UDC 004.772.2 **DOI:10.30837/rt.2019.3.198.08**

M. OSADCHUK, R. OLIYNYKOV, Dr. Sc. (Tecnology)

METHOD OF PROOF OF WORK CONSENSUS ALGORITHMS COMPARISON

Introduction

After the breakthrough paper proposed by Satoshi Nakamoto, blockchain systems have received wide distribution. The blockchain technology allows to record and secure store big amount of various transactions. The most popular usage the technology received in digital currencies. Also it is used in the areas of government, agriculture, environment, healthcare, education, and much more. Moreover it is being implemented in telecommunications area for dealing with fraud, quickly resolving disputes over roaming agreements, verification of billing and user identification (e.g. ENCRY [1]).

The decentralization has shown the new concept of trust – without any third party. So there is no central authority that can set the rules and there is no single point of failure.

There can be two types of blockchain consensus protocols – permissioned [2] and permissionless [3]. The permissioned one requires permission to read the information stored in the blockchain. The system based on permissionless protocol is publicly available, so everyone can join and participate in consensus.

The consensus algorithm is the most important part of the blockchain system. It is responsible for the way how users will come to the consensus among all honest participants. Firstly, they are used in fault tolerance real-time systems, i.e. nuclear power stations, space systems, aviation systems, and other critical systems. Secondly, they are used in fault tolerance counting systems, like clusters and database controllers. Thirdly, consensus algorithms are used in digital currencies to form the transactions base. The last one can be used either in cryptocurrencies (Bitcoin [4], Cardano [5], Ethereum [6], etc.) or in centralized currencies (e.g. Ripple [7]).

For today there are three widely spread variants of reaching consensus, i.e. Proof of Work [8], Proof of Stake [9] and Byzantine Fault Tolerance [10]. There are also a lot of algorithms derived from them, so the amount of consensus algorithms is big enough to think about "How to choose the most suitable for defined criteria algorithm among all existing?"

In that case, the comparison of algorithms should be conducted. There are publications with analysis of typical consensus algorithms and some of their contemporaries. Du Mingxiao, Ma Xiaofeng, Zhang Zhe in the paper "A review on consensus algorithm of blockchain" [11] have performed a deep analysis of consensus algorithms, their benefits and disadvantages. Zibin Zheng, Shaoan Xie and Hongning Dai have researched the scalability and security problems [12]. L.M. Bach, B. Mihaljevic and M. Zagar perform a comparative analysis of typical consensus algorithms and some of their contemporaries that are currently in use in modern blockchains [13]. They perform the overview of algorithms and their analysis focuses on the algorithmic steps taken by each consensus algorithm, the scalability of the algorithm, the method the algorithm rewards validators for their time spent verifying blocks, and the security risks present within the algorithm.

This articles provides an overview of advantages and disadvantages of consensus algorithms and then one can choose the optimal solution for their system to be developed using the proposed method to make a decision on the most suitable algorithm for given system requirements.

The method proposed in this article allows making a decision on which of algorithms will match better with known conditions and requirements to the system. This method is proposed for PoW consensus, but can be also used for other types of consensus algorithms. The method uses the weight or, in another words, the priority of algorithms properties, so the party decides which of properties have the highest priority for their system. Thus, the proposed method can be used to choose among the variety of consensus algorithms the best one, based on the priority of algorithm's properties.

1. Main features of consensus algorithm

The consensus algorithm has the following main properties. First of all it is the type of consensus mechanism. It can be Proof of Work, Proof of Stake, delegated Proof of Stake, Practical Byzantine Fault Tolerance, etc. Among all algorithms were chosen the most popular for permissionless systems Proof of Work algorithm and its variants of improvement. In this article there are compared the next algorithms: Proof of Work, delayed Proof of Work, Proof of Activity, Proof of Burn and Proof of Capacity.

The Proof of Work involves scanning for a value that when hashed the hash begins with a number of zero bits [8]. They are used to provide security to an entire network and ensure that all transactions will be processed in a timely manner [14].

Delayed Proof of Work leverages the hashrate of the Proof of Work network to protect its network [15]. Because of this process, which is called notarization, delayed Proof of Work provides the higher level of security.

Proof of Activity is a hybrid of Proof of Work and Proof of Stake. This feature provides high level of scalability [16].

Proof of Burn is a consensus algorithm, where users send their money to one defined address, or in other words burn their coins [17]. This algorithm is more environment-friendly and do not need any additional tools to increase the mining power.

Proof of Capacity is very similar to the Proof of Burn, but instead of using counting power, it uses memory [18]. That's why users do not need to have additional tools, and after they stop mining, they can use their memory for themselves.

