DOI: https://doi.org/10.15276/aait.02.2019.6
UDC 004.75

PROOF-OF-GREED APPROACH IN THE NXT CONSENSUS

Igor E. Mazurok[1)]
ORCID: https://orcid.org/ 0000-0002-6658-5262, igor@mazurok.com
Yevhen Y. Leonchyk[1)]
ORCID: https://orcid.org/ 0000-0003-1494-0741, leonchik@ukr.net
Tatyana Y. Kornylova[1)]
ORCID: https://orcid.org/0000-0001-7377-9471, t.kornilova04@gmail.com
[1)] Odessa I.I. Mechnikov National University, 2, Dvoryanska Str. Odesa, 65082, Ukraine

ABSTRACT

A fundamental problem in distributed computing systems is to make the same decision on an issue. The consensus protocol describes a process to agree on some data value that is needed during computation. The work is devoted to development of the consensus algorithm based on the Nxt consensus protocol which can be implemented to blockchain systems with PoS (Proof-of-Stake). PoS consensuses based on node balances, and unlike PoW (Proof-of-Work) methods, are environmentally friendly and more energy efficient. Nowadays such types of consensuses are getting more popular. However, they remain less scrutinized than PoW. Moreover, there are some attacks and threats that cannot be completely resolved under PoS consensuses, and in particular under the Nxt. In this article we propose a modification of the Nxt protocol which solves some problems of PoS in accordance with modern requirements. The asymmetric method was used to select the best Nxt consensus parameters for decreasing of the blocktime variance. This improves the performance and reliability of the entire blockchain system eliminating the risk of disruptions due to overflowing the transaction pool. For the Nxt consensus protocol researching, the mathematical simulating model was developed using Anylogic 8.4 software. Implementation of economic leverages (tokenomics), which we called Proof-of-Greed approach, allows to prevent some types of attacks, e.g. large stake attack, and to set a fair market-based transaction fee. The using of economic mechanisms to protect distributed systems allows to prevent a number of attacks that are resistant to cryptographic methods. But at the same time, the tokenomics of the system should be strictly consistent with the protocols for the functioning of all system objects, combining them into an integrated unitary ecosystem. Also, a payback period of harvesters was investigated within Proof-of-Greed protocol. The parameters of such approach for sustained operation of a network were obtained as a result of mathematical simulating with Anylogic 8.4 software. The Proof-of-Greed approach can be implemented not only in the Nxt consensus but in some other blockchain systems based on PoS consensuses.

Keywords: Consensus Algorithm; Distributed System; Blockchain; Tokenomics

***For citation*: Igor E. Mazurok, Yevhen Y. Leonchyk, Tatyana Y. Kornylova. Proof-of-Greed Approach in the Nxt Consensus. *Applied Aspects of Information Technology*. 2019; Vol.2 No.2: 153–160. DOI: https://doi.org/10.15276/aait.02.2019.6**

INTRODUCTION

As well known, distributed systems have a lot of advantages but they are inferior in speed to centralized systems [1, 2]. Our goal is to handle the performance demand in PoS (Proof-of-Stake) blockchain systems [3, 4], which use the Nxt consensus [3, 4], [5]. In blockchain systems based on PoS, the harvester account gets reward when it successfully creates a block. Thus, there must be an approach to define (generate) the next valid block. Such process is called forging.

In the standard version of the Nxt consensus blocks are generated every 60 seconds, on average, by network accounts that are unlocked for forging [5]. However, we have to provide decreasing of the forging time as well as increasing when the need arises. Thus, there is the problem of selecting parameters of the existing algorithm to forge block for the required time.

There is no commission adjustment framework in blockchain systems. A user can give a commission less than necessary or even more. Generally, a transaction fee is paid in tokens. However, token rates can fluctuate widely in relation to stable currencies. It leads to wide variation in prices over time. We propose the method Proof-of-Greed as an addition to the Nxt consensus which solves this problem. Such approach allows setting a fair market-based reward for transactions.

In relation to these modifications, the important question arises: what is the best harvester strategy to get the maximum profit and to decrease the payback period? The optimal parameters can be obtained with simulating. In addition, in such case, one should take a deep look at appeared new types of attack.

OBJECTIVES OF THE STUDY

Development and simulating of approaches to improve the block time characteristics of the Nxt consensus algorithm and to empower one by economic leverages.

