

УДК 004.057.4
DOI: 10.31891/2219-9365-2020-66-2-8

БЕЛЬФЕРР. Е., МЕДЗАТИЙ Д. М., ОМЕЛЬЧУК Р. В.
Хмельницький національний університет

ДОСЛІДЖЕННЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ВСТАНОВЛЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛУ КОНСЕНСУСУ PROOF-OF-ACTIVITY

У роботі проведено детальний аналіз відомих протоколів для реалізації в системах блокчейн. Виділено основні проблеми, які виникають в реальному використанні таких систем. Зокрема, це проблема енерговитрат та безпеки для користувачів. Пропонується новий соціально-орієнтований протокол, який дозволяє уникнути псевдодецентралізації та монополізації мережі, підвищити доступність системи, забезпечити безпеку учасників. Запропонований протокол передбачає створення та додавання нових блоків до блокчейну.

Розроблений алгоритм представлено узагальненими кроками і на основі нього можна створювати протокол. Враховуються принципи побудови розподілених систем та вимоги до архітектури таких систем. У процесі розробки запропонованого протоколу були опрацьовані основні аспекти безпеки, пов'язані із захистом від різних типів шкідливого програмного забезпечення, включаючи бот-мережі та комп'ютерні віруси.

Для застосування PoA мережа розроблена на архітектурі, особливістю якої є те, що вузли взаємодіють на різних рівнях відповідно до їх типізації або параметризації, що буде використано для виконання розробленого алгоритму та пошуку консенсусу.

Проведено оцінку системи, базованої на розробленому новому соціально-орієнтованому протоколі.

Ключові слова: розподілена система, протокол, мережа, блокчейн, архітектура системи.

BELFER R., MEDZATYI D., OMELCHUK R.
Khmelnitsky National University

RESEARCH AND EXPERIMENTAL ESTABLISHMENT OF PROOF-OF-ACTIVITY CONSENSUS PROTOCOL EFFICIENCY

The paper analyzes the analysis of known protocols for implementation in blockchain systems. The main problems that arise in the actual use of such systems are highlighted. In particular, this is a problem of energy consumption and safety for users.

The article proposes a new socially-oriented protocol that avoids pseudo-decentralization and monopolization of the network, increase the availability of the system, ensure the safety of participants. The proposed protocol involves creating and adding new blocks to the blockchain.

The developed algorithm is represented by generalized steps and on the basis of it it is possible to create the protocol. The principles of construction of distributed systems and requirements for the architecture of such systems are taken into account. In the process of developing the proposed protocol, the main aspects of security related to protection against various types of malware, including botnets and computer viruses, were addressed.

For PoA application, the network is developed on an architecture, the feature of which is that the nodes interact at different levels according to their typing or parameterization, which will be used to perform the developed algorithm and find consensus.

An evaluation of the system based on the developed new socially-oriented protocol was carried out.

Keywords: distributed system, protocol, network, blockchain, system architecture.

Вступ. Постановка задачі. Мережний протокол для створення децентралізованих систем для користувачів може бути одним з етапів впровадження нових принципів податкової локальної політики, де податки будуть прив'язані до активностей окремих членів громадськості, а також, оновлення виборчого права, що базуватиметься на соціальній активності учасників мережі та стане якісно новим принципом проведення нових, експериментальних але якісних виборів.

Розроблено багато таких протоколів. Частина з них активно використовується в системах блокчейн. Наявні протоколи постійно потребують вдосконалення, особливо в частині безпеки та використання енергоресурсів.

