УДК 004.75

М. О. Пастух

О. В. Романюк

АНАЛІЗ ТЕХНОЛОГІЇ БЛОКЧЕЙНА

Вінницький національний технічний університет

Анотація

Стаття присвячена аналізу технологій, які використовує система блокчейн для забезпечення децентралізації, надійності та прозорості зберігання та передачі інформації. Основними такими технологіями є: метод шифрування SHA256, асиметричне шифрування, різні методи досягання консенсусу та дерево Меркла.

Ключові слова: блокчейн, розподілені бази даних, SHA256, дерево Меркла.

Abstract

The article is devoted to the analysis of technologies used by the blockchain system to ensure decentralization, reliability and transparency of storage and transmission of information. The main technologies are: SHA256 encryption method, asymmetric encryption, various methods of reaching consensus and the Merkel tree.

Keywords: blockchain, distributed databases, SHA256, *Merkel tree.*

Вступ

Система блокчейн з'явилася в 2009 році разом з віртуальною валютою bitcoin. Ця система представляє собою набір записів про фінансові операції з електронною валютою у вигляді цифрових транзакцій на основі великої бази даних [1]. Вона забезпечує високу надійність, прозорість та децентралізацію. Для забезпечення таких переваг у системах блокчейн використовуються різні технології для шифрування, хешування, та зберігання хешованих даних.

Основна частина

Основне завдання, яке повинен вирішувати блокчейн це вчинення довірчої передачі власності на цифрові активи у ненадійному середовищі без посередників. Нехай існує умовна компанія, в якій є певні сервера з базами даних, або навіть декілька в різних дата-центрах. Коли щось відбувається з секретними даними у базі даних, реєструється транзакція, інформація про це реплікується на всі сервери в системі. Але при такому варіанті виникає декілька проблем:

1. Проблема ідентифікації учасників з одного боку і необхідність анонімності транзакцій з іншого. Тобто потрібно при виконанні транзакції не допустити витоки персональних даних.
2. Як довести, що одержувач отримав саме ту інформацію або саме ту суму грошей.
3. Проблема ненадійного середовища при передаванні транзакції або шахрайство.
4. Умовна компанія має кінцеве число серверів, які можуть стати недоступними з певних причин.
5. При виконанні транзакцій компанія сама буде вирішувати, яку комісію зняти, відповідно вона може бути доволі великою.

Відповідно до цього блокчейн вирішує поставлені проблеми за допомогою різноманітних технологій.

Ідентифікація учасників здійснюється за допомогою асиметричного шифрування. Таке шифрування ще називають «з відкритим ключем». В таких системах для зашифровування даних використовують один ключ, а для розшифровування — інший (звідси і назва — асиметричні). Перший ключ є відкритим і може

бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). При цьому ключ розшифровування не може бути визначеним з ключа зашифровування [2].

Для доведення достовірності інформації, транзакції збираються в блоки, обчислюється хеш блоку, який записується в наступний блок. Така послідовність запису хешів в блоках і дала назву технології blockchain, і вона робить неможливим непомітну зміну або видалення блоків або окремих транзакцій з блоків. Таким чином, якщо транзакція потрапила в блокчейн, то її дані залишаться незмінними.

Запобігання шахрайству досягається шляхом використання різних видів досягнення консенсусу щодо достовірності ланцюга транзакцій. Найпоширенішим є PoW (Proof-of-Work). Це принцип захисту систем від зловживання послугами (наприклад, DoS-атак або розсилок спаму), заснований на необхідності виконання стороною, яка робить запит (клієнтом) деякої досить складної тривалої роботи (POW-завдання, одностороння функція), результат якої легко і швидко перевіряється стороною, що обробляє запит [3]. Головна особливість цих схем полягає в асиметрії витрат часу — тривалість для ініціатора запиту і висока швидкість для відповіді.

Проте крім PoW, недоліком якого є висока складність обчислень при збільшенні кількості учасників, є ще PoS, DPoS та багато інших, але варто зупинитись на основних.

PoS (proof of stake) заснований на необхідності доказу зберігання певної кількості коштів на рахунку. При використанні цього методу алгоритм криптовалюти з більшою ймовірністю вибере для підтвердження чергового блоку в ланцюжку обліковий запис з великою кількістю коштів на рахунку. Метод використовують як альтернативу методу Proof-of-Work. Метод був запропонований в 2011. Позитивними рисами цього методу є те, що для проведення атаки 51% потрібно багато коштів. Атакуючому буде просто дорого виконати атаку. А якщо у атакуючого знайдеться багато коштів, він сам постраждає від атаки, оскільки це порушить стійкість криптовалюти [4].

Також можуть використовуватись спільно обидва методи – PoW використовується для початкового розподілу монет, а PoS — для підтвердження блоків.

