УДК 336.741.243 DOI: https://doi.org/10.31617/zt.knute.2019(104)08

ПАШОРІН Валерій
E-mail: vpashorin@knute.edu.ua
ORCID: 0000- 0001-6165-1147
к. т. н., професор кафедри програмної інженерії та кібер безпеки Київського національного торговельно-економічного університету
вул. Кіото, 19, м. Київ, 02156, Україна

ТЕХНОЛОГІЇ БЕЗПЕКИ КРИПТОВАЛЮТИ ТА БЛОКЧЕЙН-МЕРЕЖІ

Досліджено питання реалізації механізмів забезпечення безпеки генерації, зберігання та передання криптовалюти. Показані основні напрями вирішення проблеми захисту цифрової валюти від можливих шахрайських дій під час транзакцій і зберіганні її в електронних гаманцях. Розкрито сутність механізмів забезпечення безпеки криптовалюти біткойн та технології блокчейн.

Ключові слова: цифрова валюта, криптосистема, блокчейн, біткойн, хеш-функція, електронний гаманець.

Пашорин В. Технологии безопасности криптовалюты и блокчейн-сети. *Исследован вопрос реализации механизмов обеспечения безопасности генерации, хранения и передачи криптовалюты. Показаны основные направления решения проблемы защиты цифровой валюты от возможных мошеннических действий при транзакциях и хранении ее в электронных кошельках. Раскрыта сущность механизмов обеспечения безопасности криптовалюты биткойн и технологии блокчейн.*

Ключевые слова: цифровая валюта, криптосистема, блокчейн, биткойн, хэш-функция, электронный кошелек.

Постановка проблеми. Останні десятиліття спостерігається вражаюча динаміка впровадження інформаційних технологій у банківській сфері. Складно переоцінити перехід на електронні платіжні системи, використання електронного цифрового підпису в документообігу банків, застосування електронних грошей або цифровий валюти. Однак вкрай важливо концентруватися не тільки на позитивних моментах нових технологій, але і на питаннях безпеки їх застосування, особливо коли йдеться про гроші. Досить актуальним є вивчення питання безпеки криптовалюти. Загрози безпеці в мережі для криптовалюти такі ж, як і для будь-яких інших цифрових активів, оскільки криптовалюту фахівці розглядають як специфічний вид цифрової валюти.

Аналіз останніх досліджень і публікацій. З моменту своєї появи в 2009 р. криптовалюта зацікавила безліч дослідників з різних наукових сфер. Спроби зрозуміти, що таке цифрова валюта на блокчейні і як вона працює робилися в провідних світових університетах і дослідницьких центрах. Так, у 2017 р. кілька наукових праць, присвячених криптовалюті, опубліковано в Кембриджському університеті [1]. Сотні експертів з усього світу намагаються передбачити, як буде зміню-

ватися курс цифрових грошей, не особливо заглиблюючись у фундаментальний аналіз причин їх успіху. Існують й інші дослідження – їх автори не претендували на глибокий розгляд феномена криптовалюти, а концентрувалися на окремих питаннях [2–4], одним з яких є питання безпеки криптовалюти.

Метою статті є дослідження застосовуваних технологій безпеки використання цифровий валюти на прикладі криптовалюти біткойн та безпекових механізмів децентралізованої розподіленої мережі блокчейн, на якій базується криптовалюта біткойн.

Матеріали та методи. Інформаційною базою дослідження стали праці закордонних вчених, звіти фінансових установ [5], електронні ресурси, що порушують проблеми використання цифрової валюти. Для досягнення поставленої мети використано наукові методи теоретичного узагальнення, аналізу, синтезу та аналогій.

Результати дослідження. *Цифрова валюта* – це електронний аналог звичайної валюти, яка існує у віртуальному форматі, без фізичного еквівалента в реальному світі, але має всі характеристики валюти. Як і класичні гроші, цифрову валюту можна отримувати, переводити або обмінювати на іншу валюту, оплачувати нею товари та послуги. Цифрова валюта не має державних кордонів: гроші з електронного гаманця, що відповідає цій валюті, можуть бути переведені звідкіля завгодно і куди завгодно.

