УДК 681.3(045)

Р.В. Білик
О.В. Сілагін

Перспективи використання технології блокчейн

Вінницький національний технічний університет

Анотація

У статті розглянуто технологію блокчейн як інноваційного інструменту. Зокрема, визначено сутність та передумови розвитку блокчейн, принципи та специфіку функціонування системи, а також схему її роботи. Особливу увагу приділено дослідженню проблеми безпеки і конфіденційності, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним. Розкрито потенційні переваги та виділено проблеми, які потрібно вирішити для ефективного використання цієї технології.

Ключові слова: хеш-функція, транзакція, безпека, блокчейн, blockchain, розумні контракти, smart contracts.

Abstract

The article considers the blockade technology as an innovative tool. In particular, the essence and background of the development of blocks, the principles and specifics of the functioning of the system, as well as the scheme of its work, are determined. Particular attention is paid to the study of security and privacy by providing a new computing layer where data can be safely processed and analyzed while remaining private. The potential advantages are highlighted and the problems that need to be resolved for effective use of this technology are highlighted.

Keywords: hash function, transaction, security, blockade, blockchain, intelligent contracts, smart contracts.

Вступ

Перспективи використання технології блокчейн. Blockchain є новою інформаційною технологією, яка набуває розвитку та використання у багатьох галузях. Першим і найбільш відомим прикладом використання технології Blockchain є криптовалюта – Bitcoin **[**1**]**. На цей час криптовалюта перетворилась у визнаний платіжний засіб, віртуальну валюту, яку приймають великі та дрібні підприємства, корпорації та сервіси.

Результати дослідження

На сьогодні ведуть дослідження та здійснюють реалізацію низки проектів з використанням технології Blockchain у таких галузях, як охорона здоров'я, засоби масової інформації, електронне голосування, зберігання файлів, смарт-контракти, страхування, державний сектор (видача паспортів, збір податків, реєстрація земельних ділянок) та ін. **[2,** 3**]**.

Корпорація IBM досліджує технологію Blockchain і працює над створенням програмного забезпечення, за допомогою якого партнери зможуть укладати цифрові договори, що будуть фіксуватися у глобальній мережі. IBM також реалізує проект під назвою Adept, мета якого відстеження підключених до мережі пристроїв за допомогою технології Blockchain **[**4, 5**]**.

Завдяки децентралізованій структурі, високій надійності і відмовостійкості, технологія Blockchain може бути використана у системах автоматизованого транспортування, логістики, складських системах, хмарних обчисленнях, а також в кіберфізичних системах

[6, 7**]**.

У 2008 р. автор або група авторів під псевдонімом Satoshi Nakamoto опублікували статтю "Bitcoin: A Peer-to-Peer Electronic Cash System" з описом концепції і принципів роботи платіжної системи у вигляді однорангової мережі **[**1**]**. У 2009 р. було представлено протокол криптовалюти Bitcoin та опубліковано код програми-клієнта. Ключова особливість запропонованої концепції полягала в тому, що онлайн платежі між клієнтами здійснюються без центральної фінансової установи, яка виконує роль довіреної структури, з використанням криптографічних методів та публічної розподіленої бази даних, яка складається з ланцюжка блоків (Blockchain) **[**8**]**.

Blockchain – це розподілена структура даних, яка складається з послідовності блоків, в якій кожний блок містить хеш попереднього блоку, утворюючи, як наслідок, ланцюг блоків (рис. 1). Перший блок у ланцюжку (батьківський блок, genesis block) розглядають як окремий випадок, оскільки в нього відсутній попередній блок. Blockchain працює як розподілена база даних, яка здійснює облік усіх операцій у мережі. Операції мають відзначку часу і зберігаються у блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain повністю зберігається у кожному вузлі мережі. Для роботи Blockchain не потрібно довіри між вузлами мережі, оскільки будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах **[7]**.

