МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

КОЛЕКТИВНА МОНОГРАФІЯ

СТРАТЕГІЇ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМАХ УПРАВЛІННЯ

ХЕРСОН, 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

СТРАТЕГІЇ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМАХ УПРАВЛІННЯ

Колективна монографія
за загальною редакцією

кандидата технічних наук, доцента

Райко Галини Олександрівни

Херсон, 2019

УДК 330.111.66:005.8
С-83

Рекомендовано до друку
Вченою Радою Херсонського національного технічного університету
(протокол №7 від 05.07.2019)

Рецензенти:

Фісун М.Т. д.т.н., професор, завідувач кафедри інженерії програмного забезпечення Чорноморського національного університету ім. Петра Могили

Бараненко Р.В. к.т.н., доцент, професор кафедри професійних та спеціальних дисциплін Херсонського факультету Одеського державного університету внутрішніх справ Міністерства внутрішніх справ України

Авторський колектив: Ходаков В.Є., Соколов А.Є., Веселовська Г.В., Барташевська Ю.М., Сапрон А.В., Райко Г.О., Чебукін Ю.В., Сидорук М.В., Сидорук В.В., Данилець Є.В., Козел В.М., Цивільський Ф.М., Дроздова Є.А., Хапов Д.В., Соколова О.В., Димова Г.О., Димов В.С., Лєпа Є.В., Письменний І.В., Конох І.С., Григорова А.А., Карамушка М.В.

С-83 Стратегії, моделі та інформаційні технології в системах управління : колективна монографія / За загальною редакцією Райко Г.О. – Херсон: Книжкове видавництво ФОП Вишемирський В.С., 2019. – 152 с.

ISBN 978-617-7783-24-3

Колективна монографія присвячена застосуванню інформатичних технологій в економіці, освіті та управлінні проектами.

Колективна монографія розрахована на фахівців у галузі економіки, інформаційних технологій, фінансів, банківництва, державного управління, науковців, викладачів, аспірантів, магістрів та студентів.

Матеріали монографії представлено у авторській редакції.

ISBN 978-617-7783-24-3

ЗМІСТ

РОЗДІЛ 8

АНАЛІЗ АЛГОРИТМІВ БЛОКЧЕЙН-КОНСЕНСУСУ

Хапов Д.В.
к.т.н., доцент кафедри інформаційних технологій,
Херсонський національний технічний університет

Поточне десятиліття – цікавий час розвитку децентралізованих технологій. Незважаючи на всі зусилля, які протягом попередніх тридцяти років прикладали криптографи, математики та кодувальники, розробляючи строго спеціальні вдосконалені протоколи для захисту конфіденційності та гарантій автентичності різних систем – від електронної валюти до голосування і передачі файлів, – досягнутий прогрес був невеликий. Інноваційно блокчейн – або, взагалі кажучи, інноваційний суспільно-економічний консенсус, запропонований в 2009 році Сатоши Накамото, – виявився тим самим відсутнім фрагментом головоломки, який зміг надати цій індустрії імпульс для гігантського стрибка вперед. Замість того щоб просто сподіватися на чесність наших контрагентів, ми впроваджуємо технологічні системи з такими властивостями, які будуть забезпечувати необхідні гарантії навіть у разі, якщо багато наших партнерів поведуть себе нечесно [1].

Блокчейн – це розподілена база даних транзакцій, яку можна порівняти з величезним децентралізованим і розподіленим журналом, де, завдяки Інтернету, прозоро захищені і автономно зберігаються і перетворюються дані, при цьому центральний контролюючий орган відсутній. Ця книга активна, складена в хронологічному порядку, розподілена, перевіряема і захищена від фальсифікації за допомогою системи розподілу довіри (консенсусу) між учасниками (вузлами). Кожен учасник мережі має актуальну копію цього журналу, вміст якого весь час синхронізується з усіма іншими учасниками. Таким чином, блокчейн:

– дозволяє автоматизувати транзакції, не залучаючи при цьому третьої сторони;

– є системою розподіленого консенсусу і довіри;

– представляє собою інфраструктуру, що забезпечує підтвердження автентичності та нотарізацію [2].

