БЛОКЧЕЙН

Andreas M. Antonopoulos. Mastering Bitcoin. O'Reilly Media, Inc. December 2014

Блокчейн – це мережева архітектура для фінансових транзакцій.

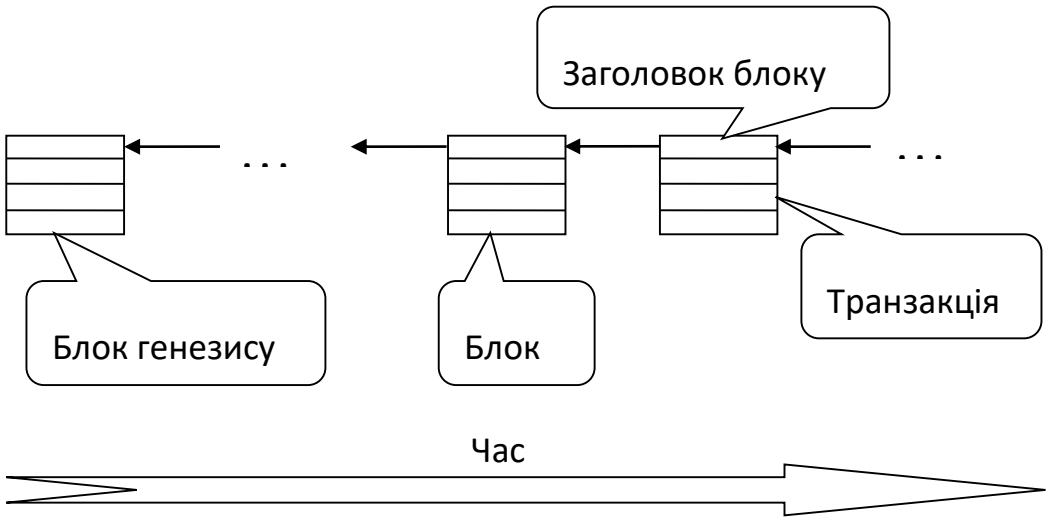

Рисунок 13.1 – Блокчейн

КОРОТКИЙ СЛОВНИК

address (aka public key) - адреса

Адреса біткойна виглядає як 1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV - вона складаються з рядка літер та цифр, починаючи з "1" (номер один). Так само, як ви просите інших надіслати електронний лист на вашу адресу електронної пошти, ви попросите інших надіслати вам біткойни на вашу біткойн адресу (адресу гаманця).

Bitcoin - біткойн, біткоін

Назва грошової одиниці, мережі і программного забезпечення

Block – блок

Група транзакцій, позначених міткою часу та ідентифікатором попереднього блоку. Заголовок блоку хешується для отримання доведення роботи і тим самим валідації транзакції. Валідні блоки додаються до основного блокчейну на основі консенсусу мережі.

Blockchain - блокчейн

Список підтверджених блоків, кожен з яких посилається на попередника, аж до блоку генезису.

Genesis block – блок генезису

Перший блок у блокчейні, який ініціалізує криптовалюту

Miner – майнер

Мережевий вузол, який знаходить дієві докази роботи нових блоків шляхом багатократного хешування

Transaction - транзакція

Простіше кажучи, передача біткойнів з однієї адреси на іншу. Точніше, транзакція - це підписана структура даних, яка виражає передачу значення. Транзакції передаються через мережу біткойн, збираються майнерами і включаються в блоки, стаючи постійними у блокчейні.

Wallet – гаманець

Програмне забезпечення, яке містить всі ваші біткойн адреси та секретні ключі. Використовується для надсилання, отримання та збереження біткойну.

ДЕЦЕНТРАЛІЗОВАНА МЕРЕЖЕВА АРХІТЕКТУРА

Біткоін побудований як мережева peer-to-peer архітектура на основі Інтернету. Термін peer-to-peer або P2P означає, що комп'ютери, що беруть участь у мережі, однорангові один до одного, всі вони рівні, що немає "спеціальних" вузлів і всі вузли поділяють тягар надання послуг мережі. Мережні вузли з'єднуються в мережевій сітці з "плоскою" топологією. Немає "сервера", ні централізованого сервісу, ні ієрархії всередині мережі. Вузли одноранговоі мережі одночасно взаємно забезпечують і споживають послуги, що діє як стимул до участі. Рівноправні мережі за своєю суттю є стійкими, децентралізованими та відкритими.

Видатним прикладом архітектури одноранговоі мережі P2P був ранній Інтернет, де вузли в мережі IP були рівними. Сьогоднішня архітектура Інтернету є більш ієрархічною, але протокол Інтернету все-таки зберігає свою суть - плоску топологію. Окрім біткоін, найбільшим і найуспішнішим застосуванням технологій P2P є файл-шарінг, ера якого продовжується з BitTorrent.

Сьогодні Біткоін – пірінгова система цифрових грошей (від peer – пара); мережева архітектура є одночасно відображенням і основою для цього. Децентралізація управління лежить в основі дизайну, а це може підтримуватись лише плоскою P2P мережею децентралізованого консенсусу.

ТИПИ І РОЛІ ВУЗЛІВ

Хоча вузли в мережі bitcoin P2P рівні, вони можуть приймати різні "ролі" в залежності від функціональності, яку вони підтримують. Вузол біткоіна - це сукупність функцій:

- Маршрутизація - N,

- база даних блоків - B,
- майнінг - M,
- гаманець - W.

Повний вузол із усіма чотирма функціями вказаний нижче.

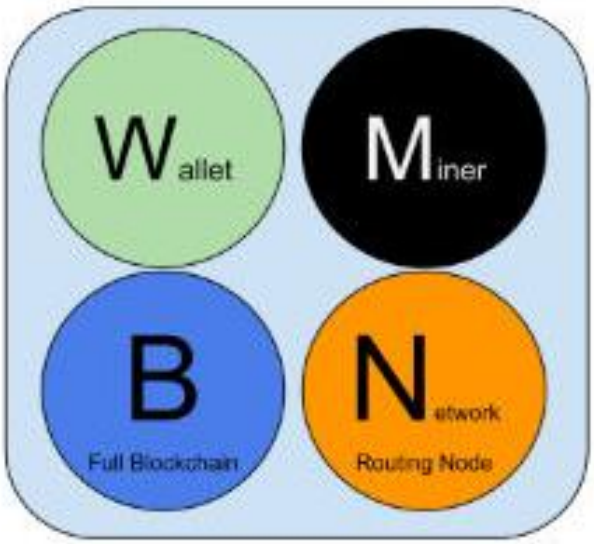

Рисунок 13.2 – Вузол мережі Біткоін, що виконує усі 4 функції

Всі вузли включають функцію маршрутизації для участі в мережі та можуть включати інші функції. Всі вузли перевіряють та поширюють транзакції та блоки, а також виявляють та підтримують зв'язки з сусідами. У наведеному вище прикладі вузла функція маршрутизації позначена помаранчевим колом під назвою "Network Routing Node" (Вузол мережевої маршрутизації).

- Деякі вузли, що називаються повними вузлами, також підтримують повну та актуальну копію блокчейн. Повні вузли можуть автономно і авторизовано перевіряти будь-яку операцію без зовнішнього посилання.
- Деякі вузли підтримують лише підмножину блокчейну та перевіряють транзакції за допомогою методу, що називається спрощеною перевіркою платежу або SPV. Ці вузли називаються SPV або легкими вузлами. У повному прикладі вищезазначеного вузла функція повної бази даних блокчейн вузла позначена синім колом, з назвою "Full Blockchain". Вузли SPV наведені без синього кола, показуючи, що вони не мають повної копії блокчейну.
- Майнінгові вузли конкурують за створення нових блоків за допомогою спеціалізованого устаткування. Деякі майнінгові вузли також є повними вузлами, зберігаючи повну копію блокчейн, а інші - легкі вузли, що беруть участь у майнінгових пулах, і залежні від сервера пулу, який підтримує повний вузол. Функція видобутку показана в повному вузлі як чорне коло "Майнер".
- Гаманці користувача можуть бути частиною повного вузла, якими зазвичай є настольні біткоін-клієнти. Все частіше гаманцями користувачів, особливо тих, що

працюють на пристроях з обмеженим ресурсом, такими як смартфони, є SPV-вузли. Функція гаманця показана на рис.13.2 як зелене коло "Wallet".

