iipp publishing

Journal of Quality and System Engineering

ISSN 2812-975X

2 (2022) 1

Journal homepage www.q-sci.rs

An overview of the blockchain consensus mechanisms

Dijana Stojić[1], Dejan Vujičić[1], Đorđe Damnjanović[1], Dušan Marković[2], Siniša Ranđić[1]

[1]University of Kragujevac, Faculty of Technical Sciences Čačak, Serbia

[2]University of Kragujevac, Faculty of Agronomy Čačak

Abstract

This paper presents the most commonly used algorithms and protocols for validation of data processing in network conditions. In order to understand the needs of the mentioned procedures, the needs and characteristics of distributed data processing are pointed out. Given the problems of management, which would bring a centralized approach to the distributed environment, the need of a new approach in terms of management was explained. Since the blockchain concept proved to be a good solution, the concept itself and the advantages over existing solutions were explained. The functioning of the blockchain from the aspect of validation of transactions, which are performed in the network environment, requires the existence of a mechanism by which the validity is confirmed. Since nodes within the network participate in the validation of transactions, algorithms are presented that achieve agreement regarding the validity of transaction results.

Key words

Distributed data processing
Data security
Blockchain
Consensus mechanism

Corresponding author

djordje.m.damnjanovic@gmail.com

Article info

Original Scientific Paper
Received 10.01.2022.
Accepted 18.05.2022.
Online available 10.10.2022.

1. Introduction section

Computer networking, especially the development of the Internet, as a global computer network, has brought a revolution in data processing. Thanks to this, in order to make a transaction, such as a payment / withdrawal in a bank, payment for goods or services, it is no longer necessary to go to a bank or store. A transaction order can be issued from anywhere in the world, provided that there is the possibility of access via the Internet. Transactions are performed faster, and it saves time and transport costs to the place of the transaction.

The data that is processed on the Internet, including applications for their processing, is located on servers distributed around the world. The servers are connected to the Internet, which ensures the integrity of the databases that are the subject of transactions. Thanks to the principle of data locality, it is possible to achieve spatial approximation of data to users through the distribution of databases. Distributing data, which is of interest to certain users on servers, which are located near the place where they are most often used, creates conditions for faster access to such data. At the same time, the load on the Internet is less, because the request is processed on a nearby server.

Distributed data processing in databases, the integrity of which is ensured via the Internet, as a communication infrastructure has enabled a new quality of processing, especially when it comes to a huge amount of data. However, this type of data processing has brought significant problems in terms of transaction security and reliability of the obtained results. Simply put, it is difficult to implement centralized transaction control in a distributed data processing system. It would only further increase the load on the communication system. This would nullify all the benefits offered by distributed data processing. Therefore, the question arose as to whether secure transactions could take place without intermediation, e.g. banks or states. One of the approaches, which shows great potential for solving this problem, is the blockchain concept [1].

A blockchain is a data structure, which consists of blocks that are interconnected and that contain information about transactions. Through this system, it is possible to perform transactions over facilities such as: cadastre data, bank accounts, birth and death registers, voter lists, etc. The blocks contain information about all executed transactions. The blockchain approach enables communication between the servers on which the data is located, over which the transaction is performed. By executing a new transaction, the relevant information, including the time when it occurred, is added chronologically to the existing chain of blocks.

This paper provides an overview of consensus mechanisms, which provide fault tolerance, as well as possible ways to verify the validity of transactions. This mechanism enables the preservation of agreement between nodes in the network within which the blockchain concept operates. The growth in the number of nodes brings the problem of preserving the agreement, so it is a very important mechanism for its preservation, especially since blockchain is a dynamic data structure.

2. Distributed data processing

Distributed data processing and management have gained in importance with the advent of new applications, which require the processing of large amounts of data. Such applications include scientific applications [3], data analysis at the WEB level [5], social networks, etc. As the amount of data stored in databases increases, they are copied to other external memory partitions or other servers. The goal is to process requests to servers in the shortest possible time, e.g. in a few milliseconds.

In order for distributed data processing to be feasible, it is necessary that there be records of processing over each copy of the database. Based on the given records, the records in the database are updated. It is not necessary to check the database to determine whether there has been a change. Thanks to this, a specific relationship between the application and the database is achieved in distributed processing. The application contains processes that monitor messages with processing records and respond to them. And it all happens in real time.

