DOI 10.31891/2307-5732-2021-297-3-30-33
УДК 637.5.02

В. В. КУЧКОВСЬКИЙ
Національний університет "Львівська політехніка"

АЛГОРИТМИ КОНСЕНСУСА БЛОКЧЕЙН-СИСТЕМ

У статті описані алгоритми консенсусу їх позитивні та негативні моменти. Дано опис алгоритмам та приведений приклад вирішення даної проблеми. Наведено приклад використання декількох консенсусів в блокчейн мережах. Описані такі консенсуси як Proof of Work, Proof of Capacity, Proof of Authority, Proof of Activity, Proof of Importance, Proof of Stake, а також його підвиди: LPoS, DPoS. Роказані нюанси про змішаний вид консенсусів та наведені приклади таких криптовалют і систем. Приведені приклади хеш-функцій, мастернод, а також ключові особливості певних криптовалют зі змішаним консенсусом. Зроблені висновки.

Ключові слова: *блокчейн, криптовалюта, консенсус, алгоритми.*

V. V. KUCHKOVSKY
Lviv Polytechnic National University

BLOCKCHAIN SYSTEM CONSENSUS ALGORITHMS

This article describes the main consensus algorithms, their positive and negative aspects. Consensus in the general sense means a way to come to an agreement. In the blockchain, which is a decentralized system that does not have a single governing body, various algorithms have been developed to achieve consensus. In a blockchain network, it does not matter whether the system participants trust each other or not. They must agree on certain principles of work that will apply to everyone. And this is a direct function of the consensus mechanism. Algorithms are described and an example of solving this problem is given, namely the problem of choosing a consensus for future systems. An example of using multiple consensuses in blockchain networks is given. Such consensuses as Proof of Work (PoW), proof of Capacity (PoC), proof of Authority (PoA), proof of activity (PoAA), proof of Importance (PoI), proof of Burn (PoB), proof of Stake (PoS) are described, as well as its subspecies: Leased Proof-of-Stake (LPoS), Delegated Proof-of-Stake (DPoS). Many different nuances about the mixed type of consensus are described and examples of such cryptocurrencies and systems are given. The subtleties of mining for each consensus are described. Examples of hash functions, masternodes, nodes, algorithms, as well as key features of certain cryptocurrencies with mixed consensus are given. It is concluded that the choice of consensus for building systems based on blockchain.

Keywords: blockchain, cryptocurrency, consensus, algorithms, pow, pos, dpos, poa, lpos, poi, pob, poc.

Постановка проблеми

Blockchain – розподілена децентралізована мережа, яка забезпечує незмінність, конфіденційність, безпеку та прозорість. Не існує центрального органу для перевірки та перевірки транзакцій, проте кожна транзакція в блокчейні вважається повністю захищеною та перевіреною. Це можливо лише завдяки наявності консенсусного протоколу, який є основною частиною будь-якої мережі Blockchain [1].

Алгоритм консенсусу – це процедура, за допомогою якої всі однолітки мережі Blockchain досягають спільної згоди щодо поточного стану розподіленої книги. Таким чином, консенсусні алгоритми досягають надійності в мережі Blockchain та встановлюють довіру між невідомими однолітками у розподіленому обчислювальному середовищі. По суті, консенсус-протокол гарантує, що кожен новий блок, який додається до блокчейну, є єдиною версією істини, узгодженою усіма вузлами в блокчейні.

Протокол консенсусу Blockchain складається з деяких конкретних цілей, таких як досягнення згоди, співпраця, співпраця, рівні права для кожного вузла та обов'язкова участь кожного вузла в процесі консенсусу. Таким чином, алгоритм консенсусу спрямований на пошук спільної згоди, яка є виграшем для всієї мережі. Останнім часом на блокчейн ринку представлено дуже багато алгоритмів консенсуса. Можна задати собі питання, який з алгоритмів є кращий, в яких є свої переваги і недоліки.

