ISSN 2181 – 8193

Бухоро мухандислик-технология институти

ФАН ВА ТЕХНОЛОГИЯЛАР ТАРАҚҚИЁТИ

РАЗВИТИЕ НАУКИ И ТЕХНОЛОГИЙ

1
2022

ФАН ВА ТЕХНОЛОГИЯЛАР ТАРАҚҚИЁТИ
ИЛМИЙ – ТЕХНИКАВИЙ ЖУРНАЛ

РАЗВИТИЕ НАУКИ И ТЕХНОЛОГИЙ
НАУЧНО – ТЕХНИЧЕСКИЙ ЖУРНАЛ

Журнал Ўзбекистон матбуот ва ахборот агентлиги Бухоро вилояти бошқармасида 2014 йил 22-сентябрда № 05-066-сонли гувоҳнома билан рўйхатга олинган

Муассис:
Бухоро муҳандислик-технология институти

Журнал Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги ОАК Раёсатининг 2017 йил 29-мартдаги №239/5- сонли қарори билан диссертациялар асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрлар рўйхатига киритилган.

Таҳририят манзили:
200100, Бухоро шаҳри, Қ. Муртазоев кўчаси, 15-уй,
Бухоро муҳандислик-технология институти биринчи биноси, 2-қават, 206-хона.
Тел: 0(365) 223-92-40
Факс: 0(365) 223-78-84
Электрон манзил:
E-mail: fantt_jurnal@umail.uz

Журналнинг тўлиқ электрон варианти билан https://journal.bmti.uz/ сайти орқали танишиш мумкин.

М У Н Д А Р И Ж А - С О Д Е Р Ж А Н И Е – CONTENT

CONSENSUS ALGORITHMS OF BLOCKCHAIN TECHNOLOGY OF INCREASING THE RELIABILITY OF INFORMATION

Akhatov A.R., Nazarov F.M., Rashidov A.E.
Samarkand State University

Annotation. *In this study, the mechanisms and algorithms of consensus algorithms in blockchain technologies are studied. The essence of consensus algorithms is given in the application cases. Consensus algorithms analyze the content and differences between the application of PoW and PoS algorithms and determine the parameters to increase data reliability. The layers of the blockchain and the mechanisms for applying consensus in these layers have been studied. The study was conducted to increase data security and reliability based on the integration of cryptographic methods with consensus algorithms.*

Key words*: Data Reliability, Blockchain Technology, Consensus Algorithms, Blockchain Layers, Cryptography, Distributed Registry.*

MA'LUMOTLAR ISHONCHLILIGINI OSHIRISHDA BLOKCHEYN TEXNOLOGIYASINING KONSENSUS ALGORITMLARI

Axatov A.R., Nazarov F.M., Rashidov A.E.
Samarqand davlat universiteti

Annotatsiya. *Mazkur tadqiqot ishida blokcheyn texnologiylarida konsensus algoritmlarining ishlash mexanizmlari va algoritmlari tadqiq etilgan. Bunda konsensus algoritmlarining mohiyati qo'llanilish holatlari keltirib o'tilgan. Konsensus algoritmlarida PoW va PoS algoritmlarining qo'llanilish mazmuni va farqlari tahlil qilinib, ma'lumotlar ishonchliligini oshirish parametrlari belgilab olingan. Blokcheynning qatlamlari va bu qatlamalarida konsensusni qo'llash mexanizmlari tadqiq qilingan. Tadqiqotda konsensus algoritmlari bilan kriptografik usullarni integratsiyatsiyalash asosida ma'lumotlar xavfsiligi va ishonchliligini oshirish amalga oshirilgan.*

Kalitli so'zlar: *ma'lumotlar ishonchliligi, Blokcheyn texnologiyasi, Konsensus algoritmlari, Blokcheyn qatlamalari, Kriptografiya, taqsimlangan reestr.*

КОНСЕНСУСНЫЕ АЛГОРИТМЫ БЛОКЧЕЙН-ТЕХНОЛОГИИ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ

Axatov A.R., Nazarov F.M., Rashidov A.E.
Самаркандский государственный университет