In distributed data processing, resistance to possible errors is of the utmost importance. Also, the distribution of data, as a consequence, has a question of their security. With a centralized database, this is facilitated through various ways in restricting access and introducing access privileges. At the same time, in distributed data processing, the integration of data based on transaction records offers certain improvements when it comes to data integrity and security. The introduction of special fields in the transaction message creates the conditions for minimizing errors when updating the state of the database. Elements of the blockchain concept can be discerned in these approaches.

3. Blockchain concept

A major problem with distributed data processing is the user's trust in the transactions that are executed. Given the distribution of data and the applications that are performed on them, centralized validation of transactions would nullify many of the benefits of distributed data processing.

Therefore, it was necessary to find an approach that would fit into the distributed concept in terms of the way it works. For now, the concept of blockchainis imposed as the best solution. This approach was introduced into practical use through the concept of digital currencies or cryptocurrencies. However, experience has shown that the possibilities of using blockchain go beyond the aspects of virtual money. This means that the blockchain concept could also be applied to different sectors, such as financial transactions, document distribution, trading and supply chains. And even apply in the election process. The blockchain concept has been used to fundamentally change the traditional approach to executing financial transactions [7]. And all with the goal of making transactions as secure as possible. On the other hand, avoiding intermediaries in transactions creates the conditions for them to be significantly accelerated. Of course, this technology is not only applicable in the financial sector. It is noticed that every area of human activity is starting to invest in blockchain in order to improve its business [8].

Behind the blockchain concept is an idea similar to databases. However, communication with blockchain, as a database, is completely different. Unlike centralized database management, blockchain validates content by all network nodes within which a particular transaction is executed. Each block contains a unique hash identifier and a link to the previous block. Therefore, data stored in the blockchaincannot be deleted or changed. In a new transaction, a new block must be added to the chain in order for the data to be updated. Figure 1 shows the blockchain structure, defined by Satoshi Nakamoto, in 2008 [5]

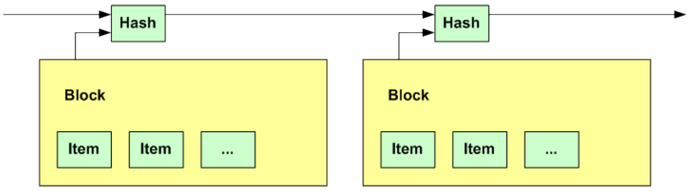

Figure 1: The structure of blockchain by Nakamoto

An important feature of blockchain is that it is a decentralized application approach. The blockchain is not located in one place. More precisely, the data stored in the blockchainis distributed on computers connected to the network. At the same time, no participant in transactions has control over the data. Thanks to that, users communicate directly without intermediaries. Due to that, there is a problem of decision making in the blockchain system. And also, the question of how transactions are recorded within the blockchain. Accordingly, for users connected to the blockchain network, algorithms are developed that achieve agreement in decision making [9].

Before pointing out some of the most common algorithms, which are used to establish agreement among blockchain users, the most important features of blockchain should be reminded once again. First of all, we should mention the immutability, according to which no one can change the information related to transactions that are written within the blockchain. Theoretically, this could be done if more than half of the users voted for it. Or if someone had control over more than half of the nodes in the network. Protection in databases, which use blockchain, is based on the formation of hash functions, which ensure the use of unique identifiers at the level of each block. The hash identifier of the block is also related to the hash identifier of the previous block, which provides additional protection. With the distributed record of transaction data, the slowdown that exists, e.g. code of classical banking systems. The speed of transactions, in a blockchain system, depends on the size of the block, the transaction costs and the network load.

The consensus mechanism has proven to be a good approach to prevent transaction verification errors. Its use ensures that the agreement between the nodes in the network is preserved. This is especially important from the aspect of network expansion and user participation in the transaction verification process.

4. Blockchain consensus mechanisms

The consensus mechanism in distributed databases is important from the aspect of preserving the efficiency of the network in which the database is distributed. In addition to ensuring that the state of the database is up-to-date, consensus is also important for security and fault tolerance of data distributed in the network. At the same time, the consensus mechanism should enable recovery from possible failures, which originate from individual nodes in the network [13].

During this century, several different classifications of consent mechanisms were introduced. One of them is shown in the Figure 2.

