Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 1 (2024)

Analyzing Blockchain Consensus Mechanisms and their Applicability to Internet of Things Systems

Maxim Melnikov[1], Elena Igonina[2]

[1]*Research Scholar, Bunin Yelets State University, Yelets, Russia*

[2]*PhD in Physical and Mathematical Sciences, associate professor, Bunin Yelets State University, Yelets, Russia*

Abstract:- The consensus mechanism is the main component of blockchain technology, which allows multiple nodes to agree on a consistent view of data within the blockchain network. A carefully selected algorithm, on the basis of which a consensus of transactions occurs, can provide the network with such properties as fault tolerance and immutability. Currently, it is relevant to apply blockchain (with all its advantages) to Internet of Things (IoT) systems, which are gaining more and more popularity every year. IoT systems are used in areas important to society such as healthcare, economics, agriculture, transport, and are also used in various forms of social security (smart cities, logistics, product tracking, parcels, etc.). Data integrity and consistency are extremely important in these areas, because hardware and software failure or discrediting the data may harm the company and its customers using IoT devices. In addition, the blockchain has become the basis for decentralized networks. The main difficulty of implementing blockchain in IoT is the lack of computing resources of these "smart devices". It follows from this that traditional consensus algorithms, for example, Proof of Work, are not applicable, as they are extremely resource-intensive. This article provides a comparative analysis of popular consensus mechanisms according to the list of developed criteria. Based on the results obtained, conclusions are drawn that help in choosing the most appropriate consensus mechanisms for applicability in IoT systems, and the conditions necessary for their integration are determined. The possibility of implementing both PoW and PoS algorithms in IoT systems using consensus algorithms specially developed for them, such as Microchain and Proof of Supply Chain Share, is also considered.

Keywords*: consensus, consensus algorithms, blockchain, IoT-systems.*

1. Introduction

Blockchain (eng. blockchain – a chain of blocks) is a cryptographically linked distributed registry, the main feature of which is that it stores the history of transactions on the network according to the bitcoin type (from the eng. bitcoin, from «bit» and «coin»). Underlying bitcoin, blockchain technology has two important properties: triple entry and resistance to hacking or falsification of data. Due to the fact that each block in the blockchain is cryptographically linked to the previous block, an attempt to interfere with the blockchain chain will result in the cancellation of the cryptographic connection between the blocks. Therefore, attackers are not able to change the history of blockchain operations.

Triple-entry accounting is a key characteristic of a distributed network. Instead of being verified by a bilateral agreement, in order to provide evidence of their activities, transactions in the blockchain are transmitted to the entire network at once. This makes it possible for any user to confirm all transactions in the blockchain, which is directly linked to the consensus mechanism. In turn, consensus mechanisms allow blockchains to converge on a network-wide agreement on the consistent and holistic state of a given registry, so all network nodes are synchronized and accept the same history. For example, in the Bitcoin system, consensus is achieved through the use of Proof of Work (hereinafter referred to as PoW) and Longest Chain Rule (hereinafter referred to as LcR) algorithms.

PoW – It is based on the search for many solutions to a cryptographic computing puzzle, which is solved by participants in a decentralized network, called miners. The solution of computational tasks by miners is accomplished by using the hardware resources of their devices. They receive a financial incentive for successfully solving the problem, which is why the network continues to be supported.

LcR – A fork resolution tool that manages competing blockchain histories and maintains the network in a single consistent state in cases where a blockchain fork occurs.

Recently, there has been an increasing interest in the use of blockchain technology in the field of the Internet of Things (hereinafter referred to as IoT). Increasingly, consensus mechanisms are being modified to achieve less resource intensity and greater suitability for deployment in the IoT. Consensus mechanisms such as Proof of Supply Chain Share (hereinafter referred to as PoSCS) and Credit-Based PoW (hereinafter referred to as CBPoW) have come to the fore in the world of IoT blockchain.

