УДК 621.38

Тищенко О.С.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Гумен Т.Ф.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Трапезон К.О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ТЕХНОЛОГІЇ BLOCKCHAIN В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПЕРЕДАВАННЯ ДАНИХ

Визначено особливості технології блокчейн, де на основі введеного поняття блоку даних розглянуто принципи створення алгоритму передавання даних між різними вузлами інформаційної системи. Проаналізовано принципи захисту даних у технології, де зазначено, що на основі криптографічного алгоритму SHA-256 рекомендується задля підвищення захисту інформації використовувати додатково схему цифрового підпису еліптичної кривої. Досліджено алгоритм, за яким формується унікальна адреса біткоїну і проаналізовано алгоритм захисту створеної адреси. За результатами проведеного дослідження можна зробити висновок, що ключові положення реалізації технології блокчейн через впроваджену процедуру передавання транзакцій можуть бути адаптовані і на етапі створення архітектури однорангової телекомунікаційної мережі.

Ключові слова: *протокол, система, інформація, телекомунікаційна мережа, захист.*

Постановка проблеми. Конфіденційність, безпека, надійність, цілісність інформації, яка передається між різними користувачами системи, останнім часом потребує від боку фахівців із розробки телекомунікаційних мереж найширшої уваги. Особливо актуальним є момент, коли передаються конфіденційні дані, які стосуються відкриття доступу до захищених банківських профілів клієнтів. Разом із тим наявні алгоритми захисту, політика їх використання не завжди можуть бути гарантом від сторонніх мережевих атак, тоді як реалізація виділеного з'єднання може бути недоцільною і фізично не реалізованою, з огляду на особливості функціонування телекомунікаційної мережі. Технології блокчейн, протоколи та архітектура як окрема реалізація новітньої інформаційної системи можуть бути взяті за основу у процесі створення нової захищеної системи передавання та обміну даними.

Постановка завдання. Розгляд технології блокчейн, її структури, визначення особливостей захисту даних, особливо під час реалізації відомого нині алгоритму майнінгу можуть бути використані у процесі створення удосконаленого прототипу банківської розрахункової системи, де основною складовою частиною передавання даних є транзакція. Натомість ресурси платіжної системи біткоїн можуть бути поштовхом до переобладнання наявних телекомунікаційних мереж із позицій забезпечення в останніх ширшої розгалуженості, підвищеної захищеності даних у відповідальних вузлах, чіткої прозорості під час отримання доступу до інформаційних ресурсів цієї мережі. Таке рішення в рамках дослідження обране з того принципу, що саме в технології блокчейн можна прослідкувати та спрогнозувати усі дії з передавання даних завдяки логічно побудованій та чітко організованій архітектурі зв'язку кінцевих вузлів.

Метою статті є дослідження технології блокчейн, визначення її особливостей до технічного спрямування у процесі конструювання удосконаленої телекомунікаційної мережі обміну даних на основі чинних алгоритмів та підходів, зокрема алгоритму біткоїн та протоколу ethereum. Так, передбачається, що розглянуті положення структури системи, захисту даних, аналізу зв'язків між вузлами можуть бути підґрунтям подальшого розгортання інформаційної мережі, яка підтримує, наприклад, платіжні банківські послуги по усьому світі.

Виклад основного матеріалу дослідження. Нині інформаційні технології розвиваються дуже

стрімко, й однією з порівняно нових технологій є Blockchain, яка вперше стала відомою завдяки терміну Bitcoin (криптографічна валюта). Основи та принципи роботи нової технології швидко поширились на широкий спектр нових проектів через певні властивості, які пропонує технологія blockchain. Незважаючи на те, що спочатку вона використовувалася для підтримки цифрової валюти, ця технологія може бути реалізована в різних галузях, які зазвичай вимагають двох або більше сторін чи вузлів, які співпрацюють між собою у формі валюти, послуги, товарів або цифрових даних. Одним із ключових понять є транзакція. Блокчейн − це фактично книга, що містить цифрову інформацію, пов'язану з транзакціями та подіями. Головну книгу зберігають на кількох комп'ютерах, які здатні порівнювати, надаючи головній книзі характеристику розподілу в кількох місцях одночасно. Єдиний спосіб змінити або додати інформацію до розподіленої книги полягає в тому, щоб більше 51% комп'ютерів погодилися на нову інформацію. Хеш транзакцій і подій об'єднуються в одну групу, відому як блок. Блоки разом із тим секвенуються за часом і використовують інформацію з попереднього блоку, значення транзакцій і третю змінну для створення наступного заголовка блоку, для позначення позиції блоку, як правило, у вигляді хеш-виходу. Вихід заголовка блоку буде включений в основу наступного блоку для збереження як блоків, ланцюгових послідовно, своєю чергою, утворюючи блокчейн.