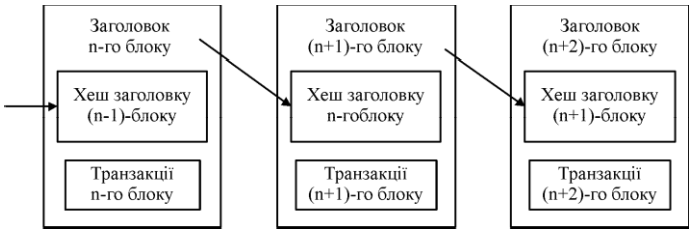

Рисунок 1 – Спрощена послідовність блоків

Принцип функціонування технології Blockchain розглянемо на прикладі криптовалюти "біткойн". Як хеш-функцію криптовалюта біткойн використовує криптографічну хешфункцію SHA-256 **[**9**]**. Для перевірки цілісності даних у блоці використовується деревоподібне хешування (дерево Меркле), яке представляє особливу структуру даних, що містить інформацію про здійснені транзакції. Для цього з кожної транзакції обчислюється хеш, а потім з кожної пари хешів обчислюється новий хеш пари. Ця процедура повторюється доти, поки не залишиться один хеш. Якщо пара в хешу відсутня, то він переноситься на новий рівень без змін (рис. 2).

Групу транзакцій після перевірки записують у спеціальний блок (див. рис. 2). Блок складається із заголовка та списку транзакцій (Tr A, Tr B, …). Заголовок блоку включає хеш даного блоку, хеш попереднього блоку (Previous Hash), хеш транзакцій (Merkle Root) та додаткову службову інформацію (Nonce, Timestamp). Відзначка про час (Timestamp) вказує, коли був створений блок, і надає докази того, що дані в блоці існували в певний момент часу.

Для формування нового блоку вузла потрібні дані: хеш попереднього блоку в ланцюжку; хеш Merkle для операцій, які потрібно помістити у блок; час (Timestamp) та одноразовий код (Nonce), вибраний псевдовипадкових чином.

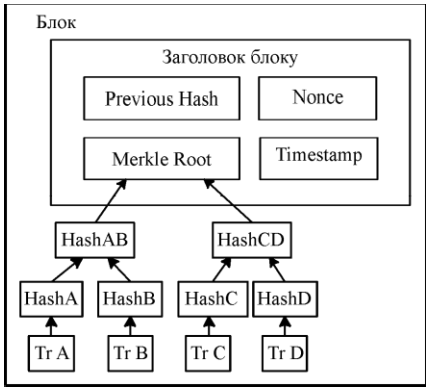

Рисунок 2 – Структура блоку

Для підтвердження коректності блоку потрібно обчислити хеш заголовка нового блоку, який повинен починатися із заданої кількості нулів. Дана задача відома, як доказ правильності роботи (proof-of-work), що базується на двох принципах: 1) зробити підтвердження транзакцій затратними для користувачів мережі у вигляді комп'ютерних обчислень; 2) здійснювати винагороду за допомогу у перевірці транзакцій.

Новий блок приймається іншими вузлами мережі, якщо значення хешу заголовка дорівнює або менше заданого числа, величина якого періодично змінюється. Коли результат знайдено, сформований блок розсилається іншим вузлам, які його перевіряють. Якщо перевірка пройшла успішно, то блок додається в ланцюжок і наступний блок повинен включати в себе його хеш.

Робота, яку вузли повинні виконати для створення нового блоку, вимагає багато часу та обчислювальних ресурсів. Це знижує ймовірність того, що два блоки будуть зроблені одночасно, але така ситуація все-таки можлива. Коли це відбувається, то створюється розгалуження в Blockchain. У такому випадку вузли можуть почати будувати ланцюг на різних гілках.

Доказ виконання роботи — принцип захисту систем від зловживання послугами 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 (сервером) . Головна особливість цих схем полягає в асиметрії витрат часу — тривалість для ініціатора запиту і висока швидкість для відповіді. Подібні схеми також відомі як client puzzle (функція клієнтської головоломки), computational puzzle (обчислювальна головоломка), або CPU pricing function. Не слід плутати цей спосіб захисту з капчі, які пропонують завдання, легкі для людини, але складні або зовсім нерозв'язні для комп'ютера. POW-завдання не призначені для людини, їх рішення комп'ютером завжди досяжне, але вимагає виконання великої кількості операцій. При цьому для перевірки отриманого рішення потрібна відносно мала кількість операцій. Прикладом POW-захисту може служити система Hashcash яка використовує хешування часткової інверсії при відправці по електронній пошті. Для розрахунку відповідного заголовка потрібно близько 2^{52} хеш-обчислень, які треба перераховувати для кожної відправки. Необхідність постійного перерахунку робить відправку спаму дуже ресурсномісткою, але не створює перешкод для відправки звичайної пошти. При цьому для перевірки коректності обчисленого коду використовується одноразове обчислення SHA-1 із заздалегідь підготовленою міткою.