RELEVANCE

In the recent years there was a burst of popularity of PoS blockchain systems. Unlike systems based on PoW such as Bitcoin and Ethereum, where miners must solve complicated cryptographic puzzles in order to create blocks, in PoS-based systems the creator of the next block is chosen in a deterministic (pseudo-random) way. The probability to be chosen depends on its stake, activity and reputation [3]. PoW consensus demands high computation requirements and high energy costs to protect against a double-spending attack and a threat of centralization by mining pools in comparison with PoS [7]. It is a disadvantage for some types of blockchain systems. Nowadays, PoS consensus methods, and in particular the Nxt, are being developed actively [8, 9]. Hence, there is a need to take into account modern challenges and to modify the standard version of the Nxt consensus.

RESEARCH METHODS

The simulating was fulfilled using AnyLogic 8.4 software [10]. The special models were developed to obtain the best parameters of the Proof-of-Greed consensus achieving these objectives.

1. Block Creation (Forging)

Two values are key to determining which account is eligible to generate a block, which account earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict:

– T_p – previous base target;

– T_b – calculated base target.

Each block on the chain has a *generation signature* parameter. To participate in the block forging process, an active account digitally signs the generation signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256 algorithm. The first 8 bytes of the resulting hash are converted to a number, referred to as the account *Hit*.

The *Hit* is compared to the current target value. If the computed *Hit* is lower than the target, then the next block can be generated. As noted in the target value formula (see below), the target value increases with each passing second. Even if there are only a few active accounts on the network, one of them will eventually generate a block because the target value will become very large. Therefore, you can calculate the time it will take any account to forge a block by comparing the account *Hit* value to the target value.

This base target value varies from block to block, and is derived from the previous block base target multiplied by the amount of time that was required to generate that block using a formula that ensures S_0 seconds average block time over the last three blocks.

Each account calculates its own target value, based on its current effective stake. This value is

$$T = T_b \cdot \mathbf{S} \cdot B \ ,$$

where: T – is the new target value;

$\mathbf{S}$ – is the time since the last block, in seconds;

B – is the effective balance of the account.

In a situation where multiple blocks are generated, nodes will select the block with the highest cumulative difficulty value as the authoritative block. As block data is shared between peers, forks (non-authoritative chain fragments) are detected and dismantled by examining the chains cumulative difficulty values stored in each fork.

2. Preforging block time

Time adjustment in the Nxt consensus is based on a few parameters and variables (model A) [11, 12], [13, 14], [15, 16]:

– $Max_{\mathbf{Ratio}} = S_0 + \mathbf{factor}$ is the max ratio by which the target is decreased when block time is larger than S_0 seconds;

– $Min_{Ratio} = S_0 - \mathbf{factor}$ is the min ratio by which the target is increased when block time is smaller than S_0 seconds;

– $0 < \gamma = 0{,}64 < 1.$

The base target T_b is calculated as follows:

If $\mathbf{S} > S_0$ set

$$T_b = T_p \cdot \frac{\min(S, Max_{Ratio})}{S_0}$$

else set

$$T_b = T_p \cdot \left(1 - \gamma \cdot \left(1 - \frac{max(S, Min_{Ratio})}{S_0}\right)\right),$$

where the factor parameter makes adjustments gradually and the γ parameter is used since the block time is bounded by 0 from below. The recommended initial base target depends on the total amount of tokens [5].

The developed simulating model with AnyLogic 8.4 software [10] allows obtaining optimal parameters to achieve any specified average time between blocks. A number of nodes, distributions of effective balance and a few initial parameters can also be varied in this model. As an illustration, the time for the last 3 blocks (the bright line) and for the last 100 blocks (the dark line) are shown

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

on the figure 1 below with the forging time parameter S_0 as 15 seconds with $\text{factor} = 0.765$.

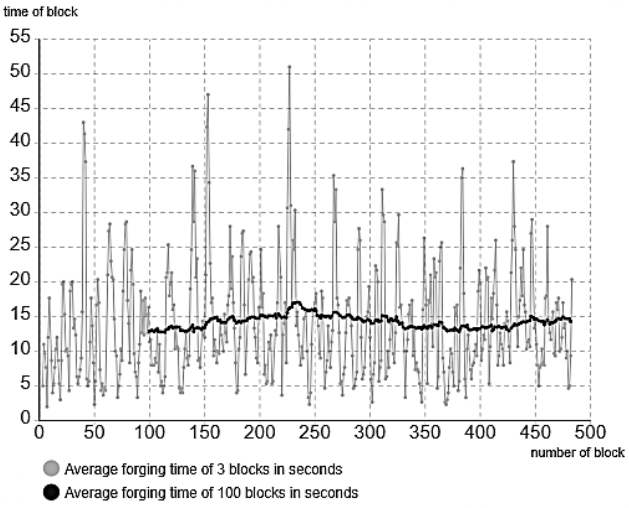

Fig. 1. **The average preforging block time, model A**

***Source*: compiled by the author**

As can be seen in the figure, there is a large block time problem when preforging time is too long. Further, the Nxt team proposed to use the alternative formulas for the base target recalculating in case of $S_0 = 60$ seconds (model B):