Структура системи

Що стосується кожної частини системи blockchain, то правила, які написані у вихідному коді Bitcoin, визначають структуру блоку Bitcoin. Блок складається з п'яти полів, як показано в байті нижче на рисунку 1. Підпис файлу, який також називається «магічним» числом, є постійним шістнадцятковим значенням D9 B4 BE F9 (рис. 1) і використовується як ідентифікатор блоку Bitcoin у мережі. Друге поле вказує розмір наступного блоку в байтах, а четверте − кількість включених транзакцій. Ці три поля складають метадані з метою організації мережевого зв'язку. Однак дві основні частини − це 80-байтовий заголовок блоку і дані про транзакції, що використовують решту блоків, які є штучно встановленою верхньою межею для одного блоку: один мегабайт.

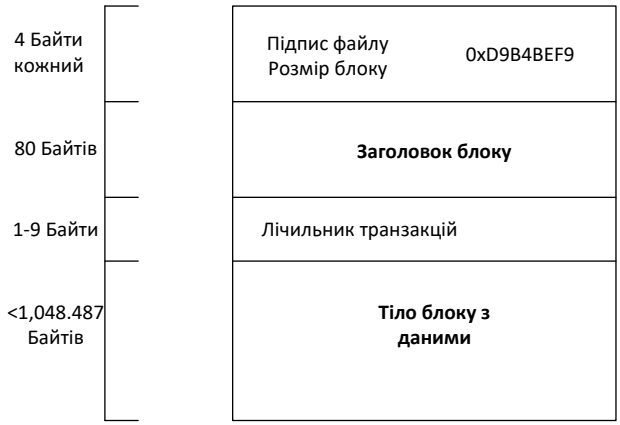

Рис. 1. Блок Bitcoin спрощений за допомогою байт-карти [1]

Блоки в блокчейні з'єднані між собою. Перший блок − блок генезису, закодований у вихідний код. Він має хеш-покажчик тільки з нулями і тому вважається, що він не має попереднього блоку. Крім того, він містить деякі довільні дані в межах своєї транзакції, що можна ідентифікувати. Використання іншого блоку генезису означає виключення, і це призводить до наявності іншого ланцюга. Кінець ланцюжка є останнім блоком, хеш якого ще не використовується як вхід для іншого блоку. Ми можемо легко уявити сценарій, в якому один і той самий блок використовується як вхід для двох різних блоків, таким чином, з'єднаний із більш ніж одним наступним блоком. Це цілком можливо. Тим не менш вихідний код визначає правило − є тільки один дійсний ланцюжок, який є найдовшим шляхом від блоку генезису до кінцевого блоку. Вона містить найбільшу кількість блоків або, більш точно, найбільшу хешівську потужність. Запуск клієнта BitcoinCore показує, що основний ланцюжок (рис. 2) має висоту близько 487 000 блоків. Всі інші блоки, що не входять до

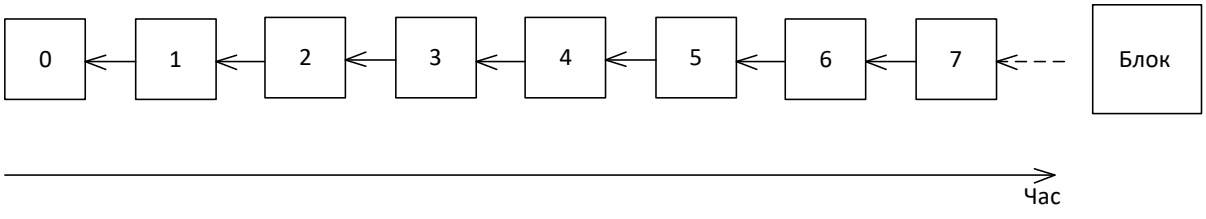

Рис. 2. Блоки в прямій ланцюга [2]

основного ланцюга, входять до складу видобувних вилок і маркуються застарілими чи сиротами. Описану архітектуру можна спроектувати під час створення зв'язків між вузлами аналогічної телекомунікаційної системи, яка спрямована на передавання інформації.