Аннотация. *В данном исследовании изучаются механизмы и алгоритмы консенсусных алгоритмов в технологиях блокчейн. Суть алгоритмов консенсуса раскрывается в примерах применения. В алгоритмах консенсуса анализируется содержание и различия в применении алгоритмов PoW и PoS и определяются параметры для повышения достоверности информации. Были изучены слои блокчейна и механизмы применения консенсуса на этих уровнях. Исследование направлено на повышение безопасности и достоверности информации за счет интеграции криптографических методов с консенсусными алгоритмами.*

Ключевые слова: *Достоверности информации, технология блокчейн, алгоритмы консенсуса, слои блокчейна, криптография, распределенный реестр.*

***I*ntroduction.** Based on the experience of leading developed countries in the development of information technologies in Uzbekistan and their introduction into production, science, education and sports, the solution on the basis of distributed register-based blockchain mechanisms will serve to improve the quality of this sector.

Nowadays, with the sharp increase in the flow and volume of information, the problem of processing this information and ensuring their security is also increasing significantly. The use of blockchain technology in increasing data reliability is a new approach. The use of blockchain technology is an effective way to ensure information reliability in improving the data reliability of automated control systems based on network technology [1, 2].

Ensuring the confidentiality, integrity and reliability of information at all stages of its timely receipt and transmission is of great importance in increasing the reliability of information. Currently, the development factors of blockchain technology are also determined by the focus on the use of decentralized technologies for database protection, ensuring the variability and implementation of actions related to security levels. Blockchain technologies and principles

allow to achieve maximum transparency and versatility of application in the rapidly changing "digital world" in their implementation.

A blockchain is a type of distributed ledger consisting of consecutive blocks chained together following a strict set of rules. Here, each block is created at a predefined interval, or after an event occurs, in a decentralised fashion by means of a consensus algorithm. Even though the terms blockchain and DLT (Distributed Ledger Technology) are used inter-changeably in the literature, there is a subtle difference between them which is worth highlighting. A blockchain is just an example of a particular type of ledger, there are other types of ledger. When a ledger (including a blockchain) is distributed across a network, it can be regarded as a Distributed Ledger [2, 3].

In general, blockchain technology is a multifunctional and multi-level information technology designed to reliably account for network procedures and actions performed on a network. This technology is a technology that keeps records of all transactions at a given time in a reliable distribution. A blockchain is a chain of information blocks, the amount of which is constantly growing due to the addition of new blocks. This is a chronological database, i.e., the time at which such a database is stored is inextricably linked to the information itself, which makes it unstable.

Blockchain consensus algorithms in increasing data reliability. Depending on the composition of the controlled systems, the use of blockchain mechanisms, the form of the data and their types, of course, the choice of one of the consensus algorithms is required. Consensus algorithms are used to validate the data contained in distributed registry technology. Consensus algorithms also include a set of hybrid solutions, including Proof-of-Burn (proof of resources), Proof-of-Activity (proof of assets), Proof-of-Capacity (proof of quantities), Proof-of-Storage (proof of savings). While these hybrid algorithms combine the advantages of the two approaches, they do not overcome the vulnerabilities in the data reliability of control systems [3, 4]. This is due to the fact that it does not comply with the principles of governance and has an excess of resources. Figure 1 shows the application of Blockchain consensus algorithms in year-round systems.

Of the consensus algorithms currently based on blockchain, the Proof of Work and Proof of Stake algorithms are the most popular.