2. Research methods and materials

In order to resolve issues related to the selection of the most appropriate consensus mechanisms for their use in IoT systems and to determine the conditions for integration with a given system, it is necessary to discuss criteria for evaluating consensus mechanisms at the beginning. In connection with the above, the first part of the article discusses the fundamental properties of the blockchain. The second part of the article is devoted to the analysis of specific consensus mechanisms. The consensus algorithms most commonly used in blockchains are analyzed, for example, such as Proof of Stake (hereinafter referred to as PoS) and Proof of Work; further, information in sources containing descriptions of four new mechanisms developed specifically for IoT consensus is studied. The analysis of the considered consensus mechanisms is carried out using the criteria proposed above. Attention is paid to the properties that positively and negatively affect the critical characteristics of IoT devices. In conclusion, recommendations are given on the choice of consensus for IoT systems and the prospects for further research work are determined.

The IoT system is represented by a wide range of service solutions. They are forced to meet a large number of heterogeneous requirements for both computing resources, data storage and energy intensity. Often, IoT equipment resides in reactive environments in which various sensors and mechanisms continuously generate data, connect and disconnect depending on energy needs, and, most often, work in decentralized ad hoc wireless networks.

Due to the high flexibility, IoT devices are widely used in applications such as smart home, smart city [1], healthcare [6] and supply chain [2-5].

The integrity of data in the blockchain is achieved through the use of consensus mechanisms (algorithms). The consensus mechanism is a set of rules or protocols that a group of systems must follow in order to make a decision on confirming a commit in the system. Consensus is a critical part of most blockchain deployments, but choice becomes even more important when working with an IoT-oriented blockchain. When choosing a blockchain, there is always a question of compromises. Some systems are more resource-intensive, some are faster, and some are less decentralized. To compare blockchains, namely consensus algorithms underlying the blockchain, we will define a number of requirements that have an impact in IoT systems:

1. *Security.* Some blockchain implementations can provide a higher level of reliability and security guarantees compared to traditional IoT networks tied to central points of failure.

2. *Consumption of processor resources.* An important factor in choosing a consensus mechanism will be to maximize the battery life of the IoT device and maintain a sufficient level of processor utilization.

3. *Data storage.* If each node of the network stores a complete copy of the blockchain, then they can independently verify transactions and help other nodes upload their blockchains. Usually, IoT devices do not have enough storage to contain tens of gigabytes of blockchain data. As a result, it is necessary to come to a compromise that ensures security and a sufficient level of decentralization.

4. *The number of transactions per second (TPS).* The more nodes involved in the consensus process, the higher the decision delay. This leads to a decrease in the speed of work, but increases decentralization. Reducing the number of nodes leads to an increase in transaction throughput in the network and reduces blocking time, which is also critically important for IoT devices [17].

5. *Decentralization.* Maximizing network decentralization allows you to diversify data storage and decision-making in the blockchain, however, it affects network scalability and speed. The decrease in decentralization leads to the opposite effect – the priority of scalability and speed.

Let's review and analyze the work of the most popular consensus algorithms and their modifications.

Proof of Work (*PoW*) – This is the consensus algorithm that is used on the Bitcoin network. It was this that formed the basis of most cryptocurrencies (through forks) [9]. Most modern PoW implementations are based on solving a cryptographic problem with a certain set of parameters, and the first user who solves this problem receives a reward in the form of special tokens (or parts thereof). The classic scheme of operation looks like this: miners are looking for a nonce (generated pseudo-random number), which is hashed together with the block header of the blockchain in order to get a hash of the block with a certain number of leading zeros [10]. The first blockchain user who calculates the hash in compliance with all requirements receives a reward as payment for the computing resources spent. The Bitcoin consensus mechanism does not stop at PoW alone; it includes the interaction of two components at once - PoW and the Longest Chain Rule (hereinafter referred to as LcR). In the literature, this connection is called the “Nakamoto consensus” [7]. In it, PoW is responsible for two of the most important functions at once - a mechanism for providing a financial incentive for the miner (blockchain participant) and protection against the Sybil attack.

Credit Base PoW (*hereinafter referred to as CBPoW).* Some blockchain researchers propose a "credit -based" PoW system that is more suitable for working with IoT devices [11]. The authors have created a consensus algorithm that dynamically adjusts the complexity of the PoW computational task depending on how well the device adheres to the consensus rules. This happens by calculating the so-called "total score" (node total score) of the network node, calculated dynamically by summing the positive score and the negative score of the device. The value of the positive score increases due to the exact following of the consensus mechanism, while the negative score increases. The node does not obey the consensus or shows signs of suspicious activity.

