Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

ПЕРШИЙ КРОК У НАУКУ

Матеріали
IX студентської конференції
(Суми, 25 лютого 2018 року)

Суми
Сумський державний університет
2018

ЯК ПРАЦЮЄ BITCOIN?

Ніколаєв Є.О., *студент*; СумДУ, гр. СУ-71

У даній тезі ми розглянемо: “Як працює Bitcoin?” та “Чому ця система є безпечною?”

Bitcoin – це математично захищена цифрова валюта, яку підтримує мережа рівноправних користувачів. Основою Bitcoin є блокчейн, або ланцюжок блоків. Блокчейн - це загальнодоступний розподілений реєстр, в який можна тільки робити записи про транзакцію, а видаляти чи змінювати – ні. Всі підтверджені транзакції включаються в ланцюг блоків. Bitcoin-гаманці зберігають конфіденціальну інформацію, так званий секретний ключ, який, в свою чергу, поділяється на приватний та загальнодоступний. Приватний використовується щоб підписати транзакцію та мати зв’язок між гаманцем відправника і отримувача, а загальнодоступний для перегляду. Криптографічна хеш-функція трансформує *“попередні транзакції (hash value)”* в альфануметричну форму, яка має назву “nonce”. Якщо ми змінимо хоча б один символ, то отримаємо інший hash, тобто змінити попередні транзакції практично неможливо оскільки відразу отримаємо інше значення hash. Усі транзакції транслюються між користувачами, і починають підтверджуватися мережею, як правило, протягом 10 хвилин, за допомогою майнінга – процесу пошуку вірного значення hash.

Таким чином технологія блокчейн забезпечує хронологічний порядок транзакцій блоків в ланцюжку, нейтральність мережі, розподіл даних, що дозволяє різним комп’ютерам “домовитися” про єдиний стан системи. Щоб транзакції отримали підтвердження, вони повинні упакуватися у блок, який задовольняє строгим криптографічним правилам алгоритму і має перевіритися мережею. Ці правила не дозволяють змінити попередній блок без підтвердження більшістю мережі. Отже, такий спосіб унеможливлює підміну попередніх блоків, а значить сам ланцюжок гарантує цілісність інформації в ньому.

Отже, результатом роботи є доказ роботи, якого важко досягти, але легко перевірити завдяки вже знайденому раніше правильному за алгоритмом nonce, який можна перевірити за лічені секунди, а щоб утворити його, потрібно провести відповідні кроки.

Керівник: Дрозденко О.О., *доцент*