Стаття аналізує види блокчейн алгоритмів консенсуса, та відповідає на питання, який з перелічених алгоритмів є самим кращим. Цілями статті є також вивчення можливостей комбінації різних алгоритмів консенсусу.

Аналіз літературних джерел

Один з головних алгоритмів консенсусу є PoW (Proof-of-Work), доказ роботи. Ймовірно завдяки біткоїну, алгоритм консенсусу PoW є найбільш відомим способом підтвердження транзакцій в блокчейні. Основна ідея полягає в тому, щоб вузли блокчейн-мережі, що підтверджують транзакції, виконували досить складну обчислювальну роботу (прорахунок алгоритму), результат роботи якого був би легко і швидко перевіряємо іншими вузлами мережі [2].

Перший вузол, який повністю провів усі необхідні обчислення, отримує винагороду від блокчейн-мережі. Усі вузли борються між собою, нарощуючи ємність обчислювальних ресурсів, щоб виявитися тим самим, першим вузлом, який отримав винагороду.

Недоліком цього алгоритму є вагомі енергетичні витрати: велика кількість вузлів виробляють обчислення, але в реальності тільки один, перший, проводить успішну роботу і отримує винагороду.

Згаданий алгоритму використовує Bitcoin та його похідні форки як Litecoin, Dash тощо.

Другий з популярних алгоритмів консенсусу є PoS (Proof-of-Stake), доказ стейкінгу. Його суть заключається в тому, що творцем наступного блоку в ланцюжку блоків вибирається вузол, який володіє

великим балансом – кількістю ресурсів. Наприклад, в криптовалютах створює блок, той, у кого на балансі величезна кількість монет. За саме створення блоку вузол винагороду не отримує. Винагорода виплачується за проведення транзакції [3].

Можливі два варіанті таких вузлів: вузол з найбільшою кількістю монет, або вузол, який був запущений раніше за всі інші, тобто чим довше вузол працює, тим є більше вірогідність того, що він підтвердить і створить блок, який внесе в блокчейн. Такі блокчейни як Stellar, Decred, Qtum, NEO використовують даний консенсус, також є монети, які використовують декілька варіантів зразу, один з таких яскравих прикладів це Dash, там і PoW і PoS зразу.

Цей вид консенсусу має більше плюсів, ніж мінусів. Один з таких плюсів є істотне зниження споживання електроенергії для генерації ланцюга порівняно з PoW методом. Але є і недолік такого підходу: з нього простіше робити атаки на мережу. Для створення атаки з подвійною розтратою (Double-spending) необхідно сконцентрувати більше 50 % від загальної кількості всіх монет, при захопленні такого вузла (node) можливо порушувати сам ланцюг і зруйнувати його.

Для боротьби з такими діями, був розроблений консенсус DPoS (Delegated Proof-of-Stake), в якого в основі лежить PoS. Одна з особливостей такого алгоритму консенсусу порівняно з Proof-Of-Stake, є те, що блоки підписують вибрані представники. Власники найбільших балансів вибирають своїх представників, кожен з яких отримує право підписувати блоки в блокчейн-мережі. Кожен представник, що володіє одним або більше відсотками від усіх голосів, потрапляє до Ради. Зі сформованої «ради директорів» по-колу вибирається наступний представник, який і підпише наступний блок. У тому випадку, якщо з якої-небудь причини представник пропустив свою чергу в підписанні, він позбавляється делегованих голосів і залишає «раду директорів», після чого на його місце вибирається наступний найбільш підходящий кандидат [4].

Власники балансів, делегуючи свої голоси, жодним чином не втрачають над ними контролю, так як в будь-який момент можу їх відкликати у свого представника. Приклад блокчейнів, де є такий вид консенсусу, – це EOS.