The principle of operation of the algorithm Proof of Work (Pow). Pow is based on the principle of proving the work done and is to guarantee the authenticity of the block by solving a complex calculation problem of each transaction involved in the network. Originally, the concept of Pow was proposed in 1993, in which it included only the theoretical aspect. In 1997, this idea was used in HashCash to protect against spam. Complex hash calculations had to be performed to send the data. No human intervention is required during Pow's operation. Each process is checked in automatic mode,

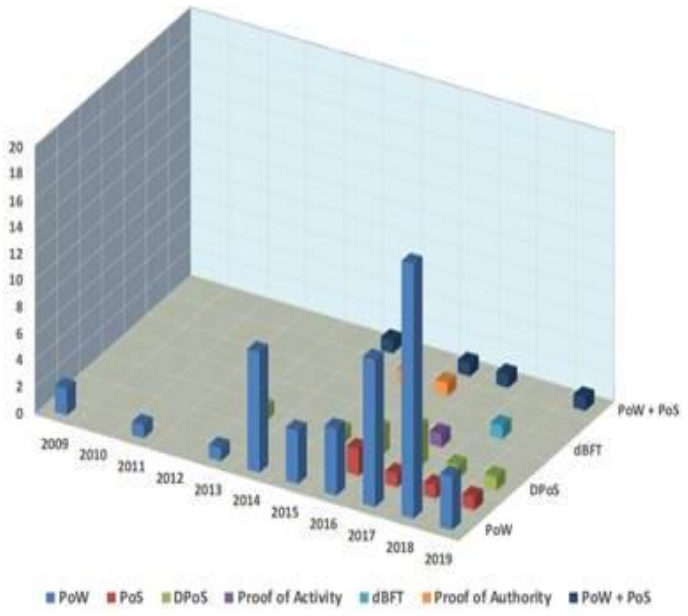

Fig 1. Application of consensus algorithms in year-round systems.

but it is an energy-intensive process and requires a large amount of computing power and, in contrast, less time and money in checking the result [5]. For a successfully completed transaction, the user is interested in receiving information on the network.

This principle was originally applied since the existence of the bitcoin system and provided a clearly available amount of bitcoin as a benefit. In our opinion, this blockchain technology is defined to expand the popularity but is very important for the functional capabilities of the benefit mechanism technology and can be applied to information systems in various fields.

Ensuring a high level of information security in Powda is a huge achievement, but it suffers from a serious shortcoming in managed systems. At the same time, inefficient use of resources and the gradual loss of centralization, that is, an increase in shares, leads to an increase in resource utilization [6, 7]. Even in the Bitcoin system, the cryptocurrencies in which Pow operates are characterized by secondary costs. However, these costs decrease with the increase in the volume of transactions performed on the network and depend on the available computing power for hackers. To maximize the risk of secondary consumption, users wait for their transactions to be approved and use additional protection mechanisms to reduce the risks. For this reason, relying on algorithms that require less resource use and do not lead to the centralization of data acquisition in the network leads to higher efficiency. The working principle of the Proof of Stake (Pos) algorithm. In blockchain-based systems today, it consists of methods and solutions based on a common (Proof-of-stake or Pos) share validation algorithm.

Pos was first used in 2012 in PPCoin (Peercoin) cryptocurrency. Objects called “stakes” are used to identify the node where each block gets access to the next block. This process performs almost the same function as Pow, but in which the load and complexity are proportionally separated. For example, digital resources in a user account are taken as the basis, i.e. the next block can most likely be created by a user who has more balance in the content of resources. Systems using the POS method are usually based on decentralized management and backup principles, which does not ensure that fraudsters know exactly which version of the blockchain [2, 7].

Determining this process requires a great deal of computation and time effort, with the result that data risk does not provide a clear benefit to success. Such a scheme is more progressive and advanced compared to Pow, because it does not require much resources and parameters of computers. The protection of such an algorithm is beyond doubt, because in order for a malicious user to attack, it must have a more resource balance than the rest of the network. However, the other side of the issue is the accumulation of large resources on the one hand, which affects the decentralization of the network.

A user or group of users with a larger amount of resources may apply their own procedures and rules. This is a serious problem for any security system. If Pos is explained in simple terms, then the definition of the algorithm principle can be given as follows. The higher your share in the system, the more likely your mine will be successful.

The taxonomy of blockchain consensus algorithms is shown in Figure 2.

