Д.Е. Марков
О.В. Сілагін

Особливості реалізації програмних продуктів(додатків) на базі блокчейн технології

Вінницький національний технічний університет

Анотація

У даній статті розглянуто технологію блокчейн і реалізацію програмних продуктів на цій технології. Визначимо, які саме додатки можуть бути створені, переваги і недоліки їх використання, схему їх роботи і правильного функціонування. Також потрібно приділити увагу і дослідити їхньому захисту, конфіденційності і проблемам безпеки.

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

Abstract

This article discusses the technology of blocks and implementation of software products on this technology. Determine which applications can be created, the advantages and disadvantages of their use, the scheme of their work and the proper functioning. It is also necessary to pay attention and to investigate their protection, confidentiality and security issues.

***Keywords:** hash function, transaction, security, blockchain, smart contracts.*

Вступ

Особливості реалізації програмних продуктів(додатків) на базі блокчейн технології. Основна «фішка» blockchain — можливість створювати на його базі не лише щось, пов'язане із криптовалютами, а будь-який сервіс, ця технологія лежатиме в його основі. На даний момент, для цього найкраще підходить блокчейн Ethereum. Платформа Ефіріум об'єднує потужності комп'ютерів, щоб її користувачі могли створювати на відповідній основі свої додатки. Ці програми, по суті, є сукупністю алгоритмів — смарт-контрактів. Блокчейн гарантує їх безпеку та незмінність, а валюта Ефір — слугує своєрідним паливом для їх запуску і роботи.

Результати дослідження

Блокчейн — спеціальна структура для запису групи транзакцій. Транзакція при цьому здійснюється лише тоді, коли вважається підтвердженою. Це зручно і надійно, якщо йдеться про здійснення платежів чи передачу конфіденційних даних. Аби транзакція вважалася достовірною («підтвердженою»), її формат і підписи мають бути перевірені. Після цього групу транзакцій записують в спеціальну структуру (так званий блок). В цих блоках інформацію можна швидко перевірити. А ще в кожному наступному зберігається інформація про попередній. При операціях із криптовалютами, наприклад, у ланцюжку блоків міститься інформація про всі вчинені коли-небудь операції з біткойнами[8].

В блок входять заголовок та список транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеши транзакцій та додаткову службову інформацію. Першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок. Для проведення транзакцій в блоці використовують деревоподібне хешування, аналогічне формуванню хеш-суми файлу в протоколі BitTorrent (тому самому, який використовується в роботі торент-трекерів). Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута

input посилання на транзакцію, за якою на цей рахунок були отримані біткойни (або інші дані чи цифрові валюти). Комісійні операції можуть містити в атрибуті будь-яку інформацію (для них це поле носить назву Coinbase parameter), оскільки у них немає батьківських транзакцій. Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується[9].

Оскільки результат хешування (функції SHA-256) непередбачуваний, немає алгоритму отримання бажаного результату, окрім випадкового перебору. Якщо хеш не задовольняє умову, то довільно змінюється блок службової інформації в заголовку — і хеш перераховується. Після співпадіння варіантів вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш. А тоді все починається спочатку[10].

Маніпулювання даними в блокчейні(Ethereum) забезпечується так званими розумними контрактами (smart contracts). Вони описують які дані зберігати на блокчейні й набір функцій для операцій над ними. Виконання функцій і отримання доступу до даних здійснюється через надається кожним контрактом інтерфейс. Цей інтерфейс генерується з вихідного коду окремо від компіляції і дозволяє виконувати бінарний код. Дані для учасників мережі відкриті, і читання їх нічого не варто, адже як уже було сказано, дані зберігаються у всіх учасників мережі. Зміна даних відбувається за допомогою транзакцій. Кожну транзакцію можна уявити структурою такого вигляду:

- одержувач транзакції;
- Цифровий підпис відправника;
- Кількість валюти, що відправляється;
- Довільні дані (необов'язково);
- Ліміт газу на транзакцію;
- Ціна за одиницю газу;

Виконання транзакцій вимагає витрат внутрішньої валюти і очікування коли черговий створений майнером блок з вашої транзакцією включиться в загальну ланцюжок. Код контракту виконується на комп'ютері майнера, у віртуальній машині EVM, а в нагороду майнер отримує комісію[7].

Основні переваги старт-контрактів:

- автономність (для укладення та підтвердження угоди не потрібно шукати посередника в особі брокера, банку, нотаріуса тощо. д.);
- надійність і безпека (багаторазово продубльований контракт зберігається в зашифрованому вигляді в блокчейні;
- безпека системи гарантується математичними законами і робить практично неможливим хакерські атаки, а також підміну інформації заднім числом;
- економія і швидкість - завдяки блокчейну усуваються багато посередників і автоматизуються процеси;
- точність - завдяки автоматизації і мінімізації ручної роботи знижується ймовірність помилок, які часто з'являються при заповненні форм в процесі узгодження і при ручному проведенні різних операцій за контрактом[7].

Недоліки:

- недостатньо розвинута інфраструктура та можливі критичні помилки в самому коді;
- багато «пробілів» в нормативно-правовому регулюванні;
- менш гнучкі, ніж звичайні контракти(оскільки ті дані, що потрапили в блокчейн вже неможливо далі змінити)[7];

Висновки

Отже, провівши дослідження можна бачити, що блокчейн технологія швидко розвивається і має дуже високий потенціал, також додатки на базі цієї технології(старт-контракти) мають багато

переваг і сфер застосувань, і після видалення недоліків стануть ще кращі і перспективніші у застосуванні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ashton K. That Internet of Things / K. Ashton // Thing. RFID Journal, 22 July 2009. [Electronic resource]. – Mode of access http://www.rfidjournal.com/articles/view?4986.
2. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. [Electronic resource]. – Mode of access http://www.gartner.com/newsroom/id/3165317.
3. Shancang Li. The internet of things: a survey / Li Shancang, Li Da Xu, and Shanshan Zhao // Information Systems Frontiers 2015, 17.2. – Pp. 243-259.
4. Whitmore Andrew. The Internet of Things – A survey of topics and trends / Whitmore Andrew, Anurag Agarwal, and Li Da Xu // Information Systems Frontiers 17.2, 2015. – Pp. 261-274.
5. Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" arXiv preprint arXiv:1608.05187, 2016.
6. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access https://bitcoin.org/bitcoin.pdf.
7. 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.
8. Brody, Paul. Device democracy: Saving the future of the Internet of Things / Paul Brody, Pureswaran Veena // IBM, September, 2014.
9. 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://www- 01.ibm.com/common/ssi/cgi-bin/ssialias? infotype=PM&subtype=XB&htmlfid= GBE03662USEN#loaded.
10. 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.
11. Ferrer E.C. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016.
12. 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.
13. Мельник А.О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Вид-во НУ "Львівська політехніка". – 2014. – № 806. – С. 154-161.
14. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. – 298 p.

Марков Дмитро Едуардович — студент групи 1КН-14б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 2kn14b.markov@gmail.com

Сілагін Олексій Віталійович— канд. техн. наук, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Dmitry E. Markov — student of Information Technologies and Computer Engineering Department, 1CS-14b, Vinnytsia National Technical University, Vinnytsia, e-mail: 2kn14b.markov@gmail.com

Oleksiy V. Silagin — Cand. Sc. (Eng.), Assistant Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.