If $S < 0.9 \cdot S_0$
set $T_b = T_p \cdot 0.93$;
If $S > 1.1 \cdot S_0$
set $T_b = T_p \cdot 1.1$
If $S_0 < S < 1.1 \cdot S_0$
If $0.9 \cdot S_0 < S < S_0$

$$\text{set} \quad T_b = T_p \cdot \left(1 - 0.7 \cdot \left(1 - \frac{S}{S_0}\right)\right)$$

And if the T_b goes out of the limiting interval, set it to the limiting value:

If $T_b < 0.9 \cdot T_0$, set $T_b = 0.9 \cdot T_0$;
If $T_b > 3 \cdot T_0$, set $T_b = 3 \cdot T_0$

Such algorithm should solve the problem of large blocktimes for good. Also, the blocktimes will become more "concentrated", i.e. the variance will decrease with it (Fig. 2).

Developed simulating model allows to obtain the best parameters for any given forging time S_0 and preferable minimum and maximum time limits.

The average block time depends on the number of nodes and their stake (balance) distribution. To reduce the percentage of large blocktime, we propose to use asymmetrical factors, when Max_{Ratio} is greater than Min_{Ratio} in the model A. Such approach achieves the result similar to the model B.

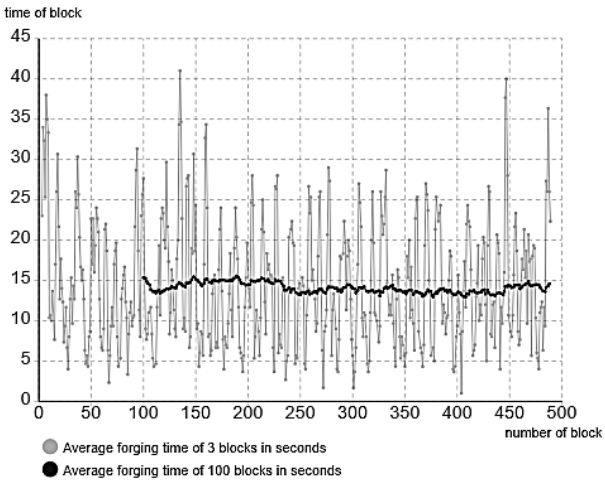

Fig. 2. **The average preforging block time, model B**

***Source*: compiled by the author**

Moreover, it provides sharper time decreasing of the next block after longtime block.

For $S_0 = 15\ sec$:

$$Max_{Ratio} = 15 + 1.025 = 16.025\ sec$$

$$Min_{Ratio} = 15 - 0.765 = 14.235\ sec$$

with the recommended the initial base target

$$T_0 = \frac{\max(Hit)}{2 \cdot S_0 \cdot B},$$

where B is the effective initial total balance and Hit is the first 8 bytes of the hash are converted to a number (hash is digitally signed generation signature of the previous block).

3. Proof of greed approach

There is no commission adjustment framework in blockchain systems. A user can give a commission less than necessary or even more. We propose the approach Proof-of-Greed which solves this problem.

Instead of indicating a fixed transaction fee, a user will offer the maximum fee that he/she could pay. Transactions get into the Transaction Pool, from there harvesters take transactions and form their own blocks and take the commission as much as they want but not more than the specified maximum. Here greed already comes in. The more the harvester took the commission, the less possibility that its block will be recorded in the blockchain.

This is achieved by such modification of the Nxt Consensus:

N – the number of nodes;

$numTr_i$ – the number of transactions in the block from the node i , $i = 1, \ldots, N$;

$actFee_{ij}$ – how much commission node i took from the transaction j, $i = 1,\dots,N$, $j = 1,\dots,numTr_i$;

$maxFee_{ij}$ – maximum that node i can take from the transaction j, $i = 1,\dots,N$, $j = 1,\dots,numTr_i$;

g_i – the greed of the node i, $i = 1,\dots,N$:

$$g_i = \frac{\varepsilon + \sum_{j=1}^{numTr_i} actFee_{ij}}{\varepsilon + \sum_{j=1}^{numTr_i} maxFee_{ij}};$$

λ_i – parameter of the node i, $i = 1,\dots,N$:

$$\lambda_i = [[1 + \Delta(1 - 2g_i)]]^k$$

where $k > 0$ and $0 \le \Delta < 1$;
and finally

$$T = T_b \cdot S \cdot B \cdot \lambda_i.$$

The λ_i is a special factor, as a function which depends on harvester greed and a few parameters, can increase or decrease the possibility to forge a block.