Proof of Elapsed Work and Luck (hereinafter referred to as PoEWAL). PoEWAL –is a consensus mechanism that is similar in its characteristics to PoW, but modified so that it can be used on devices with limited computing resources [12].

PoEWAL is still based on solving cryptographic problems, but instead of devices calculating a suitable nonce, the user just needs to "mine" (perform calculations) it for some short time period. This leads to a significant reduction in computing load and power consumption on the IoT device. After the expiration of the "mining window", miners compare their hash values obtained at the time of solving the computational problem. If the node has the largest null sequence in the hash-value, then the system issues a confirmation of receipt of the block from the previous "computational round". If several miners have the same hash values (by the number of zeros), then the Proof of Luck mechanism (hereinafter referred to as PoL) is activated. In the PoL process, the generated hashes containing the same number of consecutive zero values are compared, and then a node is selected whose value of the resulting hash is minimal [21]. In its mechanism, PoEWAL uses rounds to provide strict synchronization time limits, since the algorithm developers assume that IoT devices tend to have time synchronization..

Byzantine Agreement Protocol (hereinafter referred to as BAP). A classic example of a blockchain using BAP is Algorand [23]. Algorand is a cryptocurrency blockchain, authored by Silvio Micali (Italian-American computer scientist, Turing Award winner). Its network is based on a verifiable random function (hereinafter referred to as VRF) for the operation of a consensus mechanism based on the Byzantine agreement protocol [15]. User nodes take part in consensus by calculating a scoring function. A decentralized random beacon (DRB) enables nodes to agree on a VRF and jointly create one new output VRF in each round of computation.

In this context, VRF implies a commitment to a deterministic pseudo-random value. The function outputs remain unbiased due to their pseudo-random properties [16]. In addition, the VRF acts as a sort of lottery to select several "leaders" who propose blocks to the "committee". If a majority of the committee members meet certain conditions and the node proposes a valid block, then that block can be certified and added to the blockchain.

Proof of Stake (hereinafter referred to as PoS). PoS originated in early 2012. The first public mention occurred in the same year in an article by researchers Scott Nadalem and Sunny King [13]. A group of programmers settled on an option that involved tying the work of the consensus algorithm to the coin-age token (token age). The mechanism was developed as an alternative to PoW. The authors designed a system in which a miner uses PoW to obtain an initial supply of tokens on the network, and then the system slowly reduces the computation reward to reduce dependence on PoW.

As in the PoW implementation, the header is hashed, but PoS does not waste resources on recalculating none, since it performs the calculation only once. Then a check is made if coin age > (blockhash / target), then the miner can integrate the calculated block into the chain. Otherwise, the node waits for the next round to check if it meets the criteria to create a block [14]. PoS has skyrocketed in popularity due to its minimal hardware requirements and significantly lower power consumption (compared to PoW). Currently, the second most popular blockchain in the world, Ethereum, uses a modification of PoS as the basic consensus mechanism [10].

Proof of Supply Chain Share (hereinafter referred to as PoSCS). PoSCS is an algorithm authored by programmer, entrepreneur and researcher Patrick Tsang. The mechanism was originally developed to optimize the organization of supply chains and perishable food products [19]. The system uses an IoT network to monitor and manage nodes, and a blockchain network for various types of manipulation of food data throughout the entire supply life cycle. A decentralized database storage containing an archive of data is also used..

The authors of the mechanism note that PoW is not suitable for IoT due to high computational costs. So they settled on a consensus mechanism similar to PoS, but decided to forgo the need for a reputation currency system. Blockchain participants have several factors that are responsible for their reputation on the platform: devotion (dev), interest (int); satisfaction (sat); influence (inf). Factors are "weighted" according to one of three strategies:

- "interest comes first" strategy;
- "loyalty above all else" strategy;
- "moderation" strategies.

Sampling a set of factors and taking into account their weighting coefficients does not allow the consensus algorithm to select participants who maximize only one factor. These factors and weights are used to pseudo-randomly select the block producer that will create the block.