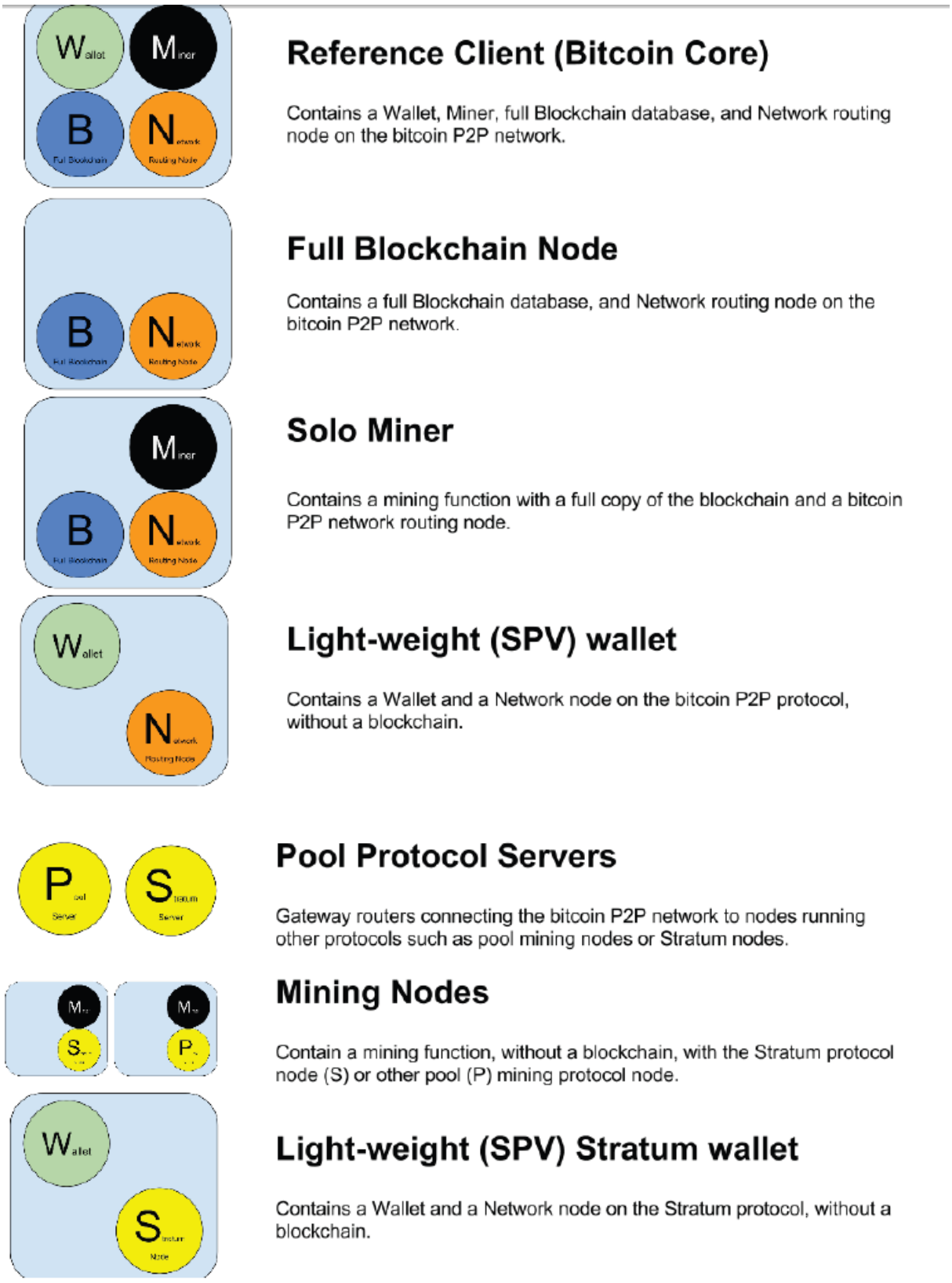

Рисунок 13.3 – Різні типи вузлів у розширеній мережі Біткоін

РОЗШИРЕНА МЕРЕЖА БІТКОІН

На додаток до основних типів вузлів протоколу P2P біткоін існують сервери та вузли, що працюють з іншими протоколами, такими як спеціалізовані протоколи майнінгових пулів та протоколи доступу до легких клієнтів.

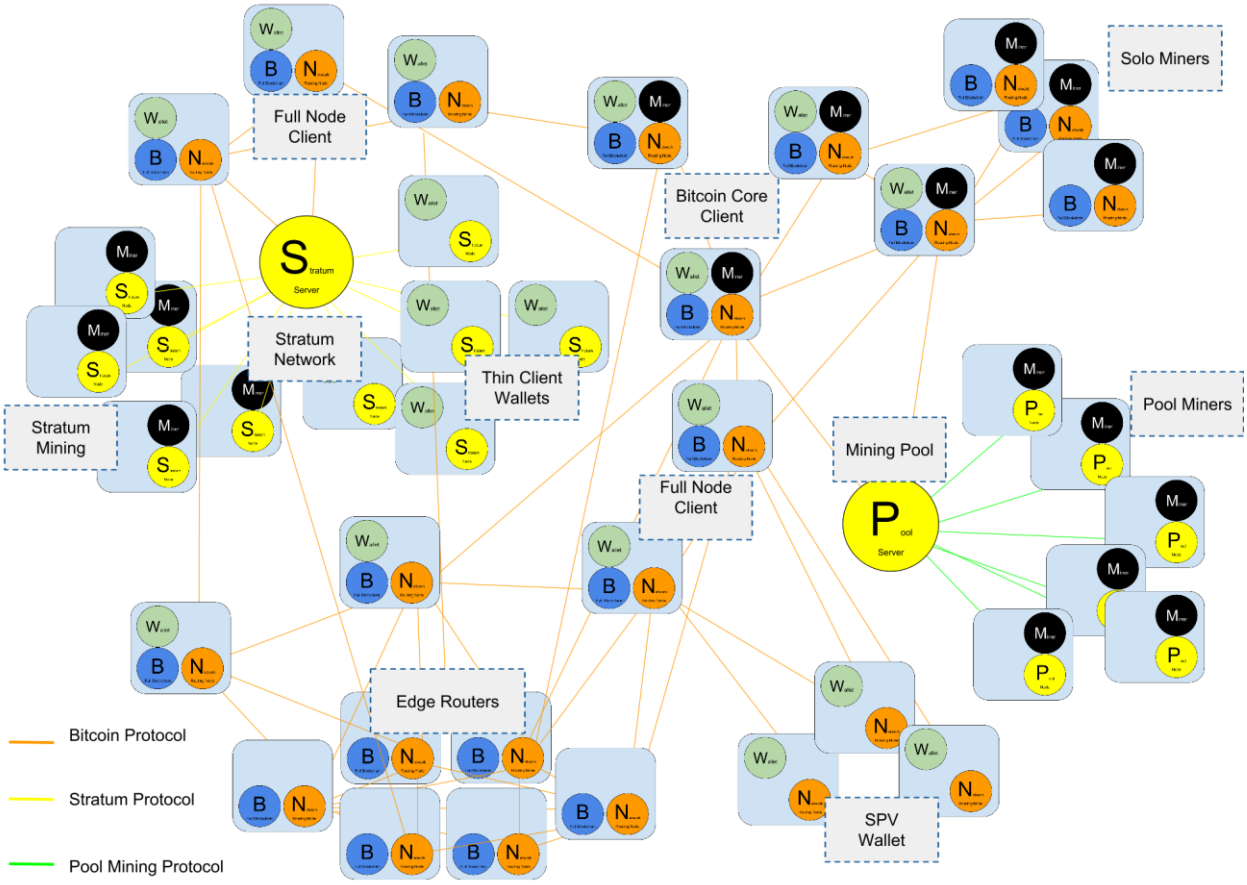

Рисунок 13.4 – Розширена мережа Біткоін, що показує різні типи вузлів, шлюзів і протоколів

Розширена мережа bitcoin включає в себе мережу, що працює на основі протоколу P2P bitcoin, описаного вище, а також вузли, що працюють за спеціалізованими протоколами. До основної мережі bitcoin P2P відносяться декілька пул-серверів і протокольних шлюзів, які з'єднують вузли з іншими протоколами. Це вузли майнінгових пулів і легкі гаманці, які не містять повну копію блокчейн.