As a result of simulating with AnyLogic 8.4 software [8], the recommended parameters for the Proof-of-Greed algorithm are:

– $\Delta = 0.5$;

– $k = 3.2$.

These parameters were adjusted to protect zero-fee attack. Thus, a few nodes, which create blocks for free, cannot get control of the system (Fig. 3). In this simulation, the first 10 harvesters do not take fees at all and have effective balances as 250,000 tokens; the last 10 harvesters take maximum fees and have effective balances as 1,000,000 tokens. The rest 280 nodes have stakes and values of greed which are distributed linearly.

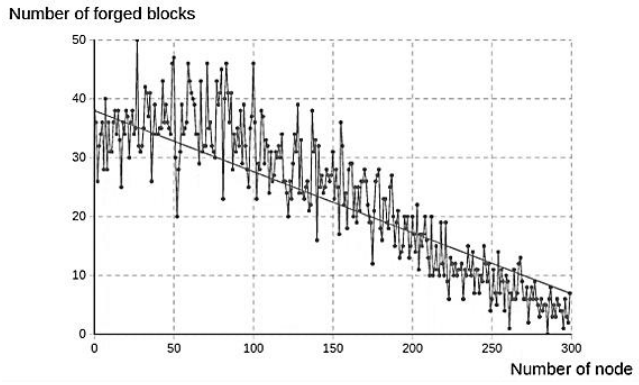

Fig. 3. **The zero fee attack**
***Source*: compiled by the author**

As a result, the first 10 nodes (and even the first 50 nodes which takes small fees) do not produce most of the blocks. Here we assume that earned tokens are not added to effective balances. Otherwise, the influence of the first harvesters will be even more reduced.

On the other hand, such altruistic nodes can help to protect against large stake attack of greedy harvesters. In the Fig. 4, the last 10 harvesters take maximum fees and have huge effective balances as 10,000,000 tokens for each node. The rest 290 harvesters have stakes from 250,000 to 1,000,000 and their greed is distributed from 0 to 100 % linearly.

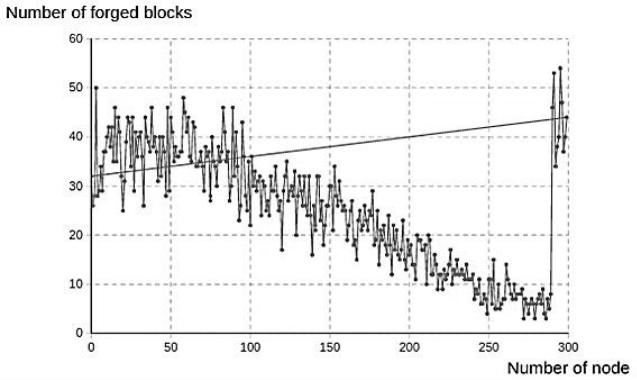

Fig. 4. **The large stake attack**
***Source*: compiled by the author**

It can be seen that very greedy nodes with huge stakes cannot impose their rules on the entire system. Thus, Proof-of-Greed stimulates the harvesters to work for a modest fee.

4. Incomes of harvesting blockchain nodes

In the modification Proof-of-Greed of Nxt consensus, harvesters independently make decisions what proportion of commission fee to take for forging a block. This may lead to the fact that some nodes will charge the maximum fee for the creation of a block in order to quickly payback their initial stake. But the more a harvester will take, the less possibility that his/her block will be recorded in the blockchain. This is achieved by modification of Nxt consensus. Also, nodes can choose the approach with the choice of the minimum fee per block, with the expectation that a greater number of blocks will provide greater profits than with the above approach. Thus, the problem is to find a proportion of fee which the nodes should charge in order to get the maximum profit and more likely to payback their initial stake [17-18], [19].

In the figure below, the chart shows the earnings of each node (without initial stake), the initial stake of each node at the level 250,000 and double the initial stake at the level 500,000. Thus, the

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

achievement of a line of 250,000 and a line of 500,000 by the graph means that the nodes have paid off their initial stake once and twice respectively.

