Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Методи захисту транзакцій в блокчейн системах
(тема)

Виконав:
студент 2 курсу, групи БІКСм-20-1
Черніков М.Ю.
(прізвище, ініціали)
Спеціальності 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Безпека інформаційних і комунікаційних систем
(повна назва освітньої програми)
Керівник доцент Власов А.В.
(посада. прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри: _____ Халімов Г.З.
(підпис)
«____»_____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Чернікову Максиму Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи захисту транзакцій в блокчейн системах

затверджена наказом по університету від 08.11.2021 р. №1685 ст.

2. Термін подання студентом роботи до екзаменаційної комісії _____.

3. Вихідні дані до роботи –
Проаналізовані методи забезпечення безпеки блокчейн транзакцій , можливі атаки із розрахунком матеріальних витрат і висунуто рекомендації до захисту від розглянуих атак.

4. Перелік питань, що потрібно опрацювати в роботі
Аналіз принципів роботи блокчейн систем
Аналіз методів побудови блоків транзакцій
Аналіз методів забезпечення безпеки транзакцій
Аналіз можливих загроз на децентралізовані мережі
Розробка стратегії захисту

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
презентаційний матеріал у вигляді слайдів

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Вибір здобувачем теми кваліфікаційної роботи	02.09.2021	Виконано
2	Затвердження плану і завдання кваліфікаційної роботи	09.11.2021	Виконано
3	Аналіз завдання, пошук та аналіз літературних джерел за темою роботи	10.11.2021-18.11.2021	Виконано
4	Виконання кваліфікаційної роботи	19.11.2021-30.11.2021	Виконано
5	Оформлення пояснювальної записки	01.12.2021-12.12.2021	Виконано
6	Здача на перевірку та підпис кваліфікаційної роботи керівнику	13.12.2021	Виконано
7	Проходження перевірки на плагіат та нормоконтроль кваліфікаційної роботи	14.12.2021	Виконано
8	Допуск завідувачем кафедри до захисту кваліфікаційної роботи	14.12.2021	Виконано
9	Захист кваліфікаційної роботи	17.12.2021	Виконано

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи _____ доцент Власов А.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка включає в себе 81 сторінка, 19 рисунків, 23 джерела, 25 формул, 4 таблиці.

БЛОКЧЕЙН, ДЕЦЕНТРАЛІЗАЦІЯ, БІТКОІН, ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА, ТРАНЗАКЦІЯ, МЕРЕЖА

Об’єктом дослідження є безпека даних (транзакцій) в блокчейн системах.

Предмет дослідження - методи захисту транзакцій в блокчейн системах.

Метою роботи є аналіз методів захисту даних, які використовуються в блокчейн системах для обґрунтування напрямків підвищення їх безпеки (з урахуванням існуючих вразливостей та сучасного вектору атак на блокчейн системи).

Методи дослідження – аналіз інформації щодо побудови та впровадження методів захисту даних (транзакцій) в блокчейн системах, аналіз найбільш поширених вразливостей та атак на транзакції в блокчейн системах.

ABSTRACT

Explanatory note to the thesis contains 81 pages, 19 figures, 23 references, 25 formulas, 4 tables.

BLOCKCHAIN, DECENTRALIZATION, BITCOIN, DECENTRALIZED SYSTEM, TRANSACTION, NETWORK

The object of research is the security of data (transactions) in blockchain systems.

The subject of research - methods of transaction protection in blockchain systems.

The purpose of the work is to analyze the data protection methods used in blockchain systems to justify ways to improve their security (taking into account existing vulnerabilities and the current vector of attacks on blockchain systems).

Research methods - analysis of information on the construction and implementation of data protection methods (transactions) in blockchain systems, analysis of the most common vulnerabilities and attacks on transactions in blockchain systems.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

API – Application Programming Interface - інтерфейс створення додатків

FTP – File Transfer Protocol - протокол передачі даних

P2P – Peer to peer - однорангова децентралізована мережа

IoT– Internet of Things - мережа речей

Usenet – комп'ютерна мережа, використовувана для спілкування та публікації файлів

Open API - специфікація машиночитабельних файлів з інтерфейсами, для опису, створення, використання і візуалізації веб сервісів

Napster - файлообмінна піринговa мережа

Tor - браузер, створений для забезпечення анонімності в мережі Інтернет.

ПЗ – програмне забезпечення

SHA - Secure Hash Algorithm - безпечний алгоритм гешування

PoW - Proof-of-work - принцип захисту системи від зловживання послугами, заснований на необхідності виконання деякої досить складної і тривалої роботи

PoS – Proof-of-Stake - принцип захисту системи від зловживання послугами, заснований на необхідності доказу зберігання певної кількості коштів на рахунку

DPoS – Delegated Proof-of-Stake – принцип захисту системи від зловживання послугами, заснований на базі PoS, але впроваджує ідею чесних виборів валідаторів

UTXO - Unspent Transaction Output – баланс невитрачених транзакцій

ВСТУП

З появою Інтернету світ почав стрімко змінюватись, а темп змін постійно збільшується. Децентралізація в інформаційних системах стала не просто черговим витком технологічної еволюції, як це було у разі появи рідкокристалічних моніторів і відмовою людей від звичних моніторів з променевою трубкою, вона пропонує кардинально новий підхід, який здатний змінити принципи взаємодії людей та побудови інформаційних систем.

