ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ПІД ЧАС ПЕРЕДАЧІ ЦИФРОВИХ ГРОШЕЙ ЗА ТЕХНОЛОГІЯМИ БЛОКЧЕЙН

FEATURES OF APPLICATION THE CRYPTOGRAPHIC ALGORITHMS IN TRANSMISSION OF DIGITAL MONEY FOR BLOCKCHAIN TECHNOLOGIES

УДК 336.74+519.684.6
https://doi.org/10.32843/bses.49-33

Койбічук В.В.
к.е.н., старший викладач кафедри економічної кібернетики
Сумський державний університет

Koibichuk Vitaliia
Sumy State University

Останніми роками спостерігається значний структурний вплив цифрової економіки на формування бізнес-процесів соціально-економічних об'єктів. Стрімкі зміни фінансового ринку тягнуть за собою впровадження інноваційних технологій блокчейна, що вимагає ретельного дослідження систем захисту, узгодженості апаратного та програмного забезпечення під час проведення грошових операцій з використанням криптовалют. Світовим трендом є вкладення в криптовалюту, яка є нечутливою до непередбачуваних змін соціально-економічного середовища будь-якої країни. У статті розглянуто особливості застосування криптографічних протоколів під час проведення транзакцій за технологіями блокчейна. Наведено переваги та недоліки найбільш популярних та використовуваних на будь-якій блокчейн-платформі алгоритмів досягнення консенсусу за методикою доказу роботи, доказу володіння, визначення делегатів для проведення сеансу у біткоїн-платіжних системах.
Ключові слова: *біткоїн, цифрові гроші, хеш-функція, технологія блокчейн, криптографічний протокол.*

В последние годы наблюдается значительное структурное влияние цифровой экономики на формирование бизнес-процессов социально-экономических объектов. Стремительные изменения рынка влекут за собой внедрение инновационных технологий блокчейна, что требует тщательного исследования систем защиты, согласованности аппаратного и программного обеспечения при проведении денежных операций с использованием криптовалют. Мировым трендом является вложение в криптовалюту, которая является нечувствительной к непредсказуемым изменениям социально-экономической среды любой страны. В статье рассмотрены особенности применения криптографических протоколов при проведении транзакций по технологиям блокчейна. Приведены преимущества и недостатки наиболее популярных и используемых на любой блокчейн-платформе алгоритмов достижения консенсуса по методике доказательства работы, доказательства владения, определение делегатов для проведения сеанса в биткоин-платежных системах.
Ключевые слова: *биткоин, цифровые деньги, хэш-функция, технология блокчейн, криптографический протокол.*

The current technological level of the Ukrainian economy cannot count on a large-scale launch of its products on the world markets, unless using the digitalization of business processes, introducing new innovative digital technologies to enterprises of any sphere of activity. In recent years, there has been a significant structural impact of the digital economy on the shaping of business processes of socio-economic entities. The rapid changes of the financial market entail the introduction of innovative blockchain technologies, which requires a careful study of security systems, consistency of hardware and software in conducting money transactions using crypto currencies. The global trend is to invest in cryptocurrency, which is not sensitive to unpredictable changes in the socio-economic environment of any country. One of the fundamental calculations and analytical methodologies in conducting transactions with securities, digital money is economic and mathematical analysis, which in modern conditions should not only give an objective assessment in the part of securities transactions but also identify and mobilize reserves to increase them, the efficiency of the use of economic potential, to develop and make optimal management decisions. The article deals with the peculiarities of application of cryptographic protocols in conducting transactions using blockchain technologies. The advantages and disadvantages are the most popular and used on any blockchain platform consensus algorithms by the method of proof of work, proof of ownership, determination of delegates for the session in bitcoin payment systems. The purpose of the article is to perform a comparative analysis of basic cryptographic protocols when using cryptocurrencies in blockchain technologies. In the development and implementation of protection systems, it is recommended to clearly state all the necessary assumptions and hypotheses, justify the results. The information security system interacts with the indicators of the internal and external environment, so this environment must meet certain conditions: explicitly and accurately indicate all the foreseen information security services (confidentiality, knowledge, authentication, inability to refuse, fixation) and explicitly distinguish individual cases of mathematical problems.
Key words: *bitcoin, digital money, hash function, blockchain technology, cryptographic protocol.*

Постановка проблеми. Нинішній технологічний рівень економіки України не може розраховувати на масштабний вихід своєї продукції на світові ринки, якщо не використовувати цифровізацію бізнес-процесів, впроваджувати нові інноваційні цифрові технології в підприємства будь-якої сфери діяльності, банки, фінансово-кредитні установи та державні органи.