On Fig. 1 the initial values of the effective node balances (stakes) equal 250,000 tokens. The payment that the nodes charge for the creation of a block is distributed linearly from 20 to 100 percent of the maximum possible by 300 nodes. As a result of this experiment, the first 100 nodes paid off earlier than others.

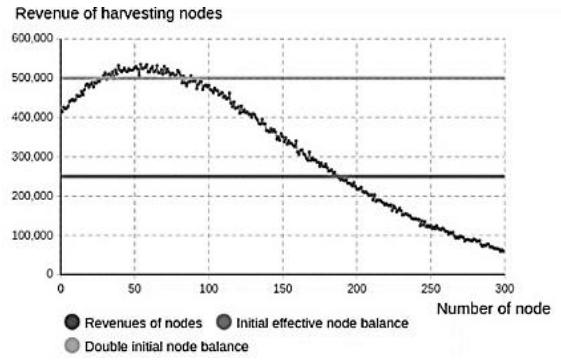

Fig. 5. **The case of equal initial balances (stakes)**
***Source*: compiled by the author**

In this simulation, the payment proportions that the nodes charge for the creation of a block is distributed linearly from 20 to 100 percent of the maximum possible by 300 nodes (Fig. 6). The initial values of the node stakes are distributed linearly from 1,000,000 to 250,000 by 300 nodes in the same order.

As a result, it was obtained that with different initial rates of nodes the optimal amount of commission is from 30 to 40 percent of the maximum possible. This approach ensures maximum profit [20, 21], [22, 23], [24, 25] and the fastest payback in the conditions of the Proof-of-Greed approach.

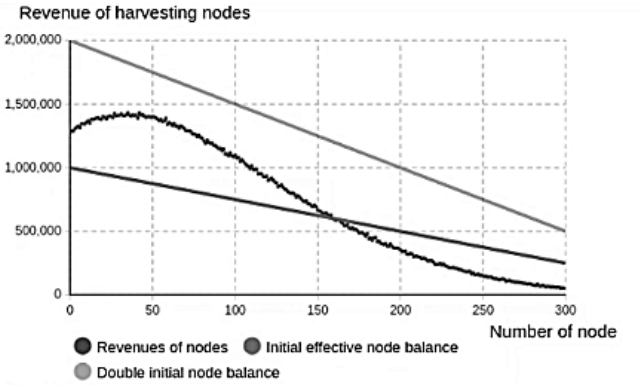

Fig. 6. **The case of different balances and proportions of fees**
***Source*: compiled by the author**

CONCLUSIONS

The new modification of the Nxt consensus solves some problems which exist in the distributed systems based on blockchain technology [26, 27], [28, 29], [30]. The best parameters to decrease the variance of forging block time were obtained. The Proof-of-Greed approach gives a possibility to set market-based commission fees for transactions and provides the protection from some new attacks. Also, the recommendations for harvester's nodes were made to achieve the fastest payback period. Despite the fact that the simulation was carried out only for the Nxt algorithm, we see prospects of the Proof-of-Greed using in other similar PoS systems where the problems of transaction cost optimization arise.

REFERENCES

1. Tanenbaum, Andrew S. & Steen, Maarten Van. "Distributed systems: principles and paradigms". Second Edition. Upper Saddle River, NJ: Pearson Prentice Hall. 2017.

2. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System". – Available from: https://bitcoin.org/bitcoin.pdf. A Peer-to-Peer Electronic Cash System. – Active link – 17.02.2019.

3. Bentov, I., Pass, R. & Shi, E. "Snow white: Provably secure proofs of stake". IACR Cryptology ePrint Archive. 2016. 919.

4. Vashchuk, O. & Shuwar, R. "Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake". *Electronics and Information Technology*. 2018; Issue 9: 106–112.

5. "Whitepaper: Nxt". – Available from: https://nxtwiki.org/wiki/ Whitepaper:Nxt#Block_Creation_. 28Forging.29, Whitepaper: Nxt. – Active link – 17.02.2019.

6. "Nxt. Own your data, control your world/privacy/money/budget/assets/choice/vote/freedom/name/rights/files/IP/records/trade/market". – Available from: https://nxtplatform.org/ Title from the screen. – Active link – 17.02.2019.

7. Bach, L., Mihaljevic, B. & Zagar. “Comparative analysis of blockchain consensus algorithms”. *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2018. p. 1791–1796.

8. “MTHCL. The math of Nxt forging”. – Available from: www.docdroid.net/ecmz/forging0-5-2.pdf.html. The math of Nxt forging. – Active link – 17.02.2019.