The second feature is the transaction confirmation latency (i.e. number of blocks needed to secure accept the transaction). In other words, it is the minimum amount of blocks that are needed to ensure security against double-spending attack.

The third feature is the attack prevention mechanism. This feature responds for the way how algorithm prevents the system from the double-spending attack. It can be based on the hashrate of the system – the bigger the system is, the harder to perform the attack. Also it can be some additional features in the algorithm (e.g. PirlGuard System [19] and ChainLock Mechanism [20]).

The next feature of consensus algorithms is their scalability – the way how an algorithm works in case of increasing number of users reaching consensus. By this feature the algorithms can be divided to easy scalable, scalable with additional conditions and not scalable. This feature is important especially for digital currencies, as the number of its users can increase very fast.

The last feature considered is the level of decentralization. Algorithms can be fully decentralized, partially decentralized and centralized.

2. The decision-making method in uncertainty conditions

Decision making [21] can be described as the process of reducing uncertainty about solution options by gaining sufficient knowledge of the options to allow a reasonable selection from among them. In this context certainty does not mean an exact knowledge of every detail relevant to the problem under consideration, but it does mean that there is a reasonably good idea of the value of all relevant factors.

To choose the most suitable consensus algorithm for the system there is applied a number of criteria, so the multi criteria decision making methods (MCDM) should be used. There can be Multi-Attribute Utility Theory (MAUT), Analytic Hierarchy Process (AHP), Case-Based Reasoning (CBR), Data Envelopment Analysis (DEA), Fuzzy Set Theory, Simple Multi-Attribute Rating Technique (SMART), Goal Programming (GP), ELECTRE, PROMETHEE and etc. The AHP method is easy to use and scalable. Also its area of application is performance-type problems, strategy development and planning [22].

Among all MCDMs it was chosen the method based on AHP proposed by Thomas L. Saaty [23]. The AHP helps the parties find one decision that best matches their goal and their understand-

ing of the problem. This process provides a holistic, rational and comprehensive decision for representing the problem, its elements and evaluating alternative solutions.

To use the AHP, the party represents their problem in the hierarchy, where the top reflects to the goal, the interim levels reflects to the technical-economic parameters, and the bottom level reflects to the set of alternatives.

The AHP hierarchy is a structured representation of the decision. The technical-economic parameter, or criteria, can be divided into the subcriteria, sub-subcriteria in as many levels as the problem requires. Also the type of the hierarchy depends on the knowledge, opinions, values and needs of the parties.

After representing the problem into the hierarchy, the properties priority is set and each alternative is estimated with each property. In the AHP the elements are pairwise compared in relation to their impact to their common property. This system of pairwise comparison can be represented into the inversely symmetric matrix. The element $a(i,j)$ of the matrix relates to the intensity of occurrence of element i regarding the element of hierarchy j. This intensity is evaluated from 1 to 9, where:

1 – the equal importance
3 – the medium leverage
5 – the supreme leverage
7 – the significant leverage
9 – the large leverage
2, 4, 6, 8 – the relative interim value

The comparisons and evaluation relies on the judgements made by experts and represent how much more, one element dominates another with respect to a given attribute.

3. The method of consensus algorithms comparison

First of all, to use these comparison methods the criteria should be defined. The set of criteria may be different for each distributed system. The following criteria help estimate and chose the consensus algorithm that will fully match the existing requirements. All requirements can be divided into required, desired and additional. The algorithm matches better, when it meets the required requirements, despite the number of desired requirements met.

In this article the requirement to the distributed system is to perform the most securely and fully decentralized system. To perform the holistic assessment of each consensus algorithm the following criteria are proposed.

- Amount of blocks for transaction confirmation – this criterion performs the amount of blocks that must be created after the block in which transaction is included, for its confirming.
- Difficulty of attack performing – this criterion performs the hashpower (or another parameter depends on the algorithm) needed for malicious user to get the control on the system.
- Scalability – this criterion shows the work principles in increasing amount of users.
- Decentralization degree – this criterion performs how much decentralized is an algorithm.
- Smart-contracts support – this criterion performs the ability of smart-contract creation and the simplicity of its usage for this consensus algorithm.

After the criteria are set, their priorities should be defined. To assess the priority of each criterion the matrix with pairwise comparison should be created. This matrix represents the result of each comparison. As mentioned above, the estimations are based on experts' decisions. In this article all estimations were made by experts from Information Systems and Technologies Security department at V.N. Karazin Kharkiv National University [24] and from the Distributed Lab Company [25].

After comparing all criteria the normalized value for each criterion should be computed. This value describes the priority weight for each criterion. In the table 1 it is given the representation of the pairwise comparison of aforementioned criteria.