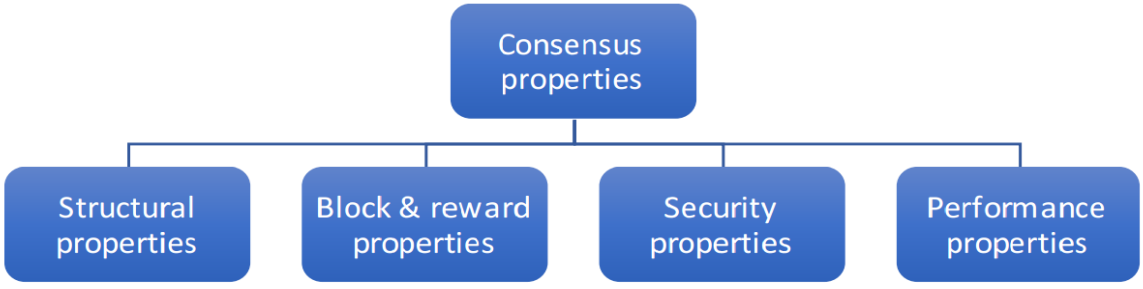

Fig 2.Taxonomy of consensus properties.

This process also applies to security, because the Proof of Stake is not only the security of the mine, but also the security of the assets. If there are a sufficient number of nodes in the system, the effect of a hacker attack on system data will most likely be eliminated. In addition, for a data attacker, the network must have a huge share of publicity and very large costs. As a result, the method based on the Pos algorithm is the most efficient method for management systems because every piece of information in management systems is classified as a share.

With the introduction and advancement of different blockchain systems, there has been a renewed interest in distributed consensus with the consequent innovation of different types of consensus algorithms. These consensus algorithms have different characteristics and functionalities. In this section, we first distinguish between two major types of consensus.

Incentivised Consensus. Some consensus algorithms reward participating nodes for creating and adding a new block in the blockchain.

Non-incentivised Consensus. Private blockchain systems deploy a type of consensus algorithms that do not rely on any incentive mechanism for the participating nodes to create and add a new block in the blockchain.

Blockchain Layers. There are several components in a blockchain system whose functionalities range from collecting transactions, propagating blocks, mining, achieving consensus and maintaining the ledger for its underlying crypto-currencies, and so on.

These components can be grouped together according to their functionalities using different layers similar to the well-known TCP/IP layer. In fact, there have been a few suggestions to design a blockchain system using a layered approach [1]. The motivation is that a layered design will be much more modular and easier to maintain. For example, in case a bug is found in a component of a layer in a blockchain system, it will only affect the functionalities of that corresponding layer while other layers remain unaffected. For example, David et al. [1, 4] suggest four layers: consensus, mining, propagation, and semantic. However, we believe that the proposed layers do not reflect the proper grouping of functionalities.

For example, consensus and mining should be part of the same layer as mining can be considered an inherent part of achieving consensus. In addition to this, some blockchain systems might not have any mining algorithms associated with it. In this paper, we, therefore, will define four layers (Figure 3): network, consensus, application, and meta-application. The functionalities of these layers are briefly presented below.

Consenus algorithms in the layers of the blockchain maintain the integrity of the data, resulting in a high level of reliability.

Data storage algorithm based on blockchain mechanisms. In the application of blockchain technology, despite the fact that the blocks are distributed on the Internet, in fact, each data can be encrypted to access the content of the block anywhere in the network, and thus allow access to secure storage. To form a database based on blockchain technology, the data stored in each block in the database is considered to be encrypted according to the parameter of the data in the previous block. In each transaction, information is classified and stored based on a knowledge base [3, 8]. According to the above mechanism, the database of information systems in the network is formed on the basis of blockchain technology according to the following algorithm:

1. Consensus algorithms are selected based on the form and type of data;
2. The cryptographic function is selected based on the encryption method;
3. The initial data block is formed;
4. Each n-block key is formed according to the parameter of the information contained in the (n-1)-block;
5. The information stored in each block is cryptographically encrypted on the basis of the generated key;
6. Encrypted information is placed in the block.