Криптовалюта є різновидом цифрової валюти. Це актив, який використовується як засіб обміну і вважається надійним, тому що в його основу покладено криптографію, технологію блокчейн і розподілений реєстр. Проте між криптовалютою та цифровою валютою можна виділити фундаментальні розбіжності.

Цифрова валюта централізована. Платіжна система цифрової валюти передбачає наявність центрального органу, який контролює мережеві транзакції. Цей орган може скасувати або заморозити транзакцію на вимогу, чи в разі підозри шахрайства або незаконної операції.

Платіжна система криптовалюти має пірингову архітектуру (*P*2*P*), тобто вся система, що забезпечує здійснення транзакцій і збереження інформації про них, заснована на децентралізованій комп'ютерній мережі. Не існує центрального сервера, який вів би облік усіх транзакцій криптовалюти. Вся інформація про транзакції зберігається на тисячах серверів, причому на кожному з них зберігається повна копія реєстру, що включає всі транзакції криптовалюти, здійснені будь-коли і будь-де. Таким чином, безліч комп'ютерів по всьому світу утворюють гігантську автоматичну, працюючу цілодобово електронну платіжну систему.

Децентралізація підвищує рівень безпеки криптовалюти, оскільки якщо й можна допустити можливість зловмисного втручання в роботу якогось одного центрального органу управління, то будь-які спроби внесення змін на окремі вузли розподіленої системи просто безглузді: доведеться зламати тисячі комп'ютерів одночасно, а не один центральний сервер. Додавання або видалення транзакцій у розподіленій системі

повинні бути прийняті всіма вузлами розподіленої мережі, в іншому випадку вони відкидаються. Таким чином, децентралізація і застосування розподіленого реєстру в обліку криптовалюти є важливим аспектом безпеки самої криптовалюти.

Цифрова валюта не підтримує анонімність. Для користування цифровою валютою потрібна ідентифікація користувача в платіжній системі та реєстрація певних документів, виданих банками або державними структурами. При цьому встановлюється особа, що здійснює операцію з валютою.

Для покупки, продажу, інвестування і будь-яких інших маніпуляцій з криптовалютою ніякої реєстрації особистості не потрібно, не потрібно також вказувати будь-якого роду особисті дані відправника та отримувача коштів. Для здійснення транзакції необхідно знати тільки публічний ідентифікатор одержувача (номер гаманця для криптовалюти), який може змінюватися для кожної транзакції.

Для запобігання шахрайству при транзакціях використовується електронний цифровий підпис (ЕЦП) власника криптовалюти. Підписуючи передання прав з використанням ЕЦП, власник бере на себе зобов'язання передання. Алгоритми ЕЦП, що застосовуються при переданні криптовалюти, не відрізняються від алгоритмів ЕЦП, застосовуваних у банківській та інших економічних сферах. Різниця в застосуванні тут полягає в тому, що при перевірці ЕЦП транзакцій в банківській сфері встановлюється, крім іншого, й особистість власника ЕЦП. При перевірці ЕЦП транзакцій криптовалюти визначається тільки номер електронного гаманця власника криптовалюти, сам же власник залишається невідомим. З точки зору захисту персональних даних, анонімність також може розглядатися як елемент технології безпеки.

Цифрова валюта непрозора. Інформація про транзакції цифрової валюти конфіденційна і відповідно недоступна для публічного перегляду.

Транзакції криптовалюти навпаки прозорі. Можна побачити список транзакцій будь-якого власника криптовалюти, знаючи його публічний (відкритий) ключ ЕЦП, оскільки всі його дії з криптовалютою фіксуються в блокчейні.