Paxos was the first proposed algorithm for achieving consensus [14]. He generally provided consent regarding the acceptance of a value or transaction in the event of a shutdown or some other error in the network. Nodes in the network are divided into proposers, acceptors and learners. Proposers send proposals, which are considered by the recipient. The time sequence of the proposal is defined by the number that the proposer joins the proposal. They are compared with known values and the proposal is accepted if it is more recent. Recipients answer whether they have accepted the proposal or not. If the majority of receivers have accepted the proposal, it is updated and considered the latest value. Consent is reached if at least N/2 – 1 of the proposal is accepted by the receiver, where N is the number of proposals.

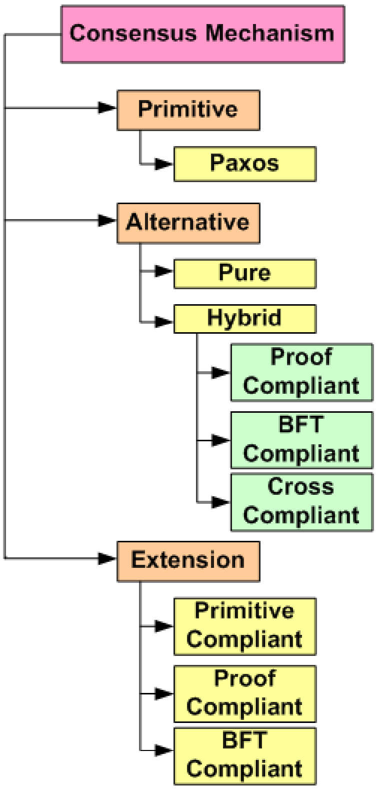

Figure 2: Consensus mechanisms classification

As already mentioned, the security of transactions within networks, using blockchain, is based on various cryptographic categories. The most important of these are the asymmetric coding key, hash functions, and consensus protocols [11]. Although some of the consensus protocols have gained popularity during implementation, shortcomings have also been noted. Through attempts to improve them, alternative consensus protocols have been developed, especially for specific areas of application. When defining the new protocols, care was taken to achieve the best possible performance, using parameters such as: throughput, scalability, security, energy requirements and finality. Finality is of special importance, because it determines the degree of confidence that the formed blocks, which are included in the blockchain system, will not be changed. Most current protocols in terms of finality are based on probability, and 51% consensus, which was defined by Nakamoto.

Consensus protocols are fundamentally important for networks that use blockchain. According to the mode of operation, protocols can be divided into two large groups: evidence-based protocols and voting-based protocols. Some of the most well-known protocols, which belong to the first group, are:

- Proof of Chain (PoC);
- Proof of Work (PoW),
- Proof of Importance (PoI);
- Proof of Elapsed Time (PoET);
- Proof of Authority (PoA);
- Proof of Burn (PoBr).

As for voting-based protocols, these are the best known:

- Proof of Stake (PoS);
- Ripple Protocol (RP);
- Practical Byzantine Fault Tolerance (PBFT);
- Federated Byzantine Agreement (FBA).

Proof of Chain (PoC) was created based on the Proof of Stake (PoS) algorithm with the goal of increasing network security, when paying with cryptocurrencies, using distribution and transparency. In the Proof of Stake concept, the importance in decision making is measured by the solvency of the user. Proof of Chain is based on client activities in a time interval. Specifically, this algorithm encourages users to execute transactions, which increases network security.

In Proof of Work (PoW), the importance of blockchain network users is determined by the computing power they have [15]. This protocol is widely used in the process of obtaining cryptocurrencies. A user who manages to complete a transaction and adds a new block to the network receives a fee for the completed transaction. In the case of the PoW protocol, computing power is used to solve hash problems. Its solution is included in the block obtained within the transaction. That is why the most famous cryptocurrencies, such as Bitcoin and Ethereum, are based on this protocol, although Ethereum is changing its consensus mechanism to Proof-of-Stake.

The Proof of Authority (PoA) is based on nodes, which are considered reliable and are called validators [16]. Since the number of validators is limited, the network has a large throughput and scalability. The cost of processing a blockchain is very small, because validators do not invest assets, but only their reputation. The disadvantage of this protocol is the tendency towards centralization of the network, because it is managed by a small number of users (validators).

