

ТЕХНОЛОГІЯ BLOCKCHAIN

Вінницький національний технічний університет

Анотація

Поняття «блокчейн» стало активно обговорюватися зі зростанням популярності електронної валюти. Сьогодні її широко обговорюють не лише у світі фінансів. Дану технологію вже використовують для зберігання та обробки персональних даних та ідентифікації, у маркетингу та комп'ютерних іграх. Блокчейн - це ланцюжок блоків, кожен з яких має мітку часу, посилання на попередній блок і зберігається на різних комп'ютерах. Вважається, що ця технологія здатна стати справжнім проривом у сфері фінансів та захищених баз даних.

Ключові слова: блокчейн, цифрова валюта.

Abstract

The concept of "blockchain" has been actively discussed with the growing popularity of e-currency. Today it is widely discussed not only in the world of finance. Blockchain is already used for storage and processing of personal data and identification, in marketing and computer games. Blockchain is a chain of blocks, each of which has a timestamp, a link to the previous block and is stored on different computers. It is believed that this technology can be a real breakthrough in the field of finance and secure databases.

Keywords: blockchain, digital currency.

Вступ

Блокчейн — це спільний, незмінний реєстр, який спрощує процес запису транзакцій і обліку активів в бізнес-мережі. Актив може бути як матеріальним (будинки, автомобіль, гроші, земля) так і нематеріальним (інтелектуальна власність, патенти, авторські права, брендинг). Відстежувати та здійснювати транзакції за допомогою блокчейну можна майже зі всім, що має цінність. Дану технологію можна використовувати для реєстру будь-яких угод — хоч із продажу та переміщення цибулин тюльпанів у ботанічному саду.

Після переходу в онлайн простір зростає ризик що будь-яка стороння людина зможе здійснити транзакцію без відома власника валюти. Впровадження блокчейна збільшує швидкість обміну, зменшує тимчасові витрати, покращує якість, надійність та доступність послуг. При цьому збільшується прозорість та надійність, знижуються ризики.

При дослідженні питання, що таке блокчейн (від англ. Block Chain), насамперед загострюють увагу на такій особливості, що в системі немає єдиного сервера, а ланцюжки блокчейна розподілені між користувачами. Блокчейн ще називають технологією розподілених реєстрів, тому що весь ланцюжок угод та актуальний список власників зберігають на своїх комп'ютерах безліч незалежних користувачів. Навіть якщо один або кілька комп'ютерів дадуть збій, інформація не зникне.

На відміну від звичайних баз даних, змінити чи видалити ці записи не можна, можна лише додати нові. Тобто, для того, щоб здійснити транзакцію без відома конкретної людини, доведеться відредагувати інформацію від моменту реєстру цінності до останнього її переказу на десятках безлічі незалежних носіїв.

Архітектура технології блокчейн

Концепція технології блокчейн запропонована Сатоші Накамото (Satoshi Nakamoto) у 2008 році. Вперше вперше застосована на практиці при появі біткойну у 2009-му. Через походження її відносять до транзакцій криптовалют, але сфера застосування технології помітно ширша.

Система працює наступним чином:

1. Створюється первинний блок, в якому відсутній запис про попередній блок.
2. Кожен наступний блок містить інформацію про попередні блоки, вид транзакції, власне заголовок, що використовується при генерації чергового блоку.
3. Користувачам системи доступні інформація кількість блоків, але мають доступ лише до своїх.

Незважаючи на розміщення блоків в загальнодоступній мережі інтернет, шифрація доступу до кожного з них дозволяє містити в безпеці дані, що зберігаються в них. Сам ланцюжок блоків може вільно передаватися будь-якому користувачеві Інтернету без ризику втрати вмісту. На цьому базуються криптовалюти, що мають матеріальну цінність у національній валюті

Розібратися в тому, що таке блокчейн стане простіше, якщо розглянути тонкощі роботи системи:

Будь-які зміни без підтвердження криптографічних ключів відхиляються. Завдяки цій функції легко організувати перевірку автентичності. Передача закритого ключа надає повний доступ до блоку (грошей та інших активів). Завдяки цьому легко реєструвати угоди через онлайн-ресурси.

