BLOCKCHAIN

Сироватська А.Ю., Хмара Є.П.
Науковий керівник – ***Костенко О.Б., канд. фіз.-мат. наук, доцент***

Що це за блоки і що за ланцюжок? Блоки - це дані про транзакції, угодах і контрактах всередині системи, представлені в криптографічній формі. Спочатку блокчейн був (і залишається досі) основою криптовалюти Bitcoin. Всі блоки збудовані в ланцюжок, тобто пов'язані між собою. Для запису нового блоку, необхідно послідовне зчитування інформації про старі блоки.

Всі дані в блокчейн накопичуються і формують постійно доповнючу базу даних. З цієї бази даних неможливо нічого видалити або провести заміну / підміну блоку. І вона «безмежна» - туди може бути записано нескінченна кількість транзакцій. Це одна з головних особливостей блокчейна.

Роботу блокчейн можна порівняти з Torrent. Функціонування торрентів відбувається в режимі P2P (peer to peer - комп'ютерна мережа, де всі учасники рівноправні). Коли ми завантажуємо якийсь файл з трекера, то ми не використовуємо центральний сервер або сховище.

Ця технологія була створена разом з появою криптовалюти Bitcoin. Сталося це в 2009-му році. Публічною особою-творцем нової віртуальної валюти і Blockchain вважають Сатоши Накамото. Однак ця особистість міфологізована в світі криптовалюти. Це псевдонім, за яким стоїть один або кілька людей, які вирішили не розголошувати свою особистість.

Існує два види ланцюжка:

Публічний Blockchain - відкрита база даних, яка доповнюється. Такий вид блокчейна використовується в криптовалюті Bitcoin. Кожен учасник може записувати і читати дані.

Приватний блокчейн має обмеження по запису або читання даних. Підвид Private Blockchain - ексклюзивний блокчейн. В такому ланцюжку встановлюється група осіб, що займається обробкою транзакцій.

Ключові особливості Blockchain:

Децентралізація - в ланцюжку немає сервера. Кожен учасник - це і є сервер. Він підтримує роботу всього блокчейна;

Прозорість - інформація про транзакції зберігається у відкритому доступі. При цьому ці дані неможливо змінити;

Теоретична необмеженість - теоретично блокчейн можна доповнювати записами до нескінченності. Тому його часто порівнюють з суперкомп'ютером;

Надійність - для запису нових даних необхідний консенсус вузлів блокчейна. Це дозволяє фільтрувати операції і записувати тільки дійсні транзакції. Здійснити підміну хеша нереально.

Blockchain - Це послідовність блоків - ланцюжок, а не замкнуте коло або щось ще. Кожен з блоків містить масив певних даних. І всі блоки пов'язані між собою. Тобто, новий «масив» може бути створений тільки після того, як закриється старий масив.

Конструкція блоків в Blockchain

Формування і закриття блоків. Кожна ланка ланцюжка містить певний ключ. Поки він не буде розшифрований, блок не закриється. Як відбувається ця сама розшифровка? У криптовалюті за це відповідає Майнінг. Майнери, що займаються видобутком криптовалюти, роблять це за допомогою потужностей відеокарт і процесорів. Ті в свою чергу виконують обчислювальні операції, головна мета яких - пошук криптографічного підпису до блоку у вигляді хешу. Як тільки вона підібрана - блок закривається. А майнер за це отримує винагороду у вигляді криптовалюта.

Охарактеризувати принцип роботи блокчейн зрозумілими звичайній людині словами спробували автори книги «Як технологія, що стоїть за Bitcoin, змінює гроші, бізнес і світ»:

«Bitcoin або інша криптовалюта не зберігається в якомусь файлі. Інформація про транзакції знаходиться в глобальній, загальнодоступній базі даних - Blockchain. У ній відбувається підтвердження і прийняття операцій цієї великої P2P-мережою. Весь ланцюг розподілен: він підтримується комп'ютерами по всьому світу. Центрального сервера, який можна було б взламати, не існує. Блокчейн публічний і дуже надійний одночасно, так як використовує зашифровані дані».

Блокчейну, здавалося б, вдається поєднувати непоєднуване. Він дуже надійний і децентралізований одночасно. По суті, гарантом виступає кожен користувач блокчейн. Децентралізація мережі дозволяє проводити передачу даних між суб'єктами, що представляють різні країни, юрисдикції просто за домовленістю між собою, без будь-яких посередників або регуляторів. Блокчейн збудований так, що операції неможливо заблокувати, тобто всі користувачі відчувають себе незалежними.