Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes

Roman Belfer[1[0000-0001-6384-8242]], Antonina Kashtalian [1[0000-0002-4925-9713]],
Andrii Nicheporuk[1[0000-0002-7230-9475]],
George Markowsky[2[0000-0003-3715-2625]] and Anatoliy Sachenko[3[0000-0002-0907-3682]]

[1] Khmelnytsky National University, Khmelnytsky, Ukraine
[2] Missouri University of Science and Technology, Rolla, USA
[3] Research Institute for Intelligent Computer Systems, Ternopil National Economic University, Ternopil, Ukraine
belfer.roman@gmail.com, yantonina@ukr.net,
andrey.nicheporuk@gmail.com, markov@mst.edu, as@tneu.edu.ua

Abstract. The paper proposes a new socially oriented protocol that avoids pseudo-decentralization and monopolization of the network, increases the availability of the system, provides a fair selection of potential validator nodes, and provides a fair reward for creating new blocks and adding them to the blockchain. Our proposed protocol provides for the creation and addition of new blocks to a blockchain. Defines a node validator, which will create the next block according to its useful activity in the network according to predefined conditions, which can be formed according to the requirements of the system and will satisfy the individual needs of the blockchain. Also in the process of developing the proposed protocol, the main aspects of security related to protection against various types of malicious software, including botnets and computer viruses, were addressed. To apply PoA, the network is designed on a Layered Peer to Peer (LP2P) architecture, the feature of which is that nodes interact at different levels according to their typing or parameterization, which will be used to execute the algorithm developed and find consensus. In addition, the protocol may be one of the steps in the implementation of new principles of local tax policy, where taxes will be tied to the activities of individual members of the public, as well as the renewal of suffrage based on the social activity of network members and a qualitatively new principle of conducting new ones, experimental but qualitative choices.

Keywords: Protocol, Network, Decentralized, Distributed, Consensus Protocol Algorithm, Blockchain, Architecture.

1 Introduction

As distributed ledger technology became incredibly popular in 2018 because of the extremely high cryptocurrency rate. Despite global cryptocurrencies prices falling and the growth of general information about the technology, blockchain remains one of the most important areas of computer science along with AI, IoT, and cloud computing. Blockchain remains an interesting topic for major financial companies, global banks, agricultural enterprises, real estate and land markets, governmental institutions, and social networks. The most usable and widespread methods of blockchain network organization are consensus protocols - Proof-of-Work (PoW) and Proof-of-Stake (PoS). But both PoW and PoS have a quite number of disadvantages which influence the security, speed of work. accessibility, scaling, and efficient energy usage.

PoW is promotes energy inefficiency in calculations, required for the PoW-based blockchain algorithms. Some basic estimates suggest that the biggest blockchain systems that used PoW, Bitcoin and Ethereum, used roughly $4.5B of electricity, which works out to more than $12M daily [2, 3]. For example, these 2 networks used more electricity for computation than Finland did. There are other PoW issues. In particular, PoW lacks transaction handling speed (one block creation takes 10 minutes - the time to solve a puzzle for validation, and the puzzle's complexity is made the way so the node spends the mentioned amount of time [1]). Another problem is pseudo-decentralization when the "power" is concentrated by the most equipped nodes. Also, the motivation of nodes to support the network is reduced because of the declining reward for mining. The decline in support might cause the security of the system to decline.

The PoS protocol strove to become the alternative to the PoW protocol [4]. The PoS protocol has a number of advantages over the PoW protocol: electricity is not needed to solve the puzzle, nodes are interested in network security as they own the coins in it, and faster transactions. Nevertheless, The PoS protocol has the pseudo-decentralization problem [5] just like the PoW protocol has. This might cause the members' motivation to be an active node in the network to decrease. Since the nodes that have the bigger stakes will be selected as the validators more often, the "rich will become richer".

The problems mentioned earlier encourage computer scientists to look for new protocols that will reduce the problems discussed earlier.

The goal of our research is to develop a new socially-oriented protocol that avoids pseudo-decentralization and network monopolization. It also increases network accessibility for new nodes, provides fair selection of validators based on their capacity for work, and provides impartial rewards for creating new blocks and adding them to the blockchain.