Є ще один варіант модифікації PoS-консенсусу, такий як LPoS (Leased Proof-of-Stake). На даний момент цей консенсус використовує не так багато криптовалют, одна з популярних криптовалют WAVES. В рамках цього алгоритму, будь-який користувач має можливість передавати свій баланс в оренду майнінг-вузлам, а за це майнінг-вузли діляться частиною прибутку з користувачами. Таким чином, даний алгоритм консенсусу дозволяє отримати дохід від майнінгової діяльності, не виконуючи самого майнінга [5].

Третій з таких алгоритмів консенсусу є PoC (Proof-of-Capacity), доказ пропускної здатності. Цей консенсус використовує тільки один альткоїн Burstcoin. Особливість PoC полягає в таких принципах:

– кожен майнер обчислює досить великий обсяг даних, який записується на дискову підсистему (жорсткий диск, хмарні системи зберігання) вузла. Такий початковий набір даних в PoC називають «ділянкою»;

– для кожного нового блоку в блокчейні, майнер читає невеликий набір даних (1/4096, що приблизно становить 0.024 %) від свого загального збереженого обсягу і повертає результат, як минулий час в секундах з моменту створення останнього блоку, після якого майнер зможе створити новий блок;

– майнер, який отримав мінімальний час дедлайну, підписує блок і отримує винагороду за транзакції.

Четвертий вид консенсусу PoI (Proof-of-Importance), доказ важливості. Алгоритм консенсусу використовуваний блокчейн-платформою NEM. Значимість кожного користувача в мережі NEM визначається як кількість коштів наявних у нього на балансі і кількість проведених транзакцій з/на його гаманець. На відміну від більш звичного PoS, який враховує тільки баланс наявних коштів у користувача, PoI враховує як кількість коштів, так і активність користувача в блокчейн-мережі. Такий підхід залучає користувачів не просто тримати кошти у себе на рахунку, а й активно використовувати їх.

П’ятий вид консенсусу PoA (Proof-of-Activity), доказ активності. Його суть полягає в тому, що автори алгоритму PoA спробували об'єднати два найбільш популярних алгоритму, такі як Proof-of-Work і Proof-of-Stake, з метою збільшення рівня захисту від потенційно можливих атак (51 % attack, Denial-of-Service attacks (DoS).

Принцип роботи такого алгоритму наступний:

– кожен майнер блокчейн-мережі пробує згенерувати заголовок порожнього блоку, який включає в себе хеш попереднього блоку, публічний адресу майнера, індекс поточного блоку в блокчейні і nonce число;

– після генерації заголовка порожнього блоку відповідає поточним вимогам складності, вузол розсилає цей заголовок в блокчейн-мережу;

– всі вузли мережі розглядають заголовок такого блоку, як дані отримані від псевдовипадкових власників. Використовуючи хеш розісланого заголовка блоку і хеш попереднього блоку + N пресетів з використанням алгоритму follow-the-satoshi вибираються стейкхолдери;

– кожен стейкхолдер, що знаходиться в онлайні, перевіряє отриманий, порожній заголовок блоку на його коректність. Під час перевірки кожен отримав заголовок перевіряє чи є він одним з перших N-1 стейкхолдерів «щасливчиків» цього блоку і в цьому випадку підписує заголовок порожнього блоку своїм секретним ключем і відправляє його в блокчейн-мережу;

– коли n-й стейкхолдер бачить, що він повинен стати підписантом цього блоку, він, на додаток до заголовка порожнього блоку, додає блок з включеними транзакціями (кількість включених транзакцій він вибирає сам), всі підписи N-1 від інших стейкхолдерів і підписує блок;

– стейкхолдер N розсилає новий, підготовлений блок. Вузли отримують цей блок, переконуються в його законності і додають цей блок в блокчейн;

– премія за виконані транзакції, яку отримав *N*-стейкхолдер, розподіляється між майнером та *N*-стейкхолдерами, так званими «везунчиками».

Одна з монет, яка використовує даний консенсус, є Decred.

