УДК 004.9

О. О. Гаврищук
С. О. Жуков

Розробка програмних продуктів на базі технології Blockchain

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто технологію блокчейн і реалізацію програмних продуктів на цій технології. Визначено, які саме додатки можуть бути створені, переваги і недоліки їх використання, схему їх роботи і правильного функціонування.

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

Abstract

This paper 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.

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

Вступ

Технологія блокчейн була створена в 2008 році Сатоші Накамото. Саме він запропонував зберігати зашифровані дані не в одному місці, а в послідовному ланцюжку блоків. Блокчейн - це не що інше, як база даних, розподілена по блоках. Кожен з цих блоків зберігає інформацію про попередній блок, і так по ланцюжку до безкінечності. У усіх цих даних немає єдиного власника - вони зберігаються на різних комп'ютерах.

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 [1, 2].

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 [3, 4].

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 [5].

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 [3].

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 [6].

Блокчейн - це універсальний інструмент для побудови різних баз даних, який має наступні переваги [7]:

1. Децентралізація - відсутній головний сервер зберігання даних. Усі записи зберігаються у кожного учасника системи.
2. Повна прозорість. Будь-який учасник може відстежити усі транзакції, що проходили в системі. Конфіденційність. Усі дані зберігаються в зашифрованому виді. Користувач може відстежити усі транзакції, але не може ідентифікувати одержувача або відправника інформації, якщо він не знає номера гаманця. Для проведення операцій потрібно унікальний ключ доступу.
3. Надійність. Будь-яка спроба внесення несанкціонованих змін буде відхилена через невідповідність попереднім копіям. Для легальної зміни даних потрібно спеціальний унікальний код, виданий і підтверджений системою.
4. Компроміс. Дані, які додаються в систему, перевіряються іншими учасниками. Якщо говорити розумними словами - вони перераховують хеш. (Хешуванню присвячена окрема стаття, але по суті вони рахують яблука з використанням складних математичних формул).

Дозволяючи цифровій інформації поширюватися, але не копіюватися, технологія блокчейн створила основу нового виду інтернету. Технологія була спочатку розроблена для цифрової валюти, биткойна, але нині технічне співтовариство шукає інші потенційні варіанти використання цієї технології [8].

Блокчейн-технологія, як і Інтернет, має вбудовану стійкість до помилок. Зберігаючи блоки інформації, ідентичні в усій мережі, блокчейн не може: Контролюватися кимось одним; Не має єдиної точки відмови. Биткойн був винайдений в 2008 р. З того часу блокчейн Биткойна працює без істотних збоїв. (На сьогодні, проблеми, пов'язані з Биткойном, були із-за злому сервісів, побудованих поверх нього, або недостатнього контролю. Іншими словами, ці проблеми виникають із-за поганих намірів і людських помилок, а не із-за недоліків в архітектурі протоколу). За майже 30 років Інтернет довів свою надійність. Це досягнення служить хорошою ознакою для блокчейн-технологии, яка продовжує розвиватися.

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. Очевидно, що технологію блокчейн доцільно використовувати для розробки продуктів які передбачають максимальний захист даних від зміни та підробки. Враховуючи вищесказане дану технологію буде використано в розробці системи моніторингу пристроїв для видобування криптовалюти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" arXiv preprint arXiv:1608.05187, 2016.
2. Brody, Paul. Device democracy: Saving the future of the Internet of Things / Paul Brody, Pureswaran Veena // IBM, September, 2014.
3. 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.
4. 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/cgibin/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.
6. 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.
7. 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.
8. 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.

Гаврищук Олексій Олегович — студент групи 3КН-15б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 3kn15b.gavryshchuk@gmail.com

Жуков Сергій Олександрович — кандидат технічних наук, доцент кафедри системного аналізу, комп'ютерного моніторингу та інженерної графіки, Вінниця, e-mail: sazhukov@gmail.com

Науковий керівник: ***Жуков Сергій Олександрович*** — канд. техн. наук, доцент кафедри системного аналізу, комп'ютерного моніторингу та інженерної графіки, Вінницький національний технічний університет, м. Вінниця.

Gavryshchuk Oleksii O. — student of Information Technologies and Computer Engineering Department, 1CS-14b, Vinnytsia National Technical University, Vinnytsia, e-mail: 3kn15b.gavryshchuk@gmail.com

Zhukov Serhii O. — Cand. Sc. (Eng.), Assistant Professor of the Department of Systems Analysis, Computer Monitoring and Engineering Graphic, Vinnytsia, e-mail: sazhukov@gmail.com.

Supervisor: ***Zhukov Serhii O.*** — Cand. Sc. (Eng.), Assistant Professor of the Department of Systems Analysis, Computer Monitoring and Engineering Graphic, Vinnytsia.