Захист даних у техноголії Blockchain

Шифрування, що використовується в технології, являє собою тип криптографічного хеш-алгоритму, відомого як Secure Hash Algorithm – 256, де хеш − це вихід алфавітно-цифрових символів, які обчислюються з вихідного звичайного тексту, який використовується як вхідний. Bitcoin не встановлює жодної форми системи балансу рахунку. Скоріше, правила вихідного коду говорять: «Кожен, хто отримує справжній логічний запуск сценарію виводу транзакції, має право використовувати суму значення параметра як вхідні дані для іншої транзакції». Доцільною аналогією для цієї концепції є публічне сховище для одноразового використання, де кожен може кинути один елемент (вхід транзакції), але тільки особа, яка знає код ключа в сховищі, може отримати цей конкретний елемент (кінець транзакції). Для реалізації цієї концепції цифровим способом Bitcoin використовує схему цифрового підпису. Схема є алгоритмом цифрового підпису еліптичної кривої (ECDSA), перевіреним і широко використовуваним у світі стандартом. Зазначимо, що Bitcoin не використовує RSA-стандарт головним чином тому, що ECDSA забезпечує ту саму безпеку з більш короткими значеннями ключів, що є необхідною властивістю для забезпечення пропускної здатності в одноранговій телекомунікаційній мережі.

Сценарій виведення транзакції містить хеш відкритого ключа. Щоб виконати скрипт з істинними даними, відправник має надати *відкритий ключ*, який при хешуванні дає адресу призначення, і *підпис*, щоб показати доказ відповідного закритого ключа. Як алгоритм хеш-перетворення Bitcoin послідовно поєднує хеш-функції SHA-256 і RIPEMD-160, а також додає байт версії і кодування двійкового тексту в Base58Check. Ця процедура робиться з метою отримання дуже високого рівня випадковості в хеш-виході і захисту від випадкових зіткнень. Це робить хеш-вивід зручним способом вираження ідентичності. Вихідний сценарій використовує цю ідентифікацію як адресу призначення. Зразковий адрес Bitcoin може виглядати так:

31qXHBL8nJc6kpVRrWNQ4XccgEsgTf9nNQ

Адреса надає людям псевдоанонімність, оскільки адреси можна простежити і пов'язати назад до транзакцій раніше, але учасник може створювати нові ідентичності дуже легко і в автономному режимі. Використання адреси лише один раз і здійснення транзакцій з якомога меншою кількістю входів і виходів приносить вищу анонімність з'єднань.

Ethereum протокол

Ethereum є альтернативним протоколом блокчейн із підходом загального призначення задля полегшення побудови всіх концепцій кінцевих машин на основі транзакцій. Будучи абстрактним фундаментним шаром, блокчейн із вбудованою мовою програмування Тьюринга дає змогу будькому писати смарт-контракти і децентралізовані програми, де вони можуть створювати свої власні довільні правила для володіння, форматів транзакцій і функцій переходу. Крім моделі валюти, машини можуть обробляти інші активи, такі як запаси та нерухомість, або відстежувати предмети в їх ланцюзі.

Отримання унікально ідентифікованих адрес в Ethereum нагадує процес у Bitcoin (рис. 4). Відкриті ключі побудовані з приватних ключів через ECDSA і використовуються як вхідні дані для алгоритму хешування. Останні 20 байтів виводу є асоційованою адресою до закритого ключа.