ВИЯВЛЕННЯ МЕРЕЖІ

Коли новий вузол стає до роботи, він повинен знайти інші вузли біткоіна, хоча б один, і підключитись до нього. Географічне розташування інших вузлів не має значення, топологія мережі bitcoin не визначена географічно. Тому будь-які існуючі вузли bitcoin можуть бути вибрані випадковим чином.

Щоб підключитися до пари, вузли встановлюють TCP-з'єднання, як правило, до порту 8333 ("добре відомий" порт bitcoin) або альтернативного порту, якщо він передбачений. Після

встановлення з'єднання вузол запускає "рукостискання" шляхом передачі повідомлення про версію, що містить базову ідентифікаційну інформацію, включаючи версію P2P-протоколу, поточний час, свою і чужу IP-адресу. Другий вузол у відповідь також може послати повідомлення version.

ПОВНІ ВУЗЛИ

Повні вузли блокчейну підтримують повну та актуальну копію блокчейн з усіма транзакціями, які вони самостійно збирають та верифікують, починаючи з самого першого блоку (блок генезису) до останнього відомого в мережі блоку. Повний вузол блокчейн може самостійно і авторитетно перевіряти будь-яку транзакцію незалежно від будь-якого іншого вузла або джерела інформації. Повний вузол блокчейна залежить від мережі в отриманні нових блоків транзакцій, які потім він перевіряє і включає у свою локальну копію блокчейн.

ОБМІН «ІНВЕНТАРЕМ»

Перше, що повний вузол зробить, коли він з'єднається з іншими пірами, це спробує побудувати повний блокчейн. Якщо це абсолютно новий вузол, взагалі без блокчейн, то він знає лише один блок (блок генезису), який статично вбудований в клієнтське програмне забезпечення. Починаючи з блоку № 0, блоку генезису, новий вузол повинен буде завантажувати сотні тисяч блоків для синхронізації з мережею і відновити повний блокчейн.

Пір, який має довший блокчейн, тобто має більше блоків, ніж інший вузол, може визначити, яких блоків бракує іншому вузлу, щоб "наздогнати". Він визначить перші 500 таких блоків і передасть їх хеші, використовуючи повідомлення inv (inventory). Вузол, де відсутні ці блоки, прийме їх, видавши серію getdata-повідомлень, що запитують повні дані блоку та ідентифікують блоки хешами з inv-повідомлення.

Цей процес порівняння локального блокчейн з пірами та отримання відсутніх блоків відбувається кожного разу, коли вузол перебуває в автономному режимі протягом будь-якого періоду часу. Якщо вузол був автономним протягом декількох хвилин, і йому треба кілька блоків, або вузол був автономним протягом місяця, і не вистачає кількох тисяч блоків, він починає з відправки getblocks, отримуючи inv на вхід і починає завантажувати відсутні блоки.

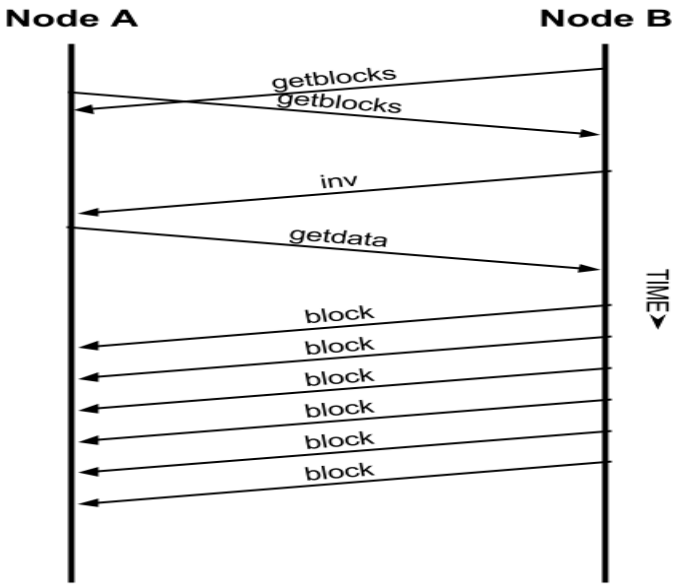

Рисунок 13.5 – Вузол синхронізується з блокчейном шляхом отримання блоків від іншого вузла

ПУЛИ ТРАНЗАКЦІЙ

У звичайному бухгалтерському обліку транзакція переміщує гроші між рахунками, кожний з яких має поточний залишок і обороти за період. У блокчейні для гаманця є вхідні транзакції, які одна за одною використовуються вихідними транзакціями для зовнішніх платежів. Залишком у гаманці є різниця між усіма вхідними і всіма вихідними транзакціями.

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Рисунок 13.6 – Транзакція у блокчейні

Майже кожен вузол в мережі bitcoin підтримує тимчасовий список непідтверджених транзакцій, який називається пулом пам'яті (memory pool) або пулом транзакцій. Вузли використовують цей пул для збереження транзакцій, які відомі мережі, але ще не включені в блокчейн. Наприклад, вузол гаманця використовуватиме пул транзакцій для відстеження вхідних платежів до кошика користувача, отриманих від мережі, але ще не підтверджених.

По мірі того, як транзакції приймаються та перевіряються, вони додаються до пулу транзакцій та передаються сусіднім вузлам для розповсюдження в мережі.

Деякі реалізації вузлів також підтримують окремий пул сирітських транзакцій. Якщо вхід транзакції відноситься до транзакції-попередниці, яка ще не відома, відсутній батько, то сирітська транзакція буде тимчасово зберігатися у сирітському пулі, поки не з'явиться батьківська транзакція.

Коли транзакція додана до пулу транзакцій, сирітський пул перевіряється для будь-яких сиріт, які посилаються на виходи цієї транзакції (для її дітей). Всі відповідні сироти валідуються. Якщо вони дійсні, вони видаляються з сирітського пулу та додаються до пулу транзакцій, доповнюючи ланцюжок, який розпочався з батьківської транзакції. Після додавання транзакції, яка більше не є сиротою, процес повторюється рекурсивно для пошуку будь-яких подальших нащадків, доки не буде знайдено всіх нащадків. Завдяки цьому процес прибуття батьківської транзакції ініціює каскадну реконструкцію цілого ланцюга взаємозалежних транзакцій шляхом повторного об'єднання сиріт з батьками повністю вниз по ланцюжку.