Блокчейн – це послідовність блоків – ланцюжок (рис. 1), а не замкнуте коло або щось ще. Кожен з блоків містить масив певних даних. І все блоки пов'язані між собою. Тобто, новий «масив» може бути створений тільки після того, як закритий старий масив.

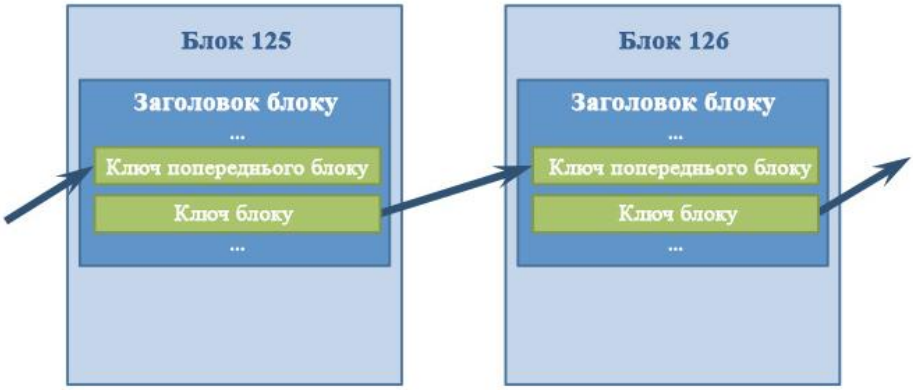

Рис. 1. Послідовність блоків блокчейну

Як видно з рис. 1, кожна ланка ланцюжка містить певний ключ. Поки він не буде розшифрований, блок не закривається. Механізми розшифрування можуть бути різними, у криптовалютах за це відповідає майнінг. Майнер, що займаються видобутком криптовалюти, роблять це за допомогою потужностей відеокарт і процесорів. Ті в свою чергу виконують обчислювальні операції, головна мета яких – пошук криптографічного підпису до блоку у вигляді хешу. Як тільки він підібраний – блок закривається, а майнер за це отримує винагороду у вигляді криптовалюти [3].

На блокчейн ринку представлено досить багато алгоритмів консенсусу, які дозволяють вибрати хто є найбільш підходящим вузлом для підписання наступного блоку. Частина з них добре відома і використовується часто, наприклад PoW (Proof of Work), а частина тільки намагається пробити собі місце "під сонцем".

Дослівно Proof of Work перекладається як «доказ роботи» або доказ виконаної роботи. Якщо інтерпретувати цей переклад на сферу криптовалют, то за роботу тут приймаються обчислювальні операції обладнання. Proof of Work – це такий собі механізм перевірки того, що робота (майнінг) була проведена.

Саме принцип PoW лежить в основі валідації транзакцій в блокчейні біткойнів. Також цей алгоритм консенсусу використовується в десятках інших криптовалют, в яких є можливість майнінгу.

Механізм Proof of Work з'явився ще до початку криптовалют. Його основна мета – це захист сервера від постійних запитів (DDos-атак, спаму) через додавання спеціального завдання, на вирішення якого необхідно витратити певну кількість часу і ресурсів. При цьому сервер (або просто валідатор) на перевірку буде витрачати набагато менше часу. Механізм PoW призначені саме для обчислювальної техніки.

Можна пояснити принцип його роботи на прикладі звичайного уроку в школі. На уроці математики вчитель дав завдання всьому класу і пообіцяв гарну оцінку (винагороду) тому, хто зробить його першим. Учневі необхідно «розкинути мізками», щоб провести ряд математичних операцій і в результаті вирішити задачу. У випадку з PoW, в якості учня виступає обчислювальна техніка, клас – це, наприклад, мережа Bitcoin з майнерами, учень – це один

майнер або комп'ютер, «розкинути мізками» – значить витратити сили або енергію у випадку з машинами, а хороша оцінка – це винагорода за майнінг.

Ця концепція вперше була презентована ще в 1993 році в науковій статті. Автори, Синтія Двор і Моні Наор пропонували зробити так, щоб доступ до якогось абстрактного ресурсу з'являвся тільки за умови виконання якоїсь ресурсномісткої завдання.

Через три роки Адамом Беком був запущений проект Hashcash, основне завдання якого полягало в захисті від спаму. Він описував механізм так: «Потрібно знайти таке значення X, при якому функція SHA(x) містила б n-ю кількість нульових біт».