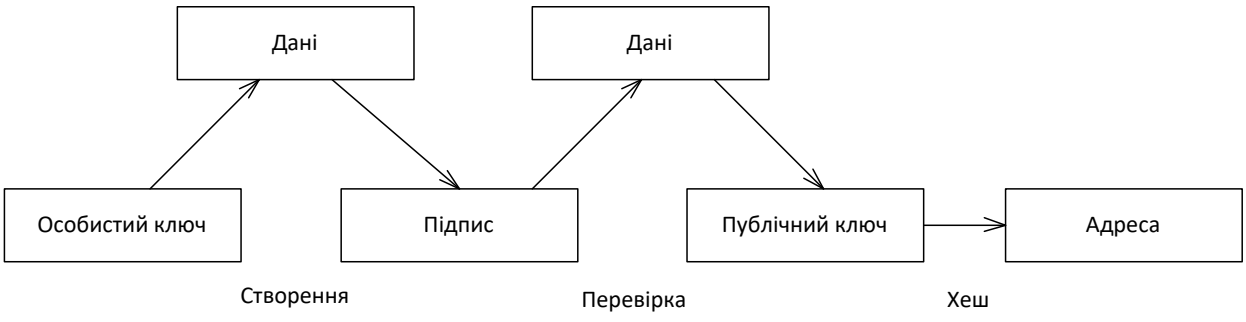

Рис. 3. Утворення адреси Bitcoin

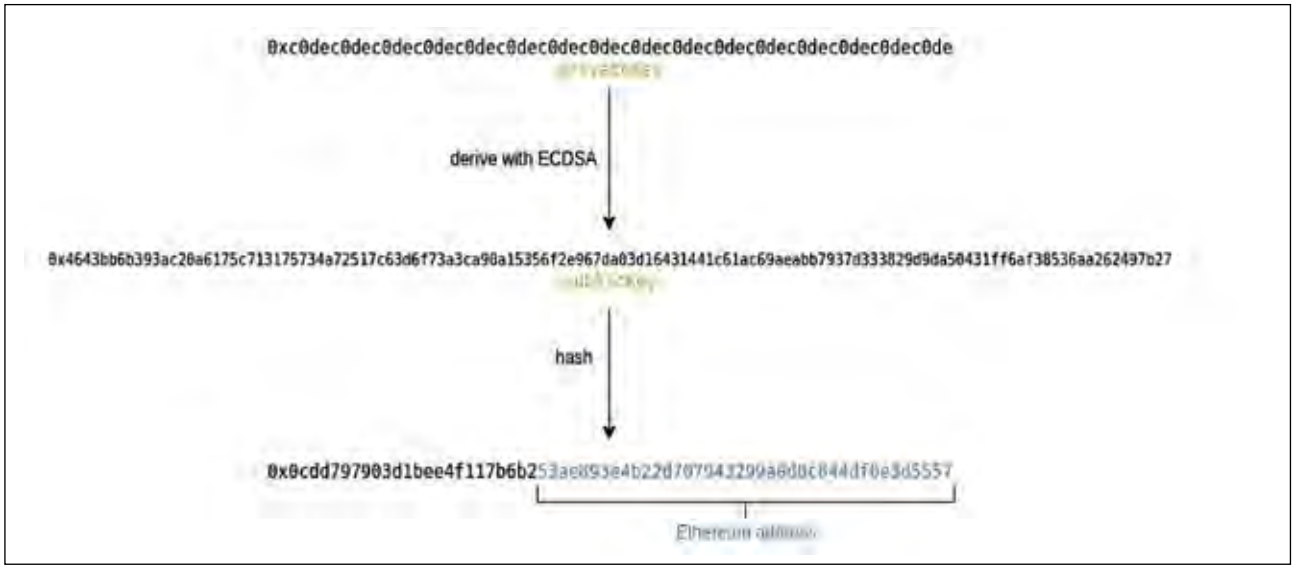

Рис. 4. Утворення адреси Ethereum

Зазначимо, що алгоритм хешування у Ethereum не SHA-256, застосований у Bitcoin, а Keccak-256 (SHA-3). Цей алгоритм є ще одним стандартом, встановленим Національним інститутом стандартів і технологій (NIST) після того, як були виявлені деякі атаки на SHA-2, які з часом виявилися невирішеними. Фонд Ethereum, однак, планує оновити можливість для рахунків індивідуально реалізувати власну схему цифрового підпису з будь-яким алгоритмом хешування. Це дозволить, наприклад, поєднання обох SHA-2 і SHA-3 послідовно, щоб зробити ідентичність більш безпечною, аби можна було б використовувати одноразову схему сигналізації Lamport для квантового опору. Це відхилення від версії, жорстко закодованої в обробку транзакцій, до версії, що реалізовується обліковим записом, надає велику перевагу гнучкості для Ethereum, щоб відповідати різноманітним потребам додатків. Це особливо справляється з розвитком криптографічної безпеки в довгостроковій перспективі.

Транзакція Ethereum складається з семи полів, як показано на рисунку 5. У "nonce" зберігається кількість транзакцій, надісланих відправником. Поле "to" вказує адресу одержувача, яка завжди точно одна, оскільки моделі облікового запису не потребують кількох виходів. Скалярне значення являє собою кількість ефіру в "Wei" для передачі. І останнє поле містить відповідний висновок з алгоритму підпису, щоб показати докази знання приватного ключа. Як пояснюється в моделі обліку, UTXO-модель Bitcoin також може розкрити всю інформацію з цих полів.