Більш того, для криптовалюти виключено шахрайство, пов'язане з транзакцією неіснуючих активів, оскільки за будь-якої транзакції передаються і відповідно перевіряються платіжною системою криптовалюти всі надходження і витрати з електронного гаманця, з якого здійснюється транзакція. Власник електронного гаманця не може передати з нього суму більшу, ніж він отримав на нього з підтверджених системою транзакцій. Така технологія насамперед є технологією, що забезпечує безпеку використання криптовалюти.

Надійність та безпека функціонування платіжної системи криптовалюти заснована на використанні криптографічних методів. Можливо, завдяки домінуючій ролі криптографії у платіжній системі криптовалюти і з'явився префікс «крипто» в назві цього виду цифрової валюти.

Криптографія як механізм забезпечення безпеки в платіжній системі криптовалюти застосовується, *по-перше*, на етапах зберігання та передання криптовалюти, а, *по-друге*, при формуванні розподіленого реєстру транзакцій, які зберігаються в блоках. У першому випадку використовується так звана сучасна криптографія з відкритим ключем для реалізації технології ЕЦП та класична або симетрична криптографія для можливого захисту сховища електронних гаманців і трафіку транзакцій.

В іншому випадку при формуванні блоків транзакцій застосовуються криптографічні хеш-функції для захисту транзакцій від можливих фальсифікацій чи підмін блоків транзакцій електронного реєстру. Тут важливо, що з усього класу можливих хеш-функцій застосовуються саме криптографічні, які мають такі властивості, що гарантують безпеку результатів своєї роботи від підміни або змін, а саме:

детермінованість – результат роботи хеш-функції завжди одне і те ж хеш-значення, якщо вхідні дані для цієї функції незмінні;

односпрямованість – властивість функції, при якій швидко і легко обчислюється значення самої функції за відомим значенням аргументу, зворотна ж процедура – обчислення аргументу за відомим значенням функції є вкрай трудомістким завданням;

колізійна стійкість – незначна ймовірність генерації однакового хеш-значення при різних вхідних параметрах;

розсіюваність – при найменшій зміні тексту результат хешування змінюється кардинально. Наприклад, якщо текст для хешування має вигляд: «Київський національний торговельно-економічний університет», то хешування за допомогою алгоритму *SHA*-256 дасть такий результат:

0dbc514017f041bf8c0a77ce045dfa2347b98b7525bba7da3f105cf9458d8f24

Додавши у вхідний текст «Київський національний торговельно-економічний університет» усього один пробіл після слова «торговельно», отримаємо зовсім інший результат хешування:

8b39bc30965d990412a3d27128279e00dc5ef2a08fb3e89a74bd358736ec69cd

Криптографічні методи застосовуються, крім зазначеного, і при самій генерації одиниць криптовалюти: при обробці чергового блоку транзакцій здійснюється пошук хеш-значення поточного блоку із заданим рівнем складності. У визначенні криптовалюти, наведеному в Оксфордському словнику, відзначається цей факт: «... цифрова валюта, в якій використовуються методи шифрування для регулювання генерації одиниць валюти та перевірки переказу коштів, що діють незалежно від центрального банку» [6].

Найбільш відома криптовалюта – це біткойн. Біткойном називається також і електронна платіжна система, через яку здійснюються операції з цією валютою.

Платіжна система криптовалюти біткойн децентралізована і функціонує на вузлах розподіленої мережі, що підтримують цю систему. У біткойн-системі для зберігання виконаних транзакцій використовується ланцюжок блоків (*блокчейн*). Кожен блок такого ланцюжка містить заголовок і обмежений список транзакцій. У заголовку записані параметри, серед яких є хеш-значення попереднього блоку. Сам попередній блок має точно таку ж структуру: заголовок з хеш-значенням відповідно попереднього блоку і список попередніх транзакцій і т д. Таким чином, весь ланцюжок блоків зберігає всі транзакції за весь час роботи біткойн-системи. Безпеку такого зберігання можна проаналізувати, якщо детальніше розглянути роботу платіжної системи.