Proof of Capacity (hereinafter referred to as PoC). This mechanism is focused on hard drive capacity, and not on mining, using graphics processing unit (GPU), central processing unit (CPU). Separately, there are special devices - ASIC (application specific integrated circuit). BurstCoin (blockchain and cryptocurrency of the same name) took PoC as a basis.

Mining BurstCoin blocks consists of two successive stages – "plotting" and "mining". Mining involves hashing a list of nonces and then storing it on HHD or SSD drives.

Hashes, like in Bitcoin, are not discarded, but are combined into "scoops" (pairs of hashes) and stored on the participant's drives. Miners calculate the scoop number and use it to build block chains [20]. BustCoin uses Shabal hashing as it is more cryptographically strong than classic SHA256 or MD5, which are used in Bitcoin and many other blockchain networks..

The Microchain consensus mechanism is a lightweight algorithm primarily designed for IoT ecosystems [18]. Microchain is conceptually similar to PoS and BAP: several validating users are added to a committee, the committee selects a node to create a block. The committee is responsible for selecting a random set of blockchain participants, thereby minimizing the likelihood of "electing" a biased or malicious miner. Consensus uses its own

committee, Dynasty. Microchain uses a combination of components: Voting based Chain Finality (VCF) and Proof of Credit (hereinafter referred to as PoC). PoC is a PoS consensus that uses the "weight" of credit to increase the chances of a particular node producing a block. Given the distribution of credit properties in a particular Dynasty, users with higher credit weight have a higher chance of being selected by the committee to produce a block.

Proof of Importance (hereinafter referred to as PoI). The PoI algorithm proposed by NEM (New Economy Movement) has much in common with PoS, where network nodes need to commit a certain number of tokens. To become a validator, a NEM wallet must have a balance of at least 10,000 tokens within a certain period of time. This importance score increases for using the NEM counting network and sending transactions..

Hybrid PoW/PoS consensus. There are distributed systems that prefer to use compromise variations of the consensus mechanism. For example, using a combination of PoW and (or) PoS elements. Thus, the cryptocurrency blockchain Decred, whose creators refused to use PoW because of the "double spending" problem and PoS because of the "nothing at stake" problem, decided to develop a hybrid algorithm that should not be subject to the problems listed above [8]. Decred is also based on mining blocks that cannot be added directly to the blockchain. The idea is that miners offer their blocks to a network of PoS nodes who buy tickets as their share of the blockchain (similar to the concept of lottery tickets) [22]. If a PoS node is pseudo-randomly selected from the ticket pool, only then does it confirm the block and add it to the blockchain.

3. Results and discussion

For a more visual representation, the above consensus mechanisms are presented with the help of illustrations. The information presented in the figures was obtained on the basis of the research and analysis of literary sources. Figure 1 shows the general properties of consensus mechanisms, such as tamper resistance (vulnerability 51% and 33%), block time and transactions per second (TPS). Figure 2 shows IoT-oriented consensus mechanisms (Microchain, CBPoW, PoSCS, PoEWAL). Figure 3 shows a comparison of the considered consensus algorithms based on the criteria proposed in this work with the subsequent assignment of a rating to each consensus.

Consensus	Blockchain	Block Time	TPS	Adversary Tolerance	L2 Network
PoW	Bitcoin	10 min	7	<51%	Lightening Network
	Litecoin	2.5 min	56		
	Monero	2 min	Variable		None
	Ethereum	12–14 s	15		Side Chains, Rollups
	Horizen	2.5 min	N/A		Side Chains
	CBPoW	Variable	500+		None
	PoEWAL	Variable	25		None
PoS	Ethereum (PoS)	12 s	TBD	<51%	TBD
	Algorand	4.5 s	1000	<33%	Off-chain Contracts
	Dfinity	Variable	Variable	<33%	None
	Cosmos	6 s	1000+	<33%	
	PIVX	60 s	173	<51%	
	Microchain	9 s	230+	<33%	
	PoSCS	Variable	Variable	<51%	
PoW + PoS	Decred	5 min	14	<51%	Lightening Network
PoC	BurstCoin	4 min	80+	<50%	None
PoI	NEM	1 min	4000	<51%	