Our Proof-of-Activity (PoA) consensus protocol allows the creation of new blocks and adding them to the blockchain. The PoA protocol also selects the validator nodes based on the value of the node's activity in the network and whatever criteria are specified by the specific blockchain system.

To use the PoA protocol the network should be designed according to the Layered Peer to Peer (LP2P) architecture. The specific point of the LP2P architecture is that each node is located on different layers based on its type or the parameters it uses for the consensus algorithm.

The PoA consensus algorithm may be implemented for every socially oriented structure: social networks, crowdfunding platform, civil or municipal sites. The PoA protocol applies to all organizational forms that have clearly-defined valuable activity performed by their members that needs to be tracked. It allows all participants to be grouped based the type of activity or other system definitions.

The PoA protocol can be used to create municipal or governmental platforms that could unify public initiatives and help to implement successful ones. Any financial systems integrated into those platforms could handle the transactions dealing with cryptocurrencies.

Also, the new PoA consensus protocol may provide the basis for advanced tax policies where tax deductions will be tied to the public activity of members of the public. The PoA protocol can potentially invigorate the election process by factoring in the social activity of citizens. This may lead to new types of elections.

Another issue for the development of a new socially oriented protocol that avoids pseudo-decentralization and monopolization of the network is its protection from malicious software, including botnets and various types of computers viruses [6-12].

2 Related works

There are two companies working on the blockchains based on socially-oriented platforms, rather than the regular Proof-of-Work and Proof-of-Stake principles - NEM [13] and Mithril [14].

NEM is based in Singapore and is using novel technologies and the original blockchain architecture as an alternative to the existing PoW and PoS protocols. They designed the first cryptocurrency based on the Proof-of-Importance (PoI) consensus protocol [15]. Their new system has fast transactions, small fees, low energy consumption, and transparent workflow. Its team of developers calls NEM the functional payment tool for the modern economy. It takes 5 seconds to create a transaction in the user’s wallet and 20 seconds to handle it. The network is ready to handle 3000 transactions per second [16].

The Proof-of-Importance consensus protocol selects the node of the network that will add a new block to the ledger - this process is called ‘harvesting’ in NEM. After finishing the harvesting, the node may take the fee from the processed transactions in a block. The nodes with the highest importance rate have will be chosen more often to create a block. Nodes should keep at least 10000 XEM (the unit of cryptocurrency in the NEM network) to be allowed to participate in harvesting.

The Proof-of-Importance protocol can resolve issues arising from difficulties between the Proof-of-Stake model and the identification of internal notes. NEM solves this problem using three factors: deposit, transaction partnership, the total amount of and the sizes of the transactions over the last 30 days.

Deposit:

- at least 10000 to be bought to participate in harvesting;
- the more coins you own, more importance you get;
- PoI approves the only coins being owned for the defined term.

Transaction partnership:

- PoI rewards users who passed transactions to other NEM users’ accounts;
- users aren’t allowed to manipulate passing the transactions between accounts, the algorithm decides which transactions to accept.

The total amount of and the sizes of transactions over the last 30 days:

- each transaction (bigger than the required size) increases the proof of importance of the account;
- bigger and more frequent transactions increase importance.

Mithril [18] is a decentralized social media platform, founded by Taiwan entrepreneur Jeffrey Huang. Mithril rewards everyone who creates media content. Users earn tokens via the “social mining” process that allows them to interact with other members. Participants get rewarded if they are famous or major brand-leaders. Using blockchain technology, Mithril is allowed to provide transaction security in order to protect all involved. Also, the distributed data technology saves the trusted and untouched transactions. The main goal of the Mithril platform is to be the best blockchain system that can be implemented using the existing social media platforms.

Social mining [19] was originally used by Mithril to run the process for basic system functionality. The core, social mining algorithm is works with user content that was created by the network participants who get MITH coin in based on the value of the content. The reward will be tied to the creator’s influence and success. The more content that is created by users of the system, more coins will be earned. For example, consider the three new users X, Y, and Z. All three users are newcomers with a 0 balance. After a week, X produces 4 stories, with 400 views and 0 likes, Y produces 5 stories with 200 views and 80 likes, and Z produces nothing. As a result, the total Mithril reward is 10000 MITH coins with 4000 MITH going to X, 6000 MITH going to by Y, and 0 MITH going to Z.

