditability of the system.

- The feature

- Users, as distrustful parties, can agree on the existence, value and transaction history of each other's accounts by maintaining consistency on the global blockchain network. This feature of blockchain network makes it possible to greatly save transaction costs, especially financial transaction costs, and improve transaction processing efficiency. It also allows financial services without the support of any banks or intermediaries.

- What is block

- In the area of blockchains, consensus algorithms are the key elements in each blockchain P2P network, because they are responsible for maintaining the integrity and security of these distributed systems and ensuring that the system can operate on a trust-free basis. Consensus algorithms can be defined as a mechanism to achieve agreement in blockchain networks. Blockchain systems have decentralized attributes and are constructed as distributed systems. Since they do not rely on a central authority, decentralized nodes need to agree on the validity of transactions, which is the function of consensus algorithms. Consensus algorithm ensures that all nodes comply with the rules defined by the system designer and that all transactions are conducted in a reliable manner.For example, in the field of cryptocurrency, each token coin used for trading can only be spent once.

Abstract - What the re

- While trying to balance security with functionality and scalability, each consensus protocol shows its own advantages and disadvantages. In this paper, we will focus on the analysis and comparison of different types of consensus protocols. In the second section, we first present the general design model of the hierarchical block chain system we envisage. We will further reveal the importance of the consensus layer by showing its importance, utility and potential interaction with other layers. Then in sections III and IV, we analyze and compare fourteen different consensus protocols. In the fifth, sixth and seventh sections, we will focus on an innovative concept of consensus protocols: proof-of-reputation protocols (PoR). PoR introduces the concept of reputation into the consensus process. We first introduce the general design model of PoR. Then we enumerate five existing por projects, compare and analyze their ideas, advantages and disadvantages, and try to provide possible trends for the future development of proof-of-reputation protocols.

Keywords: blockchain; consensus protocol; proof-of-reputation; decentralization

Declaration

Availability of data and materials

The blockchain systems data that support the findings of this study are available from “bitcointalk.org”, “www.coingecko.com/fr/pièces/”, “www.feixiaohao.com”, “coincheckup.com”, “blocktivity.info”, “bitinfocharts.com”, “www.reedit.com/r/Vechain/comments/97zmoy”.

Also, the next reported blockchain systems data were used to support this study and are available at “Practical Byzantine fault tolerance”, “Bitcoin: A peer-to-peer electronic cash system”, “https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf”, “DBFT: Efficient byzantine consensus with a weak coordinator and its application to consortium blockchains”, “The ripple protocol consensus algorithm”, “On security analysis of proof-of-elapsed-time (poet)”, “Slimcoin: A peer-to-peer crypto-currency with proof-of-burn”, “Proofs of space”, “Delegated proof-of-stake (dpos)”, “Komodo: An Advanced Blockchain Technology, Focused on Freedom”, “Komodo: An Advanced Blockchain Technology, Focused on Freedom", "Solana: A new architecture for a high performance blockchain v0.8.13", "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain", "Algorand: Scaling byzantine agreements for cryptocurrencies", "gochain.io/assets/gochain-whitepaper-v2.1.2.pdf", "Blockchain: The State of the Art and Future Trends". These prior studies (and datasets) are cited at relevant places within the text as references [8-11, 13-23].

Competing interests statement

The authors declare that they have no competing financial interests.

Fundings

//TO DO

Authors' contributions

Y has drafted the work. Y was the major contributor in writing the manuscript and also substantively revised it. O and SB ahve made substantial contriubtions to the conception and the design of the work. O and SB have also substantively revised the manuscript. L and H have drafted the work, and have made important contributions to the conception of the work. T have made important contributions on the substantive amendments. All authors read and approved the final manuscript thus the submitted version.