Пов'язані роботи. Технологія розподіленої книги стала надзвичайно популярною в 2018 році через надзвичайно високий курс криптовалюти. Блокчейн є однією з найважливіших галузей інформатики поряд з AI, IoT та хмарними компіляціями, які активно використовуються і розвиваються в останні роки. Відомі і поширені методи організації мереж блокчейнів є консенсусні протоколи – Proof-of-Work (PoW) та Proof-of-Stake (PoS). Але вони мають недоліки, які впливають на безпеку, швидкість роботи, доступність, масштабування та ефективне використання енергії. PoW має енергоефективність [2, 3]. Розробники протоколу PoS створювали його як альтернативу протоколу PoW [4] з певними перевагами перед протоколом PoW. Ці переваги: електроенергія не потрібна для вирішення головоломки, вузли зацікавлені в безпеці мережі, оскільки вони володіють монетами в ній, і швидші транзакції. Але він має проблему псевдодецентралізації [5], як і протокол PoW. Для розробки нового соціально орієнтованого протоколу, який дозволяє уникнути псевдодецентралізації та монополізації мережі, є захист від шкідливого програмного забезпечення,

включаючи бот-мережі та різні типи комп'ютерних вірусів [6–10]. Ці проблеми спонукають дослідників шукати нові протоколи, в яких таких проблем не буде.

Метою дослідження є розробка нового протоколу, який дозволяє уникнути псевдодецентралізації та монополізації мережі, а також проведення оцінки результатів.

Основна частина. Компанії NEM [11] та Mithril [12] працюють над блокчейнами на основі соціально-орієнтованих платформ, а не звичайних принципів Proof-of-Work і Proof-of-Stake. Вони розробили першу криптовалюту на основі консенсусного протоколу Proof-of-Importance (PoI) [13]. На створення транзакції потрібно 5 секунд, а на її обробку – 20 с. Мережа готова обробляти 3000 транзакцій в секунду [14].

Децентралізована платформа соціальних медіа Mithril [15] винагороджує кожного, хто створює медіа-контент. Використовуючи технологію блокчейну, Mithril може забезпечувати безпеку транзакцій, щоб захистити всіх залучених. Крім того, технологія розподілених даних зберігає надійні та недоторкані транзакції. Соціальний майнінг [16] спочатку використовувався Mithril для запуску процесу базової системної функціональності.

Консенсус-протокол Proof-of-Brain [16] розробила компанія Steem, який базується на діяльності користувачів і винагороджує виробництво високоякісного вмісту на конкретних платформах. Майнінг базується на «колективному інтелекті», що робить алгоритм «розумним» [17].

Basic Attention Token [18] є соціально-орієнтованою технологією блокчейну. Браузерний браузер відстежує активність користувачів та їх взаємодію з опублікованою рекламою.

Проведений аналіз робіт [19–34] приводить до результату, що частина проблем пов'язаних з безпекою вирішена в певних протоколах, але це досягнуто за рахунок складності аутентифікації користувачів. Від такого результату частина користувачів не хочуть користуватись таким протоколом. При послабленні вимог безпеки відбувається втрата довіри зі сторони користувачів до такого ресурсу. Подальші використання таких протоколів не можуть бути основою для соціально-орієнтованих платформ. Тому, це питання потребує подальшого дослідження.

В роботі [35] пропонується варіант соціально-орієнтованого протоколу, який усуває частину важливих недоліків відомих протоколів. Консенсусний протокол Proof-of-Activity (PoA) дозволяє створювати нові блоки та додавати їх до блокчейну. Протокол PoA також вибирає вузли валідатора на основі значення активності вузла в мережі та будь-яких критеріїв, визначених конкретно системою блокчейнів. Для використання протоколу PoA мережа повинна бути спроектована відповідно до архітектури Layer Peer to Peer (LP2P). Алгоритм консенсусу PoA може бути впроваджений для будь-якої соціально орієнтованої структури: соціальних мереж, платформи краудфандингу, цивільних або муніципальних сайтів. Протокол PoA може бути використаний для створення муніципальних чи урядових платформ, які могли б об'єднати громадські ініціативи та допомогти реалізувати успішні.

