УДК 004.75

Л.В. Кузьменко
Г.Л. Лисенко

ВИКОРИСТАННЯ BLOCKCHAIN ТЕХНОЛОГІЙ ДЛЯ «РОЗУМНИХ» ЗАСТОСУВАНЬ

Вінницький національний технічний університет

Анотація

В роботі наведено детальний аналіз принципів технології Blockchain. Описані основні функції та застосування Blockchain, блоки транзакції та хешування функцій.

Ключові слова: Blockchain, bitcoin, хеш-функції, блок транзакцій, криптовалюта

Abstract

The thesis provides a detailed analysis of the principles of Blockchain technology. The basic functions and application of Blockchain, transaction blocks, and hashing functions are described.

Keywords: Blockchain, bitcoin, hash functions, block of transactions, crypto-currency

Вступ

Blockchain по суті являє собою розподілену базу даних записів або публічної книги всіх транзакцій або цифрових подій, які були виконані і розподілені між сторонами. Кожна транзакція в публічній книзі перевіряється консенсусом більшості учасників системи. І, після введення, інформація ніколи не може бути видалена. Блок-ланцюжок містить певну інформацію і піддається перевірці на запис кожної транзакції, яка коли-небудь буде [1].

Використання технології Blockchain

Blockchain спеціальна структура для запису групи транзакцій.

Фінансові установи та банки більше не бачать технології у Blockchain загрозу традиційним бізнес-моделям. Найбільші у світі банки шукають можливостей у цій галузі, проводячи дослідження щодо інноваційних застосувань Blockchain. Дана база є найбільш перевіреним і безпечним для деяких банківських та фінансових програм [2].

Нефінансові програми також мають безліч використань. Можна передбачити докази існування всіх юридичних документів, контрактів, приватних цінних паперів, медичних записів та платежів лояльності в музичній індустрії у Blockchain. Зберігаючи відбиток цифрового ресурсу, а не зберігати сам цифровий ресурс, можна досягти мети анонімності або конфіденційності [2].

Технологія Blockchain може бути застосованою до будь-якої транзакції цифрових активів, що обмінюється в Інтернеті.

Блок транзакцій — 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 криптовалютою.

В блок входять заголовок та список транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеши транзакцій та додаткову службову інформацію. Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується [3].

Оскільки результат хешування (наприклад 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.

Властивості хеша такі, що неможливо з обчисленого результату отримати вхідні дані. При цьому, маючи ті ж вхідні дані, і знаючи спосіб обчислення, завжди можна обчислити хеш повторно - і це наріжний камінь криптографії та мережі bitcoin.

У реальності, звичайно, все набагато складніше, оскільки алгоритми шифрування - це ціла наука, а Blockchain bitcoin хешує 64-значні ключі в шістнадцятковій системі числення, використовуючи алгоритм шифрування SHA-256 [4].

У заголовок кожного наступного блоку записується хеш-сума всіх даних з попереднього блоку, яку не можна обчислити в зворотному порядку. Якщо зловмисник спробує замінити сторінку і передати неіснуючий bitcoin, це буде відкинуто мережею, тому що хеш суми в сусідніх блоках, та й у всій подальшій ланцюжку - не збігатимуться.

Висновки

Створення програмних продуктів на базі технології Blockchain є перспективним напрямком сучасних досліджень по децентралізації сховищ даних та створенню смарт-контрактів. Окремі елементи Blockchain, такі як криптографічні хеш-кодування і розподілені бази даних, самі по собі не нові. Однак їх поєднання створює дуже ефективну нову форму передачі даних і активів, здатну усунути потребу в посередниках, сторонніх центральних органах і дорогих процесах [5].

В 2017 році технологія Blockchain була використана для оновленої системи електронних торгів конфіскованим майном сетам. У жовтні 2017 року із використанням Blockchain була реалізована оновлена версія інформаційної системи державного земельного кадастру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Andreas M. Antonopoulos – K. : NGITS, 2014. – C. 150 – 290

2. Don Tapscott, Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott Blockchain – K. : Information Systems, 2016 – C. 100 – 150.

3. Paul Vigna, Michael Casey The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / Paul Vigna, Michael Casey – K. : Economic, 2015 – C. 200 – 210.

4. Chris Skinner Value Web / Chris Skinner – K. Information technologies, 2016 – C. 150 – 175.

5. Roger Wattenhofer The Science of the Blockchain / Roger Wattenhofer – K. : Information technologies, 2016 – C. 94 – 120.

Лисенко Геннадій Леонідович – к.т.н., проф. кафедри Лазерної та оптикоелектронної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.

Кузьменко Лілія Вікторівна – аспірантка кафедри Лазерної та оптикоелектронної техніки, Вінницький національний технічний університет, м. Вінниця, Україна.

Lysenko Hennadii Leonidovich - candidate of technical sciences, prof. Department of Laser and Optoelectronic Technology, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Kuzmenko Lilia Viktorivna - post-graduate student of the Department of Laser and Optoelectronic Technology, Vinnytsia National Technical University, Vinnytsia, Ukraine.