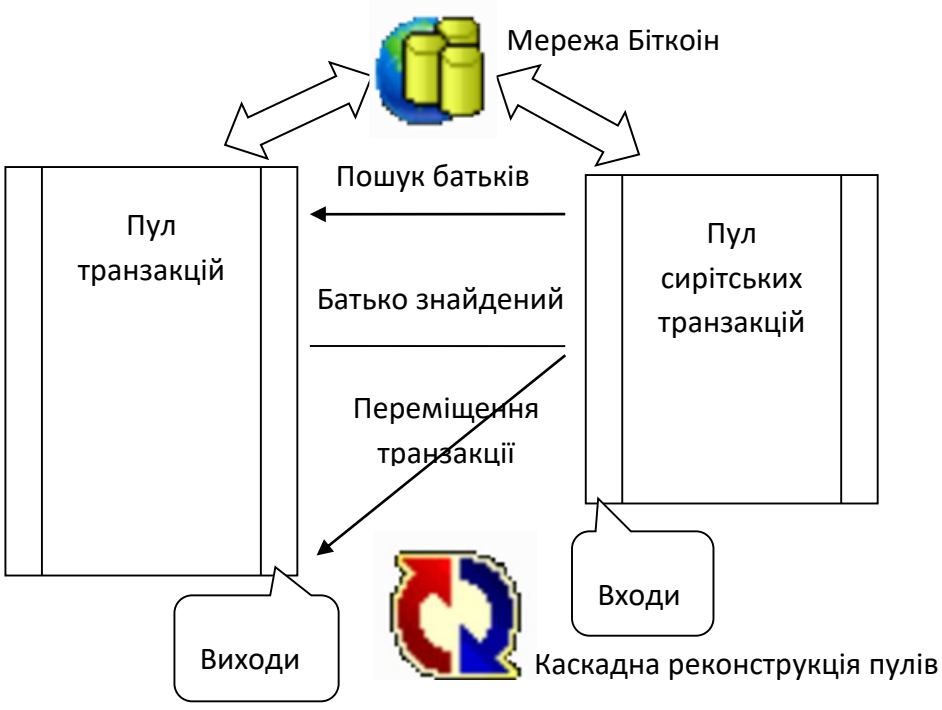

Рисунок 13.5 – Обробка пулу сирітських транзакцій

Як пул транзакцій, так і сирітський пул (де він є) зберігаються в локальній оперативній пам'яті, не на постійних накопичувачах (дисках). Коли вузол запускається, обидва пули порожні і поступово заповнюються новими транзакціями, отриманими в мережі.

СТРУКТУРА ДАНИХ БЛОКЧЕЙН

Структура даних блокчейн - це впорядкований у зворотньому порядку список блоків транзакцій. Блокчейн може зберігатися у плоскому файлі або в простій базі даних. Клієнт Bitcoin Core зберігає метадані блокчейну в базі даних LevelDB від Google. Блоки пов'язані "назад", кожен з них посилається на попередній блок в ланцюжку.

На кінець 2017р. поточна висота останнього блоку (вершини) 500425, на кінець 2018р. - 553181, на початок 2023р.- 770378. Див. https://www.blockchain.com/explorer

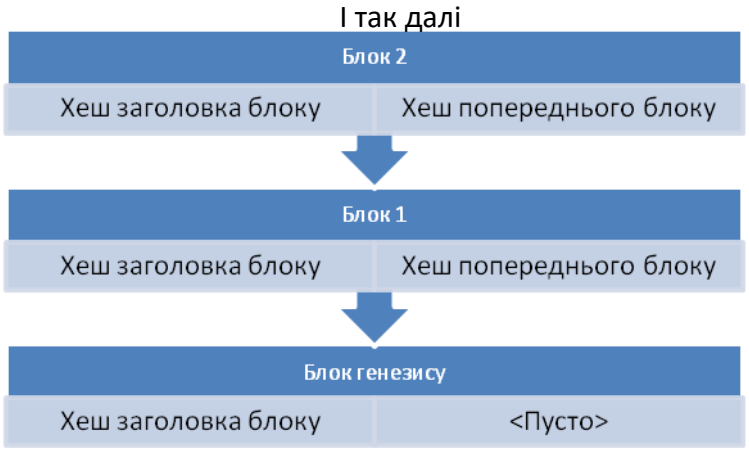

Рисунок 13.6 – Представлення блокчейну по шарах

Кожен блок в блок-схемі ідентифікується хешем, який генерується за допомогою криптографічного алгоритму хешу SHA256 в заголовку блоку. Кожен блок також посилається на попередній блок, відомий як батьківський блок, через поле "хеш попереднього блоку" в заголовку блоку. Іншими словами, кожен блок містить хеш свого батька всередині власного заголовка. Послідовність хешей, що з'єднує кожен блок з його батьком, створює ланцюжок, який тягнеться до першого створеного блоку, відомого як блок генезису.

Поле хешу попереднього блоку знаходиться всередині заголовка блоку, і тим самим впливає на хеш поточного блоку. Хеш дочірнього блоку змінюється, якщо змінюється хеш батьківського блоку. Будь-які зміни в батьківському блоці тягнуть зміни в його хеші, має змінитись хеш батьківського блоку в дочірньому блоці, хеш дочірнього блоку, хеш внучатого блоку і так до вершини. Цей каскадний ефект гарантує, що після того, як за блоком з'явилось багато поколінь, його неможливо змінити без перерахунку всіх наступних блоків. Оскільки для такого перерахунку потрібні величезні обчислення, існування довгого

ланцюга блоків робить глибоку історію блокчейну незмінною, що є головною особливістю безпеки біткоіну.

Останні кілька блоків можуть бути переглянуті в результаті розгалуження (форку). Кілька тисяч блоків тому (місяць) блокчейн має сталу історію для всіх практичних цілей.

Рисунок 13.7 – Розповсюдження зміни у блокчейні

ІДЕНТИФІКАТОРИ БЛОКУ: ХЕШ І ВИСОТА

Основний ідентифікатор блоку – криптографічний хеш, отриманий при хешуванні заголовку блоку двічі алгоритмом SHA256. Для нього використовується лише заголовок блоку, наприклад:

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- хеш блоку генезису.

Хеш блоку не включений у структуру даних блоку, ні коли він зберігається в базі даних вузлів, ні коли він передається по мережі, тому що він може бути отриманий з заголовка. Хеш обчислюється кожним вузлом, як тільки блок отриманий з мережі. Хеш однозначно ідентифікує блок. А от певна висота блока (порядковий номер блоку в блокчейні) може ідентифікувати більше одного блоку. Два або більше блоків можуть конкурувати за одну висоту в блокчейні.