Шостий вид консенсусу PoAuthority (Proof-of-Authority), доказ авторитетності. Цей вид консенсусу використовує одна з популярних монет, як VeChain. PoA алгоритм консенсусу відрізняється від інших алгоритмів тим, що для своєї роботи йому не потрібно мати взагалі ніякого майнінга, як у випадку з PoW або POS. У блокчейн-мережі, що базується на PoAuthority, всі транзакції і блоки перевіряються за допомогою схвалених акаунтів (валідаторів). Проведення транзакцій і створення блоків, проходить в автоматичному режимі за допомогою обчислювальних потужностей валідатора.

Позитивним моментом даного алгоритму є відсутність майнінгу і, як наслідок, величезне зниження витрат на його обслуговування.

Негативний момент використання даного алгоритму: валідатори приводять до централізації мережі. Це робить мережу вразливою, так як сама суть блокчейну це децентралізований ланцюг блоків. В приватних мережах, для вузько-направлених задач ймовірно це має сенс, так як там не потрібно децентралізації як такої.

Сьомий вид алгоритму консенсусу Proof-of-capacity або Proof-of-space (PoSpace) – метод захисту криптовалют, заснований на використанні вільного місця на пристрої зберігання файлів заздалегідь виділеного користувачами. Метод є менш енерговитратним способом у порівнянні з PoW. Прикладом монет на такому консенсусу є Chia. За допомогою відкритого ключа генерується файл певного розміру, в якому генеруються усі можливі ключі. Далі вказаний файл використовується для пошуку наступних блоків. Майнінг на жорсткому диску відрізняється тим, що для виконання роботи не потрібно купівлі дорогих відеокарт, блоків живлення великої потужності і материнських плат з величезним числом рознімів.

Алгоритм Proof of Space дуже схожий на алгоритм консенсусу Proof of Work, тільки в ньому замість обчислювальної потужності використовується обсяг пам'яті для зберігання.

Восьмий і заключний алгоритм консенсусу є PoB (Proof-of-Burn), доказ спалювання. Цей алгоритм є популярний в монетах, де є величезна кількість монет, тобто велика емісія. Він відбувається наступним чином: майнер відправляє монети на випадкову адресу з випадкового генерованого хешу, витратити кошти з цієї адреси практично неможливо, так як ймовірність підібрати до нього ключі прагне до нуля. За таке спалювання монет майнер отримує постійний шанс знайти PoB блок і отримати за нього нагороду. Шанси на майнінг збільшуються при збільшенні кількості спалених монет. Економічно цей процес спалювання монет можна уявити як купівлю бурової установки для майнінгу. Природно, такий алгоритм має сенс використовувати тільки на пізніх етапах існування тієї чи іншої криптовалюти, тоді коли є що «спалювати». Сам алгоритм не є популярний, його використовують дуже мало монет. Однією з таких монет була Slimcoin.

Виклад основного матеріалу. Комбінування алгоритмів консенсусу

Як було зазначено у попередньому підрозділі, в кожного консенсусу є позитивні і негативні моменти. Щоб обійти дану проблему, необхідно комбінувати алгоритми. Одна з таких популярних комбінацій є PoS + PoW. Це є актуально, коли Proof-of-Work консенсус впирається в складність мережі, комбінування допомагає добувати блоки зразу двома способами і збільшувати кількість користувачів криптовалюти. Одні майнять за допомогою апаратури і знаходять блоки по певному алгоритму, а інші запускають основні вузли (master node) з великою кількістю монет і теж добувають блоки.

Метою гібридних систем Proof of Work і Proof of Stake є виявлення переваг відповідних підходів і їх використання для врівноваження слабких сторін один одного. Decred – це одна з небагатьох криптовалют, яка використовує PoW і PoS в їх початкових формах і об'єднує їх разом для створення багатофакторного або гібридного консенсус механізму.