Система працює за такими правилами:

- клієнт, здійснюючи транзакцію, передає інформацію про неї у мережу платіжної системи, яка розсилає її усім вузлам мережі;
- кожен вузол мережі об'єднує транзакції, що прийшли за певний період у блок і обчислює хеш-значення всього блоку, яке повинно задовольняти заданому рівню складності;
- як тільки хеш-значення із заданим рівнем складності для всього блоку транзакцій буде обчислено, вузол мережі, який виконав це, відправляє тепер уже новий блок транзакцій у розподілену мережу;
- вузли мережі перевіряють блок і транзакції усередині нього на валідність і приймають цей блок, тільки якщо всі транзакції в ньому коректні та не використовують уже витрачені кошти;
- свою згоду з новими даними вузли висловлюють, починаючи роботу над наступним блоком, використовуючи хеш-значення попереднього блоку.

За такої схеми роботи платіжної системи, щоб ввести зміни в якусь транзакцію в блоці без втрати довіри до нього з боку всієї мережі, потрібно буде забезпечити незмінність хеш-значення всього блоку. А це практично неможливо, так як використовується крипто графічно стійка хеш-функція для отримання хеш-значення всього блоку. Щоб платіжна система прийняла блок транзацій уже зі зміненим хеш-значенням усього блоку, потрібно буде змінити хеш-значення і в подальшому блоці, в заголовку якого міститься інформація про хеш-значення попереднього блоку і т. д. Таким чином, для того, щоб поміняти інформацію про транзакції в одному з блоків, потрібно буде перегенерувати весь ланцюжок блоків. Імовірність реалізації такої процедури незначна і сильно корелює з обчислювальною потужністю мережі біткойн, яка нині перевищує обчислювальні ресурси гіпотетичної мережі з 500 найпотужніших суперкомп'ютерів, наявних у світі.

За даними *bitcoinwatch.com*, хешрейт мережі біткойн перевищив 1 екзафлоп. Звичайно, це приблизне число, оскільки сам процес обчислення хеш-значень окремих транзакцій і їх блоків у мережі не вимагає проведення операцій з плаваючою комою.

Щоб надійно функціонувати, система блокчейн повинна весь час створювати нові блоки, причому в розподіленій системі нові блоки мають створюватися не єдиним суб'єктом, а мережею в цілому.

Консенсус у всій мережі по включенню конкретного блоку в ланцюг (після його верифікації) за відсутності довірчих відносин між вузлами мережі досягається угодою, що в ланцюжок розподіленого реєстру буде внесений саме той блок транзакцій з великої кількості претендентів, який задовольняє вимогам до хеш-значення цього блоку. Хеш-значення блоку транзакцій, в свою чергу, є результатом роботи криптографічного алгоритму хешування. Багаторазове застосування цього алгоритму, з циклічною зміною заданої константи на вході, вимагає значних обчислювальних ресурсів, рівень яких залежить від заданих вимог до хеш-значення блоку. Перевірка ж хеш-значення на відповідність заданим вимогам не має обчислювальної складності, тому криптографічне хешування є гарною реалізацією відомого механізму досягнення консенсусу «*proof-of-work*» (доказ роботи) в розподіленій децентралізованій платіжній системі [7].

Само по собі хешування не несе ніякої корисної мети, крім збільшення складності пошуку правильного блоку. Це гарантує, що ніхто поодинці, з будь-яким існуючим набором ресурсів, не зможе взяти під контроль всю систему. Такий підхід також є технологією безпеки.

Важливим елементом платіжної системи криптовалюти біткойн є електронні гаманці, які можна розглядати як аналог банківських рахунків у централізованій платіжній системі. Наразі вже існує досить багато різних реалізацій електронних гаманців (програмних, апаратних, гібридних, онлайн-гаманців), але здебільшого спрямування цих інструментів приблизно однаково:

- генерація і зберігання ключів (приватного і публічного) для постановки та перевірки ЕЦП;
- здійснення транзакцій;
- генерація біткойн-адрес для вхідних транзакцій;
- доступ до історії транзакцій та інформації про поточний баланс.