9. Popov, S. A. “Probabilistic Analysis of the Nxt Forging Algorithm”. *Journal of Cryptocurrency and Blockchain Technology Research “Ledger”*. 2016; Vol. 1: 69–83.

10. “AnyLogic: Multimethod Simulation Software 8.4”. – Available from: http://www.anylogic.com/. AnyLogic simulation software. – Active link – 17.02.2019.

11. MTHCL. “BaseTarget adjustment algorithm”. – Available from: https://nxtforum.org/proof-of-stake-algorithm/basetarget-adjustment-algorithm/ (registration on nxtforum.org required), BaseTarget adjustment algorithm. – Active link – 17.02.2019.

12. Schilling, M. “The Longest Run of Heads”. The College Math J. 1990; 21 (3): 196–206.

13. Ross, Sheldon M. “A First Course in Probability”. 8th ed. Pearson Prentice Hall. 2009. 520 p.

14. Ross, Sheldon M. “Introduction to Probability Models”. 10th ed. Elsevier. 2012. 784 p.

15. Yung, M., Dodis, Y., Kiayias, A., Malkin, T. & Bernstein, D. J. “Curve25519: New Diffie-Hellman Speed Records”. *Public Key Cryptography*. 2006. 207-228. DOI: https://doi.org/10.1007/11745853_14.

16. Qin, W. & Zhou, N. “New concurrent digital signature scheme based on the computational Diffie-Hellman problem”. *The Journal of China Universities of Posts and Telecommunications*. 2010; 17(6): 89–100. DOI: https://doi.org/ 10.1016/S1005-8885(09)60530-6.

17. “Profitability calculator for cryptocurrency mining and the pay-back period for mining equipment (GPU graphics cards and ASIC miners)”. – Available from: https://coinsbase.org/mining/mining-calculator/, Profitability calculator for cryptocurrency mining and the pay-back period for mining equipment. – Active link – 17.02.2019.

18. “Save Big with Cryptocurrency Tax Loss Harvesting”. – Available from: https://medium.com/cointracker/save-big-with-cryptocurrency-tax-loss-harvesting-5abd2e68d65c. Save Big with Cryptocurrency Tax Loss Harvesting. – Active link – 17.02.2019.

19. Cryptofees. – Available from: http://cryptofees.net/. Cryptofees. – Active link – 17.02.2019.

20. “Bitcoin Users Are 'Overpaying' in Transaction Fees, Data Suggests”. – Available from: https://www.cryptoglobe. com/latest/2019/04/bitcoin-users-are-overpaying-in-transaction-fees-data-suggests/. Bitcoin Users Are 'Overpaying' in Transaction Fees, Data Suggests. – Active link – 17.02.2019.

21. “Learn Cryptography 51 % Attack (n.d.)”. – Available from: http://learncryptography.com/51-attack/, 51 % Attack. – Active link – 17.02.2019.

22. “In cryptoland, trust can be costly”. – Available from: https://securelist.com/in-cryptoland-trust-can-be-costly/86367/. In crypto land, trust can be costly – Active link – 17.02.2019.

23. “Forging vs. Mining”. Part 1. – Available from: https://medium.com/metahash/forging-vs-mining-part-1-88405d0c5664, Forging vs Mining. Part 1. – Active link – 17.02.2019.

24. “The most profitable PoS coins to Forge”. – Available from: https://medium.com/@poolofstake/the-most-profitable-pos-coins-to-forge-ffe24745c917. The most profitable PoS coins to Forge. – Active link – 17.02.2019.

25. “Cyber Attacks Cryptographic Attacks”. – Available from: http://www.valencynetworks.com/articles/cyber-attacks-cryptographic-attacks.html, Cyber Attacks Cryptographic Attacks. – Active link – 17.05.2019.

26. “Attacks on Cryptosystems>“. – Available from: https://www.tutorialspoint.com/cryptography/ attacks_on_cryptosystems.htm, Attacks on Cryptosystems. – Active link – 17.02.2019.

27. ““Fake Stake” attacks on chain-based Proof-of-Stake cryptocurrencies”. – Available from: https://medium.com/@dsl_uiuc/fake-stake-attacks-on-chain-based-proof-of-stake-cryptocurrencies-b8b05723f806. “Fake Stake” attacks on chain-based Proof-of-Stake cryptocurrencies. – Active link – 17.02.2019.