Figure 1: An overview of consensus mechanisms

Consensus	Similar to	Decentralised	Features	Apps	Drawbacks
PoSCS	PoS	No	Reputation System	Supply Chains	Cloud Reliance
Microchain	PoS	Partially	Crypto Sortition	IoT Blockchain	Synchronous Networks
PoEWAL	PoW	Partially	Time-limited PoW	IoT Dapps	Synced Clocks
CBPoW	PoW		Credit System	Industrial IoT	DAG Coordinator

Figure 2: An overview of the considered consensus mechanisms for IoT-systems

Consensus	Processor Usage	Security	Decentralisation	Storage	TPS	Suitable?
PoW	High	High	High	High	Low	No
PoS	Medium	High	Medium	High	Variable	Partially
PoW + PoS	High	High	High	High	Low	No
PoC	Low	High	High	High	Low	No
PoI	Low	High	High	High	High	Partially
PoSCS	Low	High	Low	Low	Variable	Partially
CBPoW	Low	High	Medium	Low	Medium	Yes
PoEWAL	Low	High	High	High	low	Partially
Microchain	Medium	High	Medium	High	Medium	Yes

Figure 3: Applicability of the consensus mechanism for IoT-systems in accordance with the proposed criteria

Our analysis of consensus mechanisms allows us to assess their applicability for IoT systems in accordance with the criteria proposed in this work.

PoW can be immediately excluded from the list of suitable algorithms. It is extremely power and processor intensive and requires specialized hardware. All this is critically unacceptable for IoT devices.

It can be argued that PoS is partially suitable and can potentially be used in IoT. This consensus does not require much energy or processing power. However, PoS still has challenges for use in IoT: TPS may not be sufficient depending on the use case, and the monetary concept may not be suitable for some IoT applications. Transaction throughput varies from 90 to over 1100 TPS, as shown in Figure 1. PoS performance largely depends on the specific implementation of the algorithm. Therefore, PoS is suitable for IoT, but only under certain conditions, for example, if having a more decentralized network is critical.

Hybrid PoW/PoS mechanisms are an alternative solution if solving the “51% attack” and “nothing at stake” problems is paramount. However, the presence of PoW as a starting mechanism brings back the same problematic issues that “pure” PoW faces. Theoretically, the PoW part of the algorithm can be transferred to a separate ASICS, and the PoS part can be transferred to IoT devices. However, in our opinion, the configuration of the proposed system will not be justified, and therefore the use of such a mechanism for IoT is not recommended.

CBPoW is able to dynamically adjust the mining difficulty of the PoW part and has a mechanism for regulating unscrupulous nodes, making the mining difficulty for them very high, to the point where mining becomes almost impossible. CBPoW is also capable of replacing traditional blockchain with DAG, which makes it possible to independently reduce the size of the blockchain stored locally on the device. In addition, this mechanism shows good results (Fig. 1) in terms of throughput (500 TPS). A set of characteristics define CBPoW as suitable for IoT, specifically the DAG structure allows for a reduction in size, as well as a lightweight PoW consensus mechanism and a fairly high transaction throughput. Due to these characteristics, CBPoW was noted by us in Figure 3 as favorable for IoT devices.

PoEWAL also appears to be a modified version of PoW. A special feature of PoEWAL is that the mining process is time limited. The devices mine in short intervals, which reduces power consumption and the use of hardware resources. PoEWAL relies on the device being used to have a synchronized clock, which is acceptable for IoT devices on a wireless network that collect various metrics over time. However, this factor may not be appropriate for some implementations where devices are susceptible to desynchronization. So PoEWAL has two significant limitations: dependence on synchronized time and low throughput. As a consequence, in Figure 3 we have marked PoEWAL as partially suitable for IoT..

PoC is a fairly new consensus mechanism that is conceptually based on the use of data storage capacity as the basis of the algorithm. However, the storage capacity of IoT devices is limited due to hardware features. Thus, it is obvious that PoC is not suitable for use in IoT systems.