Алгоритм роботи протоколу при створенні нового блоку

Передумовою початку роботи алгоритму є наявність у множині вхідних транзакцій готових до запису у блок. Аналогічно до стандарту Bitcoin, розмір блоку транзакцій дорівнює 1 mb інформації. Отже, на вхід алгоритму подається така кількість транзакцій, що $\sum_{i=1}^N \text{size}_i = \text{const}_{\text{size}}$, де size – розмір транзакції, N – кількість транзакцій готових до запису в блок, $\text{const}_{\text{size}}$ – сталий розмір блоку транзакцій = 1 mb.

Узагальнені кроки алгоритму знаходження консенсусу між вузлами та виділення єдиного вузла валідатора, що матиме право здійснити створення блоку, його підпис та додавання до блокчейну.

Крок 1. Для множини з N рівнів $[A, B, C \dots M]$, розміщених згідно мережевої архітектури LP2P, та множини вузлів кожного рівня, де вузол $a_i \in A$, де $i \leq k$, вузол $b_i \in B$, де $i \leq l$, вузол $c_i \in C$, де $i \leq k, \dots$, вузол $n_i \in N$, де $i \leq p$, для кожного з рівнів виконуються визначена функція відбору потенційного

валідатора f . Отже, для множини рівнів $[A, B, C \dots M]$ та множинам вузлів що належать кожному з рівнів, отримуємо множину функцій: $f_a(a_1, a_2, a_3 \dots a_k), f_b(b_1, b_2, b_3 \dots b_l), f_c(c_1, c_2, c_3 \dots c_m) \dots f_n(n_1, n_2, n_3 \dots n_p)$.

Результатом виконання функції f для кожного з рівнів з множини $[A, B, C \dots M]$ та множини вузлів, що належать кожному з рівнів, є потенційний валідатор. Відповідно отримано результуючу множину потенційних валідаторів $[a', b', c' \dots n']$.

Крок 2. Множина потенційних валідаторів $[a', b', c' \dots n']$ використовується як параметр для функції випадкового визначення результуючого вузла валідатора – $\text{random}([a', b', c' \dots n'])$. Результатом виконання функції є кінцевий вузол v – визначений випадковим чином серед вузлів множини $[a', b', c' \dots n']$.

Крок 3. Кінцевий вузол v використовується як параметр для додавання блоку транзакцій до блокчейну та підпису цього блоку хеш значенням, отриманого в результаті попереднього виконання хеш функції, $\text{block}(v, T, \text{hash})$, де v – вузол валідатор, T – множина валідних транзакцій готових до запису в блок, hash – хеш-ключ, яким буде підписано блок.

Кожний об'єкт розподіленої системи повинен мати певний набір атрибутів доступу, який включає унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього. Атрибут доступу використовується для опису інформації, яка використовується при керуванні доступом і зв'язана з користувачами, процесами або пасивними об'єктами. Відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною. Атрибути доступу об'єкта є частиною його подання в архітектурі системи. Коли користувачі або процеси намагаються одержати доступ до пасивних об'єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть «прийняти рішення» про легальність запиту. Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати довірче керування доступом, адміністративне, контроль за цілісністю та інші види керування доступом.

Для відображення функціональності розподіленої системи у простір, в якому не розглядаються права власності, використовується концепція матриці доступу. Матриця доступу є таблицею, уздовж кожного виміру якої відкладені ідентифікатори об'єктів, а в якості елементів матриці виступають дозволені або заборонені режими доступу. Матриця доступу може бути двовірною (наприклад, користувачі/пасивні об'єкти або процеси/пасивні об'єкти) або тримірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною, тобто містити вздовж кожної з осей ідентифікатори всіх існуючих на даний час об'єктів КС даного типу, або частковою. Повна тримірна матриця доступу дозволяє точно описати, хто (ідентифікатор користувача), через що (ідентифікатор процесу), до чого (ідентифікатор пасивного об'єкта), який вид доступу може одержати.