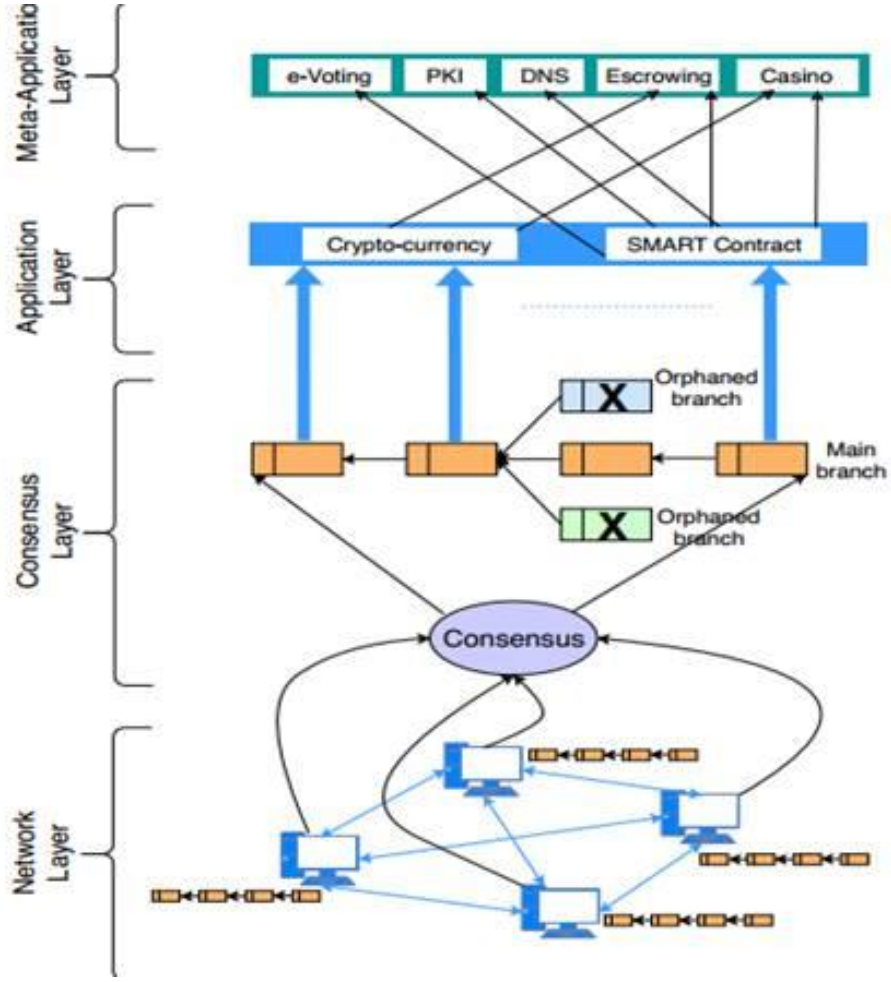

Fig.3. Layers of blockchain.

Forming a cryptographic chain in the process of blockchain-based data storage serves to ensure data reliability. The statistics on data storage and security based on Blockchain for the last 4 years are shown in Figure 4.