А в 1999 вперше з'явився термін Proof of Work – він був запропонований Маркусом Якобсеном і Арі Джуелсом в науковій статті для журналу Communications and Multimedia Security.

Ще в 2004 році Хел Фінні, який пізніше проведе першу транзакцію в історії мережі Bitcoin, пропонував «токенізіровать» PoW, а вірніше RPoW (Reusable-Proofs-of-Work). Тобто, результатом перевірок стали б токени, які в подальшому могли б використовуватися як електронна валюта.

Ну а потім ініціативу в свої руки взяв (взяли, взяла) Сатоши Накамото, заклавши механізм Hashcash як алгоритм консенсусу в мережу Bitcoin, а також запровадивши алгоритм хешування SHA-256. Механізм PoW і використовується в мережі Bitcoin для генерації блоку і безпеки всього блокчейну. У цих блоках і міститься хеш-функція, сума якої завжди менше target (поставленої мети). Це як би показує або пруфірує (proof), що необхідні розрахунки (work) для пошуку блоку були проведені і дає сигнал до того, що блок можна записати в загальний ланцюжок (блокчейн) [4, 5].

При використанні алгоритму SHA256 вихідні дані завжди мають довжину 256 бітів незалежно від розміру вхідних даних. При додаванні будь-якого символу буде отримано інше хеш-значення. Хеш-значення здаються абсолютно випадковими, але отримані в одному випадку результати завжди можна точно відтворити на будь-якому комп'ютері і побачити ті ж самі хеш-значення. Значення nonce застосовується для зміни вихідних даних криптографічною функцією, в нашому прикладі – для зміни SHA256-відбитка для заданого рядка.

Щоб ускладнити завдання із застосуванням цього алгоритму, встановимо конкретну мету: знайти рядок, для якого генерується шістнадцяткове хеш-значення, що починається з нуля. З точки зору теорії ймовірності, якщо вихідні дані хеш-функції розподіляються рівномірно, то нам слід очікувати появи результату з шістнадцятковим префіксом 0 через кожні 16 хеш-значень (оскільки це одна з 16 шістнадцяткових цифр від 0 до F). З точки зору обчислювальної математики це означає пошук хеш-значення, меншого 0x1000000000000000000000000000000000000000000000000000000000000000.
Це значення називають граничним значенням (threshold) цілі (target), а завдання полягає в тому, щоб знайти хеш-значення, яке в числовому вираженні менше мети. Якщо ми зменшуємо цільове (порогове) значення, то задача пошуку хеш-значення, яке менше цільового, стає все більш і більш складним.

Значення nonce, що «перемогло» може бути підтверджено будь-яким «гравцем», незалежно від інших. Будь-який бажаючий може додати значення nonce в кінець рядка, обчислити хеш-значення і перевірити, чи дійсно результат менше цільового значення. Успішний результат також є доказом виконання роботи, оскільки підтверджує, що дійсно виконана робота з пошуку цього значення nonce. Для перевірки потрібно лише одне обчислення хеш-значення, в той час як для знаходження правильного значення nonce було потрібно безліч обчислень, що залежать від складності. Якщо встановити більш низьке цільове значення (складність збільшується), то буде потрібно набагато більше обчислень хеш-значень, щоб знайти відповідне значення nonce, але для перевірки як і раніше буде потрібно лише одне обчислення в будь-якому випадку. Більш того, знаючи цільове значення, будь-хто може оцінити рівень складності, використовуючи для цього статистичні методи, отже, може дізнатися, який обсяг роботи потрібно виконати, щоб знайти правильне значення nonce.