The Proof of Importance (PoI) protocol was created under the auspices of the NEM (New Economy Movement) movement, whose desire is to advance the blockchain concept [17]. The influence of the node on decision making is measured by the amount of cryptocurrency that the node has at its disposal. The NEM organization has its own currency XEM. The minimum amount that allows a node to make decisions is 10,000 XEM. Nodes, which have a smaller amount than this, have zero importance. Accordingly, they will not be able to create new blocks.

Proof of Elapsed Time (PoET) was created as a replacement for the Proof of Work protocol. It was introduced by Intel in 2016. [18] The principle of competition applies to this protocol. Nodes are randomly assigned waiting times. To be eligible to add a new block, the node must show that it had the shortest waiting time in which it did not generate its own block. This protocol allows the system to be more decentralized. Also, the system allows easy verification of the legitimacy of the node that gets the chance to broadcast the block. The disadvantage is that it is not suitable for public blocks. And also, it has the disadvantage that it is related to the use of specialized Intel hardware.

Unlike other protocols, which involve investing in computer resources, the Proof of Burn (PoBr) protocol uses the number of cryptocurrencies burned, as a criterion for selecting block creators [19]. De facto burning of cryptocurrencies is analogous to buying the level of commitment of the node to the entire network. The currency is burned by sending it to a specific address. And the process is irreversible.

Proof of Capacity (PoC) is a protocol based on allocating a certain amount of space in memory or disk [20]. This space is intended for solving the problems of the service provider. The memory space that is reserved is an indicator of the commitment of a given node to the network. In order to confirm this, a node that requires a particular service must go through a verification process. In practice, a node can hardly go through the verification process if it has not reserved memory. Cryptocurrencies such as Burstcoin, Chia and SpaceMintare based on this protocol.

As for voting-based protocols one of the best known is the Practical Byzantine Fault Tolerance protocol. The validation process takes place by the selected node generating an ordered list of transactions, which are sent to other nodes for verification [21].

As the nodes execute the transactions, the nodes that perform the validation generate a hash code for the new block. If two-thirds of the received hash codes are the same, the block corresponds to a local copy of the blockchain. One of the main disadvantages of this protocol is the problem of practical implementation of the algorithm, which involves a huge number of calculations.

In Reaple Protocol (RP), a set of validators, also called a single list of nodes, evaluates transactions [22]. It is assumed that there is no agreement between these nodes, ie. that they are honest. When most validators agree on a particular set of transactions, the selected transaction joins the next version of the blockchain. The validation process is iterative, ie. take place until agreement is reached. For the consent to be valid, at least 80% of the validator must be correct.

In recent years, there have been new alternative protocols for reaching consensus in the process of updating blocks in the blockchain. Some of them, such as Proof of Familiarity (PoF), Proof of Benefit (PoB), Proof of Participation and Fee (PoPF), Proof of Vote (PoV) have a specific purpose. On the other hand, protocols such as Proof of Reputation (PoR), Proof of Phone (PoP), Proof of Learning (PoL), Proof of Search (PoSe), Proof of Sincerity (PoSn), Proof of Adjourn (PoAj), proof of Evolution PoE), Proof of Experience (PoEx) and Proof of Accuracy (PoA) have a more general purpose. Also, some of the alternative protocols can be included in several categories.

5. Conclusion

One of the most important issues that arises in distributed data processing concerns the trust that users have in the transactions performed and the results achieved. In the case of centralized data processing, the authorities of the state, banks, large retail chains or transport organizations under whose supervision the transactions are executed stand as a guarantor of the validity of transactions.

A potentially large amount of distributed data requires intensive communication between users, databases, and processing applications. Validation of transactions on a centralized basis would further intensify this communication. In such conditions, the blockchain concept has proven to be a good alternative to centralized transaction management in a distributed environment. Practically the validity of transactions is confirmed by all participants, which eliminates the possibility of changes in the content of blocks, which are connected in the blockchain.

Starting from the basic concept of blockchain, one of the most important elements of this system is the way of maintaining the consensus of participants in transactions that a transaction is valid. As well as that all users can be sure that the results of the executed transaction are reliable and unchangeable. Consequently, research and attempts to find the best possible algorithms for reaching agreement on the validity of transactions are very important.