The Steem company developed the very interesting Proof-of-Brain consensus protocol [37]. It is based on user activity and rewards the production of high-quality content on specific platforms. The mining process consists of content creation, interaction with voting (likes or comments), or viewing. The more likes, comments or verified views the content gathers, the more coins will be mined. Thus, mining is based on “collective intelligence” which makes the algorithm smart as well as social [35]. The PoB consensus protocol is based on two major features: the pool of tokens dedicated to content creation and curation, and the voting system that leverages the wisdom of the crowd to assess the value of content and to distribute tokens on that basis. This protocol inherits the PoW principle of mining, but requires human work to distribute tokens to community participants. The Proof-of-Brain protocol is a tool for building perpetually growing communities that encourage their members to add value to the community though the built-in reward structure.

Another great example of socially-oriented blockchain technology is the Basic Attention Token [36]. The Brave browser monitors users’ activity and how they interact with published advertising. Using the Brave browser, the user may get rewarded based on paying attention to the advertising. The browser uses an anonymous shield to protect users' personal data. This system uses the BAT as its internal cryptocurrency rewards [37].

3 Main section

3.1 Layered Peer-to-Peer (LP2P) network architecture

To design a blockchain network according to the Proof-of-Activity consensus protocol principles, some clarifications regarding the architecture should be added. The classic blockchain network, for example Bitcoin which uses the Proof-of-Work consensus protocol, is based on the Peer-to-Peer network architecture. In that case, each node is an equal unit in the global system workflow. But, to design the network to handle the PoA protocol, the node's type or parametrization is required. It's necessary to follow the stages of the defined consensus algorithm to select the validator nodes.

Designing a PoA peer-to-peer network requires additional details which is why multiple layers are suggested for handling the different types of parameters of the network. Each layer (or level) contains a subset of the nodes that are grouped by some specific condition. Nevertheless, the network still keeps the properties of the classic P2P network of nodes being equal. We refer to this enhance clarified architecture by the name Layered Peer-to-Peer (LP2P). The difference between the network architectures is compared in Figure 1. According to the quantity and the quality of its activity in the network, a node may be transferred through the layers, promoting itself and increasing the possibility of being selected as the validator. Note that the location of a node in the network is not static and may change. According to Figure 2, if the condition $activityIndex(node) \geq index_1$ for $node_0K$ is true, the transformation $node_0K \rightarrow node_1L+1$ happens. If the node located on layer N gets the level of activity, that's at least equal to activity index N+1, this node moves to the next layer and becomes a layer N+1 node.

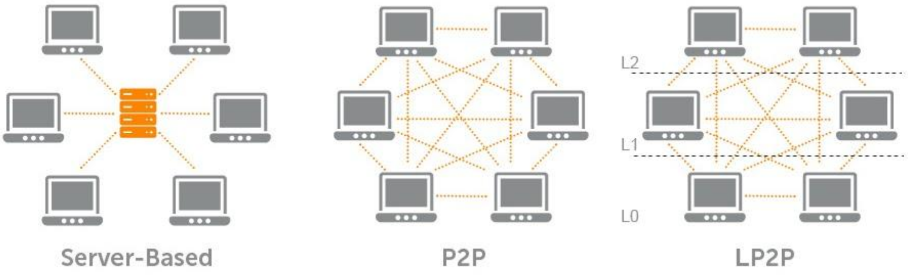

Fig. 1. Different network architectures: server-based, Peer-to-Peer and Layered Peer-to-Peer

Nodes will be grouped in layers based on their activity and will be able to participate in selecting nodes for validation roles (Fig. 3).