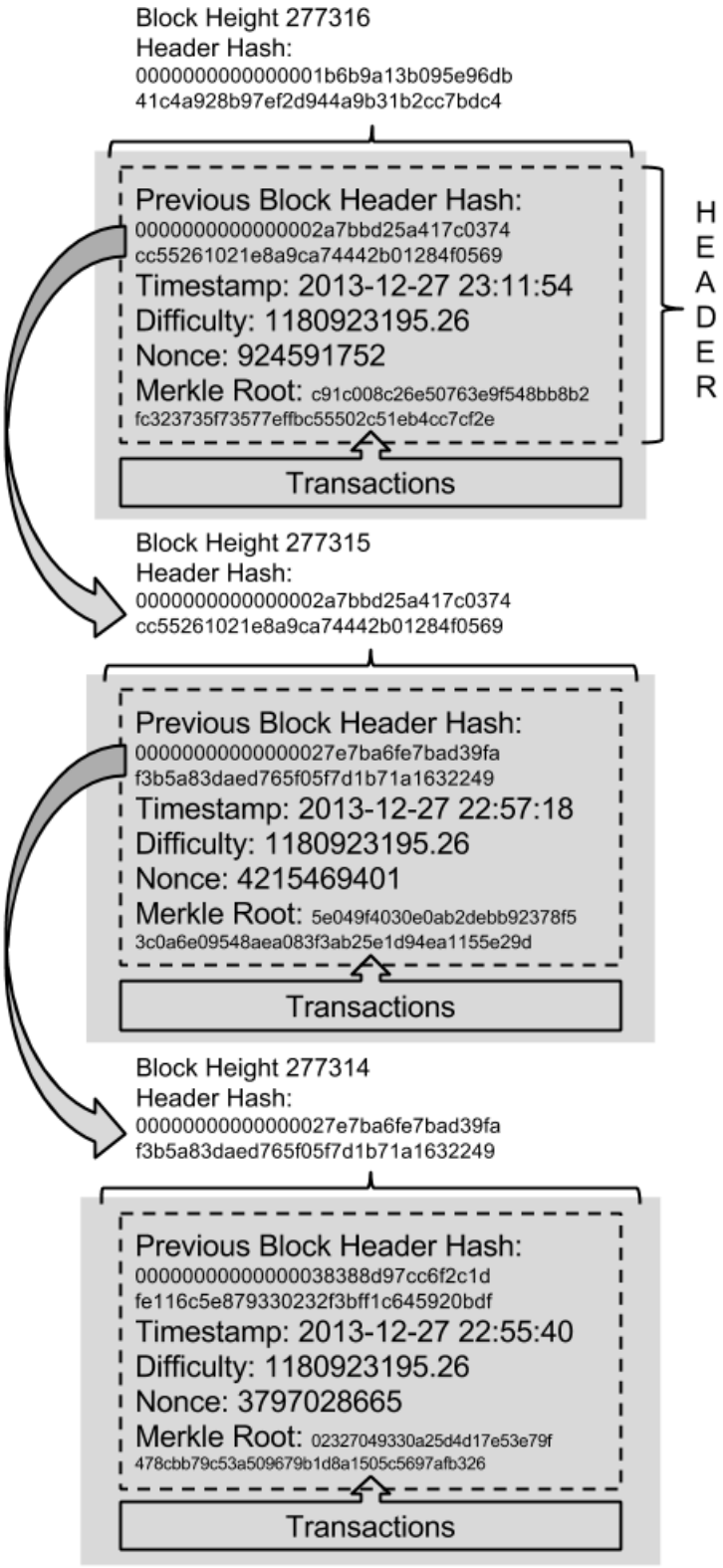

Рисунок 13.8 – Ланцюжок блоків у блокчейні

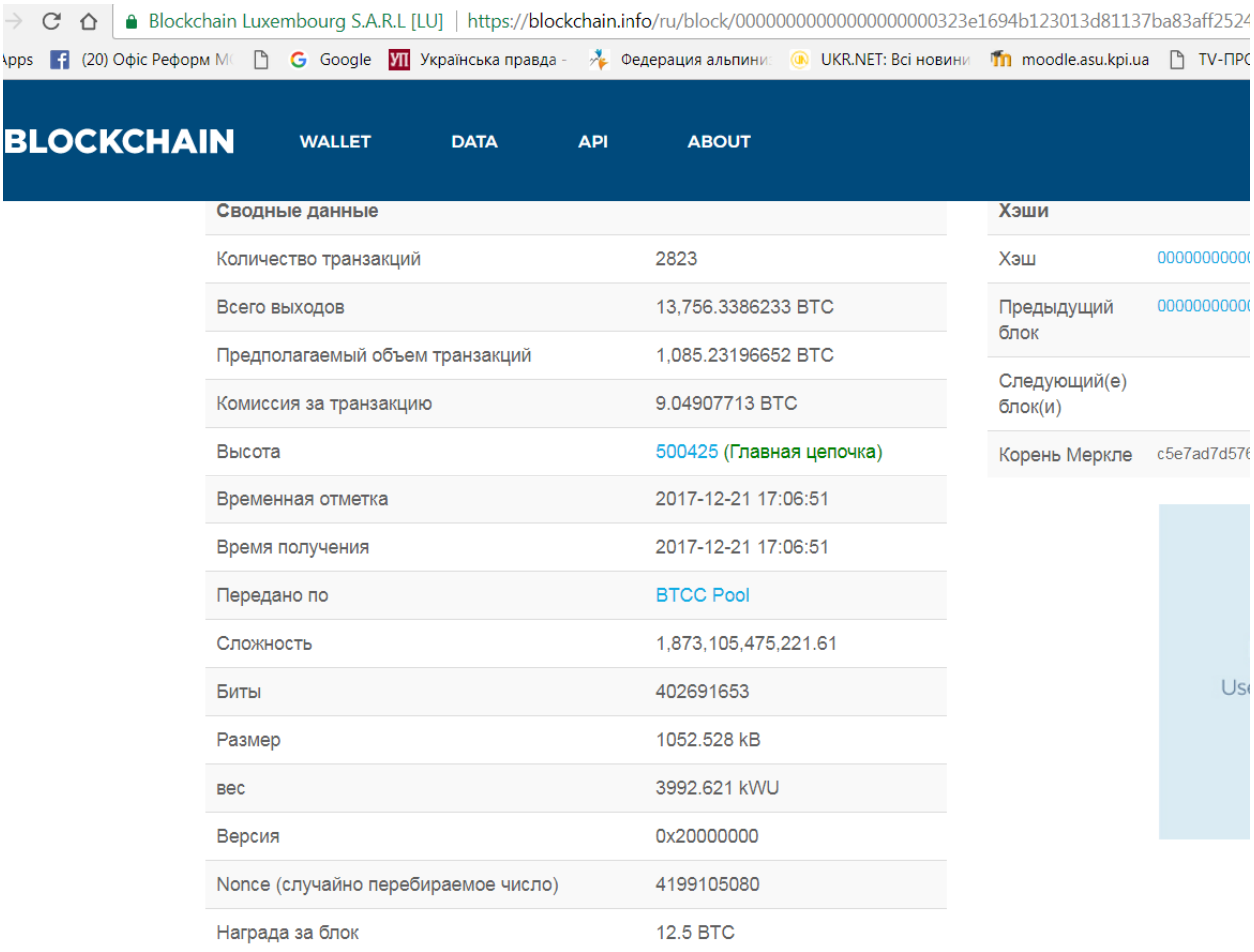

Рисунок 13.9 – Останній блок у блокчейні на час написання лекції (2017р.)

МАЙНІНГ І КОНСЕНСУС

Майнінг – процес, за допомогою якого новий біткоін додається до грошової маси. Майнінг також служить для захисту біткоін-системи від шахрайських транзакцій або транзакцій, які витрачають одні і ті ж біткоіни більше одного разу (подвійні витрати). Майнери забезпечують обчислювальну потужність мережі біткойн в обмін на можливість отримувати винагороду в біткоінах.

Майнери перевіряють нові транзакції та записують їх у загальний обліковий регістр (Ledger – бухгалтерська книга). Новий блок з транзакціями, що відбулися після останнього блоку, "видобувається" приблизно кожні 10 хвилин (на рис.13.8 це 14 і 2 хвилини), тим самим додаючи ці транзакції до блокчейну. Транзакції, які стають частиною блоку та додаються до блокчейну, вважаються "підтвердженими", що дозволяє новим власникам біткойнів витратити біткойн, який вони отримали в цих операціях.

Майнери отримують два типи винагороди за видобуток: нові монети, створені з кожним новим блоком, і комісійні збори від усіх транзакцій, включених до блоку. Щоб заробити цю нагороду, майнери змагаються з вирішення складної математичної задачі на основі криптографічного алгоритму хешування. Рішення проблеми, яке називається *доведенням*

роботи (proof-of-work), входить до нового блоку і є доказом того, що майнер витратив значні обчислювальні зусилля.

Конкуренція за вирішення задачі і доведення роботи, щоб заробити винагороду, та право записувати транзакції у блокчейн, є основою моделі безпеки біткойн.