Table 1

The numeric estimations of pairwise comparisons

Pairwise comparison of consensus protocol properties	Amount of blocks for transaction confirmation	Difficulty of attack performing	Scalability	Decentralization degree	Smart-contracts support	Summary	Normalized value
Amount of blocks for transaction confirmation	1	1/5	1/3	1/7	2	3.67619	0.08813
Difficulty of attack performing	5	1	2	1/3	2	10.33333	0.24775
Scalability	3	1/2	1	1/5	2	6.7	0.16063
Decentralization degree	7	3	5	1	2	18	0.43156
Smart-contracts support	1/2	1/2	1/2	1/2	1	3	0.07193
Summary	-					41.70952	1

The next step is the pairwise comparison of defined algorithms. The comparison should be performed with each criterion, i.e. the number of matrices with algorithms comparison is the same as the number of criteria. Also the normalized value should be counted for each algorithm.

Below are presented the tables 2 - 6 with pairwise comparison of consensus algorithms.

Table 2

The pairwise comparison of consensus algorithms with criteria “Amount of blocks for transaction confirmation”

Consensus protocol	Nakamoto	dPoW	PoA	PoB	PoC	Summary	Normalized value
Nakamoto	1	1/9	1/7	1/9	1/7	0.50794	0.01006
dPoW	9	1	2	1	2	15	0.29698
PoA	7	1/2	1	1/2	1	10	0.19799
PoB	9	1	2	1	1/2	13.5	0.26728
PoC	7	1/2	1	2	1	11.5	0.22768
Summary	-					50.50794	1

Table 3

The pairwise comparison of consensus algorithms with criteria “Difficulty of attack performing”

Consensus protocol	Nakamoto	dPoW	PoA	PoB	PoC	Summary	Normalized value
Nakamoto	1	1/3	1/5	1	1	3.53333	0.09037
dPoW	3	1	1/2	3	3	10.5	0.26854
PoA	5	2	1	5	5	18	0.46036
PoB	1	1/3	1/5	1	1	3.53333	0.09037
PoC	1	1/3	1/5	1	1	3.53333	0.09037
Summary	-					39.09999	1

Table 4

The pairwise comparison of consensus algorithms with criteria “Scalability”

Consensus protocol	Nakamoto	dPoW	PoA	PoB	PoC	Summary	Normalized value
Nakamoto	1	1/9	1/5	1/5	1	2.51111	0.0504
dPoW	9	1	2	2	9	23	0.46164
PoA	5	1/2	1	1	5	12.5	0.25089
PoB	5	1/2	1	1	1	8.5	0.1706
PoC	1	1/9	1/5	1	1	3.31111	0.06646
Summary	-					49.82222	1

Table 5

The pairwise comparison of consensus algorithms with criteria “Decentralization degree”

Consensus protocol	Nakamoto	dPoW	PoA	PoB	PoC	Summary	Normalized value
Nakamoto	1	1/9	1/5	1/5	1	2.51111	0.04736
dPoW	9	1	2	2	9	23	0.43378
PoA	5	1/2	1	1	5	12.5	0.23575
PoB	5	1/2	1	1	5	12.5	0.23575
PoC	1	1/9	1/5	1/5	1	2.51111	0.04736
Summary	-					53.02222	1

Table 6

The pairwise comparison of consensus algorithms with criteria “Smart-contracts support”

Consensus protocol	Nakamoto	dPoW	PoA	PoB	PoC	Summary	Normalized value
Nakamoto	1	1/3	1/5	1	1	3.53333	0.09037
dPoW	3	1	1/2	3	3	10.5	0.26854
PoA	5	2	1	5	5	18	0.46036
PoB	1	1/3	1/5	1	1	3.53333	0.09037
PoC	1	1/3	1/5	1	1	3.53333	0.09037
Summary	-					39.09999	1

The last step of the method is making the decision. For this, the final value should be counted including all normalized values received from pairwise algorithms comparisons and the priority weight for each criterion. The table 7 represents the results of this summarizing.

Table 7

The results of calculations

Protocol properties / Consensus protocols	Amount of blocks for transaction confirmation	Difficulty of attack performing	Scalability	Decentralization degree	Smart-contracts support	Summary
	Weight of criteria					
	0.08813	0.24775	0.16063	0.43156	0.07193	1
Nakamoto	0.01006	0.09037	0.0504	0.04736	0.09037	0.05831
dPoW	0.29698	0.26854	0.46164	0.43378	0.26854	0.37338
PoA	0.19799	0.46036	0.25089	0.23575	0.46036	0.30666
PoB	0.26728	0.09037	0.1706	0.23575	0.09037	0.18159
PoC	0.22768	0.09037	0.06646	0.04736	0.09037	0.08006

The results of method usage shows that among defined consensus algorithms and defined requirements for the system the delayed Proof of Work algorithm is the most suitable that is indicated by its value 0,37338 that is the highest among all other.

