

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗДІЙСНЕННЯ ТРАНЗАКЦІЙ

Вінницький національний технічний університет

Анотація

Технологія блокчейн трансформує, і очікується, що вона матиме величезний економічний вплив, подібний до того, який мав Інтернет за останні кілька десятиліть.

Оскільки технологія блокчейн лежить в основі біткоїна інших віртуальних валют, можна принаймні очікувати, що в майбутньому вона забезпечить ще більш значущі засоби обміну. Однак віртуальні валюти – це лише перший випадок використання технології блокчейн.

Ключові слова: блокчейн, транзакції, біткоїн.

Abstract

Blockchain technology is transformative, and is expected to have a massive economic impact similar to the one the Internet has had in the past few decades.

Since blockchain technology is at the heart of Bitcoin and other virtual currencies, it can at the very least be expected to power even more consequential mediums of exchange in the future. However, virtual currencies are merely the first use case of blockchain technology.

Keywords: blockchain, transactions, bitcoin.

Основи блокчейна

Блокчейн – це відкритий розподілений реєстр. Він використовує структуру даних лише для додавання, що означає, що нові транзакції та дані можна додавати в блокчейн, але попередні дані не можна стерти [1]. Це призводить до підтвердженого та постійного запису даних та транзакцій між двома або більше сторонами. Це може підвищити прозорість і підзвітність, а також позитивно покращити наші соціальні та економічні системи.

Блокчейн створюється шляхом запуску програмного забезпечення та з'єднання кількох вузлів разом. Блокчейн – це не одна глобальна сутність – існує кілька блокчейнів. Уявіть собі мережу підключених комп'ютерів у високозахищеному офісі, які з'єднані один з одним, але не з Інтернетом. Блокчейн подібний до цього: він може мати безліч підключених вузлів, але залишатися повністю окремим і унікальним від інших блокчейнів. Установи та банки можуть створювати внутрішні блокчейни зі своїми функціями для різних організаційних цілей.

Для підтримки цілісності та функціональності блокчейну необхідні механізми консенсусу та система винагород. У блокчейні біткоїнконсенсус досягається шляхом «майнінгу», а система винагород – це протокол, який надає майнеру певну кількість біткоїнів після успішного видобутку блоку. Майнінг здійснюється за допомогою потужних комп'ютерів, які вирішують складні математичні головоломки.

Після того, як транзакція підтверджена і прийнята всією мережею як істинна, майнери починають працювати над наступним блоком. Таким чином, блокчейн продовжує рости (пов'язуючи кожен новий блок з попереднім).

Наслідки для транзакцій

Ведення обліку операцій є основною функцією всіх підприємств. Ці записи призначені для відстеження минулої ефективності та допомоги у прогнозуванні та плануванні на майбутнє. Створення записів більшості організацій займає багато часу та зусиль, і часто процеси створення та зберігання схильні до помилок [2]. Наразі транзакції можна виконати негайно, але розрахунки можуть зайняти від кількох годин до кількох днів. Наприклад, хтось, хто продає акції корпорації на фондовій біржі, може продати негайно, але розрахунки можуть зайняти кілька днів. Аналогічно, угоду про купівлю будинку або автомобіля можна швидко обговорити та підписати, але процес реєстрації (перевірка та реєстрація зміни власності на нерухомість) часто займає кілька днів і може залучати юристів та державних службовців. У кожному з цих

прикладів кожна сторона веде свою власну книгу і не може отримати доступ до бухгалтерських книг інших залучених сторін.

У блокчейні процес перевірки та запису транзакцій є негайним і постійним. Реєстрація розподіляється між кількома вузлами, тобто дані реплікуються та миттєво зберігаються на кожному вузлі в системі. Коли транзакція записується в блокчейні, такі деталі транзакції, як ціна, актив і право власності, записуються, перевіряються та розраховуються протягом секунд на всіх вузлах. Перевірена зміна, зареєстрована в будь-якій одній книзі, також одночасно реєструється на всіх інших примірниках книги. Оскільки кожна транзакція прозора та постійно реєструється в усіх книгах, доступна для перегляду будь-кому, немає необхідності в перевірці третьою стороною.

Безпечність блокчейну

Технологія блокчейн забезпечує децентралізовану безпеку та довіру кількома способами. Почнемо з того, що нові блоки завжди зберігаються лінійно і хронологічно. Тобто вони завжди додаються в «кінець» блокчейну. Після того, як блок був доданий в кінець блокчейна, дуже важко повернутися назад і змінити вміст блоку, якщо більшість мережі не досягли консенсусу щодо цього. Це тому, що кожен блок містить власний хеш, а також хеш блоку перед ним, а також вищезгадану позначку часу. Хеш-коди створюються математичною функцією, яка перетворює цифрову інформацію в рядок цифр і букв. Якщо цю інформацію будь-яким чином редагувати, хеш-код також змінюється.

Скажімо, хакер, який також керує вузлом у мережі блокчейн, хоче змінити блокчейн і вкрати криптовалюту у всіх інших. Якби вони змінили свою власну копію, вона більше не відповідала б копіям інших. Коли всі інші перехресно посилатимуть свої копії один на одного, вони побачать, що ця копія виділяється, і ця хакерська версія ланцюга буде відкинута як нелегітимна.

Від віртуальних валют до корпоративного використання

Блокчейн, що лежить в основі біткойн, на даний момент є найбільшим і найвідомішим блокчейном.

Ethereum – це окремий блокчейн: хоча він підтримує валюту Ether, він також діє як розподілена обчислювальна платформа, яка має функціональні можливості смарт-контракту [3]. Тому, незважаючи на наявність елемента віртуальної валюти, він має набагато більше застосувань, ніж біткойн. Наприклад, компанії в різних галузях, які залучають кошти через ICO, використовують Ethereum для своїх проєктів.

Висновки

Технологія блокчейн все ще знаходиться на ранній стадії становлення, і криптовалюти є лише першим великим випадком її використання. Крім криптовалюти, технологія блокчейн змінить те, як ми здійснюємо транзакції, а також як ми реєструємо та перевіряємо транзакції. Це революціонізує контракти та зменшить тертя в обміні активами. Протягом наступних кількох десятиліть технологія блокчейн проникне в наші організації та установи та вплине на те, як ми взаємодіємо один з одним. Так само, як Інтернет продовжує підтримувати нові технології, ми можемо очікувати нових випадків використання технології блокчейн у всіх галузях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дон Тапскотт Блокчейн революція / Дон Тапскотт. — Торонто : М. Демків, 2019. — 492 с.
2. Андреас М. Антонопулос Освоєння Ethereum : створення смарт-контрактів / Антонопулос Андреас М. — Лондон : О'Рейлі Медія, 2018. — 200 с.
3. Вей-Мен Лі Початок програмування смарт-контрактів Ethereum / Лі Вей-Мен — Лондон : Apress, 2019. — 310.

Мельник Денис Олександрович — студент групи ЗПІ-186, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: den_melnikk@icloud.com.

Melnyk Denys Oleksandrovych —Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: den_melnikk@icloud.com.