Proof-of-stake (PoS) — метод захисту в криптовалютах, 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 (PoW) (доказ виконання роботи), в якому більшу ймовірність підтвердження блоку має обліковий запис з великими обчислювальними потужностями. Метод був запропонований в 2011. Спільно обидва методи — PoW і PoS — використовуються, наприклад, в криптовалютах EmerCoin, NovaCoin. У криптовалютах PeerCoin і Reddcoin метод PoW використовується для початкового розподілу монет, а PoS — для підтвердження блоків. У криптоплатформі Nxt і BlackCoin метод PoS використовується на всіх етапах.

- Аргументи, що вказують на спроможність методу
- Для проведення атаки потрібно багато коштів. Атакуючому буде просто дорого виконати атаку;
- Якщо у атакуючого знайдеться багато коштів, він сам постраждає від атаки, оскільки це порушить стійкість криптовалюти.

Аргументи, що викликають побоювання:

- PoS дає додаткову мотивацію до накопичення коштів в одних руках, що може негативно позначитися на децентралізації мережі;
- Якщо утвориться невелика група, яка сконцентрує у себе досить великі кошти, вона зможе нав'язувати свої умови функціонування криптовалюти, з яким будуть незгодні більшість міноритаріїв, які не контролюють процесинг.

Технологія Blockchain пропонує рішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним.Переваги технології **Blockchain**. Переваги технології Blockchain, які забезпечують її ефективне використання у середовищі Інтернет речей **[**1**,**6, 8-10**]**:

1) Blockchain є публічною розподіленою базою всіх транзакцій у мережі, яка підтримується одноранговою мережею;
2) мережа Blockchain стійка до збоїв, оскільки вона функціонує без єдиної точки відмови;
3) Blockchain є незмінною і довговічною розподіленою базою і, як тільки транзакції записані в Blockchain, вони не можуть бути змінені або видалені;
4) мережа Blockchain має високий ступінь масштабованості;
5) усі транзакції в мережі Blockchain захищені криптографічними методами;
6) Blockchain дає змогу пристроям здійснювати операції автономно без довіреної сторони. Технологія Blockchain пропонує рішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним.

Висновки

Blockchain є відносно новою концепцією з високим потенціалом, відповідно потребує додаткових досліджень для її ефективного застосування у нових галузях, таких як кіберфізичні системи та Інтернет речей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access https://bitcoin.org/bitcoin.pdf.

2. Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" *arXiv preprint arXiv:1608.05187,* 2016.

3. Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. [Electronic resource]. – Mode of access http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408.

4. Brody, Paul. Device democracy: Saving the future of the Internet of Things / Paul Brody, Pureswaran Veena // IBM, September, 2014.

Veena P. Empowering the Edge-Practical Insights on a Decentralized Internet of Things. Empowering the Edge-Practical Insights on a Decentralized Internet of Things / P. Veena, S. Panikkar, S. Nair, P. Brody // IBM Institute for Business Value, 17 Apr. 2015. [Electronic resource]. – Mode of access http://www01.ibm.com/common/ssi/cgi-bin/ssialias? infotype=PM&subtype=XB&htmlfid= GBE03662USEN#loaded.

5. Boohyung Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment / Lee Boohyung, Lee Jong-Hyouk. The Journal of Supercomputing, 2016. – Pp. 1-16.

6. Мельник А.О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Видво НУ "Львівська політехніка". – 2014. – № 806. – С. 154-161.

7. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. – 298 p.

8. Ferrer E.C. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016.

9. Bahga Arshdeep. Blockchain Platform for Industrial Internet of Things / Bahga Arshdeep, Vijay K. Madisetti // Journal of Software Engineering and Applications. – 2016. – № 9. – Pp. 533-546.

10. Щербіна Є. С. Месюра В. І. Аналіз мов написання смарт контрактів існуючих крипто валют / Збірник праць XI Міжнародної науково-практичної конференції «Інтернет-Освіта-Наука - 2018» (ІОН-2018) – Вінниця : ВНТУ, 2018, с.184-185.

Білик Руслан Володимирович – студент групи 1 КН-14б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: rusbilyk1@gmail.com

Сілагін Олексій Віталійович– к.т.н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Bilik Ruslan Volodymyrovych - student of group 1 KN-14b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsya, e-mail: rusbilyk1@gmail.com

Silagin Aleksey Vitaliyovych - Ph.D., Associate Professor, Department of Computer Science, Vinnytsia National Technical University, Vinnytsia.