Conclusions

In blockchain-system development the key role belongs to a consensus algorithm. It is a huge variety of consensus algorithms proposed in the literature for solving various amount of different tasks, but there is no algorithm how to compare them and choose the one for very this system.

For making a decision in uncertainty conditions with multi criteria there exist methods like Multi-Attribute Utility Theory (MAUT), Analytic Hierarchy Process (AHP), Case-Based Reasoning (CBR), Data Envelopment Analysis (DEA), Fuzzy Set Theory, Simple Multi-Attribute Rating Technique (SMART), Goal Programming (GP), ELECTRE, PROMETHEE and etc. It was decided to use the method by T. Saati because it is oriented to strategy and planning and it is scalable.

In this method the analytic hierarchy process is used. It represents the problem in the hierarchy, where the top reflects to the goal, the interim levels reflect to the technical-economic parameters, and the bottom level reflects to the set of alternatives.

Basing on the Saati's method, the method of consensus algorithms comparison was proposed. There were defined 5 criteria: the amount of blocks for secure transaction confirmation, difficulty of attack performing, scalability, decentralization degree and the possibility of smart-contracts. The priority of each criterion was calculated via pairwise comparison. After performing the pairwise comparison of consensus algorithms it was defined that the algorithm delayed Proof of Work gets higher value and has best correspondence to given criteria than the other consensus algorithms researched in this article.

References:

1. Electronic resource: https://encry.com/.
2. Novotny P., Qi Zhang, Hull R., Baset S., Laredo J., Vaculin R., Ford D. L., Dillenberger D. N. Permissioned Blockchain Technologies for Academic Publishing // https://arxiv.org/ftp/arxiv/papers/1809 /1809.08529.pdf.
3. Chunpeng Ge, Siwei Sun, Szalachowski P. Permissionless Blockchains and Secure Logging // https://arxiv.org/abs/1903.03954.
4. Electronic resource: https://bitcoin.org.
5. Electronic resource: https://www.cardano.org.
6. Electronic resource: https://www.ethereum.org.
7. Electronic resource: https://www.ripple.com.
8. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System // https://bitcoin.org/bitcoin.pdf.
9. Ganesh Ch., Orlandi C., Tschudi D. Proof-of-Stake Protocols for Privacy-Aware Blockchains // Cryptology ePrint Archive: https://eprint.iacr.org/2018/1105.pdf.
10. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem // https://pdfs.semanticscholar.org/1689/f401f9cd18c8fd033d99d1e2ce99b71e6047.pdf.
11. Du Minigxiao, Ma Xiofeng, Zhanh Zhe, Wang Xiangwei, Chen Qijun A review on consensus algorithm of blockchain // https://ieeexplore.ieee.org/abstract/document/8123011.
12. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends // https://ieeexplore.ieee.org/abstract/document/8029379.
13. Bach L. M., Mihaljevic B., Zagar M. Comparative analysis of blockchain consensus algorithms // https://ieeexplore.ieee.org/abstract/document/8400278.
14. Proof of Work: A History & Overview of Proof of Work Systems // https://komodoplatform.com/proof-of-work.
15. Security: Delayed Proof of Work (dPoW) // https://komodoplatform.com/security-delayed-proof-of-work-dpow.
16. Bentov I., Lee Ch., Mizrahi A., Rosenfeld M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake // Cryptology ePrint Archive: https://eprint.iacr.org/2014/452.pdf.
17. What is Proof of Burn (ELI5)? // http://slimco.in/proof-of-burn-eli5.
18. What is Proof-of-Capacity? // https://www.burst-coin.org/proof-of-capacity.
19. PirlGuard – Innovative Solution against 51% // https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-87dd45aa1109.
20. Block A. Mitigating 51% attacks with LLMQ-based ChainLocks // https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9.
21. Electronic resource: https://www.decision-making-solutions.com/how-to-make-a-decision.html.
22. Velasquez M., Hester P. T. An Analysis of Multi-Criteria Decision Making Methods // https://www.researchgate.net/profile/Patrick_Hester/publication/275960103_An _analysis _of_multi-criteria_decision_making_methods/links/55eefed208ae199d47bff202. pdf.
23. Thomas L. Saaty Decision making with the analytic hierarchy process // https://pdfs.semanticscholar.org/e3c5/61049eb532e328fc2b8288c490986cd9403f.pdf.
24. Electronic resource: https://www.univer.kharkov.ua.
25. Electronic resource: https://distributedlab.com.

Kharkiv National V.N. Karazin University;
Kharkiv NationalUniversity of Radio Electronics

Received 15.09.2019