Надзвичайно важливими та актуальними питаннями сьогодення є дослідження, особливості та можливості використання цифрових технологій блокчейна в стратегічно значущих сферах економіки, особливо у фінансово-банківській діяльності. Вкладення в криптовалюту за умов сучасного сьогодення стало вже світовим трендом. Її перевага полягає в тому, що курс децентралізованої цифрової валюти біткоїн не контролюється жодним урядом світу, її неможливо конфіскувати чи «заморозити».

Незважаючи на стрімке освоєння технологій блокчейна, залишаються нерозкритими питання вдосконалення наявних алгоритмів обміну даними в цифровій мережі, питання організаційно-економічного характеру, що пов'язані з активізацією інноваційних можливостей як для фізичних осіб, так і для юридичних. Найбільша сфера питань пов'язана з розробленням нових криптопротоколів, що є базою реалізації технологій блокчейна, математичних моделей опису процедур обміну цифровими грошима. Зазначена проблематика потребує

вдосконалення наявного теоретичного обґрунтування, розроблення методичного забезпечення та рекомендацій для практичного застосування.

Аналіз останніх досліджень і публікацій. Дослідженням принципів роботи біткоїн-мереж з технічної точки зору, розвитку технологій блокчейна, можливостей їх сфер застосування для конкретних компаній присвячена велика кількість форумів, онлайн-публікацій на вітчизняних [1; 2] та зарубіжних сайтах [3–5], де спікерами та авторами є експерти, провідні фахівці сфери комп'ютеризації та інформатизації бізнес-процесів. Зокрема, більшість публікацій засновника декількох блокчейн-компаній А. Антонопулоса [6] присвячена опису технологій створення смарт-контрактів, децентралізованих додатків "Dapp".

Постановка завдання. Метою статті є детальний аналіз процедур обміну даними у відкритій розподіленій мережі за блокчейн-технологією. Перевірка правильності передачі та способів збереження даних здійснюється на основі криптографічних протоколів, тому слід провести порівняльний аналіз базових криптографічних протоколів, а саме протоколів, що використовуються під час здійснення транзакцій у криптовалюті.

Виклад основного матеріалу дослідження. Говорячи про технологію блокчейна (blockchain), можемо порівняти її з відкритою, децентралізованою, публічно розподіленою цифровою книгою, де транзакції між людьми записуються на багатьох комп'ютерах, отже, запис не можна змінювати заднім числом без зміни всіх наступних блоків та консенсусу мережі. Відомо, що в основі технології блокчейна лежить криптографія, яка дає змогу передавати цифрові монети від людини-відправника до людини-отримувача через мережу. Передача здійснюється блоками, кожному присвоюється цифровий підпис у вигляді хеш-суми, що слугує унікальним ідентифікатором [7]. Передача блоків здійснюється за вказаним порядком, заданим хеш-функцією. За спроби зміни порядку передачі блоків система видає помилку невідповідності між структурою та ідентифікатором. Хеш-функція загалом є алгоритмом відображення даних довільної (змінної) довжини до фіксованих.

Розглянемо одну з типових задач, що виникає під час передачі цифрової валюти між учасниками сеансу. Дані передаються великими масивами записів у вигляді блоків (blocks) від одного вузла-передача до іншого. Виникає питання про те, яким чином можна зберегти та швидко знайти поточне розташування (стан) запису певного блоку. Відповідь надає хеш-функція загального вигляду:

$$h(k) = k \bmod n, \qquad (1)$$

де n – кількість доступних місць зберігання; k – число; mod – залишок від ділення числа. Передача даних та фрагмент коду, що перевіряється хеш-функцією, зображені на рис. 1.

Під час використання хеш-функцій поширеною є проблема виникнення колізій, коли два різних записи мають однакову інтерпретацію перевірки збереження (рис. 2).