Безпека самого електронного гаманця багато в чому заснована на безпеці операцій з ключами.

Для публічного ключа не існує якихось вимог щодо забезпечення його таємності. Більш того, він відомий у платіжній системі, так як публічний ключ (а точніше хеш-значення від публічного ключа) є адресою електронного гаманця, куди переводиться криптовалюта біткойн. Адресою електронного гаманця є унікальна послідовність символів, що генерується платіжною системою. Процедура генерації є досить складною сукупністю криптографічних перетворень з метою підвищення безпеки використання електронного гаманця.

Скорочений алгоритм генерації адреси електронного гаманця [8]:

- вибирається відкритий ключ довжиною 65 байт (1 байт – ідентифікатор, а наступні 64 байти відповідають координаті X і координаті Y однієї з точок еліптичної кривої у кінцевому полі):

04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb6
49f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f

➢ проводиться хешування відкритого ключа за алгоритмом *SHA*-256:

261c1eb21fc4708c6acbe1cfc6d4565652e9e768b620782898936b93000a6c02

➢ виконується хешування попереднього результату роботи за алгоритмом *RIPEMD*-160 для отримання 20-байтної адреси:

62e907b15cbf27d5425399ebf6f0fb50ebb88f18

➢ додається байт-ідентифікатор перед хеш-значенням і контрольна сума з 4 байт у кінці хеш-значення для перевірки коректності введення адреси;

➢ результат конвертується в заданий у біткойн-мережі формат *base58*:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Це і є *адреса електронного гаманця*. Такий формат запису використовується для компактності, хоча по суті ключ являє собою дуже велике просте число.

Публічний ключ використовується також платіжною системою для перевірки легальності транзакцій від власника приватного ключа, яким підписується транзакція, оскільки публічний і приватний ключі математично пов'язані між собою.

Приватний ключ також формується платіжною системою. Обчислення приватного ключа за відомим публічним ключем є складною математичною задачею, оскільки використовується алгоритм *ECDSA* (*Elliptic Curve Digital Signature Algorithm*). Крипостійкість цього алгоритму ґрунтується на проблемі дискретного логарифма в групі точок еліптичної кривої. Криптосистеми на еліптичних кривих використовуються сьогодні практично у всіх сучасних технологіях захисту цифрової інформації і гарантують високий рівень безпеки цифрових активів. При використанні цього алгоритму приватний ключ практично неможливо підібрати обчислювальним шляхом, але можна вкрасти. Тому необхідно зберігати значення приватного ключа в таємниці, оскільки той, хто знає або має доступ до приватного ключа, відповідно має доступ і до електронного гаманця.

Висновки. Застосування сучасних криптографічних методів для нової цифрової валюти забезпечує необхідний рівень безпеки від можливих прихованих і відкритих шахрайських дій на всіх етапах життєвого циклу криптовалюти: генерації, переданні, зберіганні. Важливо, що для генерації ключів електронного гаманця використовується алгоритм *ECDSA* з доведеною криптостійкістю. Використання ж у платіжній системі криптовалюти пірингової архітектури мережі вузлів розподіленого реєстру і технології блокчейн істотно підвищує рівень безпеки застосування криптовалюти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dr Garrick Hileman, Michel Rauchs. Global cryptocurrency benchmarking study. Cambridge Centre for Alternatve Finance. 2017.
2. Juan A. Garay, Aggelos Kiayias, Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings. Part II. p. 281-310.
3. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. URL: http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.
4. Reuben Grinberg. Bitcoin: An Innovative Alternative Digital Currency. Hastings Science and Technology Law Journal. January 6, 2012. URL: http://scienceandtechlaw.org/bitcoin-an-innovative-alternative-digital-currency.
5. CPMI report on digital currencies. Digital currencies. Committee on Payments and Market Infrastructures. November, 2015.
6. Cryptocurrency. URL: https://en.oxforddictionaries.com/definition/cryptocurrency.
7. Nakamoto S. Bitcoin: F Peer-to-Pear Electronic Cash System. URL: http://bitcoin.org/bitcoin.pdf.
8. Technical background of Bitcoin addresses. URL: http://en.bitcoin.it.