Використання технології

Ключова особливість технології блокчейн полягає у децентралізації системи. Якщо базу даних, розташовану на єдиному сервері, зламати теоретично можна за умови застосування будь-яких існуючих засобів захисту, з блокчейнами жоден з цих методів не спрацює. Простими словами – у них нема що зламувати. Залишається лише варіант спроби крадіжки особистих ключів окремих користувачів.

Одна з причин впровадження блокчейнів у фінансову сферу – безпека

Якщо методом блокчейна захищати файл, що передається, незважаючи на ймовірність доступу до нього необмеженого кола осіб, прочитати вміст зможе лише той користувач, кому були передані ключі. Єдиною слабкою ланкою залишається метод копіювання захисного коду, що тут не виключається «людський фактор», здатний призвести до його втрати. Зовні застосування блокчейна виглядає як переказ грошей із кодом протекції.

Під час здійснення такого платежу одержувач бачить суму, дату перерахування та іншу інформацію, але скористатися коштами до отримання секретного коду не може.

Технічно така передача блоків є повністю безпечною. У процесі може брати участь багато комп'ютерів, і на кожному з них буде повна копія блоку. Якщо на одному з етапів відбудеться збій, достатньо відключити зіпсовану ланку і передати блок заново.

Існують проблеми технологічного характеру. Насамперед, масштабованість: сьогодні багато популярних систем розподілених реєстрів не можуть обробляти велику кількість транзакцій, що призводить до гальмування обороту та процесингу транзакцій у них. Інший мінус — нестача конфіденційності у зв'язку із квазіанонімністю блокчейну. Деякі типи блокчейна потенційно вразливі перед «атаками 51%» — коли, у повній відповідності до правил системи, коаліція користувачів, що володіють великими комп'ютерними потужностями, може змінити записи в конкретному блокчейні. Цей процес аналогічний тому, як перехоплює контроль мажоритарний акціонер АТ. Крім того, регуляторні та правові ризики, а також ресурсо- та енергоємність, що іноді зашкалює, залишаються специфічними ризиками криптовалютного сектора блокчейн-індустрії.

Висновки

Блокчейн — це відносно нова перспективна технологія яка базується на децентралізації системи що дозволяє зберігати активи, здійснювати транзакції та обліку активів в бізнес-мережі. Використання даної технології збільшує швидкість обміну трранзакціями, зменшує тимчасові витрати, покращує якість, надійність та доступність послуг. При цьому збільшується прозорість та надійність, знижуються ризики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технологія Блокчейн: використання у фінансах [Електронний ресурс]. – Режим доступу: <https://trends.rbc.ru/trends/industry/5f05c0a79a7947aac5c7577a> (дата звернення 16.11.2021).
2. Блокчейн технолоія та мобільні додатки? [Електронний ресурс]. – Режим доступу: <https://azure.microsoft.com/ru-ru/solutions/blockchain/> (дата звернення 11.11.2021).
3. Що таке технологія блокчейн? [Електронний ресурс]. – Режим доступу: <https://www.ibm.com/ru-ru/topics/what-is-blockchain> (дата звернення 19.11.2021).

Богомолів Сергій Віталійович – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: bogomolovsergiy@vntu.edu.ua

Азаров Олексій Дмитрович – д-р техн. наук, професор, завідувач кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: azarov2@vntu.edu.ua

Білоус Ганна Олександрівна – студентка групи 2КІ-20М, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: anna21bell@ukr.net

Sergey V. Bohomolov – PhD, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: bogomolovsergiy@vntu.edu.ua

Oleksiy D. Azarov – Professor, Head of the Department of Computer Science, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: azarov2@vntu.edu.ua

Hanna O. Bilous – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia. e-mail: anna21bell@ukr.net