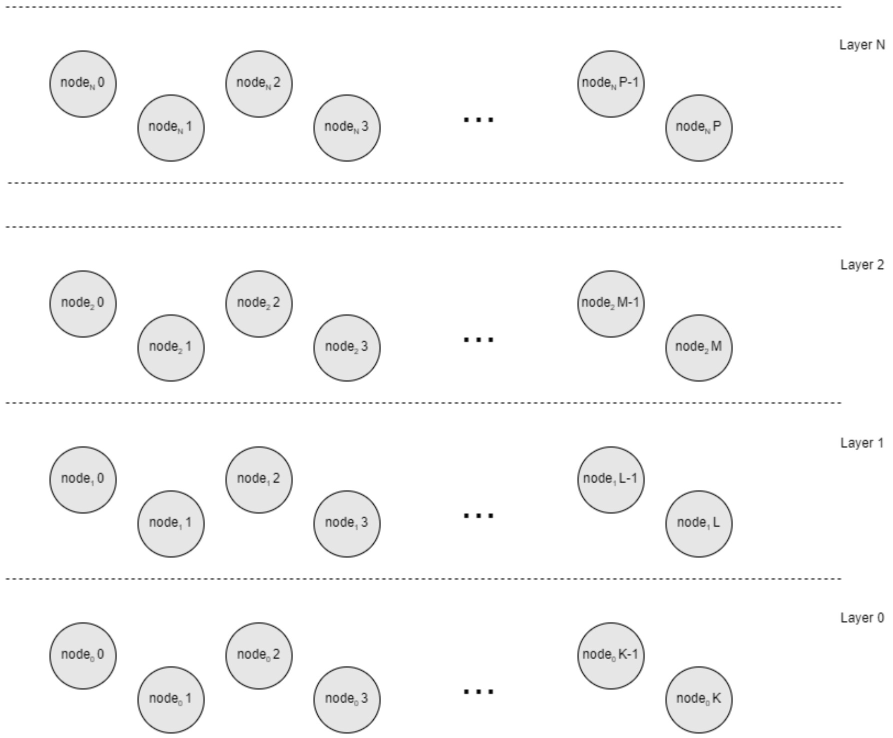

Fig. 2. Multilayered Peer-to-Peer network and layered nodes

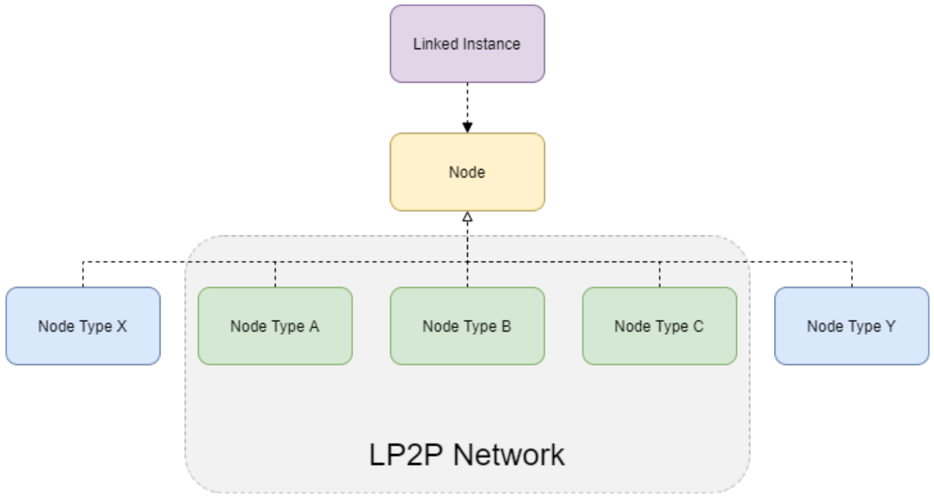

Fig. 3. Network types class diagram for active nodes (Node Type A, Node Type B, Node Type C) and passive nodes (Node Type X, Node Type Y)

3.2 The Proof-of-Activity consensus protocol

As stated earlier, the main goals of the Proof-of-Activity consensus protocol is to provide efficiency, fair rewards, a socially-oriented transaction validation process, and a method for adding blocks of transactions to the blockchain. We will address these points in more detail.

Energy Efficiency

The PoA consensus protocol is quite similar to the Proof-of-Stake protocol and totally different from the Proof-of-Work protocol - there is no puzzle to solve, which is the main criterion for block creation, signing and adding to the ledger. The PoA protocol doesn't require hardware for the transaction verification process and doesn't follow the "Mining Rush" which means wasting huge amounts of resources for hash function calculations that become more and more complex to solve requiring ever more powerful equipment to provide fast calculations.