Based on the presentations given in this paper, it can be seen that during the application of the blockchain concept in distributed data processing, a large number of algorithms for the transaction validation process were developed. The algorithms are based on a wide range of criteria. What they have in common is the aspiration to achieve the highest possible processing performance and the highest possible processing security.

6. Acknowledgment

This work was supported by the Serbian Ministry of Education, Science and Technological Development (Agreement No. 451-03-9/2021-14/200132 Faculty of Technical Sciences Čačak, University of Kragujevac).

7. Reference

[1] Özsu, T., Valduriez, P., "Principles of Distributed Database Systems", 3rd edition, Springer, Heidelberg, 2011

[2] Ailamaki, A., Kantere, V., Dash, D., "Managing scientific data", CACM 53(6), 2010, pp. 68–78

[3] Nathan, S., Govindarajan, C., Saraf, A., Sethi, M., Jajachandran, P., "Blockchain Meets Database: Design and Implementation of a Blockchain Relational Database", Proceedings of VLDB Endowment, Volume 12, Issue 11, July 2019, pp 1539 - 1552, https://doi.org/10.14778/3342263.3342632

[4] Tan, W., Blake, M. B., Saleh, I., Dustdar, S., "Social - Network - Sourced Big Data Analytics", IEEE Internet Computing, September/October 2013, pp 62 - 69

[5] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.org: 9, 2008, DOI: 10.1007/s10838-008-9062-0.

[6] Girish, B. V. S., "Blockchain Technology: Concepts", Whitepaper, Sasken Technologies Limited, May 2018

[7] Sultan, K., Lakhani, R., "Conceptualizing Blockchains: Characteristics & Applications", 11th IADIS International Conference Information Systems, 2018, pp 49 - 57

[8] Rawat, D. B., Chaudhary, V., Doku, R., "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems", Journal of Cybersecurity and Privacy, 1, 2021, pp 4 - 18, https://doi.org/10.3390/jcp1010002

[9] Yang, S., "Interpretation of Consensus Mechanism in Block Chain and its Future Development Trend", International Symposium on Communication Engineering & Computer Science, Advanced in Computer Science Research, Volume 86, pp 441 - 446, 2018

[10] Zhu, Y., "Research on Blockchain Consensus Mechanism and Implementation", AMIMA 2019, IOP Conference Series: Materials Science and Engineering 569, 042058, 2019, doi:10.1088/1757-899X/569/4/042058

[11] Oyinloye, D. P., Teh, J. S., Jamil, N., Alwida, M., "Blockchain Consensus: An Overview of Alternative Protocols", Symetry, 13, 1363, 2021, . https://doi.org/10.3390/sym13081363

[12] A. Baliga, “Understanding blockchain consensus models,” Persistent, vol. 2017, no. 4, pp. 1–14, 2017

[13] Lashkari, B., Musilek, P., "A Comprehensive Review of Blockchain Consensus Mechanisms", IEEE Access Journal, Volume 9, 2021, pp. 43620 - 43652, DOI: 10.1109/ACCESS.2021.3065880

[14] Lamport, L., "Paxos made simple", SIGACT News, 32, 2001.

[15] Ouattara, H. F., Ahmat, D., Ouédraogo, F. T., Bissyandé, T. F., Sié, O., "Blockchain Consensus Protocols", In Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer International Publishing: Cham, Switzerland, 2018; pp. 304–314.

[16] Barinov, I.; Baranov, V.; Khahulin, P. POA Network Whitepaper; Technical Report; 2018

[17] "NEM Technical Reference", Technical Report, NEM Foundation, 2018

[18] Xiao, Y.; Zhang, N.; Li, J.; Lou, W.; Hou, Y.T. "Distributed Consensus Protocols and Algorithms", John Wiley & Sons, Trenton, NJ, USA, 2019

[19] Karantias, K., Kiayias, A., Zindros, D., "Proof-of-Burn", Cryptology ePrint Archive, Report 2019/1096 (to be Presented at Financial Cryptography and Data Security 2020). 2019

[20] Gennaro, R., Robshaw, M., (Eds.), "Advances in Cryptology—CRYPTO 2015"; Springer: Berlin/Heidelberg, Germany, 2015

[21] Cho, H., "ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols", IEEE Access 2018, 6, 66210–66222

[22] "The Ripple Consensus Algorithm", Technical Report; Ripple