Кількість біткойнів, створених новим блоком, зменшується приблизно кожні чотири роки (або точно кожні 210 000 блоків). Вона почалася з 50 біткойн на блок в січні 2009 року і зменшилась до 25 біткойн на блок в листопаді 2012 року. Вона знову зменшилась удвічі до 12,5 біткойн на блок в 2016 році. Дохід від майнінгу біткойнів зменшується експоненційно до приблизно 2140 року, коли будуть випущені всі біткойни (20.99999998 млн.). Після 2140 року нові біткойни не емітуватимуться, весь дохід від майнінгу буде в вигляді комісійних.

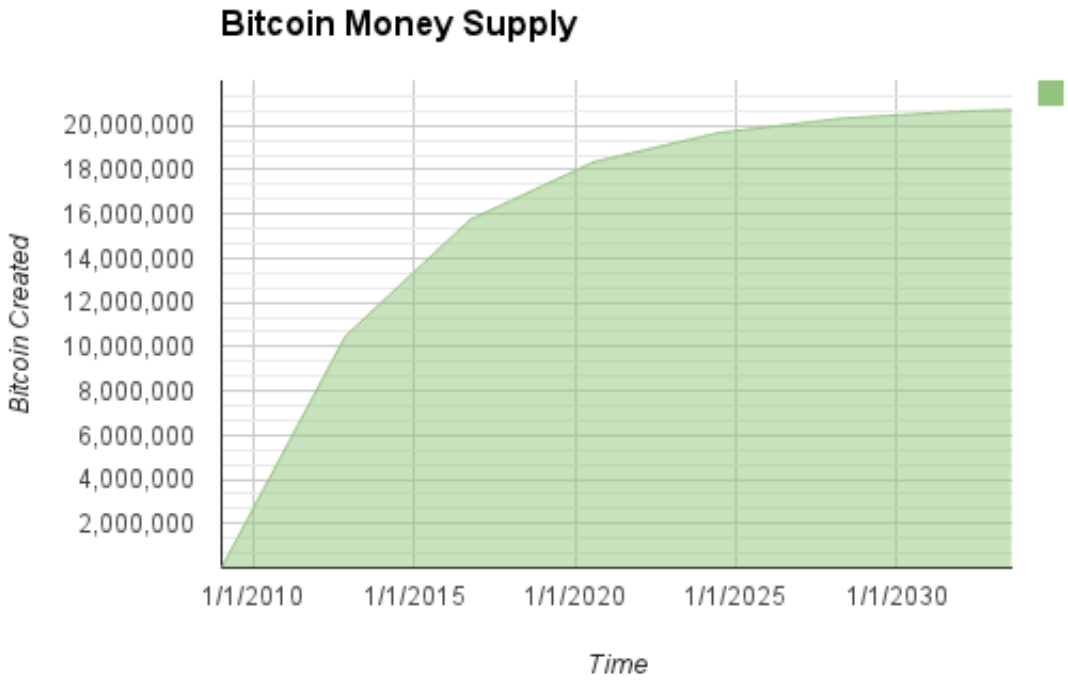

Рисунок 13.10 – Емісія біткойнів

Хоча майнінг стимулюється нагородою, основною метою видобутку не є нагорода або створення нових монет. Майнінг є основним процесом децентралізованого клірингового центру, за допомогою якого операції перевіряються та очищуються. Майнінг забезпечує систему біткойн і забезпечує появу загального консенсусу без центральної влади.

ДЕЦЕНТРАЛІЗОВАНИЙ КОНСЕНСУС

Основним винаходом Сатоши Накамото є децентралізований механізм неявного консенсусу. Консенсус не досягнуто явним чином - немає виборів або фіксованого моменту, коли відбувається консенсус. Натомість, консенсус є невід'ємним артефактом асинхронної взаємодії тисяч незалежних вузлів, які дотримуються простих правил.

Децентралізований консенсус Bitcoin виникає з взаємодії чотирьох процесів, які відбуваються незалежно в вузлах мережі:

• Незалежна перевірка кожної транзакції кожним повним вузлом на основі широкого переліку критеріїв;

• Незалежна агрегація цих транзакцій у нові блоки майнерами в поєднанні з демонстрованим обчисленням за допомогою алгоритму доказу роботи;

• Незалежна перевірка нових блоків кожним вузлом та складання в ланцюжок;

• В разі наявності альтернативних ланцюгів - незалежний відбір кожним вузлом ланцюга з найбільш складним обчисленням, продемонстрованим за допомогою алгоритму доведення роботи.

МАЙНІНГ БЛОКУ

Майнінг - це процес багатократного хешування заголовку блоку, зі зміною одного параметру, доки результуючий хеш не стане відповідати певній меті. Для цього використовується хеш-функція SHA256, яка на виході дає код у 256 біт (32 байти).

Конкретно, мета полягає в тому, щоб знайти хеш, що чисельно менший заданого числа - цілі. Якщо ми зменшимо ціль, це завдання стає дедалі складнішим.

Знайдене рішення (ціле число, хеш заголовку блоку з яким менше цілі, на рис.13.9 воно дорівнює 4199105080) записується у поле транзакції nonce. Для його знаходження майнінговий вузол має перебрати мільярди, трільйони і квадрільйони значень nonce. Для перевірки результату треба усього одне обчислення.

Майнер будує блок транзакцій-кандидатів. Далі майнер обчислює хеш заголовка цього блоку і дізнається, чи він менше, ніж поточна ціль. Якщо хеш не менше цілі, майнер буде змінювати значення nonce (зазвичай просто збільшуючи його на одиницю) і повторить спробу. За нинішньої складності мережі біткойн, майнери повинні виконати квадрільйони спроб, для знаходження nonce, що дає достатньо малий хеш заголовка блоків.

Як можна бачити, збільшення складності на 1 біт (збільшення кількості нулів зліва) тягне зменшення простору пошуку у 2 рази і збільшення кількості обчислень теж у 2 рази. На кінець 2014 року мережа будувала блок, хеш заголовку якого був би менше ніж

000000000000004c296e6376db3a241271f43fd3f5de7ba18986e517a243baa7

Для знайдення блоку знадобилось у середньому 150 квадрильйонів обчислень хешів у секунду для мережі. На щастя, потужність мережі складає 100 петахешів у секунду, що дозволяє знайти блок приблизно за 10 хвилин.

Аби зберегти час генерації блоку у 10 хвилин, складність періодично коректується. Перепланування рівня складності відбувається автоматично на кожному повному вузлі незалежно один від одного, кожні 2016 блоків (приблизно 2 тижні). Якщо мережа

знаходить блоки швидше, ніж за 10 хвилин, складність збільшується, якщо повільніше, то зменшується.

*Нова складність = Стара складність * (20160 хвилин / Фактичний час останніх 2016 блоків)*

Цільова складність тісно пов'язана з вартістю електроенергії та обмінним курсом біткойн до валюти, що використовується для оплати електроенергії. Продуктивність майнінгових систем у перетворенні електроенергії в обчислення хешування велика наскільки це можливо з нинішнім поколінням мікросхем. Головний вплив на ринок майнінгу - це ціна кіловат-години в біткойнах, що визначає прибутковість майнінгу і, отже, стимули для входу або виходу на цей ринок.

ВАЛІДАЦІЯ НОВОГО БЛОКУ

Щойно майнери отримують і перевіряють блок, вони припиняють зусилля, щоб знайти блок на тій же висоті і негайно розпочинають обчислення наступного блоку в ланцюжку.

Коли вузол отримує новий блок, він перевіряє блок, перевіряючи його по довгому списку критеріїв, які всі повинні бути виконані; інакше блок буде відхилено. Ці критерії включають в себе наступне:

• Структура даних блоку є синтаксично вірною;

• Хеш заголовка блоку менший, ніж цільова складність (підтвердження роботи);

• Часова мітка блоку убігає вперед менше ніж на дві години (дозволяючи помилки часу);

• Розмір блоку знаходиться в межах допустимих значень;

• Перша транзакція (і лише перша) є coinbase-транзакція для генерації винагороди майнеру;

• Всі транзакції в блоці проходять валідацію транзакцій.