Fairness

Unlike the PoS protocol, one is not required to own the biggest cryptocurrency stake to have a chance to become a validator and get a reward. The PoS protocol increases the importance of owning more coins which makes the system more centralized and monopolized. The PoA protocol makes the system more decentralized and increases the user's motivation to participate in the network and reduces the need to get as many coins as possible as quickly as possible. Unlike the PoW protocol, it is not necessary to increase power consumption dramatically in order to increase the probability of being rewarded. Under the PoA protocol, the probability of getting rewarded is proportional to the user's activity which inspires all nodes to increase activity and become more socially useful.

Social Orientation

Being socially oriented, the PoA platform might interest public companies to implement the PoA blockchain algorithm. The PoA protocol might encourage members to be more active in solving different tasks, challenges and problems. For example, launching such a system by a municipality, might encourage its citizens to earn rewards by becoming more publicly active. It might develop into a local cryptocurrency that might affect the local tax laws. It might also strengthen the security of the election process by using blockchain technology in a variety of ways.

These uses of the PoA protocol might create new local markets and stimulate regional innovation. These new e-government services might become integrated into the overall system of municipal government.

3.3 The new consensus block creation algorithm

Before a block can be created, we must have a set of income transactions ready to be added to the block. Like the Blockchain block, a PoA block will contain at most

1MB of information. So, as input there is the following number of transactions: $\sum_{i=1}^{n} size_i \sum_{i=1}^{n} size_i = const_{size} const_{size}$, where $size$ – is the transaction size, N – the transactions amount to be added to the block, $const_{size} const_{size}$ – constant block $size$ = 1 MB.

Below we go through the stages of the consensus algorithm that will select the single node-validator that will be allowed to create a block, sign the block and add it to the blockchain. This algorithm is sketched in Figure 4.

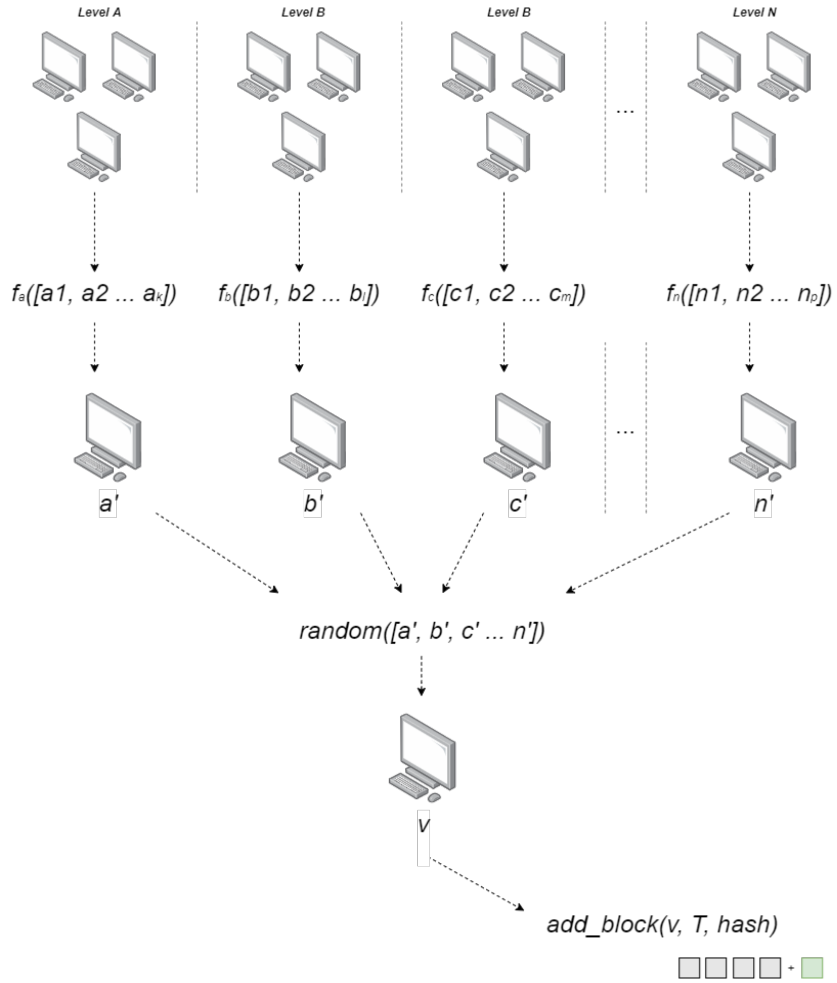

Fig. 4. The PoA protocol algorithm for finding the consensus among the nodes and adding a new block to the blockchain

