УДК 003.26

«ДОКАЗ РІВНОГО ВКЛАДУ» В ТЕХНОЛОГІЇ BLOCKCHAIN

М. С. Соловйова[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі запропоновано новий підхід «майнінгу» та досягання узгодження в технології побудови ланцюгу блоків (*«блокчейн»*). Розроблений метод дає змогу зменшити використання зовнішніх ресурсів для генерації кожного наступного блоку ланцюга, не знижуючи при цьому децентралізацію всієї системи.

Ключові слова: ланцюг блоків, майнінг, децентралізація, алгоритм доказу роботи

Вступ

Технологія блокчейн – потужний інструмент, який при узгодженні та верифікації дій користувачів усуває використання сторонніх інстанцій, посередників та централізованих джерел довіри. Електронна валюта («криптовалюта») біткоін [1], побудована на технології блокчейн, стала першою в історії децентралізованою базою даних нового виду фінансового кругообігу. Забезпечення децентралізації, що надає всебічну довіру користувачів, є ключовим моментом технології блокчейн і стає все більш актуальним з плином часу.

1. Модель використання блокчейну та альтернативи підходу «Proof-of-works»

В основі структури зберігання транзакцій в біткойнах та інших криптовалютах лежить розподілена база даних блокчейн, в якій знаходиться вся історія транзакцій. Блокчейн отримав свою назву тому, що транзакції збираються в блоки; кожен блок (крім найпершого) посилається на попередній. Кожен вузол, який бере участь в мережі біткойнів, має свою копію блокчейна.

Вузли синхронізуються між собою за допомогою пірингової (P2P) мережі [2]. Будь-яка реалізація криптовалюти повинна бути здатна захистити свій блокчейн від можливих атак. Так як безпека блокчейна не покладається на єдиний центр, користувачі не знають, яка версія бази даних є дійсною. У біткойнів безпека мережі забезпечується алгоритмом доказу роботи («Proof-of-works») у формі здобутку («майнінгу») блоків. Кожен вузол, який бажає брати участь в майнінгу, повинен вирішити обчислювально складну задачу, щоб гарантувати дійсність нового блоку; нагорода за рішення виплачується у вигляді нових біткойнів.

Таким чином, функціонування розподіленого алгоритму узгодження підтримується фізично рідкісними ресурсами, серед яких спеціалізоване обладнання для проведення обчислень та електрика, необхідна для роботи обладнання.

«Proof-of-works», крім споживання величезної кількості енергії, також має суттєві недоліки. Майнери організовуються в майнінг-пули («mining pools»), і оператор пулу теоретично може контролювати більшу частину обчислювальних потужностей мережі. З цієї точки зору децентралізація втрачається, і один великий гравець може контролювати всю мережу. Це породжує пошук нових підходів забезпечення верифікації блоків, що додаються до блокчейну.

Розглянемо функціонування підходу «Proof-of-stake», що став однією з найпопулярніших альтернатив «Proof-of-works». Він полягає у тому, що складність вирішення деякої задачі для додавання блоку в блокчейн в даному випадку розподіляється пропорційно і відповідно до балансу кожного майнера. Таким чином, вузол мережі з великим балансом має більше шансів згенерувати наступний блок. Ця схема виглядає досить привабливою, перш за все через невеликі вимоги до обчислювальних ресурсів. Але звичайний перехід до «Proof-of-stake» здатний знизити стійкість протоколу консенсусу [3]. Іншою запропонованою альтернативою став «Proof-of-activity» [4], що по суті став поєднанням «Proof-of-works» та «Proof-of-stake», але, на жаль, він є лише теоретичним.

2. «Доказ рівного вкладу»

В даній роботі пропонується модель під назвою «Доказ рівного вкладу», що може виступати алгоритмом доказу роботи разом із підходом «Proof-of-works», усуваючи основні його недоліки.

2.1. Ідея пропонованого підходу

Основним критерієм, якому повинна задовольняти нова модель, є зниження можливості монополізації майнінг-пулами, що мають найбільшу обчислювальну потужність, ринку здобутку блоків у блокчейні, що в свою чергу зменшить використання зовнішніх ресурсів програмного забезпечення.