Smartcontracts

Ця програма вважається найбільш амбітною. Ключова ідея інтелектуальних контрактів полягає в тому, що умови та інформація можуть бути укладені в контракт, і якщо терміни реалізуються, контракт виконується автоматично. Однак, якщо умови не виконуються, контракт не набуває чинності. Можливість вбудовування інформації в блокчейн дає змогу здійснювати захищені контракти між особами, які не потребують підтвердження третьою стороною. Крім того, жодна зі сторін не може порушити умови угоди в інтелектуальному контракті. Інтелектуальні контракти можуть бути адаптовані до всіх видів контрактів; біткоїни можуть бути відправлені в правильних обставинах, і організації можуть запрограмувати у свої контракти, щоб вони автоматично виплачували дивіденди своїм зацікавленим особам, якщо і коли досягнуто певного рівня прибутку. Ці інтелектуальні контракти революціонізують те, як нині укладаються контракти, роблячи їх дешевшими, коли необхідність посередника перевіряти контракти усувається. Надійність посилюється однією з ключових функцій блокчейну, а саме тим, що вона захищена від несанкціонованого доступу.

Висновки. Визначено особливості технології блокчейн, де на основі введеного поняття блоку даних розглянуто принципи створення алгоритму передавання даних між різними вузлами інформаційної системи. Проаналізовано принципи захисту даних у технології, де зазначено, що на основі криптографічного алгоритму SHA-256 рекомендується задля підвищення

захисту інформації використовувати ще схему цифрового підпису еліптичної кривої. Досліджено алгоритм, за яким формується унікальна адреса біткоїну і проаналізовано алгоритм захисту створеної адреси. За результатами проведеного аналізу можна зробити висновок, що ключові положення реалізації технології блокчейн через процедуру передавання транзакцій можуть бути адаптовані на етапі створення архітектури однорангової телекомунікаційної мережі.

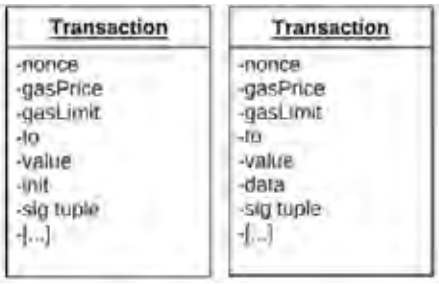

Рис. 5. Операції Ethereum для створення контракту (ліворуч) і виклику повідомлення (праворуч)

Список літератури:

1. Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. Європа : Ексмо, 2018. 256 с.

2. Тапскотт А., Тапкскотт Д. Технология блокчейн. То, что движет финансовой революцией сегодня. Європа : Ексмо, 2016. 448 с.

3. Могайар В. Блокчейн для бізнеса. Європа : Ексмо, 2017. 224 с.

4. Що таке блокчеін простими словами. Prostocoin – провідник у світі криптовалют. URL: https://prostocoin.com/blog/blockchain-guide (дата звернення: 23.01.2019).

5. Блокчеін (цепочка блоків). *Альфарі вільне джерело*. URL: https://alpari.com/ru/beginner/glossary/blockchain/ (дата звернення: 30.01.2019).

6. Райт А., Де Фліппі П. Децентралізована технологія блокчейн і підйом Lex Cryptographia. 2015. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (дата звернення: 30.01.2019).

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ТЕХНОЛОГИИ BLOCKCHAIN В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ

Определены особенности технологии блокчейн, где на основе введенного понятия, блока данных рассмотрены принципы создания алгоритма передачи данных между различными узлами информационной системы. Проанализированы принципы защиты данных в технологии, где отмечено, что на основе криптографического алгоритма SHA-256 рекомендуется для повышения защиты информации использовать еще схему цифровой подписи эллиптической кривой. Исследован алгоритм, по которому формируется уникальный адрес биткоина и проанализированы алгоритм защиты созданного адреса. По результатам проведенного анализа можно сделать вывод, что ключевые положения реализации технологии блокчейна через процедуру передачи транзакций могут быть адаптированы на этапе создания архитектуры одноранговой телекоммуникационной сети.

***Ключевые слова**: протокол, система, информация, телекоммуникационная сеть, защита.*

INVESTIGATION OF THE CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGY IN DATA TRANSMISSION INFORMATION SYSTEMS

The peculiarities of Blockchain technology are determined, where on the basis of the introduced concept of the data block the principles of creation of the algorithm of data transmission between different nodes of the information system are considered. The principles of data protection in technology have been analyzed, where it is noted that on the basis of the cryptographic algorithm SHA-256, it is recommended to use the scheme of the digital signature of the elliptic curve to improve the information security. The algorithm, which forms the unique bitcoin address and analyzes the algorithm for the protection of the created address, is investigated. According to the results of the analysis, it can be concluded that the key provisions of the implementation of the blockchain technology through the transaction transfer procedure can be adapted at the stage of creating the architecture of a peer-to-peer telecommunication network.

***Key words**: protocol, system, information, telecommunication network, protection.*