Проблема може бути вирішена за рахунок використання послідовностей хеш-функцій, які перевіряють наступне доступне місце в пам'яті комп'ютера:

$$\begin{aligned} h_0(k) &= k \bmod n, \\ h_1(k) &= (k+1) \bmod n, \\ &\ldots \\ h_m(k) &= (k+m) \bmod n, \end{aligned} \qquad (2)$$

Модифікацій алгоритмів перевірки правильності запису та наступного розташування переданого блоку інформації існує величезна кількість. Проте для того, щоби хеш-функція вважалася криптографічно стійкою, необхідним і достатнім є виконання таких трьох умов [8], як незворотність (стійкість) до відновлення прообразу, стійкість до

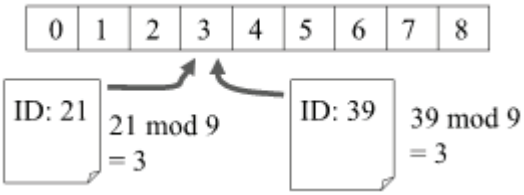

Рис. 2. Результат різних сеансів обміну цифровими грошима має одну й ту ж саму адресу збереження

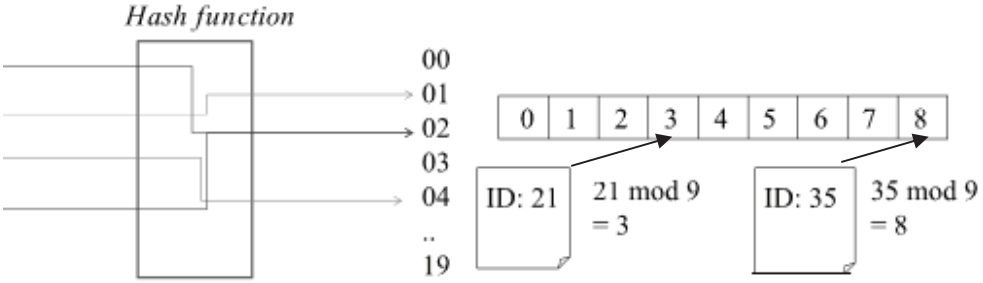

Рис. 1. Передача даних та пошук запису в блоці інформації на основі перевірки правильності залишку від ділення цілого числа

колізій першого роду, відновлення других прообразів. Цю умову слід інтерпретувати так: для заданого повідомлення *M* має бути обчислювально неможливо підібрати інше повідомлення *N*, для якого *H (N) = H (M)*. Колізією хеш-функції *H* називається наявність двох різних вхідних блоку даних *x* та *y* таких, що *H* (x) = *H* (y). Третя умова криптостійкості хеш-функцій говорить про стійкість до колізій другого роду, тобто має бути обчислювально неможливо підібрати пару повідомлень (*M*, *M*'), що мають однаковий хеш. Ці вимоги не є незалежними.

Захист від підробки цифрових підписів здійснюється використанням різних криптографічних протоколів. Найбільш поширеним є використання протоколів Proof of Work (доказ роботи, PoW) [9] та Proof of Stake (доказ володіння, PoS) [10].

Розглянемо особливості основних алгоритмів консенсусу, що дають змогу вибрати вузол, який буде найкращим для підпису наступного блоку.

Використання алгоритму консенсусу PoW полягає в проведенні вузлами blockchain мережі обчислювальної роботи для підтвердження операцій-транзакцій, а результат перевіряється всіма вузлами. Винагороду отримує перший вузол, що провів всі обчислення на основі хеш-функції. Алгоритм має великий недолік, пов'язаний з нераціональним використанням енергоресурсів, оскільки обчислення проводять всі вузли, а винагороду отримує лише перший.

Методика консенсусу PoS полягає в тому, що в ролі ресурсу виступають частки (stake), що володіють більшими ресурсами (криптомонетами, токенами). Найбільш «багаті» або «найстаріші» вузли випадковим чином вибираються для визначення вузла, який отримає в даний момент привілей на проведення транзакції та отримання винагороди. У цьому підході вузли хешують дані, щоби знайти результат, який був би менше заданого значення. Трудомісткість розподіляється пропорційно й відповідає кількості токенів конкретного вузла. Слід підкреслити таку відмінність між токенами та коїнами: токени можна використовувати у вигляді як винагороди в тому чи іншому криптовалютному проєкті, так і розрахункової одиниці. Крім того, токени використовуються задля проведення аутентифікації, яку можна розділи на такі три види, як аутентифікація джерела даних (аутентифікація повідомлення), аутентифікація сутності й генерація аутентіфіційованих ключів.