PoI develops the ideas of PoS and combines them with the mechanism of "significance" (importance, value). The higher the importance score of a node relative to the total number of tokens staked by a user, the higher the likelihood that the node will be selected to mine a block. PoI satisfies most of the criteria presented in Figure 1, making it a suitable candidate for IoT systems. However, its sufficient implementation is presented only in the NEM blockchain. PoI is mentioned in various sources, for example, [9], where only a general description of the mechanism's operation is provided. Therefore, PoI for IoT can only be partially recommended.

PoSCS operates a bet mechanism, but instead of financial incentives, it is based on a rehearsal system. Reputation is calculated based on how a user interacts with the blockchain. PoSCS uses cloud storage to archive the "history" of the blockchain. Due to this, it is not necessary to store all the data directly on IoT devices, which solves the problem of low data storage capacity on IoT devices. Given the results of [19], PoSCS transaction throughput may be low for some IoT use cases, and the additional dependence on the cloud may be a reason to avoid using this algorithm in some smart system implementations. Therefore, we consider PoSCS to be partially suitable for some IoT implementations.

Microchain adapts PoS concepts and makes it more suitable for IoT. Nodes operate on a trust rating, not a monetary system. Disadvantages include the fact that Microchain uses the cryptographic VRF function to operate the algorithm, which can result in a high load on the device's processor as the network grows. Microchain has made some improvements regarding the network environment, for this reason it has become unsuitable for public blockchains. At the same time, the mechanism demonstrates acceptable performance, providing more than 230 TPS..

Characteristics due to which Microchain can be used in the IoT field:

- implementation not tied to the monetary system;
- high TPS;
- low CPU usage in controlled private networks.

These features allowed the Microchain algorithm to be recognized as the most suitable in comparison with other algorithms discussed above, which is reflected in Figure 3.

4. Conclusion

This work identified the factors of existing consensus mechanisms, which in turn impose additional conditions on resource-limited IoT devices. The definitions of criteria for ranking consensus mechanisms such as security,

speed, decentralization, etc. are considered. A brief description of the concepts of mechanisms is proposed and a definition of their general operating scheme is given. Such popular mechanisms as PoW and PoS, and some algorithms specialized for IoT (CBPoW, Microchain, PoEWAL and PoSCS) are analyzed. It is noted that the above mechanisms modify the already existing PoW and PoS consensus mechanisms, but eliminate (or minimize) the need for energy-inefficient systems and (or) monetary systems. The analysis identified the advantages and disadvantages of each consensus mechanism, and also assessed the possibility of their use for IoT systems.

The research results show that Microchain and CBPoW are sufficiently suitable for IoT. Microchain is suitable for IoT in private environments, and CBPoW solves the issue of storing blockchain locally on devices. PoSCS, PoEWAL, PoI (theoretically) and PoS are also considered partially suitable. Some of them solve problems with monetarity, computational costs and data storage limitations. However, they also have a number of problems: controversial synchronization mechanisms, insufficient coverage of performance issues, and dependence on cloud infrastructure.

The current trend in consensus algorithm research in industrial and academic environments has focused on developing mechanisms that are lightweight enough for low-power hardware devices. In the future, the task is to study new approaches to the consensus process. In particular, carrying out modifications to the mechanisms that will be deployed to achieve specific business objectives in both private and potentially public operating environments.

Refrences

[1] Singh S., Sharma P.K., Yoon B., Shojafar, M., Cho G.H., Ra I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city // Sustain. Cities Soc. 2020. Vol. 63. 102364. doi: https://doi.org/10.1016/j.scs.2020.102364

[2] Min H. Blockchain technology for enhancing supply chain resilience // Bus. Horizons. 2019. Vol. 62. pp. 35–45. doi: https://doi.org/10.1016/j.bushor.2018.08.012

[3] Dujak D., Sajter D. Blockchain Applications in Supply Chain. In SMART Supply Network // Springer: Berlin/Heidelberg, Germany. 2019. pp. 21–46.

[4] Sternberg H.S., Hofmann E., Roeck D. The Struggle is Real: Insights from a Supply Chain Blockchain Case // J. Bus. Logist. 2021. Vol. 42. pp. 71–87. doi: https://doi.org/10.1111/jbl.12240

[5] Casado-Vara R., Prieto J., Prieta F.D., Corchado J.M. How blockchain improves the supply chain: Case study alimentary supply chain // Procedia Comput. Sci. 2018. Vol. 134. pp. 393–398. doi: https://doi.org/10.1016/j.procs.2018.07.193

[6] Werner R., Lawrenz S., Rausch A. Blockchain Analysis Tool of a Cryptocurrency // PervasiveHealth: Pervasive Computing Technologies for Healthcare, Springer: Berlin/Heidelberg, Germany. 2020; pp. 80–84.

