

ЛЕКЦІЯ

БЛОКЧЕЙН ТА ЙОГО ЗАСТОСУВАННЯ В SMART-ТЕХНОЛОГІЯХ

Однією з найпопулярніших та швидко зростаючих технологій в ІТ-секторі стала технологія блокчейну. Відомо, що вона зробила суттєвий поступ у галузі і відкрила нам нові можливості для створення систем із високим рівнем захищеності.

Блокчейн – це цифровий реєстр, який безпечно записує дані транзакцій у розподіленій мережі комп'ютерів. Блокчейн забезпечує цілісність даних завдяки своїй незмінній природі за допомогою криптографії та механізмів консенсусу, що означає, що після запису інформація не може бути змінена заднім числом.

Технологія блокчейну – це технологія упорядкування в зростаючий список записів, які називають блоками, що пов'язані між собою з використанням методів криптографії.



Коли ми говоримо слова «блок» і «ланцюг» (англ. chain) у цьому контексті, ми фактично говоримо про цифрову інформацію («блок»), що зберігається в

зв'язаній публічній базі даних («ланцюжок»). Кожен користувач системи, може додавати нові записи до бази даних, але не може їх змінювати. У блоці міститься інформація та обчислені дайджести (хеш-функції) цього і попереднього блоків. Хеш ідентифікує блок. Хеш попереднього блоку створює ланцюжок блоків і робить блокчейн безпечним. Коли створюється новий блок, він надсилається усім учасникам мережі. Кожен з вузлів верифікує блок і перевіряє, чи не був він сфальшованим. Якщо перевірка проходить успішно, кожен користувач додає його у свій власний блокчейн.

З чого складається блокчейн-технологія?

Блоки, які містять інформацію про проведені транзакції, мають також посилення на попередній блок, створюючи ланцюг даних. Такий ланцюг інформації одночасно зберігається в багатьох місцях, що унеможливорює будь-які зовнішні втручання чи зміну в базах даних.

Транзакції. Це інформація про проведені операції між двома чи кількома особами, яка групується в блоки, утворюючи ланцюги.

Ноди. Це вузли — комп'ютери з програмним забезпеченням, що підтримують блокчейн-мережу. Вони створюють нові блоки даних, оперують транзакціями, передають інформацію, зберігають копії всіх проведених операцій. Нодою в блокчейні може бути людина, у якої на комп'ютері є відповідна програма.

Консенсус. Це принцип роботи блокчейн-мережі, за допомогою якого забезпечується узгодженість даних між нодами (вузлами) та підтверджується достовірність інформації у блоках. Завдяки алгоритму консенсусу система блокчейну не потребує централізованого нагляду з боку третіх осіб.

Хеш-функції перетворюють інформацію в рядок символів певної фіксованої довжини. Ці криптографічні алгоритми створюють унікальний «хеш» - ряд знаків для кожного блоку, і захищають його від будь-яких шахрайських дій. На сьогодні ще нікому не вдалося зламати це шифрування, бо кожен новий блок містить дані попереднього.

Криптографічні цифрові підписи використовуються для підтвердження справжності криптовалютних операцій.

Які є види блокчейну

Загальнодоступні (публічні) блокчейни досить популярні серед користувачів, оскільки вони дозволяють залишатися в мережі анонімними. Будь-яка людина, що має доступ до інтернету, може стати учасником блокчейн-мережі.

Приватні мережі. Цей тип має обмеження для участі, його використовують приватні підприємці для своїх цілей: управління ланцюгом постачання, обміну даними чи контролю за фінансовими операціями.

У блокчейн-консорціумах мережею керує група осіб чи організацій, що працюють разом та перевіряють транзакції. До такого типу мережі належать приватні підприємства, державні установи або інші організації.

Гібридний блокчейн включає в себе функції приватних та публічних мереж, поєднуючи безпеку та прозорість проведених транзакцій. Гібридні блоки даних можуть бути як відкритими для громадськості, так і з обмеженим доступом. Такий тип мережі налаштовують відповідно до конкретних видів бізнесової діяльності.