Перший вид аутентифікації означає перевірку оголошеної властивості повідомлення та обов'язково пов'язаний з каналами зв'язку. Вона є службою безпеки одержувача, призначеною для верифікації джерел повідомлень. Аутентифікація сутності – це процес обміну інформацією, під час якого користувач встановлює справжність іншого користувача. Третій вид аутентифікації призначений для організації захищеного каналу обміну секретними ключами.

Перевага алгоритму консенсусу «доказ володіння» порівняно з методикою PoS полягає у суттєвій економії енергозатрат та обчислювальних ресурсів.

Модифікацією протоколу PoS є більш ефективний алгоритм консенсусу Delegated Proof-of-Stake (DPoS) [11]. Особливість його полягає в тому, що блоки підписують представники (делегати), яких обирають власники найбільших балансів на основі голосування. Вплив голосу пропорційний кількості біткоїнів, якими володіє кожен учасник сеансу. Під час проведення нового криптовалютного проєкту проводиться нове голосування власників ресурсів. Винагорода, що отримана делегатами в результаті проведення транзакцій, здебільшого розподіляється пропорційно між учасниками, які обрали цього делегата. Отже, формується репутація делегата, а якщо вузол працює неправильно чи неефективно, то цього делегата видаляють з мережі. Знову бачимо, що є як переваги, так і недоліки порівняно з розглянутими алгоритмами PoW та PoS. Перевагою є можливість делегувати свої голоси та утримувати баланс.

Найбільшим недоліком є висока ймовірність виникнення та настання ризикових ситуацій. При цьому навіть із застосуванням математичних методів прогнозування настання ризикових випадків модель не завжди надає реальний прогноз, оскільки не враховується непередбачуваний вплив складних факторів політико-економічного становища.

Узагальнюючи порівняльну характеристику роботи криптопротоколів, можемо навести схему, що є первинною базою для всіх сеансів передачі та накопичення цифрових грошей за технологіями блокчейна (рис. 3).

Учасниками безпечного зв'язку є клієнт, сервер і центр розподілу ключів (Key Distribution Center, KDC), який виступає в ролі довіреного посередника.

На рис. 3 *A*, *B* – це принципали (люди, які здійснюють обмін цифровими грошима), *S* – довірений посередник (сервер аутентифікації), *T* – мітка часу, *L* – термін придатності мандата, K_{ab} – загальний ключ для *A* і *B*. Як бачимо з повідомлення 2, сервер генерує сеансовий ключ, загальний для *A* і *B*, таємно доставляє його (захований всередині двох мандатів), шифруючи довготривалими секретними ключами, який він розділяє з *A* і *B*.

Повідомлення 1: $A \to S : A, B$

Повідомлення 2: $S \to A : \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$

Повідомлення 3: $A \to B : \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$

Повідомлення 4: $B \to A : \{T_a + 1\}_{K_{ab}}$

Рис. 3. Обмін повідомленнями між учасниками сеансу із забезпеченням захисту

Отримавши протокольні повідомлення від сервера, користувачі можуть виявити, що їх послання залишилися без відповіді, перевіривши таку нерівність:

$$|Час - T| < \Delta t_1 + \Delta t_2. \quad (3)$$

Час означає локальний час одержувача, Δt_1 – інтервал, який представляє допустиму різницю між часом сервера й локальним часом, Δt_2 – часова затримка, що очікується.

Висновки з проведеного дослідження. В рамках дослідження підтверджено, що кожен алгоритм консенсусу має високу чутливість до виникнення та настання ризикових ситуацій, що пов'язані з внутрішньою відмовою інформаційних систем, відмовою учасників біткоїн-платіжної мережі від вибраної схеми проведення транзакцій, розбіжністю між запитами користувачів і фактичними можливостями та технічними характеристиками блокчейн-платформ.

