Ендрес В. С.
Здобувач вищої освіти обліково-фінансового факультету,
Миколаївський національний аграрний університет,
м. Миколаїв, Україна
vitally.andres@gmail.com
Бурковська А. В.
Канд. екон. наук, доцент
Миколаївський національний аграрний університет
м. Миколаїв, Україна

ЗРОСТАЮЧА СКЛАДНІСТЬ МАЙНІНГУ BITCOIN ЯК ЗАГРОЗА ЙОГО РОЗВИТКУ

У роботі розглядається проблема постійно зростаючої складності майнінгу Bitcoin, яка негативно впливає на його прибутковість. Зниження прибутковості майнінгу є значною загрозою для функціонування платіжної системи Bitcoin.

Ключові слова: криптовалюта, Bitcoin, майнінг, складність, блок, пул.

Тема криптовалют є однією з найбільш обговорюваних у сучасному суспільстві. Актуальність теми зумовлена великою кількістю переваг віртуальних валют, які роблять їх привабливішими за традиційні види грошей. Проте варто зазначити, що, незважаючи на значну кількість переваг криптовалют, існують і недоліки, які створюють певні загрози розвитку ринку віртуальних грошей. Одним із таких недоліків є висока складність майнінгу. Сьогодні ця проблема є дійсно нагальною для платіжної системи Bitcoin.

Процес видобування криптовалюти називається майнінгом. Саме майнінг дозволяє криптовалютним системам функціонувати, тому користувачі віртуальних грошей мають бути зацікавленими в видобуванні. Сутність цього процесу полягає в генерації цифрових блоків, відомості про які відправляються в систему. В свою чергу користувач, в вигляді винагороди, отримує цифрові монети. Кількість отриманих «монет» залежить від потужності комп’ютера.

Прибутковість майнінгу залежить від двох показників: винагороди за блок та складності. Постійно зростаюча складність видобування зумовлює зниження прибутковості майнінгу.

З січня 2015 р. майнінг Bitcoin (BTC) з використанням малої кількості

графічних карт став нерентабельним, оскільки дохід не міг покривати витрати на оплату електроенергії. Тепер генерація криптовалюти переважно проходить в умовах, так званих, «ферм», які є каскадами з графічних процесорів або спеціальних пристроїв, що підключені до одного або кількох комп'ютерів. Комп'ютери всієї цієї системи генерують певні ланцюги – блоки. Кожен комп'ютер збирає власний ланцюжок окремо від інших і, якщо йому вдасться виконати цю задачу раніше за інших, то він отримує винагороду у вигляді фіксованої суми. Видобування електронних «монет» відбувається блоками, а не по одному Bitcoin. Спочатку такий блок становив 50 BTC, а потім поступово зменшувався. Періодичне зменшення таких блоків не дозволяє створити більше ніж 21 млн. BTC.

Для оцінки зусиль, які необхідно докласти для майнінгу використовують показник складності (complexity) – відносна складність генерування необхідного підпису блоку. Складність еквівалентна 1 відповідає досягненню мети, в якій тридцять два перших біта нулі. Отже, для генерації підпису блоку необхідно в середньому 2^{32} помноженому на складність спроб (ХЕШ SHA-256). Складність перераховується усіма біткоін-клієнтами приблизно раз на 2 тижні, таким чином, щоб швидкість генерації блоків складала приблизно 6 блоків за годину. Складність генерації має тенденцію до постійного зростання [1].

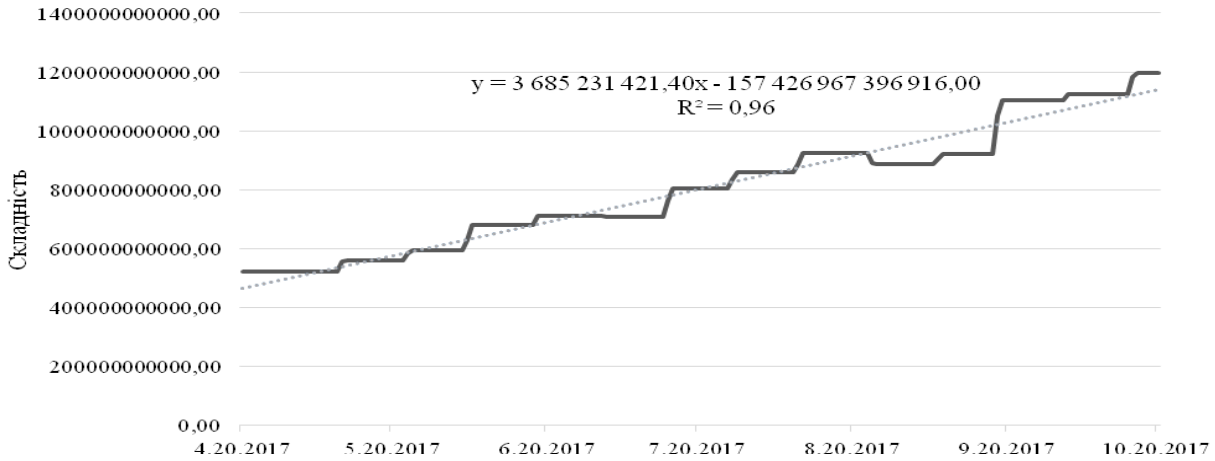

Рисунок 1 – Складність майнінгу Bitcoin в період 20.04.2017р. – 20.10.2017р.

Джерело: побудовано автором за даними [2]

Для зменшення впливу стохастичного фактору і рівномірного та передбачуваного отримання Bitcoin, майнери долучаються до пулів. Особливістю криптографічної задачі є змога застосувати максимальне розпаралелювання обчислень, тобто кожен член пулу генерує власний ланцюг, який не пов'язаний з діями інших та відсилає його пулу, який здійснює соло-майнінг. Отримані Bitcoin пул розподіляє між учасниками за заздалегідь встановленими пулом правилами (рис. 2).

Рисунок 2 – Види нарахування винагород

Джерело: побудовано на основі [1]

Отже, постійно зростаюча складність майнінгу Bitcoin є загрозою розвитку криптовалюти, адже зі збільшенням рівня складності зменшується прибутковість майнінгу, що змушує майнерів видобувати інші криптовалюти. Зменшення кількості активних майнерів є негативним явищем, адже саме вони забезпечують функціонування криптовалютних платіжних систем.

Список використаних джерел:

1. Сложность сети биткоин [Электронный ресурс]. – Режим доступа: http://bitcoin-evolution.com/bitcoin-network-complexity-history/

2. Bitcoin stats [Electronic resource]. – Access mode: https://blockchain.info/stats

V. Andres, A. Burkovska. The increasing complexity of Bitcoin mining as a threat to its development.

Summary

The paper considers the problem of the ever-increasing complexity of the Bitcoin property, which negatively affects its profitability. Reducing the profitability of the property is a significant threat to the functioning of the Bitcoin payment system.

Keywords: cryptocurrency, Bitcoin, mining, complexity, block, pool.