[7] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, Portal Unicamp: Campinas, Brazil. 2008.

[8] Polge J., Robert J., Traon Y.L. Permissioned blockchain frameworks in the industry: A comparison // ICT Express. 2021. Vol. 7. pp. 229–233. doi: https://doi.org/10.1016/j.icte.2020.09.002

[9] Salimitari M., Chatterjee M., Fallah Y.P. A survey on consensus methods in blockchain for resource-constrained IoT networks // Internet Things. 2020. Vol. 11, 100212. doi: https://doi.org/10.1016/j.iot.2020.100212

[10] Conti M., Sandeep K.E., Lal C. Ruj S. A survey on security and privacy issues of bitcoin // IEEE Commun. Surv. Tutorials. 2018. Vol. 20. pp. 3416–3452. doi: https://doi.org/10.1109/COMST.2018.2842460

[11] Huang J., Kong L., Chen G., Wu M.Y. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism // IEEE Trans. Ind. Inform. 2019. Vol. 15. pp. 3680–3689. doi: https://doi.org/10.1109/TII.2019.2903342

[12] Andola N., Venkatesan S., Verma S. PoEWAL: A lightweight consensus mechanism for blockchain in IoT // Pervasive Mob. Comput. 2020. Vol. 69. 101291. doi: https://doi.org/10.1016/j.pmcj.2020.101291

[13] Zhang S., Lee J.H. Analysis of the main consensus protocols of blockchain // ICT Express. 2020. Vol. 6. P. 93–97. doi: https://doi.org/10.1016/j.icte.2019.08.001

[14] Gilad Y., Hemo R., Micali S., Vlachos G., Zeldovich N. Algorand: Scaling Byzantine Agreements for Cryptocurrencies // In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China. 2017. pp. 28–31.

[15] Galindo D., Liu J., Ordean M., Wong J.M. Fully Distributed Verifiable Random Functions and their Application to Decentralised Random Beacons // IACR Cryptol. EPrint Arch. 2020. P. 96-97.

[16] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger // Ethereum Foundation: Bern, Switzerland. 2022

[17] Xu R., Chen Y., Blasch E., Chen G. Microchain: A Hybrid Consensus Mechanism for Lightweight Distributed Ledger for IoT // arXiv. 2019. arXiv:1909.10948.

[18] Tsang Y.P., Choy K.L., Wu C.H., Ho G.T., Lam H.Y. Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism // IEEE Access. 2019. Vol. 7. 129000–129017. doi: https://doi.org/10.1109/ACCESS.2019.2940227

[19] Petr C. Review of Existing Consensus Algorithms Blockchain // In Proceedings of the 2019 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies IT and QM and IS. Sochi, Russia. 2019. pp. 124–127

[20] Wen Y., Lu F., Liu Y., Cong P. Huang, X. Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey // In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer: Berlin/Heidelberg, Germany. 2020. Vol. 12454 LNCS. pp. 564–579

[21] Esgin M.F., Kuchta V., Sakzad A., Steinfeld R., Zhang Z. Practical Post-quantum Few-Time Verifiable Random Function with Applications to Algorand // Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer: Berlin/Heidelberg, Germany 2021. Vol. 12675 LNCS. pp. 560–578

[22] Li J., Li N., Peng J., Cui H., Wu Z. Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies // Energy. 2019. Vol. 168. pp. 160–168. doi: https://doi.org/10.1016/j.energy.2018.11.046

[23] Zhang P., Schmidt D.C., White J., Dubey A. Chapter Seven—Consensus mechanisms and information security technologies // Adv. Comput. 2019. Vol. 15. pp. 181–209

[24] Silvano W.F., Marcelino R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future Gener. Comput // Syst. 2020. Vol. 112. pp. 307–319. doi: https://doi.org/10.1016/j.future.2020.05.047