Чому майнер не «намалює» собі транзакцію на тисячу біткойнів замість правильної винагороди?

Тому що кожен вузол перевіряє блоки відповідно до тих самих правил. Недійсна coinbase-транзакція зробить весь блок недійсним, що призведе до того, що блок буде відхилено, і тому ця транзакція ніколи не стане частиною головної книги. Майнер повинен побудувати ідеальний блок, який ґрунтується на загальних правилах, яких дотримуються всі вузли, і надавати правильне рішення доказу роботи. Для цього вони витрачають велику кількість електроенергії і часу на майнінг, і в разі обману все буде даремно. Ось чому незалежна перевірка є ключовим компонентом децентралізованого консенсусу.

ФОРКИ БЛОКЧЕЙНУ

Оскільки blockchain є децентралізованою структурою даних, різні копії її не завжди узгоджуються (див. CAP-теорему). Блоки можуть надходити в різні вузли в різний час, і вузли можуть мати різні блокчейни. Щоб вирішити цю проблему, кожен вузол завжди вибирає і намагається розширити ланцюжок блоків, який представляє доказ найбільшої виконаної роботи, також відомий як найдовший ланцюг або найбільший сукупний ланцюг складності. Сумуючи складність, записану в кожному блоці по ланцюгу, вузол може обчислити загальну кількість доказів роботи, витрачених на створення цього ланцюга. Поки всі вузли вибирають найдовший сукупний ланцюг складності, глобальна мережа біткойн в кінцевому рахунку збігається до сталого стану. Форки виникають у вигляді тимчасових невідповідностей між версіями блокчейну, які узгоджуються шляхом додавання блоків до одного з форків.

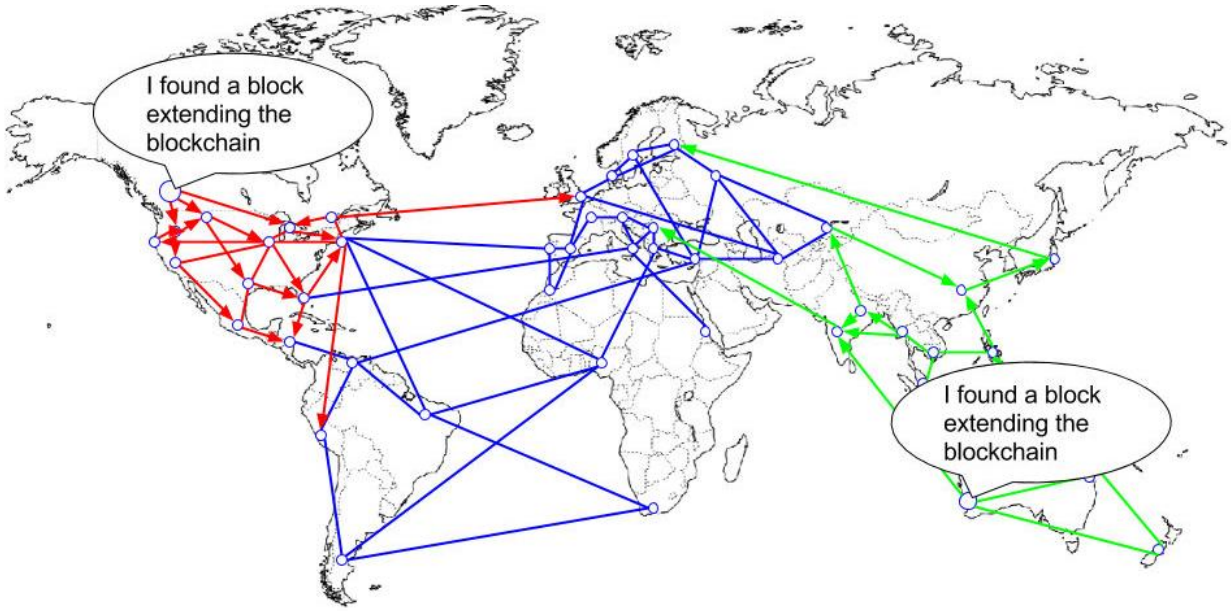

Рисунок 13.11 – Виникнення двох форків у результаті одночасного знайдення різних нових блоків

При подальшому додаванні блоків до форків один з них починає переважати по складності інший і інший форк відкидається.

АТАКИ НА КОНСЕНСУС

Механізм консенсусу біткойну, принаймні теоретично, є вразливим до нападу майнерів (або пулів), які можуть спробувати використати свої хешуючі потужності для нечесних або руйнівних цілей. Як ми бачили, механізм консенсусу залежить від того, аби більшість майнерів діяли чесно згідно власних інтересів. Проте, якщо майнер або група майнерів зможуть отримати значну частку потужностей майнінгу, вони можуть атакувати механізм консенсусу, щоб порушити безпеку та доступність мережі біткойн.

Для організації дуже глибокого форку потрібні надто великі майнінгові потужності, що практично гарантує незмінність старих блоків. Ці атаки не можуть украсти біткоіни, витратити їх без підпису, перенаправити їх, іншим чином змінити минулі транзакції чи записи власності. Ці атаки можуть вплинути лише на останні блоки.

Чим більшу потужність хешування має зловмисник, тим довше форк, який він може навмисно створити, тим більше блоків у недавньому минулому він може зробити недійсними або тим більше блоків у майбутньому він зможе контролювати. Групи досліджень з питань безпеки застосували статистичне моделювання і обгрунтували, що різні типи консенсусних атак можливі з лише 30% потужності хешування.

Один із сценаріїв потенційного нападу полягає в тому, що зловмисник має намір порушити мережу біткойну без можливості заробити на цьому. Така атака вимагатиме величезних інвестицій і прихованого планування, але може бути запущена зловмисником, який добре фінансується, найімовірніше, державою.

Безумовно, серйозний напад на консенсус може призвести до зниження довіри до біткойну в короткостроковій перспективі, що може призвести до значного зниження курсу. Проте мережа і програмне забезпечення біткойн постійно розвиваються, тому консенсусні напади будуть зустрінуті негайними контрзаходами спільноти, що робить біткойн жорсткішими, стійкими та надійнішими.

СМАРТ-КОНТРАКТИ

Сьогодні існує мережа Ethereum, яка має архітектуру, відмінну від класичного Bitcoin і яка здатна підтримувати смарт-контракти.

Ethereum використовує спосіб підтвердження правильності блоків proof-of-stake, відмінний від способу proof-of-work, прийнятого в традиційному біткоіні. Аби виконувати валідацію, користувач має внести заставу 32eth, тобто приблизно $50тис. Під час валідації блоку виконується перевірка ряду логічних співвідношень. Для прийняття блоку як валідного треба, аби за це проголосували більшість валідаторів. Якщо валідатор робить невірний висновок щодо блоку, тобто визначає валідний блок як невалідний або невалідний блок як валідний, з застави валідатора знімається значна сума на користь мережі.

Смарт-контракт (англ. smart contract — «розумний контракт») — різновид угоди в формі закодованих математичних алгоритмів, де укладення, зміни, виконання і розривання можна виконати лише з використанням комп'ютерних програм (блокчейн-платформ) у рамках мережі Інтернет[1].

Підписанти — сторони розумного контракту, які беруть або відмовляються від умов з використанням електронних підписів. Прямим аналогом є підпис відправника коштів в мережі Bitcoin, яка підтверджує внесення транзакції в ланцюжок блоків.

[1] https://uk.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%B0%D0%BA%D1%82

Предмет договору. Предметом договору може бути тільки об'єкт, що знаходиться всередині середовища існування розумного контракту (наприклад, у мережі Ethereum), або ж повинен забезпечуватися безперешкодний, прямий доступ розумного контракту до предмету договору без участі людини (наприклад, доступ до публічних і відомчих реєстрів).