I Introduction

- The composition of a b

Blockchain technology was first implemented by Nakamoto with Bitcoin applications in 2009[9]. It combines the application of encrypted hash functions, digital signature, Merkle tree, consensus protocol and peer-to-peer (P2P) network, so as to build a distributed and decentralized system based on trust-free P2P network. It could be used not only for financial trading systems[1],[2], but also Scientific research, resource management[3],[4], political domain[6],[7], etc. Using blockchain technologies, we can build a distributed database system based on distributed P2P network. The system could record a public account book, or called a "public ledger" – this ledger sorts groups of transactions in chronological order and uses encrypted hash function such as SHA256 to encryptedly link each group of transactions. Those sets of transactions in the record are stored in a specific data structure, which we call a data block. As new transactions continue to be completed, they are packaged into data blocks, which are submitted to the end of the list of data blocks on the public ledger. That's also why we call this technology blockchain.

- Features blo

The information contained in the ledger shows transaction history up to the current time through block chains. These transaction records prove the existence and value of each account. Therefore, in a decentralized block chain system, every update of the ledger must be authenticated by each account holder in the network. Of course, this means that there is a need for consensus among participants. In the real world, we may not be able to find application examples with the same limitations. For example, when an entity (bank or country) decides to issue legitimate digital currency, it does not need to establish a public ledger that must be confirmed in real time by each currency holder, because the entity, as the central agency, is responsible for the verification needed to use such digital currency for transactions and ensures the security of transactions. In blockchain networks, this is not the case: nodes operate independently. In order to reach consensus, it is essential and necessary for nodes to communicate with each other through the network.

- An introductio

It can be imagined that in such a distributed system, there will be many kinds of errors in the process of sending messages between nodes. We can generally divide them into two types: the first is the error including node crash, data packet loss and network failure. The characteristics of these errors are that the nodes themselves are not malicious to the system. We call them "non-Byzantine errors". The second type of errors refers to the arbitrary actions of the nodes and deliberate violations of the rules of action formulated by the system designers. At this point, the wrong node may itself be malicious. The behaviors include sending messages with different contents at the same time to different nodes, delaying or rejecting messages in networks, deliberate attempts to submit illegal transaction records, and so on. Such errors are called "Byzantine errors''. In serious cases, there may be collaboration between malicious nodes, making Byzantine errors a serious problem.

- Introduction of the

The consensus protocol is designed to build a distributed blockchain system a Byzantine fault-tolerant system. In the face of two mentioned types of errors, the design of a qualified consensus protocol can keep the consistency and the liveness of system. Consistency means that honest and harmless system participants agree on records in the public ledger. The liveness represents that the ledger can be updated continuously, efficiently and effectively. There are a lot of practices of consensus protocols: Bitcoin which made successes on marketing, uses the Proof-of-Work protocol where users profit from computing proofs. They randomly find the node determining the next block[9]; or PoS protocol[10], which is used by Peercoin, where users profit there locked stake within the blockchain system prove that they are trustworthy, and to compete to win the right of generating subsequent blocks; or as PBFT protocols, all nodes identity should be known under this configuration. All nodes have equivalent voting rights, and they consumes numerous rounds of communications to reach consensus[8].

- New paragraph-

In this paper, we will focus on consensus protocols. First, we will give a general blockchain model which is widely used in practice. Next, we will introduce fourteen different consensus protocols that have been applied in practical projects, and analyze and compare them. Finally, we will mention a new and noteworthy consensus protocol concept, proof-of-reputation. We will focus on its introduction and analysis, and explain its unique advantages. The rest of this paper is organized as follows. Section II introduces the general design model for blockchain system. Section III shows the state-of-art of fourteen different consensus protocols. Section IV summarizes the precedent ones by giving tables and explanations showing the analysis results of those protocols, with a detailed explanation for these table and figures. Section V introduces the idea of proof-of-reputation, explains its idea, its operation principles, its general model, advantages and disadvantages. Section VI is an another state-of-art section where we list and present five different existing por blockchain projects. Section VII concludes.

II Background

In this section, we will introduce a general, layered and modular blockchain system model. It can be regarded as a template for blockchain projects that are now in operation. We will explain its composition, analyze which functional units the system consists of, which functions and operations the system supports, and which technologies the system uses to achieve them. The model in this section is inspired by the work of Yuan et al.[23]. Some changes have been made in the specific content, then in the layers and modules division. This basic model will consist of five layers: the data layer, the network layer, the consensus layer, the incentive schemes and the application layer.