Припустимо, наприклад, що на вузлу є 277 314 блоків в локальній копії структури блокчейну. Останнім відомим вузлу є блок 277 314 с хеш-значенням заголовка:

00000000000000027e7ba6fe7bad39faf3bSa83daed765f05f7d1b7131632249

Потім цей вузол отримує з мережі новий блок і виконує його синтаксичний розбір (парсинг) наступним чином:

{
"size” : 43560,
"version" : 2,
"previousblockhash" :
“00000000000000027e7ba6fe7bad39faf3bSa83daed765f05f7d1b7131632249",
"merkleroot" :
"5e049f4030e0ab2debb92378f53c0a6eO9548aea083f3ab25eld94eall55e29d",
"time" : 1388185038,
"bits" : 1903a30c,
"difficulty" : 1180923195.25802612,
"nonce" : 4215469401,
"tx" : [
"257e7497fb8bc68421eb2c7b699dbab23483160Oe7352f0d9e6522c7cf3f6c77"
,
#[... много транзакций пропущено ...]
"05cfd38f6ae6aa83674cc99e4d75al458cl65b7ab84725eda41d018a09176634"
}

Досліджуючи цей новий блок, вузол знаходить поле previousblockhash, що містить хеш-значення батьківського блоку. Знайдене хеш-значення відомо вузлу – це хеш останнього блоку в ланцюжку з висотою 277 314. Отже, отриманий новий блок є нащадком останнього блоку в ланцюжку і розширює існуючу структуру блокчейну. Вузол додає новий блок в кінець ланцюжка, збільшуючи висоту структури блокчейну до 277 315. На рис. 2 показаний ланцюжок з трьох блоків, пов'язаних з допомогою посилань в поле previousblockhash.

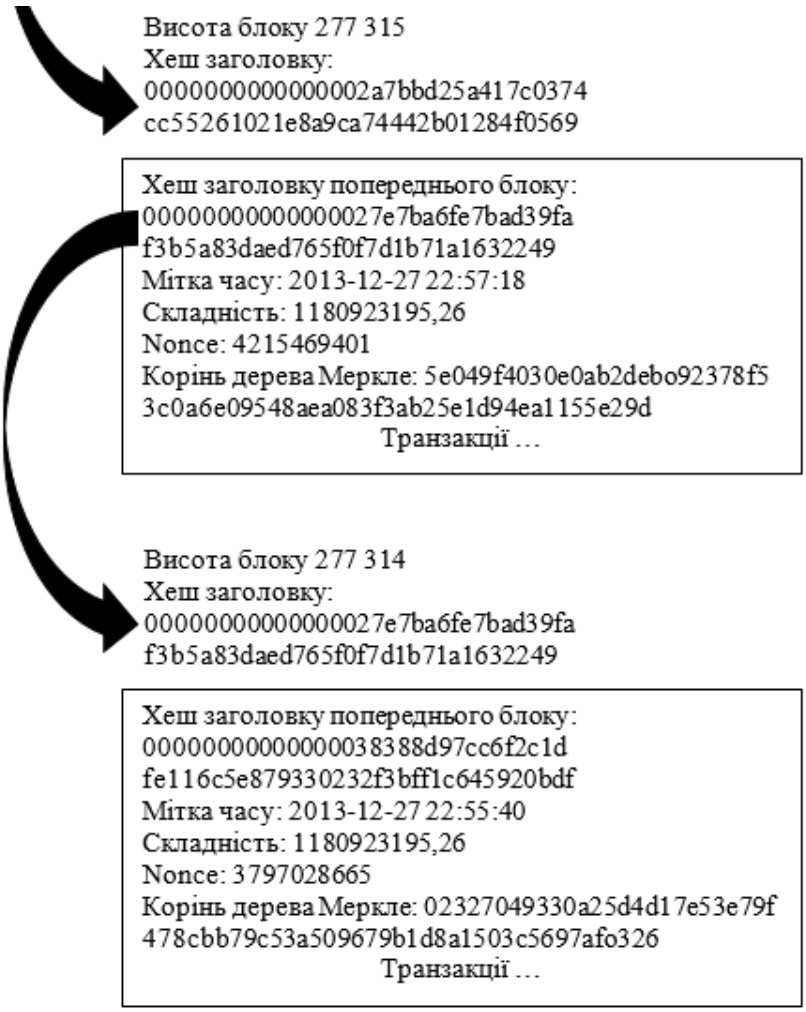

Рис. 2. Блоки, пов'язані в ланцюжок за допомогою посилань на хеш-значення заголовка попереднього блоку

В наведеному вище прикладі ми бачили, що в блоці міститься цільове значення, яке назване «цільовими битами» (target bits) або просто «бітами» (bits). У блоці 277 315 це значення дорівнює 0x1903a30c. Ця форма запису відображає цільове значення завдання доказу виконання роботи (PoW) в форматі коефіцієнт/показник ступеня, де перші дві шістнадцяткові цифри – показник ступеня, а наступні шість шістнадцяткових цифр – коефіцієнт. Таким чином, в розглянутому блоці показник ступеня дорівнює 0x19, а коефіцієнт – 0x03a30c [6].