Програмні компоненти з погляду користувачів КС можна розділити на дві категорії: компоненти без внутрішнього стану, що зберігається між віддаленими викликами своїх методів (stateless components); компоненти із внутрішнім станом, що зберігається між віддаленими викликами своїх методів (statefull components). Під станом у цьому випадку розумітимемо сукупність значень полів об'єктів, що реалізують компоненти, що зберігаються в пам'яті адміністратора. Якщо компонента в ході своєї роботи зберігає які-небудь дані в зовнішньому сховищі, наприклад у базі даних або черги повідомлень, це звичайно не розглядається як її внутрішній стан. Модель єдиного виклику не зберігає стану віддаленого об'єкта між викликами його методів, у силу чого дана модель може використовуватися тільки з розподіленими компонентами без внутрішнього стану. Модель одного екземпляра може бути використана для виклику компонентів із внутрішнім станом. Модель активації по запиту компонента може бути використана з будь-якими компонентами, але для компонент без внутрішнього стану такий підхід звичайно призводить до непродуктивного використання пам'яті при деякому виграші у витратах часу процесора в порівнянні з моделлю одного виклику. Компоненти без збереження внутрішнього стану, що використовуються разом з моделлю єдиного виклику з пулом об'єктів, мають найбільші можливості масштабування системи при оптимальному балансі між витратами пам'яті й навантаженням на процесор.

Таким чином, розроблений протокол, алгоритм та вимоги до архітектури системи на основі нового соціально-орієнтованого протоколу дозволяють вирішити ряд проблеми безпеки.

Експерименти та оцінка. Протокол консенсусу Proof-of-Activity та алгоритм додавання нових блоків до блокчейну базується на 3-рівневому наборі тексту [35].

На рис. 1 показано розрахункове споживання електроенергії, що використовується різними консенсусними протоколами. Протоколи консенсусу PoA та PoB мають нульове розрахункове споживання електроенергії. У той же час протокол PoW вимагає найбільшої кількості електроенергії. Протоколи PoS та PoI можуть вимагати певного споживання електроенергії на початкових етапах, якщо для початкового видобутку використовується алгоритм PoW.

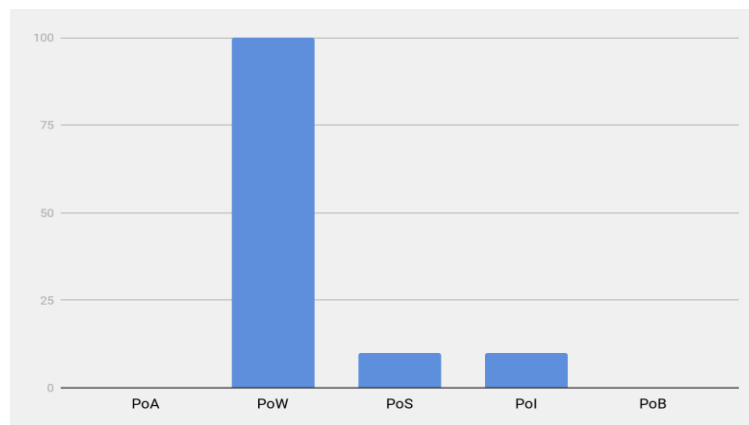


Рис. 1. Розрахункове споживання електроенергії, яке вимагається різними консенсусними протоколами

У таблиці 1 порівнюється протокол консенсусу Proof-of-Activity з деякими найпопулярнішими та найрелевантнішими протоколами. Для порівняння були розглянуті такі критерії, як споживання електроенергії, децентралізація, моніторинг діяльності, соціальна орієнтація, масштабованість, труднощі в приєднанні до мережі тощо.

