УДК 004.9

Алексюк В.В. студент

ЯК ПРАЦЮЄ ТЕХНОЛОГІЯ «БЛОКЧЕЙН» В МЕРЕЖІ BITCOIN ТА ІНШИХ ГАЛУЗЯХ

Донецький національний університет імені Василя Стуса, м.Вінниця

Блокчейн – це особливий тип бази даних. Його ще називають «технологія розподіленого реєстру» або ж «DLT»[1]

Основа кожного блокчейна - це алгоритм майнінгу, як приклад розглянемо алгоритм Bitcoin-a. Він називається SHA-256, скорочено від 'Secure hash algorithm 256 bits' (Безпечний хеш алгоритм 256 біт). Він приймає вхідні дані, які можуть бути будь-чим: текстом, числами або навіть комп'ютерним файлом будь-якого розміру. Отриманий результат називається «хеш» і щоразу він матиме однакову довжину – 256 біт у машинному коді. Один і той же вхід видаватиме той самий результат щоразу, це не випадковість. Але якщо ви зробите невелику зміну на вході, вихід повністю зміниться. Це також називається односторонньою функцією, яка означає, що якщо у вас є лише вихідні дані, ви не зможете розрахувати, що було на вході. Ви можете тільки здогадуватися про вхідні дані, і можливість вгадати:

1 шанс на 2^256, що практично неможливо, і отже, безпечно.[2]

Припустимо ви хочете перевести певну кількість біткоїнів на інший рахунок. Ви передаєте повідомлення з транзакцією, яку ви хочте зробити, усім майнерам у мережі. У цій транзакції ви повідомляєте майнерам публічну інформацію рахунка на який ви хочте перевести біткоїн, кількість біткоїнів, цифровий підпис та ваш відкритий ключ. Підпис в свою чергу, зроблено за допомогою вашого закритого ключа і майнери можуть підтвердити, що ви фактично є власником біткоїну і що ви хочете здійснити транзакцію.

Коли майнери впевнені, що транзакція дійсна, вони можуть помістити її в блок разом з багатьма іншими транзакціями та спробувати майнити. Це робиться шляхом розміщення блоку за алгоритмом SHA-256. Висновок повинен починатися з певної кількості нулів, щоб вважатися дійсним. Необхідна кількість нулів залежить від того, що називається складністю, яка змінюється в залежності від того, скільки обчислювальної потужності є в мережі.

Для того, щоб на початку створити вихідний хеш з бажаною кількістю 0, майнери додають в блок те, що називається «nonce number» (є двійковим кодом, який шукається майнерами в процесі PoW-майнінгу.), перед тим, як запустити його через алгоритм. Оскільки невелика зміна вхідних даних повністю змінює вихідні дані, майнери пробують випадкові “nonce” числа, доки знайдуть потрібний вихідний хеш.

Як тільки блок здобутий, майнер передає цей новий блок решті всіх майнерів. Потім вони перевіряють, чи є блок дійсним, щоб додати його до своєї копії ланцюжка блоків, і транзакція завершена. Але в блоці майнери також повинні включити вихідний хеш із попереднього блоку, щоб усі блоки були

пов'язані разом, звідси й назва block-CHAIN. Це важлива частина, тому що система працює на доказі виконаної роботи.

Кожен майнер має свою копію блокчейна на комп'ютері, і кожен довіряє блокчейну з найбільшою обчислювальною роботою, який є найдовшим (має найдовший ланцюжок блоків). Якщо майнер змінює транзакцію в попередньому блоці, вихідний хеш для цього блоку буде змінюватися, що призводить до того, що всі хеші після нього також змінюються через блоки, пов'язані з хешами. Майнеру довелося б переробляти всю роботу, щоб змусити будь-кого визнати, що його блокчейн правильний. Тому, якщо майнер захоче схитрувати, йому знадобиться понад 50% обчислювальної потужності мережі, що є малоймовірним. Таким чином, мережеві атаки називаються 51% атаками.

Модель забезпечення роботи комп'ютерів для блоків називається Proof-of-Work (PoW) (Доказ виконаної роботи). Існують також інші моделі, такі як Proof-of-Stake (PoS) (Підтвердження частки володіння), які не вимагають такої великої обчислювальної потужності та вимагають менше електроенергії, надаючи можливість масштабування для більшої кількості користувачів.[3]

На даний момент сучасний світ перебуває на порозі революції впровадження і використання децентралізованих процесів, що й ініціювало розвиток системи блокчейн. Є досить багато спроб впровадити блокчейн в різні сфери діяльності, такі як: фінанси, банкові системи, ресторанний бізнес, авіакомпанії і т.д.

Список використаних джерел

1. Що таке блокчейн, повний посібник [Електроний ресурс] – Режим доступу: https://academy.binance.com/uk/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners#pros

2. Как работает блокчейн [Електроний ресурс] – Режим доступу: https://academy.binance.com/ru/articles/how-does-blockchain-work

3. Кращі інструменти веб-розробки в 2020 році [Електроний ресурс] – Режим доступу: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D1%8B_%D0%BD%D0%B0_%D0%B1%D0%B0%D0%B7%D0%B5_%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8

УДК 004.9

Гуменюк К.В., студентка 2 курсу спеціальності 122 «Комп'ютерні науки»
Потапова Н. А., к.е.н., доцент, доцент кафедри інформаційних технологій