Для обчислення рівня складності рішення задачі за поданням цільового значення застосовується наступна формула:

$$target = coefficient * 2^{8*(exponent-3)}$$

Використовуючи цю формулу і значення бітів складності (цільових бітів), отримуємо:

$$target = 0x03a30c * 2^{0x08*(0x19-0x03)} = 0x03a30c * 2^{0xB0}$$

У десятковому форматі це значення представлено числом:

$$target = 238348 * 2^{176}$$
$$= 22{,}829{,}202{,}948{,}393{,}929{,}850{,}749{,}706{,}076{,}701{,}368{,}331{,}072{,}452{,}018{,}388{,}$$
$$575{,}715{,}328$$

Основним недоліком цього алгоритму є безглузді енергетичні витрати – велика кількість вузлів виробляють обчислення, але в реальності тільки один (перший) проводить успішну роботу і отримує винагороду.

На противагу Proof of Work був створений інший механізм – Proof of Stake. Дослівно цей термін можна перекласти як доказ частки володіння. Якщо криптовалюта використовує цей алгоритм консенсусу, тоді валідація транзакцій відбувається через вузли мережі. Грубо кажучи, чим більше криптовалюти у людини лежить на гаманці, тим більше шансів у нього знайти новий блок і підтвердити справжність транзакції, отримуючи за це ще й винагороду.

Механізм консенсусу Proof-of-Stake – це вже «криптовалютне» дітище. Тобто, цей метод захисту придуманий суто для використання в криптовалютах. Запропоновано ця ідея до речі була на форумі BitcoinTalk в 2011 році користувачем QuantumMechanic як альтернатива використовуваного в блокчейні Bitcoin Proof-of-Work.

Вже в 2012 році з'явилася перша PoS-криптовалюта – Peercoin (PPC). Хоча в ній використовувався «гібридний» алгоритм. Спочатку це був PoW – на етапі початкового розподілу койнів, а коли їх всіх добули, то вже здійснився перехід на PoS. Перші криптовалюти зі 100% механізмом консенсусу Proof-of-Stake – це Nxt і Blackcoin.

У PoS в якості ресурсу використовується розмір частки (Stake), який і визначає, хто з вузлів в результаті знайде блок і отримає винагороду. Якщо говорити просто і дуже неграмотно, то тут майнінг (видобуток нових монет) відбувається за рахунок наявності монет на гаманці, і чим їх більше – тим вище нагорода. Правда не зовсім майнінг, а форджінг. Вузол, який одержує винагороду за утримання певної частки (stake) ще називають мастернодой.

Мотивація впровадження Proof-of-Stake наступна:

– цей механізм консенсусу в мережі вимагає набагато менше ресурсів в порівнянні з доказом роботи;

– класичної атаки 51% в блокчейні з PoS бути не може – тому що обчислювальні потужності не грають ролі при ранжируванні нодів;

– потенційна атака може статися тільки в тому випадку, якщо в руках одного вузла зосереджено 51% всіх монет – а це дуже і дуже дорого;

– навіть якщо атака відбудеться, то робота блокчейну буде порушена і стороні, що атакувала буде складно отримати з цього вигоду;

– у довгостроковій перспективі комісії при транзакціях в PoS-мережах нижче. Загалом, Proof-of-Stake здається дешевшим, простішим і менш ресурсномістких алгоритмом.

Переваги начебто очевидні. Тим часом, є у PoS і очевидний недолік – потенційно в мережі може виникнути монополія, коли розмір Stake одного

учасника перевищить 51%. Хоча в дестабілізуваному блокчейні з цього складно отримати вигоду, але інші учасники можуть зазнати збитків.

Інша проблема – це потенційна змова групи нод, що може привести до зміни правил блокчейну. Тобто, в PoS існує проблема централізації.