Де ще використовують технологію блокчейну?

Блокчейн-технологія застосовується не тільки для проведення криптовалютних операцій. Її давно та активно використовують ще в декількох сферах: освітній, логістичній, в медицині тощо. Технологія постійно розвивається та вдосконалюється, тому прогнозовано, що в майбутньому список сфер її застосування значно розшириться.

Блокчейн використовують в логістиці для захисту даних про всі операції, що проводяться в ланцюгу постачання, від шахрайських втручань. Це підвищує контроль за ефективністю, підзвітністю та прозорістю операцій.

В медицині завдяки технології блокчейну можна безпечно зберігати та контролювати медичні картки, відстежувати якість та розповсюдження ліків. Блокчейн забезпечує також збереження особистих даних від шахрайських дій.

Ще блокчейн-технологією користуються під час купівлі-продажу нерухомості, з метою захисту даних про всі проведені операції.

Одним з недавніх оновлень технології блокчейну стало застосування **смарт контрактів**. Смарт контракти реалізують як програми, що зберігаються в блокчейні і можуть бути використані для контролю і надання інформації про володіння об'єктом. Після створення їх неможливо змінити і вони є розподіленими, тобто вихідні дані контракту підтверджені усіма користувачами мережі. Вони дозволяють здійснювати транзакції та угоди між сторонами без наявності центрального органу, правової системи чи зовнішнього механізму примусового виконання.

Розглянемо приклади застосування вище розглянутих технологій в соціальній сфері.

1. Автомобільна техніка. Наведемо приклад: злочини з одометром. Відомою практикою є зміна показників одометра і продаж автомобілів по ціні більшій, ніж мала б бути насправді. Зазвичай практикують фіксувати кілометраж автомобіля під час інспекцій, але, очевидно, що цього недостатньо. Вирішенням проблеми може стати заміна звичайних одометрів на розумні, що будуть підключені до мережі інтернет і записуватимуть пробіг автомобіля у блокчейн. Це дасть можливість створити електронний сертифікат для кожного автомобіля і відповідно кожен отримає доступ до історії автомобілів, що підключені до цієї системи.

2. Захист інтелектуальної власності. Можна підтвердити достовірність підпису на юридичних документах, використовуючи блокчейн. Прикладом є сайт, де можна подати документ, автоматично записавши його в блокчейн. В такому разі отримується підтвердження авторства документа і можливість його перевірити у будь-який момент часу.

3. Цифрове голосування. Існуючі системи проведення голосувань недостатньо надійні та легко піддаються фальсифікаціям. Системи голосування на основі блокчейну будуть прозорими і максимально надійними, так як

«голоси» будуть пов'язані в ланцюжок, що робить фальсифікацію надзвичайно складною.

4. Харчова індустрія. Прикладом можливого використання є відстежування руху харчових продуктів з моменту їх збору/виготовлення до моменту потрапляння до покупця. Це дасть змогу створити цифровий сертифікат для кожної одиниці продукції, що підтверджуватиме її походження, і у разі знаходження будь-якого роду порушення можливо відслідкувати його появу і миттєво вжити заходів та повідомити інших покупців. Ця система може бути використана не тільки для харчової індустрії, але і для трекінгу інших типів продукції.

Завдяки використанню функції хешування, алгоритму консенсусу та децентралізації, блокчейн є максимально безпечною технологією, робить передачу даних швидшою та дешевшою. За допомогою смарт контрактів можливо проводити транзакції без участі посередників. Технології блокчейну і смарт контрактів мають великий потенціал у застосуванні в соціальній сфері, зокрема, у автомобільній техніці, сільському господарстві, захисті інтелектуальної власності, логістиці, цифровому голосуванні та ін.

Матеріали лекції:

1. Блокчейн і криптовалюта: <https://www.youtube.com/watch?v=OpPHn-JkjJk>
2. Michael Casey and Paul Vigna. The truth machine: the blockchain and the future of everything. Picador, 2019, 336p.
3. Anthony Lewis. The basics of bitcoins and blockchains. Mango, 2018, 408p.