Таблиця 1

Порівняння протоколів консенсусу

Критерій	PoA	PoW	PoS	PoI	PoB
Споживання електроенергії	–	+	+/-	+/-	–
Питання псевдодецентралізації	–	+/-	+	–	–
Монополізація ресурсів	–	+	+	+/-	–
Легко приєднатися	+	+/-	–	+/-	+
Моніторинг діяльності	+	–	–	+/-	+
Соціальна спрямованість	+	–	–	–	+
Масштабованість	+	+	+	+	+
Широке застосування	+	+	+	+	–
Потрібне початкове володіння монетами	–	–	+	+	–

Протокол PoB найбільш подібний до протоколу Proof-of-Activity: він соціально орієнтований, уникає псевдодецентралізації, не вимагає первинного володіння монетами та не вимагає багато електроенергії. Основна відмінність між протоколами PoA та PoB полягає в тому, що PoB може використовуватися лише для медіа-мереж – він вимагає оцінки та голосування вмісту. З іншої сторони, протокол PoA може використовуватися для немедіа-мереж, таких як платформи для краудфіндингу, муніципальні сайти та ресурси для управління проектами.

Висновки. Розроблено новий соціально орієнтований протокол, основними задачами якого є уникнення псевдо-децентралізації та монополізації мережі, збільшення доступності участі у підтримці роботи системи для всіх активних вузлів мережі. Він покращує безпеку. Також, розроблено вимоги до розподіленої системи та алгоритм за яким функціонуватиме система.

Напрямок подальших досліджень є розробка складових архітектури мережної системи та методів взаємодії компонентів системи.

Література

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-b2afbc874d9>.
6. 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).
7. 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).
8. 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).
9. 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)
10. Kehret, O., Walz, A., Sikora, A.: Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. International Journal of Computing, Vol. 15, Issue 1, pp. 24-32 (2016).
11. NEM, New Economy Movement. Available: <https://nem.io/>.
12. Mithril, The Future of Social Networks. Available: <https://mithril.io/>.
13. "What is PoI?" Available: <https://docs.nem.io/ja/gen-info/what-is-poi>.
14. Introduction to NEM (XEM): The Proof-of-Importance Coin. Available: <https://cryptoslate.com/nem/>.
15. Proof of Importance Explained. Available: <https://www.mycryptopedia.com/proof-of-importance/>.
16. Beginner's Guide to Mithril: Social Platform Which Rewards Content Creators. Available: <https://blockonomi.com/mithril-guide/>.
17. Huang, J.: The Future of Social Networks. Mithril (MITH) Whitepaper, pp. 1-30.
18. Blockchain White Paper, China Academy of Information and Communication Technology, Trusted Blockchain Initiatives, pp. 1-49 (2018).
19. Blockchain Technology Beyond Bitcoin. Available: <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>.
20. Blockchain disruption and smart contracts. Available: <https://www.nber.org/papers/w24399.pdf>.
21. Blockchain in Trade Facilitation. Available: <http://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaper/Blockchain.pdf>.
22. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873, pp. 1-24 (2017)
23. Wahab, A., Memood, W.: Survey of Consensus Protocols. arXiv:1810.03357, pp. 1-12 (2018).
24. 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).
25. Daian, P., Pass, R., Shi, E.: Snow White: Provably Secure Proofs of Stake, Cryptology ePrint Archive, Report 2016/919, pp. 1-62 (2016).
26. Buterin, V.: Slasher: A punitive proof-of-stake algorithm. Available: <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>.

27. Chen, J., Micali, S.: Algorand: the efficient and democratic ledger, arXiv: 1607.01341 (2016).
28. Proof of Stake FAQ. Available: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>
29. Analysis of the main consensus protocols of blockchain. Available: <https://www.sciencedirect.com/science/article/pii/S240595951930164X>
30. Mazieres, D.: Stellar Consensus Protocol. Available: <https://www.stellar.org/papers/stellar-consensus-protocol>
31. Basic Attention Token (BAT) Blockchain Based Digital Advertising, Available: <https://basicattentiontoken.org/wp-content/uploads/2017/05/BasicAttentionTokenWhitePaper-4.pdf>
32. 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>
33. Proof of Brain Bluepaper. Available: <https://steem.com/steem-bluepaper.pdf>
34. Basic Attention Token. "Introducing blockchain based digital advertising". Available: <https://basicattentiontoken.org/>.
35. Belfer R. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes / R. Belfer, A. Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky – CEUR-WS. – 2020. Vol. 2623. – Pp.239-251.