28. Berengueres, J. “Valuation of Crypto-Currency Mining Operations”. *The Journal of Cryptocurrency and Blockchain Technology Research “Ledger”*. 2018; Vol. 3: 60–67.

29. Kiayias, A., Russell, A., David, B. & Oliynykov, R. “Ouroboros: A provably secure proof-of stake blockchain protocol”. Tech. rep. Cryptology ePrint Archive, Report 2016/889, http://eprint.iacr.org/2016/889. 2016.

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)

30. Wenting Li, Sebastien Andreina, Jens-Matthias Bohli & Ghassan Karame. “Securing Proof-of-Stake Blockchain Protocols”, European Symposium on Research in Computer, Security International Workshop on Data Privacy Management Cryptocurrencies and Blockchain Technology. Lecture Notes in Computer Science. 2017. DOI: https://doi.org/10.1007/978-3-319-67816-0_17.

Received 05.02.2019
Received after revision 17.04.2019
Accepted 22.04.2019

DOI: https://doi.org/10.15276/aait.02.2019.6
УДК 004.75

МЕТОД PROOF-OF-GREED У NXT КОНСЕНСУСІ

Ігор Євгенійович Мазурок[1)]
ORCID: https://orcid.org/ 0000-0002-6658-5262, igor@mazurok.com
Євген Юрійович Леончик[1)]
ORCID: https://orcid.org/ 0000-0003-1494-0741, leonchik@ukr.net
Тетяна Юріївна Корнилова[1)]
ORCID: https://orcid.org/ 0000-0001-7377-9471, t.kornilova04@gmail.com
[1)] Одеський національний університет імені І.І. Мечникова, вул. Дворянська, 2. Одеса, 65082, Україна

АНОТАЦІЯ

Фундаментальна проблема у розподілених обчислювальних системах полягає у тому, щоб прийняти одне й те ж рішення щодо якого-небудь питання. Протокол консенсусу описує узгодження даних, необхідних під час такого процесу. Робота присвячена розробці алгоритму консенсусу, заснованого на протоколі Nxt, який може бути реалізований у системах блокчейн з PoS (Proof-of-Stake). Консенсуси типу PoS, засновані на балансах вузлів, та на відміну від методів PoW (Proof-of-Work), є більш екологічно чистими та енергоефективними. У наш час такі типи консенсусів стають все більш популярні. Проте вони залишаються менш ретельно вивченими, ніж PoW. Більше того, існують деякі атаки та загрози, які не можуть бути повністю вирішені за допомогою консенсусу PoS, і зокрема, Nxt консенсусом. У даній статті ми пропонуємо модифікацію протоколу Nxt, який вирішує деякі проблеми з PoS відповідно до сучасних вимог. Для вибору найкращих параметрів консенсусу Nxt, які зменшують дисперсію часу блоків, було використано асиметричний метод. Це підвищило продуктивність та надійність усієї блокчейн системи, усуваючи загрозу збоїв у роботі внаслідок переповнення пулу транзакцій. Для дослідження протоколу Nxt консенсусу була розроблена математична імітаційна модель з використанням програмного забезпечення Anylogic 8.4. Реалізація економічних важелів (токеноміка), яку ми називаємо підходом Proof-of-Greed, дозволяє попередити деякі види атак, наприклад, атаку вузлів з великим балансом та встановленню справедливої, ринково обґрунтованої плати за транзакцію. Застосування економічних механізмів захисту розподілених систем дозволяє запобігти ряду атак, стійких до криптографічних методів. Але при цьому токеноміка системи повинна строго узгоджуватися з протоколами функціонування всіх об'єктів системи, об'єднуючи їх в єдину інтегровану екосистему. Також було досліджено термін рентабельності вузлів, що створюють блоки у протоколі Proof-of-Greed. Параметри такого підходу для стійкого функціонування мережі були отримані за результатами математичного моделювання з програмним забезпеченням Anylogic 8.4. Метод Proof-of-Greed може бути реалізовано не тільки у Nxt консенсусі, а й у деяких інших блокчейн системах, що засновані на консенсусах типу PoS.