Стаття надійшла до редакції 14.02.2019.

Pashorin V. Technologies of cryptocurrency security and block chain networks.

Background. *The dynamics of the introduction of information technology in the banking sector in recent decades cannot fail to impress. It is difficult to overestimate the accomplished transition to electronic payment systems, the use of electronic digital signatures in banks' document flow, the use of electronic money or digital currency. However, it is extremely important to focus not only on the positive aspects of new technologies, but also on the safety issues of their use, especially when it comes to money. It is quite relevant to study the issue of digital currency security.*

The ***aim*** *of the article is to study the applied security technologies for using digital currency on the example of Bitcoin cryptography and the security mechanisms of a decentralized distributed block chain network, on which Bitcoin cryptocurrency is based.*

Materials and methods. *The information base of the study was the work of foreign scientists, reports of financial institutions [5], electronic resources, raising the problems of using the digital currency. To achieve this goal, scientific methods of theoretical analysis, synthesis and analogies are used.*

Results. *Decentralization increases the level of cryptocurrency security, since if it is still possible to allow malicious intervention in the work of a single central authority, then any attempt to make changes to individual nodes of a distributed system is simply meaningless. Thus, the decentralization and application of a distributed registry in accounting for cryptocurrency is an important security aspect of the cryptocurrency itself. From the point of view of personal data protection, the anonymity of cryptocurrency can also be considered as an element of security technology. Cryptography as a security mechanism in the cryptocurrency payment system is used, firstly, at the stages of storing and transferring cryptocurrency, and, secondly, it is used when forming a distributed registry of transactions stored in blocks. In the first case, the modern cryptography is used to implement digital signature technology and classical cryptography for the possible protection of electronic purse store and transaction traffic.*

Conclusion. *The use of modern cryptographic methods for the new digital currency provides the necessary level of security against possible hidden and open fraudulent actions at all stages of the life cycle of cryptocurrency: generation, transmission, storage. The use in the payment system cryptocurrency the peering architecture of the distributed nodes and technology block chain significantly increase the security of the use of cryptocurrency.*

Keywords: digital currency, cryptosystem, blockchain, bitcoin, hash function, electronic wallet.

REFERENCES

1. Dr Garrick, Hileman, & Michel, Rauchs (2017). Global cryptocurrency benchmarking study. Cambridge Centre for Alternatve Finance [in English].
2. Juan A., Garay, Aggelos, Kiayias, & Nikos, Leonardos (2015). The Bitcoin Backbone Protocol: Analysis and Applications. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, Proceedings. Part II. (pp.281-310) [in English].
3. Joseph, Bonneau et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *www.jbonneau.com*. Retrieved from http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf [in English].
4. Reuben, Grinberg (2012). Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal*, *January 6*, Retrieved from http://scienceandtechlaw.org/bitcoin-an-innovative-alternative-digital-currency [in English].
5. CPMI report on digital currencies (2015). Digital currencies. *Committee on Payments and Market Infrastructures*. November [in English].
6. Cryptocurrency. *en.oxforddictionaries.com.* Retrieved from https://en.oxforddictionaries.com/definition/cryptocurrency [in English].
7. Nakamoto S. Bitcoin: F Peer-to-Pear Electronic Cash System. *bitcoin.org.* Retrieved from http://bitcoin.org/bitcoin.pdf [in English].
8. Technical background of Bitcoin addresses. *en.bitcoin.it.* Retrieved from http://en.bitcoin.it [in English].