В цілому у Proof-of-Stake здається є ряд очевидних переваг: більш висока швидкість валідації, менші витрати ресурсів для захисту, менші комісії. Але при цьому атакувати мережу з алгоритмом Proof of Work практично неможливо – для цього необхідно супер (багато разів) суперкомп'ютер і кілька електростанцій для його обслуговування.

У Proof-of-Stake все побудовано таким чином, що учасники прагнуть захопити якомога більшу частку койнів, щоб отримувати більшу винагороду за комісію. Через це виникає централізація. Але навіть якщо дестабілізація мережі і не принесе нічого власникам мажоритарної Stake, все одно у цього алгоритму консенсусу є один недолік.

Йдеться про атаку Nothing-at-Stake – це коли створюється ланцюжок порожніх блоків групою користувачів, що в підсумку може призвести до подвійного витрачання, конфлікту версій блокчейну і неминучого форку. Саме над усуненням цієї проблеми займаються розробники нового протоколу Casper, який в майбутньому буде впроваджений в платформу Ethereum. Творець Ефіріума, В.Бутерін, вважає, що перехід на PoS допоможе знизити комісії і загальну вартість обслуговування мережі. А від майнінгу як такого доведеться відмовитися.

У обох протоколів є свої переваги і недоліки. Начебто Proof-of-Stake економічно вигідніше і раціональніше з технічної точки зору, але в таких глобальних платформах як блокчейн Bitcoin або інших криптовалютах з мільярдної капіталізацією, PoW здається більш надійним варіантом. Ще в 2012-2013 роках на ринку почали з'являтися монети з гібридними PoS/PoW протоколами. Серед них Peercoin, Emerecoin, Novacoin і інші.

У міру становлення криптовалют, і все більш глибоких розробок у сфері блокчейну були запропоновані й інші алгоритми, крім механізмів доказів роботи і частки. Деякі з них вже були реалізовані в нових криптовалютах, інші тільки на етапі проекту (табл. 1) [4, 5].

Таблиця 1

Алгоритми знаходження консенсусу

Назва протоколу	Суть
Proof-of-Activity (PoA)	Опис алгоритму опубліковано в 2014 році, як потенційно нового і більш надійного алгоритму. 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 алгоритму: - кожен майнер блокчейн-мережі пробує згенерувати заголовок порожнього блоку, який включає в себе хеш попереднього

	блоку, публічну адресу майнера, індекс поточного блоку в блокчейні і nonce; - після генерації заголовка порожнього блоку, що 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 онлайн, перевіряє отриманий, порожній заголовок блоку на його коректність. Під час перевірки, кожен, хто 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 заголовку порожнього блоку, додає блок з включеними транзакціями (кількість транзакцій, що включаються він обирає 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 транзакції, яку отримав N-стейкхолдер, розподіляється між майнером і N стейкхолдерами "щасливчиками". Класичний приклад – криптовалюта DASH.
Delegated Proof-of-Stake (DPoS)	Одна з різновидів алгоритму консенсусу Proof-Of-Stake, в якій блоки підписують обрані 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 всіх голосів потрапляє до ради. Із сформованої "ради директорів" вибирається (по-колу) 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 обирається наступний найбільш підходящий кандидат. Власники балансів делегуючи свої голоси, аж ніяк не втрачають над ними контролю, так як в будь-який момент можуть їх відкликати у свого представника. Основними перевагами алгоритму DPoS є: - власники балансів мають можливість делегувати свої голоси (при цьому не передаючи сам баланс),