Ключові слова: алгоритм консенсусу; розподілені системи; блокчейн, токеноміка

DOI: https://doi.org/10.15276/aait.02.2019.6
УДК 004.75

МЕТОД PROOF-OF-GREED В NXT КОНСЕНСУСЕ

Игорь Евгеньевич Мазурок[1)]
ORCID: https://orcid.org/ 0000-0002-6658-5262, igor@mazurok.com
Евгений Юрьевич Леончик[1)]
ORCID: https://orcid.org/ 0000-0003-1494-0741, leonchik@ukr.net
Татьяна Юрьевна Корнилова[1)]
ORCID: https://orcid.org/ 0000-0001-7377-9471, t.kornilova04@gmail.com
[1)] Одесский национальный университет имени И. И. Мечникова, ул. Дворянская, 2. Одесса, 65082, Украина

АННОТАЦИЯ

Фундаментальная проблема в распределённых вычислительных системах заключается в том, чтобы принять одно и то же решение по поводу какого-нибудь вопроса. Протокол консенсуса описывает согласование данных, необходимых во

время такого процесса. Работа посвящена разработке алгоритма консенсуса, основанного на протоколе Nxt, который может буть, реализован в системах блокчейн с PoS (Proof-of-Stake). Консенсусы типа PoS, основаны на балансах узлов, но в отличии от методов PoW (Proof-of-Work), является более экологически чистыми и энергоэффективными. В наше время такие типы консенсусов стают всё более популярными. Однако, они остаются менее тщательно изученными, чем PoW. Более того, существуют некоторые атаки и угрозы, которые не могут быть полностью разрешены с помощью консенсуса PoS, и в частности, Nxt консенсусом. В данной статье мы предлагаем модификацию протокола Nxt, который разрешает некоторые проблемы с PoS в соответствии с современными требованиями. Для выбора наилучших параметров консенсуса Nxt, которые уменьшают дисперсию времени блоков, был использован асимметричный метод. Это повысило производительность и надежность всей блокчейн системы, устраняя угрозу сбоев в работе вследствие переполнения пула транзакций. Для исследования протокола Nxt консенсуса была разработана математическая имитационная модель с использованием программного обеспечения Anylogic 8.4. Реализация экономических рычагов (токеномика), которую мы называем подходом Proof-of-Greed, позволяет предотвратить некоторые виды атак, например, атаку узлов с большим балансом и установлению справедливой, рыночно обоснованной платы за транзакцию. Применение экономических механизмов защиты распределенных систем позволяет предотвратить ряд атак, устойчивых к криптографическим методам. Но при этом токеномика системы должна строго согласовываться с протоколами функционирования всех объектов системы, объединяя их в единую интегрированную экосистему. Также был исследован срок рентабельности узлов, которые создают блоки в протоколе Proof-of-Greed. Параметры такого подхода для устойчивого функционирования сети были получены по результатам математического имитационного моделирования в программном обеспечении Anylogic 8.4. Метод Proof-of-Greed может быть реализован не только в Nxt консенсусе, но также и в некоторых других блокчейн системах, основанных на консенсусах типа PoS.

Ключевые слова: алгоритм консенсуса; распределённые системы; блокчейн; токеномика

ABOUT THE AUTHORS

Igor E. Mazurok, PhD (Eng), Associate Professor, Associate Professor of the Department of Optimal Control and Economical Cybernetics, Odessa I. I. Mechnikov National University, 2, Dvoryanska Str. Odesa, 65082, Ukraine
igor@mazurok.com. ORCID: https://orcid.org/ 0000-0002-6658-5262

Ігор Євгенійович Мазурок, кандидат технічних наук, доц. каф. Оптимального управління та економічної кібернетики. Одеський національний університет імені І. І. Мечникова, вул. Дворянська, 2. Одеса, 65082, Україна

Yevhen Y. Leonchyk, PhD (Phys.-Math), Associate Professor, Associate Professor of the Department of Mathematical Analysis. Odessa I. I. Mechnikov National University, 2, Dvoryanska Str. Odesa, 65082, Ukraine
leonchik@ukr.net, ORCID: https://orcid.org/ 0000-0003-1494-0741

Євген Юрійович Леончик, кандидат фізико-математичних наук, доцент каф. Математичного аналізу. Одеський національний університет імені І.І. Мечникова, вул. Дворянська, 2. Одеса, 65082, Україна

Tatyana Y. Kornylova, fourth-year student of Faculty of Mathematics, Physics and Information Technologies, Odessa I. I. Mechnikov National University, 2, Dvoryanska Str. Odesa, 65082, Ukraine
t.kornilova04@gmail.com, ORCID: https://orcid.org/0000-0001-7377-9471

Тетяна Юріївна Корнилова, студентка четвертого курсу факультету Математики, фізики і інформаційних технологій. Одеський національний університет імені І. І. Мечникова, вул. Дворянська, 2. Одеса, 65082, Україна

ISSN 2617-4316 (Print)
ISSN 2663-7723 (Online)