Консенсус Delegated PoS (DPoS) розділяє учасників на тих, хто голосує і тих, хто валідує. Тримачі монет (голосуючі учасники) делегують своє право перевіряти і записувати транзакції в блокчейн іншим учасникам. Таким чином, валідатори виконують всю обчислювальну роботу і отримують за це винагороду, а наявність голосуючих учасників гарантує чесність валідаторів, тому що їх можна змінити в будь-який момент. Проте такий варіант підходить для приватних блокчейнів, тому що відкриває можливості шахрайства, тому всі учасника цього блокчейну повинні бути відомі.

Надійність функціонування мережі досягається тим, що блокчейн є публічним, де кожен учасник може запустити свою ноду, отримати повну копію блокчейна і, більш того, самостійно почати перевіряти транзакції на правильність. Треба відзначити, що сучасні блокчейни дозволяють будувати не тільки публічні (відкриті), а й приватні (закриті) блокчейни, а також використовувати комбіновані схеми.

Щодо комісії за транзакції, то повністю від комісії в блокчейн не позбувається, але комісія стає практично частиною транзакцій, і зменшується при збільшенні часу її виконання.

Також у системі блокчейн потрібно вирішувати проблему збільшення необхідного дискового простору для зберігання всього ланцюжка блоків для подальшого прослідкування за правильністю доданих блоків. Для цього використовується структура даних – геш-дерево або дерево Меркла.

Дерево Меркла (геш-дерево, tiger tree tashing, англ. Merkle tree) представляє собою особливу структуру даних, яка містить підсумкову інформацію про якийсь більший обсяг даних. Використовується для перевірки цілісності даних.

Дані поділяються на малі частини (блоки), які індивідуально гешуються за допомогою Leaf Tiger Hash, потім з кожної пари гешів по черзі обчислюється Internal Tiger Hash. Якщо до гешу немає пари, то він переноситься в новий ланцюжок без змін. Далі в ланцюжку для кожної пари знову обчислюється Internal Tiger Hash.

Дерево гешів це двійкове дерево гешів, в якому листи є геш-блоками даних, наприклад, файлу або набору файлів. Верхні вузли дерева є гешами своїх «дітей». Наприклад, на зображенні hash 0 є результат гешування конкатенації hash 0-0 та hash 0-1 . Тобто, hash 0 = hash (hash 0-0 + hash 0-1) , де + означає

конкатенацію. Більшість реалізацій геш-дерев є двійковими (два дочірні вузли під кожним вузлом), але вони можуть використовувати також і багато інших дочірніх вузлів під кожним вузлом. Як правило, для гешування використовується криптографічна геш-функція, така як SHA-2. Якщо геш-дерево потребує лише захисту від ненавмисного пошкодження, може бути використана необов'язкова контрольна сума, така як CRCs.

У верхній частині геш-дерева є верхній геш (root hash). Перш ніж завантажувати файл у мережу P2P, в більшості випадків верхній геш отримується з надійного джерела, наприклад, веб-сайту, який, як відомо, має хороші рекомендації щодо завантаження файлів. Коли доступний верхній геш, геш-дерево може бути отримано з будь-якого неперевіреного джерела, як і будь-який рівноправний вузол у мережі P2P. Потім отримане геш-дерево порівнюється з перевіреним верхнім гешем, а якщо дерево гешування пошкоджене або підроблене, буде братися інше дерево гешу з іншого джерела, поки програма не знайде той, який дорівнює верхньому гешу [5].

Висновки

Технологія блокчейн є ефективною реалізацією розподіленої бази даних. Проте вона набула такої популярності і має переваги за рахунок використання у ній багатьох технологій, які були винайдені раніше блокчейна і успішно використовуються в інших системах. Але їх спільне використання у системі блокчейн дозволяє вивести їх використання на новий рівень. До того ж блокчейн продовжує розвиватись і змінюватись доповнюючи свою структуру додатковими інструментами, які направлені на розширення його вузьких місць.

Основними технологіями, що стали основою для створення блокчейну стати асиметричне шифрування, симетричне шифрування SHA256 та дерево Меркла.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пастух М. О. Технологія блокчейн і можливості її застосування. [Електронний ресурс] // М.О.Пастух, О.В.Романюк / L Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (2021), м. Вінниця, 10 – 12 березня 2021 р. – Вінниця: Вінницький національний технічний університет, 2021. – Режим доступу до ресурсу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/12148
2. Stallings, William (3 May 1990). Cryptography and Network Security: Principles and Practice. Prentice Hall. c. 165.
3. Jakobsson, Markus; Juels, Ari (1999). "Proofs of Work and Bread Pudding Protocols"
4. Saleh, Fahad (1 March, 2021). Blockchain without Waste: Proof-of-Stake.
5. Becker, Georg (2008-07-18). "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis

Пастух Михайло Олексійович – студент групи 1ПІ-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: pastukhmikhailo@gmail.com

Романюк Оксана Володимирівна – к.т.н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: romaniukoksanav@gmail.com

Pastukh Mykhailo – student of group 1PI-17b, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: pastukhmikhailo@gmail.com

Oksana Romaniuk – Candidate of Technical Sciences, Associate Professor of the Software Chair, Vinnytsia National Technical University, Vinnytsia, e-mail: romaniukoksanav@gmail.com