Під час розроблення та реалізації систем захисту рекомендовано чітко формулювати все необхідні припущення та гіпотези, обґрунтовувати результати. Система захисту інформації взаємодіє з показниками внутрішнього та зовнішнього оточення, тому це оточення має відповідати таким умовам: явно та точно зазначати всі передбачувані послуги щодо захисту інформації (забезпечення конфіденційності, доведення знань, аутентифікація, неможливість відмови, фіксація); явно виділяти окремі випадки математичних задач.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Спікери 9-го блокчейн-форуму 2019. URL: http://kyiv.blockchainforum.com (дата звернення: 19.12.2019).

2. Blockchain Association of Ukraine. URL: https://bau.ai/ru (дата звернення: 10.01.2020).

3. The truth machine: the blockchain and the future of everything / Global Blockchain Business Council. URL: https://gbbcouncil.org (дата звернення: 10.01.2020).

4. Bashir I. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. 2nd Edition. Birmingham : Packt Publishing Ltd., 2018.

5. Bambara J.J., Allen P.R. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions, 1st Edition. New York : Mc-Grow Hill Education, 2018.

6. Antonopoulos A. Mastering Bitcoin. URL: https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf (дата звернення: 21.01.2020).

7. Бойко А.О., Горбенко І.Д. Обґрунтування архітектури функції хешування з використанням паралельних обчислень. URL: http://mia.univer.kharkov.ua/13/30046.pdf (дата звернення: 21.01.2020).

8. Cynthia D., Moni N. Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology. *CRYPTO'92: Lecture Notes in Computer Science*. 1993. No. 740. Springer. P. 139–147. DOI: 10.1007/3-540-48071-4_10.

9. Markus J., Ari J. Proofs of Work and Bread Pudding Protocols. *Secure Information Networks: Communications and Multimedia Security*. 1999. Kluwer Academic Publishers. P. 258–272. DOI: 10.1007/978-0-387-35568-9_18

10. Vasin P. BlackCoin's Proof-of-Stake Protocol v2. URL: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (дата звернення: 23.01.2020).

11. Consensus Algorithm. Opporty DPoS pBFT Solution for Distributed Ledger Security. URL: https://clever-solution.com/case-studies/consensus-algorithm-opporty-dpos-pbft-solution-for-distributed-ledger-security (дата звернення: 23.01.2020).

REFERENCES:

1. Spikery 9-gho blokchejn forumu 2019 [*The speakers of the 9th Blockchain Forum 2019*]. Available at: http://kyiv.blockchainforum.com (accessed 19 December 2019).

2. Blockchain Association of Ukraine. Available at: https://bau.ai/ru (accessed 10 January 2020).

3. The truth machine: the blockchain and the future of everything / Global Blockchain Business Council. Available at: https://gbbcouncil.org (accessed 10 January 2020).

4. Imran Bashir (2018) Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Second Edition. Birmingham: Packt Publishing Ltd.

5. Joseph J. Bambara, Paul R. Allen (2018) Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions, 1st Edition. New York: Mc-Grow Hill Education.

6. Andreas M. Antonopoulos Mastering Bitcoin. Available at: https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf (accessed 21 January 2020).

7. Bojko A.O., Ghorbenko I.D. Obgruntuvannja arkhitektury funkciji kheshuvannja z vykorystannjam paraleljnykh obchyslenj [Substantiation of the architecture of the hash function using parallel computing]. Available at: http://mia.univer.kharkov.ua/13/30046.pdf (accessed 21 January 2020).

8. Dwork Cynthia, Naor Moni (1993). Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology. *CRYPTO'92: Lecture Notes in Computer Science*. No. 740. Springer: 139–147. DOI: 10.1007/3-540-48071-4_10.

9. Jakobsson, Markus, Juels, Ari (1999). Proofs of Work and Bread Pudding Protocols. *Secure Information Networks: Communications and Multimedia Security*. Kluwer Academic Publishers: 258–272. DOI: 10.1007/978-0-387-35568-9_18

10. Vasin P. BlackCoin's Proof-of-Stake Protocol v2. Available at: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed 23 January 2020).

11. Consensus Algorithm. Opporty DPoS pBFT Solution for Distributed Ledger Security. Available at: https://clever-solution.com/case-studies/consensus-algorithm-opporty-dpos-pbft-solution-for-distributed-ledger-security (accessed 23 January 2020).