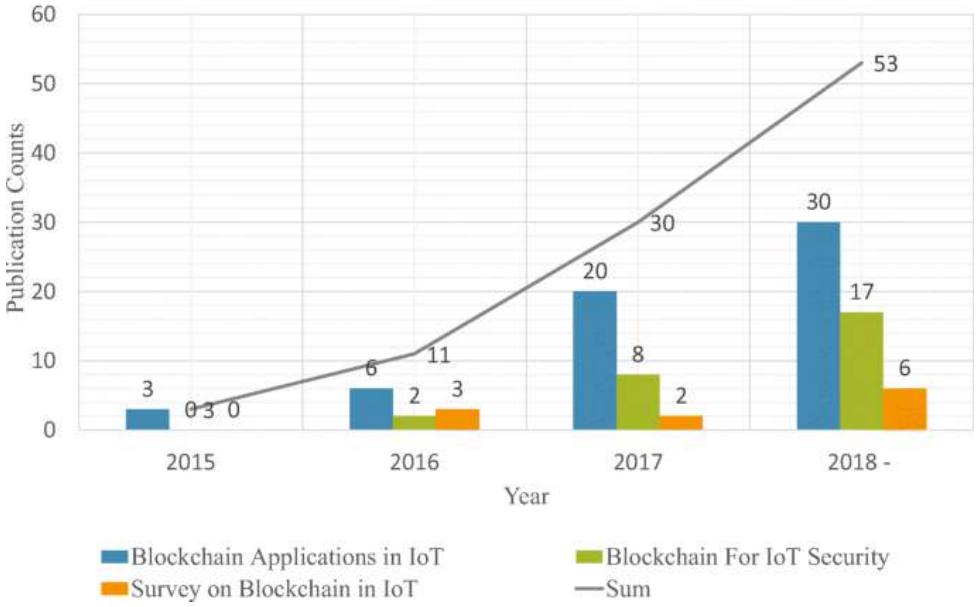

Fig.4. Blockchain application and security parameters over the years.

Forming a database based on the above algorithm serves to ensure database security. As a result, based on this algorithm, it is possible to increase the data reliability of the control system.

Conclusion.

The study examined increasing data reliability based on consensus algorithms of Blockchain technologies. Consensus algorithms, operating principles, and application cases were analyzed. A data storage algorithm based on consensus algorithms of blockchain technology has been developed. The mechanism and algorithms developed above allow the integration of blockchain mechanisms with cryptographic methods. As a result, it is possible to increase the efficiency of data reliability based on the security of the database of information systems.

References:

1. Mohammad Jabed Morshed Chowdhury, Mohammad Hoque and Alan Colma. Blockchain Consensus Algorithms: A Survey. Md Sadek Ferdous, Member, IEEE. All content following this page was uploaded by Md. Sadek Ferdouson 07 February 2020.
2. Ахатов А.Р., Назаров Ф.М. Методы реализации блокчейн на основе криптографической защиты для системы обработки данных с ограничением и запаздыванием в электронном документообороте. “Вестник компьютерных и информационных технологий” международный научный журнал.// Москва. ООО Издательский дом «Спектр» №10.[3-13] с. Doi: 10.11489 /issn.1810-7206. 2019.
3. Akhatov A.R., Nazarov F.M., Meliyev F.F. Development of Models and Algorithms for Improving the Reliability of Transfer of Information Based on the Application of Cryptographic Methods to the Distributed Register Technology. “International Journal of Control and Automation” Australia.pp. 1118 – 1129, Vol. 13, No.2, (2020).
4. L.Wang, X.SHen, J.Li, J.SHao, Y.Yang. Cryptographic primitives in blokcheyns. Journal of Network and Computer Applications, vol. 127, P. 43 – 58, 2019.
5. Pierre-Yves Piriou., Jean-Francois Dumas. Simulation of stochastic blockchain models. CHatou, France. P.[1-8]. 2018.
6. R.Mayank, G.Danilo, K.Katina. SoK of Used Cryptography in Blockchain. Department of Information Security and Communication Technologies, Norwegian University of Science and Technology. P 54. 2019.
7. С.П.Панасенко. Современные методы вскрытия алгоритмов шифрования. Ч. 1. CIOWorld. – 23.10.2006.
8. П.И.Тутубалин, А.П.Кирпичников. Отсенка криптографической стойкости алгоритмов асимметричного шифрования. Вестник технологического университета. Т.20, №10, с. 94-99, 2017.

Akhatov Akmal Rustamovich - Head of the Department of Natural and Applied Sciences, Samarkand State University, Doctor of Technical Sciences, Professor. Tel .: +998902716418. E-mail: akmalar@rambler.ru

Nazarov Fayzullo Mahmadiyarovich - Head of the Department of Information Technology, Samarkand State University, Doctor of Philosophy in Engineering, PhD. Tel .: +998944798640. E-mail: fayzullo-samsu@mail.ru

Rashidov Akbar Ergash oglu - Assistant of the Department of Information Technology, Samarkand State University. Tel .: +998941816422. E-mail: researcher.are@gmail.com