Stage 1:

Let the set of levels be *[A, B, C … N]* located according to the LP2P network architecture. We will use lowercase letters to denote the nodes at each level. Thus, node $a_i \in A, where\ i \leq k$, node $b_i \in B, where\ i \leq l$, node $c_i \in C, where\ i \leq k$,…, node and node $n_i \in N, where\ i \leq p$. For each layer, we run the function f_{level} to select the potential validator for each layer, e. g., $f_a(a_1, a_2, a_3, ..., a_k)$, $f_b(b_1, b_2, b_3, ..., b_l)$, $f_c(c_1, c_2, c_3, ..., a_m)$ … $f_n(n_1, n_2, n_3, ..., n_p)$.

Stage 2:

The set of the potential validators *[a’, b’, c’ … n’]* is used as a parameter for the random function we use to select the final node-validator – *random([a’, b’, c’…n’]).* We label the final node v.

Stage 3:

The final node *v* is used as a parameter for adding the new block to the blockchain and signing it using the previously formed hash value – *block(v, T, hash) block(v, T, hash),* where *v* – node-validator, *T* – the set of valid transactions ready to be added to the block, *hash* – hash value for signing the block with.

4 Experiments and evaluation

The Proof-of-Activity consensus protocol and the algorithm for adding new blocks to the blockchain is based on 3-level typing. Figure 5 visualizes the algorithm for getting the consensus for the LP2P designed network with 3-leveled typing using the set of levels [A, B, C].

Figure 6 shows the estimated electricity consumption used by various consensus protocols. The PoA and PoB consensus protocols have zero estimated electricity consumption. At the same time the PoW protocol requires the largest amount of electricity. The PoS and PoI protocols might require some electricity consumptions in the initial stages if the PoW algorithm is used for the initial mining.

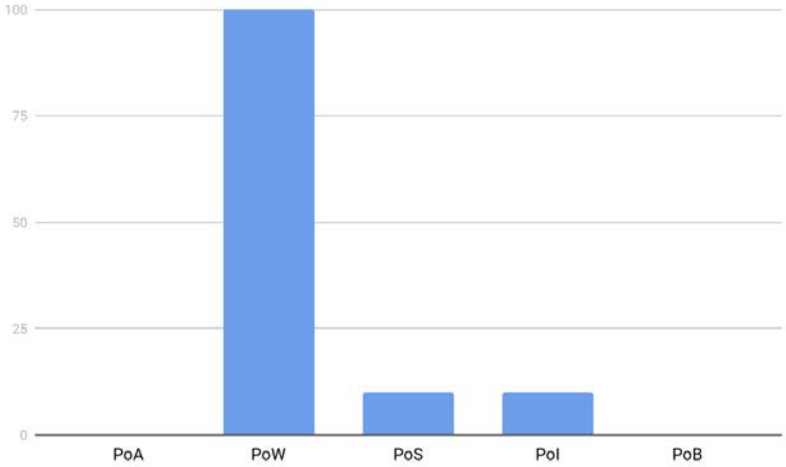

Fig. 5. Estimated electricity consumption required by various consensus protocols