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-b2afbc874d9>.
6. 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).
7. 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).
8. Savenko, O., Lysenko, S., Kryshchuk, A.: Multi-agent based approach of botnet detection in computer systems. Communications in Computer and Information Science, Vol. 291, pp.171-180 (2012).
9. 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)
10. Kehret, O., Walz, A., Sikora, A.: Integration of Hardware Security Modules into a Deeply Embedded TLS Stack. International Journal of Computing, Vol. 15, Issue 1, pp. 24-32 (2016).
11. NEM, New Economy Movement. Available: <https://nem.io/>.
12. Mithril, The Future of Social Networks. Available: <https://mithril.io/>.
13. "What is PoI?" Available: <https://docs.nem.io/ja/gen-info/what-is-poi>.
14. Introduction to NEM (XEM): The Proof-of-Importance Coin. Available: <https://cryptoslate.com/nem/>.
15. Proof of Importance Explained. Available: <https://www.mycryptopedia.com/proof-of-importance/>.
16. Beginner's Guide to Mithril: Social Platform Which Rewards Content Creators. Available: <https://blockonomi.com/mithril-guide/>.
17. Huang, J.: The Future of Social Networks. Mithril (MITH) Whitepaper, pp. 1-30.
18. Blockchain White Paper, China Academy of Information and Communication Technology, Trusted Blockchain Initiatives, pp. 1-49 (2018).
19. Blockchain Technology Beyond Bitcoin. Available: <https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>.
20. Blockchain disruption and smart contracts. Available: <https://www.nber.org/papers/w24399.pdf>.
21. Blockchain in Trade Facilitation. Available: <http://www.unec.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaper/Blockchain.pdf>.
22. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873, pp. 1-24 (2017)
23. Wahab, A., Memood, W.: Survey of Consensus Protocols. arXiv:1810.03357, pp. 1-12 (2018).
24. 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).
25. Daian, P., Pass, R., Shi, E.: Snow White: Provably Secure Proofs of Stake, Cryptology ePrint Archive, Report 2016/919, pp. 1-62 (2016).
26. Buterin, V.: Slasher: A punitive proof-of-stake algorithm. Available: <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>.
27. Chen, J., Micali, S.: Algorand: the efficient and democratic ledger, arXiv: 1607.01341 (2016).
28. Proof of Stake FAQ. Available: <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ>
29. Analysis of the main consensus protocols of blockchain. Available: <https://www.sciencedirect.com/science/article/pii/S240595951930164X>
30. Mazieres, D.: Stellar Consensus Protocol. Available: <https://www.stellar.org/papers/stellar-consensus-protocol>
31. Basic Attention Token (BAT) Blockchain Based Digital Advertising, Available: <https://basicattentiontoken.org/wp-content/uploads/2017/05/BasicAttentionTokenWhitePaper-4.pdf>
32. 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>
33. Proof of Brain Bluepaper. Available: <https://steem.com/steem-bluepaper.pdf>
34. Basic Attention Token. "Introducing blockchain based digital advertising". Available: <https://basicattentiontoken.org/>.
35. Belfer R. Proof-of-Activity Consensus Protocol Based on a Network's Active Nodes / R. Belfer, A. Kashtalian, A. Nicheporuk, A. Sachenko, G. Markovsky – CEUR-WS. – 2020. Vol. 2623. – Pp.239-251.

Надійшла / Paper received: 15.09.2020

Надрукована / Paper Printed : 01.12.2020