Умови. Умови розумного контракту повинні мати повний математичний опис, який можливо запрограмувати в середовищі існування розумного контракту. Саме в умовах описується логіка виконання пунктів предмета договору.

Наприклад, мешканці будинку мають намір зібрати кошти на будівництво дитячого майданчику. Треба зібрати певну суму (скажімо, 50 тис.грн у валюті ETH) до певної дати (скажімо, до 01.03.2024). Якщо сума зібрана, вона перераховується будівельній організації. Якщо сума не зібрана, надіслані кошти повертаються відправникам.

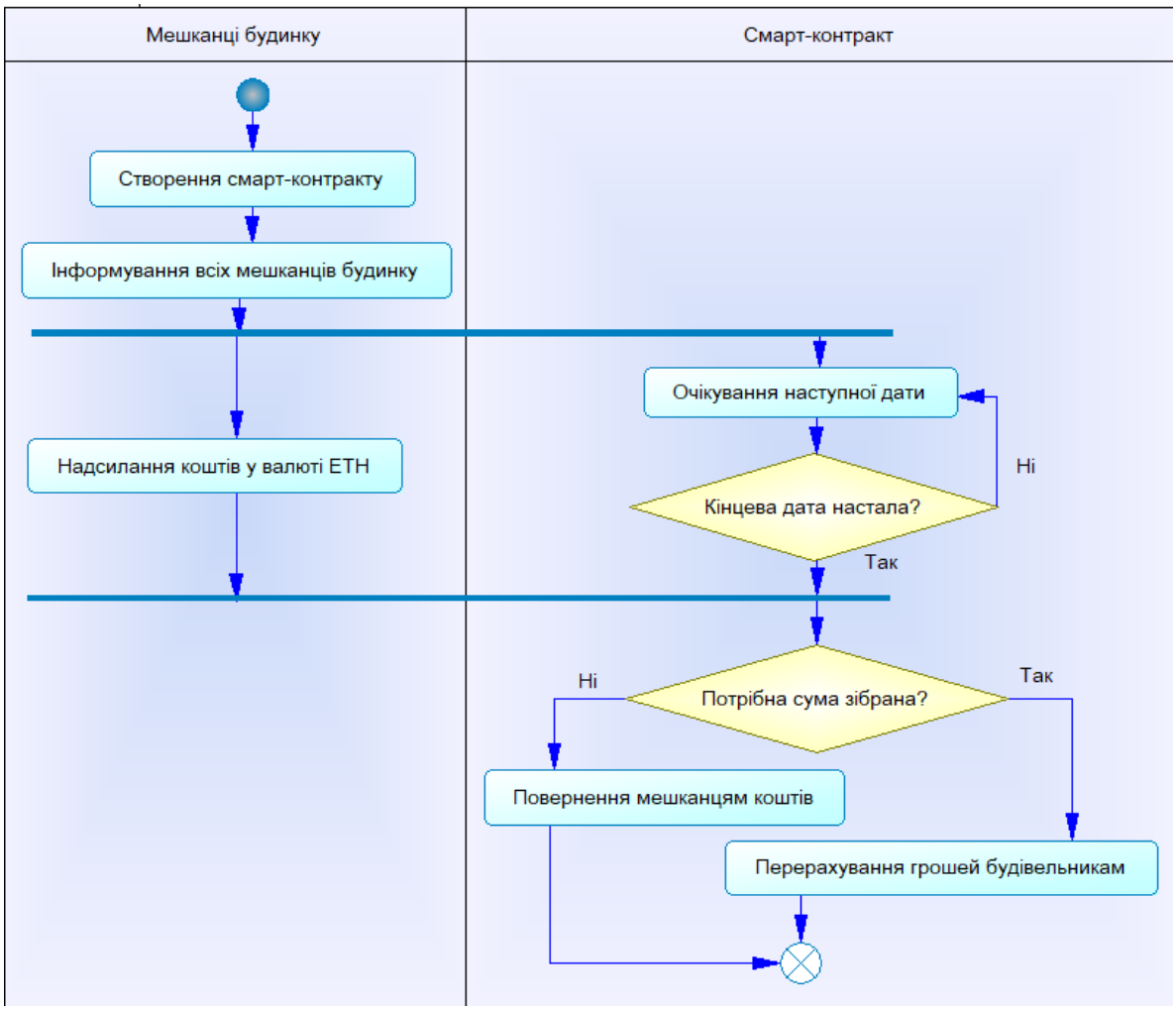

Рисунок 13.12 – Приклад смарт-контракту на побудову дитячого майданчика

АГЕНТ В МЕРЕЖІ ETEREUM

В мережу Ethereum запускається програмний агент, який шукає джерела прибутку – Maximum Extractable Value (MEV). Агент може отримати прибуток на підставі виконання смарт-контрактів.

Агент бачить всі транзакції в мережі: ще не виконані, взяті на виконання і виконані, які далі включаються в блоки. Кожний користувач чи агент може створити власну криптовалюту.

Наприклад, існують такі джерела прибутку.

DEX ARBITRAGE

В Ethereum програмно створюються віртуальні обмінники на основі смарт-контракту. Інвестори інвестують в обмінник кілька криптовалют (внутрішніх для Ethereum), аби в обміннику були гроші для обміну. Коли обмінник завершує роботу, інвестори забирають свої гроші плюс зароблені комісійні, які утворюються за рахунок різниці курсів купівлі і продажу валют.

Масові обмінні операції між валютами вирівнюють їх курси.

SANDWICH

Серед транзакцій можуть бути операції по обміну валют. Агент бачить невиконану операцію по обміну достатньо крупної суми валюти А на валюту ETH. Ця операція має підвищити курс ETH. Тоді агент формує транзакцію по купівлі собі певної суми ETH та звертається до посередника, аби той вставив цю останню транзакцію безпосередньо перед першою транзакцією по купівлі крупної суми валюти ETH. Таким чином вартість валюти в агенту збільшиться.

LIQUIDATIONS

На підставі смарт-контракту для застави користувач перераховує «ломбарду» суму застави і бере борг в іншій валюті, вартістю не більше 30% від застави на момент взяття боргу. Якщо згодом застава знеціниться відносно боргу (що можливо завдяки волатильності криптовалют), інший суб'єкт (searcher) може заплатити «ломбарду» борг і забрати собі заставу. Searcher може на цьому заробити, якщо згодом застава відновить свою ціну.

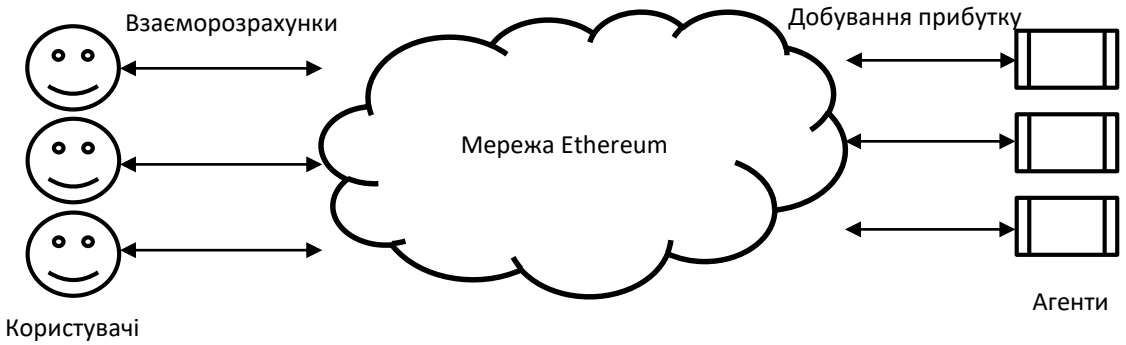

Рисунок 13.13 – Роль агентів у мережі Ethereum