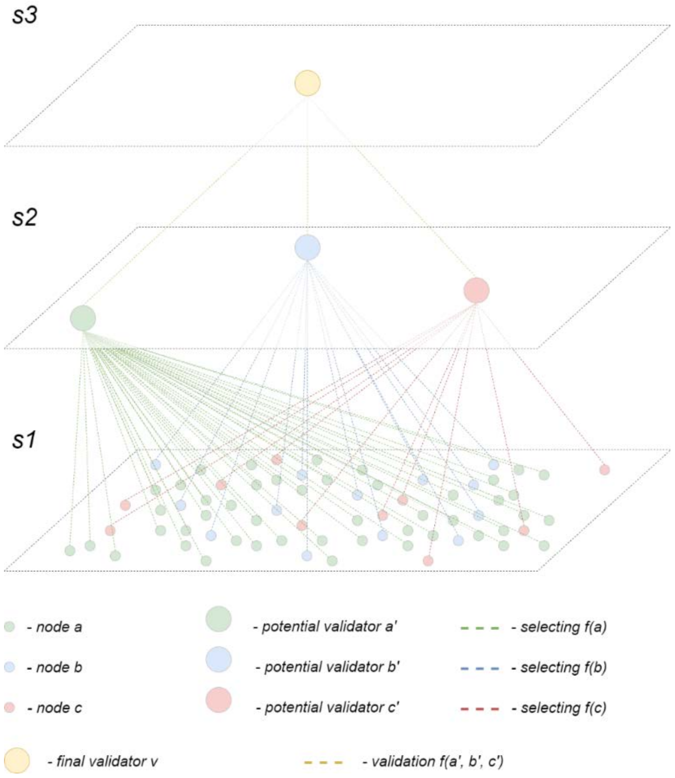

Fig. 6. PoA algorithm visualization for generating the consensus among the LP2P network nodes with 3-leveled typing

Table 1 compares the Proof-of-Activity consensus protocol to some of the most popular and relevant protocols. Such criteria as electricity consumption, decentralization, activity monitoring, social-orientation, scalability, difficulties in joining the network, etc., were reviewed for the comparison.

Table 1. Consensus protocols comparison

	PoA	PoW	PoS	PoI	PoB
Electricity consumption	-	+	+/-	+/-	-
Pseudo-decentralization issue	-	+/-	+	-	-
Resource monopolization	-	+	+	+/-	-
Easy to join	+	+/-	-	+/-	+
Activity monitoring	+	-	-	+/-	+
Social orientation	+	-	-	-	+
Scalability	+	+	+	+	+
Wide applicability	+	+	+	+	-
Requires initial coin ownership	-	-	+	+	-

The PoB protocol most resembles the Proof-of-Activity protocol: it's socially-oriented, avoids pseudo-decentralization, doesn't require initial coin owning, and doesn't require much electricity. The major difference between the PoA and PoB protocols is that PoB may only be used for media-networks – it requires the content to be rated and voted upon. On the other hand, the PoA protocol can be used for non-media networks, such as crowdfunding platforms, municipal sites, and project-handling resources.

5 Conclusions

The new PoA socially oriented network protocol was introduced in this paper. Among its advantages are:

- it minimizes pseudo-decentralization;
- it minimizes the monopolization of resources and power;
- it increases the accessibility of the network for each active node;
- it properly selects node-validators based on efficient activity;
- it fairly rewards the nodes involved in the creation of blocks and blockchain support.

The network handles transaction signing and adding transactions to the distributed ledger. It selects the node-validator for this process according to valuable social activity in the network and due to the predefined conditions and requirements which might be adopted for the given blockchain-based system.

The network uses the Proof-of-Activity consensus protocol based on the Layered Peer-to-Peer network architecture. It allocates nodes to different layers depending on their type or parameters, but at the same time, keeps the nodes on each layer equal.

This ensures the correctness of the algorithm and enables it to adapt for individual networks.

The PoA protocol can be implemented in any socially oriented setting: social networks, crowdfunding platforms, public sites, and municipal systems. It can be used in all forms of organizations where it is easy to determine whether activity is valuable, It can help to structure of organization based on activities or permissions. Also during process of developing the proposed protocol, the main aspects of security related to protection against malicious software, including botnets and computer viruses, were addressed

In addition, the new Proof-of-Activity protocol may be used as one of the stages for implementing a new tax policy – the amount of taxes due could be determined from the activity level of the users, who might receive some privileges in they are very socially active. This might lead to modifications in election law that might make elections more fair.