«Монети мастернод» в певному сенсі також є гібридами в тому, що вони мають один з компонентом пов'язаний з Proof of Work, який виконує ту ж роль, що і в біткойн, і додаткову роль для спеціальних вузлів. Як правило, існує обов'язкова вимога, щоб ці спеціальні вузли тримали певну кількість валюти, щоб продемонструвати, що їм можна довіряти, і вони діють в найкращих інтересах мережі, що за аналогією має відношення до Proof of Stake.

Це непоганий варіант так як пропонує на вибір різні альтернативи. Хороший приклад такої монети - це Dash. Дана монета має алгоритм X11, його дуже складно майнити, так як сам алгоритм використовує ланцюжок з 11 алгоритмів типу криптографічної хеш-функції для доведення виконання роботи. Сам алгоритм X11 придумав головний розробник Dash з метою ускладнити використання спеціалізованого обладнання для майнінгу. Для того було в монеті введена альтернатива як мастерноди. На адрес відправляються 1000 монет і реєструється в мережі мастер-нода. Мастерноди використовуються для приватної відправки монет через змішування (неможливість відслідкувати відправника).

Можна ще для прикладу навести монету NIX. Алгоритм генерації монет Lyra2REv2. Цей алгоритм якісно обробляється на GPU. Тобто, майнери майнять монету на відеокартах, та збільшують емісію. Спочатку був консенсусу PoW (для початкової генерації монет в обіг), а потім вся криптовалюта перейшла в консенсус LPoS, коли майнінг вже не можливий, а тільки стейкінг через мастерноди.

На даний момент на ринку представлено понад 8000 різних криптовалют, які працюють на різних алгоритмах консенсусу, на різних алгоритмах генерації монет, та з абсолютно різними функціями.

Висновки

Залежно від необхідних функцій майбутньої блокчейн-системи потрібно вибирати і його консенсус. Конкретних правил, які треба дотримуватись тут немає. Аналізувати користь консенсусу треба на основі позитивних і негативних аспектів при плануванні самої блокчейн-системи. Тобто в залежності від майбутнього функціоналу, можна комбінувати консенсуси. Proof-of-Stake консенсус можна використовувати для анонімних транзакцій, а стандартний Proof-of-Work для емісії.

Перспективами подальших досліджень є комбінування алгоритмів консенсусу для досягнення стійкості та невразливості системи.

Література

1. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

2. Plotnikov, V., & Kuznetsova, V. (2018). The Prospects for the Use of Digital Technology “Blockchain” in the Pharmaceutical Market. In *MATEC Web of Conferences* (Vol. 193, p. 02029). EDP Sciences.

3. Pastor, I. G., Olaso, J. R. O., & Fuente, F. S. Unveiling the Opportunities of Using Blockchain in Project Management. *Research and Education in Project Management (Bilbao, 2018)*, 22.

4. Kushch, S., & Prieto Castrillo, F. (2017). A review of the applications of the Block-chain technology in smart devices and dis-tributed renewable energy grids.

5. Andreas M. Antonopoulos. (2014, December). Mastering Bitcoin: Programming the Open Blockchain, 28.

References

1. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

2. Plotnikov, V., & Kuznetsova, V. (2018). The Prospects for the Use of Digital Technology “Blockchain” in the Pharmaceutical Market. In *MATEC Web of Conferences* (Vol. 193, p. 02029). EDP Sciences.

3. Pastor, I. G., Olaso, J. R. O., & Fuente, F. S. Unveiling the Opportunities of Using Blockchain in Project Management. *Research and Education in Project Management (Bilbao, 2018)*, 22.

4. Kushch, S., & Prieto Castrillo, F. (2017). A review of the applications of the Block-chain technology in smart devices and dis-tributed renewable energy grids.

5. Andreas M. Antonopoulos. (2014, December). Mastering Bitcoin: Programming the Open Blockchain, 28.

В. В. КУЧКОВСЬКИЙ ORCID ID: 0000-0002-7941-6329 volodymyr@kuchkovskiy.com

Рецензія/Peer review : 07.05.2021 р. Надрукована/Printed :30.06.2021 р.