	- власники балансів мають можливість отримати додатковий дохід від їх володіння, - мінімізація витрат на підтримку блокчейн-мережі. На відміну від класичного PoS, знижується кількість "непотрібної роботи" при виборі наступного голосуючого.
Leased Proof-of-Stake (LPoS)	Можна перевести як доказ орендованої частки. Даний протокол впроваджений в платформу Waves. В рамках цього алгоритму, будь-який користувач має можливість передавати свій баланс в оренду майнінг-вузлів, а за це майнінг-вузли діляться частиною прибутку з користувачами. Таким чином, даний алгоритм консенсусу дозволяє отримати дохід від майнінгової діяльності, не ведучи самого майнінгу.
Proof-of-Burn (PoB)	Ще один цікавий тип алгоритму консенсусу Proof-of-Burn. При його використанні майнер відправляє монети на випадкову адресу згенерованого 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 покупка бурової установки для майнінгу. Природно такий алгоритм має сенс використовувати тільки на пізніх етапах існування тієї чи іншої криптовалюти, тоді коли є що "спалювати". Цікавою думкою є те, що цей метод також добре підходить для трансферу з "старих" в "нові" криптовалюти. Наприклад, "стара" криптовалюта знаходиться у фінальній точки свого майнінгу, ми можемо використовувати метод PoB тоді, коли для того, щоб отримати "нову" криптовалюта, нам необхідно спалити "стару". Даний алгоритм використовується на платформі Slimcoin.
Proof-of-Signature	PoSign – абсолютно новий механізм, який ще навіть не до кінця дороблений. Застосовується в блокчейні криптовалюти XTRABYTES. Ідея полягає в тому, що кожен з статистичних нодів мережі підписує нові блоки. Якщо нода спробує провести атаку, то вона потрапляє в чорний список.
Proof-of-Capacity (PoC)	Іноді ще званий Proof-of-Space (PoSpace). Піонер PoC – криптовалюта Burst. PoC працює за наступним принципом: - кожен майнер обчислює досить великий обсяг даних, який записується на дискову підсистему (жорсткий диск, хмарні системи зберігання) вузла. Такий, початковий набір даних в PoC називається "ділянка"; - для кожного нового блоку в блокчейне, майнер читає невеликий набір даних (1/4096, що приблизно становить 0.024%) від свого загального збереженого обсягу і повертає результат (дедлайн), як час, що пройшов 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. Таким чином обчислювальні ресурси необхідні майнеру для цієї роботи обмежені часом, який необхідний для читання файлів з дискової підсистеми. Саме цей фактор дозволяє виробляти майнінг з досить високою енергоефективністю. Майнери змагаються між собою за розміри збережених даних, на відміну від швидкості роботи обладнання, яке є головним в майнінгу побудованому на PoW.
Proof-of-Importance (PoI)	Доказ важливості – це 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.
Proof-of-Authority (PoAuthority)	PoA алгоритм консенсусу, який стоїть дещо осібно від інших алгоритмів, так як для своєї роботи йому не потрібно мати взагалі будь-якого майнінгу, як у випадку з PoW або PoS. У блокчейн-мережі, що базується на PoAuthority, всі транзакції і блоки перевіряються за допомогою схвалених аккаунтів (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, істотне зниження витрат на його обслуговування. Негативний момент використання даного алгоритму: як зрозуміло з самого опису – ключовими особами, є валідатори, що призводить до централізації. Ймовірно в деяких випадках, в приватних мережах і за допомогою повністю (на скільки це можливо) довірених аккаунтів це має сенс.

Таким чином можна зробити наступні висновки:

– Proof-of-Work і Proof-of-Stake – це два найпопулярніших протоколи досягнення консенсусу серед блокчейнів криптовалют;

– PoW – доказ роботи, захист забезпечується за рахунок обчислювальних операцій і пошуку хешу;

– PoS – доказ володіння частки, валідація проводиться нодами з активними балансами;

– PoW в цілому більш надійний, але вимагає набагато більше ресурсів, а в PoS-системах існує централізація і можливі доказі без ресурсу;

Все частіше з'являються криптовалюти з гібридними протоколами або зовсім новими концепціями механізму консенсусу.

Список використаних джерел.

1. Могайар У. Блокчейн для бизнеса. М.: ООО «Издательство «Эксмо». – 2016. – 198 с.

2. Лоран Л. Блокчейн от А до Я. М.: ООО «Издательство «Эксмо». – 2018. – 256 с.

3. Что такое блокчейн простыми словами [Електронний ресурс]. – Режим доступу: https://prostocoin.com/blog/blockchain-guide

4. PoW vs PoS – описание терминов, сравнение и отличия [Електронний ресурс]. – Режим доступу: https://prostocoin.com/blog/pos-pow

5. Обзор 9 алгоритмов блокчейн консенсуса [Електронний ресурс]. – Режим доступу: https://digiforest.io/blog/blockchain-consensus-algorithms

6. Антонопулос А.М. Осваиваем биткойн / пер. с анг. А.В. Снастина. – М.: ДМК Пресс, 2018. – 428 с.