[a] marinaby13@gmail.com

Перше, що варто розглянути, це яку саме задачу доведеться вирішити майнеру згідно з підходом «Proof-of-works», щоб додати блок до ланцюгу інших, адже новий підхід «Доказ рівного вкладу» вирішує ту саму задачу, але у свій спосіб. Отже, під час добування майнером блоку працює програмне забезпечення, яке шукає розв'язок дуже складного математичного завдання (знаходження гешу, що відповідає деяким вимогам [5]), складність якого заздалегідь точно відома. Коли рішення буде знайдено, майнер може повідомити всім про існування знайденого ним рішення поряд з іншою інформацією, яке разом з нею утворює блок. Майнери не просто використовують транзакції в блоці для генерації гешу. Деякі інші фрагменти даних використовуються, наприклад, геш останнього блоку, що зберігається в блокчейні. І оскільки гешування кожного блоку проводиться з використанням геш-блоку перед ним, він стає цифровою версією воскової печатки. Вона підтверджує, що цей блок – і кожен блок після нього – є легітимними, бо якщо навпаки, то він буде помічений як підробка й всі користувачі знатимуть про це. Крім того, майнери не повинні втручатися в дані транзакції, тому вони доповнюють їх додатковими випадковими фрагментами, що мають назву «nonce», щоб геш відрізнявся. Якщо результат не відповідає необхідному формату, то цей фрагмент змінюється, і все гешується знову. Таким чином, геш починається з певного числа нулів. Число нулів визначається ціллю (target), що являє собою 256-бітове число і тому воно надзвичайно довге. Всі біткоін-клієнти знають ціль.Чим складніше здобувати біткоіни, тим більше провідних нулів потрапило у геш. Саме рішення – віднайдений геш, що задовольняє всі необхідні умови, і є доказом правильності роботи.

2.2. Опис моделі

Загальна складність вирішення задачі знаходження потрібного гешу з самого початку ділиться на частини *«targetParty»* фіксованого розміру S, що не буде змінюватися у майбутньому. Так, чим більша складність встановленої задачі, тим з більшої кількості *targetParties*-частин вона буде складатися. Нагорода за кожен здобутий блок розподіляється між всіма майнерами по-рівну і лінійно залежить від кількості *targetParties*.

«Доказ рівного вкладу» використовує протокол BitTorrent [6] для визначення майнерів, які будуть брати участь у додаванні певного блоку в блокчейн. Завдяки BitTorrent протоколу вузли поєднуються P2P [7], а це означає, що комп'ютери в BitTorrent мережі мають можливість передавати дані між собою без необхідності центрального сервера. Після підключення до мережі BitTorrent клієнт отримує біти файлів в торрентах у частинах визначеного розміру S. Оскільки кожен вузол отримує новий сегмент файлу він стає джерелом (тієї частини) для інших вузлів, звільняючи вихідний об'єкт від того, щоб відправити цю частину до кожного комп'ютера або користувача, бажаючого копію. Кожна частина захищена за допомогою криптографічного гешу, що міститься в дескрипторі торрента. Це гарантує, що будь-яка зміна сегменту може бути виявлена, що, таким чином, запобігає випадковій і шкідливі модифікації кожної із частин, отриманих на інших вузлах. За допомогою BitTorrent завдання розповсюдження файлу доступне для тих, хто хоче його отримати. Але з іншого боку число клієнтів обмежене, адже коли всі частини від загальної складності вирішення задачі розподілені, поширення цих частин в мережі припиняється. Крім того, майнери, щоб отримати можливість здобути одну з *targetParties*, повинні задовольняти вимогам програмного забезпечення в залежності від складності задачі [8], адже здобуття блоку має виконуватися за обмежений відрізок часу, що є загально еталонним. Додатковим обмеженням для майнерів також є неможливість переходу до отримання іншої *targetParty*, тобто розпочинати роботу надо наступним блоком, поки не закінчене опрацювання попереднього.

Висновки

У даній роботі запропоновано новий підхід майнінгу «Доказ рівного вкладу», що допомагає досягнути узгодження в побудові ланцюгу блоків блокчейну. Він усереднює можливість для кожного майнера здобувати блоки, фіксуючи потреби у програмному забезпечені,і тим самам зменшує використання зовнішніх ресурсів, не знижуючи при цьому децентралізацію мережі.

Перелік використаних джерел

1. Antonopoulos Andreas M. Mastering Bitcoin. — 2015. — URL: http://chimera.labs.oreilly.com/books/1234000001802.
2. Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008. — P. 9. — URL: https://bitcoin.org/bitcoin.pdf.
3. Patterson Ray. Alternatives for Proof of Work, Part 1: Proof Of Stake. — 2015. — URL: https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/.
4. Patterson Ray. Alternatives for Proof of Work, Part 2: Proof of Activity, Proof of Burn, Proof of Capacity, and Byzantine Generals. — 2015. — URL: https://bytecoin.org/blog/proof-of-activity-proof-of-burn-proof-of-capacity/.
5. What is bitcoin difficulty? — 2015. — URL: http://bitcoin-difficulty.com/.
6. BitTorrent.org. For developers. — 2008. — URL: http://www.bittorrent.org/beps/bep_0003.html.
7. Johnsen Jahn Arne, Karlsen Lars Erik, Birkeland Sebjørn Sæther. Peer-to-peer networking with BitTorrent. — 2005. — URL: http://web.cs.ucla.edu/classes/cs217/05BitTorrent.pdf.
8. How Bitcoin Mining Works. — 2011. — URL: https://www.bitcoinmining.com/.