УДК 004.01

Захарова К.В., *студентка 3 курсу спеціальності 122 «Комп'ютерні науки»*
Катаєва А.І., *старший викладач кафедри комп'ютерних наук та інформаційних технологій*

ЧОМУ БЛОКЧЕЙН – ЦЕ ЦІННО

Донецький національний університет імені Василя Стуса, м. Вінниця

Застереження: Стаття несе ознайомчу мету, а не фінансову пораду.

03 січня 2009 року в 20:15 (GMT +2) невідомий створив перший (нульовий) блок першої в світі криптовалюти у розмірі 50 монет, вартістю $0.00 [1]. Станом на 18 квітня 2021 року 17:50 (GMT +3) цей блок коштував би $2,782,134.50. Через 12 років після запуску до обігу блокчейну, сьогодні вже створено більше 9 тис. різноманітних криптовалют, з загальною капіталізацією у розмірі більше 2-ох трильйонів доларів [2].

Як випадковий набір чисел може бути переведений на реальні, чималі, кошти? Відповідь полягає в унікальності проекту.

Все, що потрапляє в блокчейн, навіки там і залишається.

«Блок-Чейн» (з англ. «Block» – блок, «Chain» – ланцюг) – збірна назва впорядкованих транзакцій (блоків), що зв'язані хешами (ланцюгами). Оскільки кількість платежів та переводів невпинно збільшується, збільшується і кількість блоків, так зародилася інтернет-система у вигляді хеш-дерева.

Кожен блок є цілком захищеним від підробки та будь-яких змін. Блок містить у собі наступну інформацію:

1. Хеш – унікальний ідентифікатор блока;
2. Підтвердження – скільки разів «проходили» через даний блок – чим більше підтверджень, тим «старіший» блок;
3. Час створення блоку;
4. Ріст – кількість блоків підключених до блокчейну;
5. «Шахтар» – хто підтвердив транзакції в блоці;
6. Кількість транзакцій, що включені в даний блок;
7. Складність – математичне значення, наскільки важко знайти дійсний хеш для цього блоку;
8. Корінь Меркла – кореневий вузол дерева Меркла, нащадок усіх хешованих пар у дереві;
9. Версія –версія блоку, що відноситься до пропозицій протоколів, які тривають на даний час
10. Біти – суб-одиниця валюти, що дорівнює 10^{-6} однієї монети;
11. Вага – вимір для порівняння розміру різних транзакцій між собою пропорційно обмеженню розміру блоку;

12. Розмір блоку;
13. Nonce – випадкове значення, яке можна регулювати, щоб отримати доказ роботи;
14. Об’єм транзакцій – орієнтовно загальна сума транзакцій у даному блоці;
15. Нагорода за блок – статична винагорода «шахтарю», який розрахував хеш для цього блоку;
16. Комісія за нагороду – сума комісій за транзакції, що повертається «шахтарю» за обчислення хешу для цього блоку.

Як можна побачити, усе цілком прозоро, можна дізнатися звідки, куди та скільки монет було переправлено. Відкритий блокчейн надає рівні права усім користувачам. Електронні платежі не проходять через посередників та не покладаються на довіру між покупцем та продавцем. Запропонована однорангова (peer-to-peer) мережа з використанням підтвердження роботи (proof-of-work) для запису публічної історії транзакцій, стає обчислювально непрактичним для зловмисника [3]. Така система цілковитого захисту і приваблює нових інвесторів.

Категорична заява: «істинної» децентралізації мереж криптовалют, сьогодні, або вже не існує, або її дуже важко зустріти.

Блокчейни поділяються на децентралізовані, частково централізовані та повністю централізовані.

Повна централізація часто зустрічається у валютах бірж, тобто керівництво та сама мережа належить розробникам валюти. Це не відповідає повному захисту вкладень, оскільки вкладники покладаються на довіру, тобто є високий рівень можливого шахрайства з боку керівництва, але це може зменшувати комісію за транзакцію, бо передача відбувається без стороннього підтвердження.

Часткова централізація – коли керівництво централізоване, а мережа децентралізована. Тобто розробники мають право змінювати умови нагород «шахтарям», випускати оновлення мережі, змінювати кількість доступних монет, тощо, але не мають безпосереднього доступу до самих блоків. Захист вкладень настільки ж потужний, наскільки і в повністю децентралізованому блокчейні, але існує опосередкований вплив на курс зі сторони розробників.

Децентралізація – коли блокчейн належить усім одночасно, але ніхто не може його змінити. Для користування децентралізованою мережею потрібно встановити на свій пристрій інформацію про всі минулі блоки та мати простір для збереження наступних блоків. На даний час, для найбільшої криптовалюти, загальна вага мережі перевищує 350ГБ [4].

Чому ж спочатку було сказано, що «істинної» децентралізації не існує? Вище було багато разів згадано «шахтарів», хто ж вони? «Шахтарі» або «майнери» - це ті, хто підтверджує транзакції, та отримують плату за це. Зазвичай, для цього використовують технічні потужності, тому, чим більша потужність, тим більше транзакцій підтверджується, та тим більше отримує «шахтар». Звідси й випливає інша сторона – якщо хтось отримає 50%

потужностей мережі, це буде пряма загроза захисту мережі. Є поняття – “Атака 51%” – коли власник найбільшої частки загальної потужності може змінювати ланцюги транзакцій, для відправлення одних і тих самих монет різним отримувачам. Але найближчим часом це не передбачається, оскільки більша потужність мережі рівномірно розподілена між п’ятьма пулами [5] (веб-платформа, що групує «шахтарів-учасників», для більш-менш рівномірного розподілення нагород).

Висновки. Створюється все більше цікавих проектів, що використовують за основу технологію блокчейнів. І це не лише криптовалюти, а й державні проекти, чи фінансове забезпечення компаній. При над швидкому збільшені різноманіття блокчейнів потрібно швидко орієнтуватися в їх характеристиках.

Блокчейн – це технологія створення захищеної бази даних для забезпечення прозорості будь-яких операцій з фінансами.

Список використаної літератури:

1. Bitcoin Explorer. Блок 0. URL: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (дата звернення: 18.04.2021)

2. Today's Cryptocurrency Prices by Market Cap. URL: https://coinmarketcap.com/ (дата звернення: 18.04.2021)

3. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper. URL: https://bitcoin.org/bitcoin.pdf

4. Завантажити Bitcoin Core. Остання версія: 0.21.0. URL: https://bitcoin.org/uk/download (дата звернення: 18.04.2021)

5. Пулы для майнинга криптовалют: рейтинг крупнейших и лучших, принцип работы, критерии выбора, рекомендации. URL: https://profinvestment.com/mining-pools/ (дата звернення: 18.04.2021)

УДК 519.257: 004.9 (477)

Зінченко Б.В., *студент 3 курсу спеціальності 122 «Комп’ютерні науки»*
Крикун І.Г., *к.ф.-м.н., доцент кафедри прикладної математики*

ЕКОНОМІКА КІБЕРСПОРТУ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. Кіберспорт [1] це спортивні змагання з відеоігор. Як правило змагання проходять між командами, але є дисципліни де змагання проходять між гравцями поодинці. Змагання проходять з різних дисциплін і гравці з різних куточків світу приймають участь в них. Призові фонди різних змагань досягають мільйонів доларів. Кіберспорт став продуктом, що привертає мільйони глядачів