References

1. Nakamoto, S.: Bitcoin: “A Peer-to-Peer Electronic Cash System”. Available: https://bitcoin.org/bitcoin.pdf.
2. Ethereum Energy Consumption Index. Available: https://digiconomist.net/ethereum-energy-consumption.
3. Bitcoin Energy Consumption Index. Available: https://digiconomist.net/bitcoin-energy-consumption.
4. “A Next-Generation Smart Contract and Decentralized Application Platform.” Available: https://github.com/ethereum/wiki/wiki/White-Paper.
5. “Redefining Internet Protocols Through Effective Decentralization”, Available: https://hackernoon.com/redefining-internet-protocols-through-effective-decentralization-b2afbcb874d9.
6. Komar, M., Golovko, V., Sachenko, A., Bezobrazov, S. Intelligent system for detection of networking intrusion. Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011, pp. 374-377.
7. Savenko, O., Nicheporuk, A., Hurman I., Lysenko, S.: Dynamic Signature-based Malware Detection Technique Based on API Call Tracing. CEUR Workshop, Vol. 2393, pp. 633–643 (2019).
8. Markowsky, G. Savenko, O. Lysenko, S. Nicheporuk, A.: The technique for metamorphic viruses' detection based on its obfuscation features analysis. CEUR Workshop, Vol. 2104, pp. 680-687 (2018).
9. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proc. of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, pp. 363-368 (2013).
10. Savenko, O., Lysenko, S., Kryschuk, A.: Multi-agent based approach of botnet detection in computer systems. Communications in Computer and Information Science, Vol. 291, pp.171-180 (2012).
11. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A. and Nicheporuk, A.: A technique for detection of bots which are using polymorphic code. In: 21st International Conference, CN, Springer, Brunów, Poland, pp. 265-276 (2014)

12. Kehret, O., Walz, A., Sikora, A.: Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. Computing, Vol. 15, Issue 1, pp. 24-32 (2016).
13. NEM, New Economy Movement. Available: https://nem.io/.
14. Mithril, The Future of Social Networks. Available: https://mith.io/.
15. “What is PoI?” Available: https://docs.nem.io/ja/gen-info/what-is-poi.
16. Introduction to NEM (XEM): The Proof-of-Importance Coin. Available: https://cryptoslate.com/nem/.
17. Proof of Importance Explained. Available: https://www.mycryptopedia.com/proof-of-importance/.
18. Beginner’s Guide to Mithril: Social Platform Which Rewards Content Creators. Available: https://blockonomi.com/mithril-guide/.
19. Huang, J.: The Future of Social Networks. Mithril (MITH) Whitepaper, pp. 1-30.
20. Blockchain White Paper, China Academy of Information and Communication Technology, Trusted Blockchain Initiatives, pp. 1-49 (2018).
21. BlockChain Technology Beyond Bitcoin. Available: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
22. Blockchain disruption and smart contracts. Available: https://www.nber.org/papers/w24399.pdf.
23. Blockchain in Trade Facilitation. Available: http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf.
24. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873, pp. 1-24 (2017)
25. Wahab, A., Memood, W.: Survey of Consensus Protocols. arXiv:1810.03357, pp. 1-12 (2018).
26. Schwartz, D., Youngs, N., Britto, A.: The Ripple Protocol Consensus Algorithm. Ripple Labs, Inc. White Paper; Ripple Labs, Inc.: San Francisco, CA, USA, Vol. 5, pp. 1-8. (2014).
27. Daian, P., Pass, R., Shi, E.: Snow White: Provably Secure Proofs of Stake, Cryptology ePrint Archive, Report 2016/919, pp. 1-62 (2016).
28. Buterin, V.: Slasher: A punitive proof-of-stake algorithm. Available: https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.
29. Chen, J., Micali, S.: Algorand: the efficient and democratic ledger, arXiv: 1607.01341 (2016).
30. Proof of Stake FAQ. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
31. Analysis of the main consensus protocols of blockchain. Available: https://www.sciencedirect.com/science/article/pii/S240595951930164X
32. Mazieres, D.: Stellar Consensus Protocol. Available: https://www.stellar.org/papers/stellar-consensus-protocol
33. Basic Attention Token (BAT) Blockchain Based Digital Advertising, Available: https://basicattentiontoken.org/wpcontent/uploads/2017/05/BasicAttentionTokenWhitePaper-4.pdf
34. SMT Whitepaper. A technical paper on the proposed Smart Media Tokens protocol. Available: https://steem.com/wp-content/uploads/2018/11/smt-whitepaper-nov-3-2018.pdf
35. Proof of Brain Bluepaper. Available: https://steem.com/steem-bluepaper.pdf
36. Basic Attention Token. “Introducing blockchain based digital advertising”. Available: https://basicattentiontoken.org/.
37. Steem. Powering communities and opportunities. Available: https://steem.com/.