Це особливо помітно, коли йдеться про політичний устрій або забезпечення довіри до систем обліку фінансів. У сучасному світі користувачі все частіше прагнуть не довіряти один одному, а мати можливість перевіряти будь-яку інформацію.

Зацікавленість у прозорих облікових системах стала особливо високою після появи цифрових платіжних систем, які висували суворі обмеження щодо часу обробки інформації та безпеки в цілому (в першу чергу етапи підтвердження та безпеки обробки транзакцій). Побічним ефектом підвищення продуктивності різних інформаційних систем стала сильна централізація та повна непрозорість таких систем, що позначилося на інформаційному просторі (житті груп людей, різних спільнот та коаліцій, і навіть країн). Можливість підключення/відключення від платіжних систем використовується як важіль політичного тиску, непрозорість цих систем знижує довіру та обмежує вільну конкуренцію (особливо в галузі електронній комерції), а доступ до історії даних (транзакцій) мають лише обмежене (вузьке) коло організацій та установ. В цілому це впроваджує де-які функціональні обмеження на процеси життєдіяльності.

До появи децентралізованих цифрових платіжних систем (Bitcoin) всі фінансові системи були закритими і захищалися традиційними методами: за допомогою спеціалізованих програмно-апаратних засобів та систем (фаєрволів, систем управління доступом тощо). Ідеологія децентралізованих цифрових

платіжних систем та їх функціонування практично доказали, що фінансова система може не тільки існувати без єдиного центру прийняття рішень та контролю/обліку/обробки даних, але також бути прозорою для всіх користувачів (з одночасним контролем та аудитом даних). При цьому зберігається приватність дій користувачів і гарантується (підвищується) безпека даних (транзакцій) за рахунок структури даних, організації їх взаємозв'язків та впровадження математичних (криптографічних) методів для їх захисту.

Принципи та архітектура системи Bitcoin, яка заснована на блокчейн технології можуть бути застосовані для вирішення широкого класу завдань, починаючи від голосування, взаєморозрахунків між різними користувачами до управління ланцюжками постачання товарів та управління різними технологічними процесами. Блокчейн як спосіб спільної обробки та зберігання інформації є технологією, що дозволяє проектувати та впроваджувати безпечні та прозорі інформаційні системи.

Крім того все більше виникає нових систем децентралізованої ідентифікації користувачів, що базуються на технології Blockchain. Тому актуальним є завдання проведення аналізу існуючих рішень забезпечення безпеки при проведенні транзакцій на базі технології Blockchain, покликаної усунути залежність від однієї компанії та децентралізувати механізм обміну даними в мережі Інтернет.

Для досягнення мети в роботі вирішуються наступні задачі:

1. Аналіз принципів роботи блокчейн систем.
2. Аналіз методів побудови блоків даних.
3. Аналіз методів забезпечення безпеки даних.
4. Аналіз потенційних вразливостей та атак на блокчейн системи.

1 БЛОКЧЕЙН СИСТЕМИ

1.1 Застосування децентралізованих систем в інформаційних мережах

В 1970-х роках. у пошуках надійнішого способу зберігання цифрових даних звернули увагу на децентралізацію, і одним з перших був реалізований проект під назвою Usenet [1]. Основний принцип полягав у тому, що сервери обмінювалися даними спеціальним алгоритмом, який забезпечував синхронізацію цих серверів між собою. Таким чином, кожен сервер являв собою локальну копію, що оновлюється, будь-якого іншого зі своєї мережі. У разі відмови в його роботі ці дані зберігалися на будь-якому іншому.

Порівняно з наявними на той момент централізованими альтернативами, підхід Usenet дозволив підвищити надійність зберігання даних.

Ідея Usenet дала уявлення про новий підхід до зберігання та синхронізації даних, тому цілком закономірно, що пізніше вона лягла в основу подальших спроб реалізувати надійний спосіб передачі даних.

У цей час було запропоновано протокол передачі файлів - FTP (File Transfer Protocol) [2]. Він дозволив користувачам незалежно передавати файли один одному і дав поштовх виникненню децентралізованих файлообмінних мереж та протоколів обміну повідомленнями, які почали активно розвиватися пізніше, у 1990-х роках. Серед них можна відзначити Topsites, IRC, Napster тощо.

На початку 1980-х світ побачив стек протоколів передачі даних TCP/IP, з яким з'явився звичний нам сьогодні Інтернет. Це стало революцією в інформаційному світі, оскільки комп'ютери отримали можливість підключатися до глобального цифрового простору. Бізнес теж отримував великі вигоди від переходу процесів у цифрову форму, і держави здебільшого підтримували цю інновацію.

Інтернет став вільною мережею для поширення інформації та прикладом для інших сфер, які стали застосовувати принципи децентралізації у пошуку та обробці даних – зараз вони називаються їх Open API та sharing economy[3]. Їхня основна ідея полягає у прямій взаємодії користувачів один з одним та у спільному використанні ресурсу, послуги, контенту, пристрою тощо.

Стрімкий розвиток децентралізації в мережі почався з появою сервісів та протоколів для кооперативного обміну файлами (рис. 1.1).

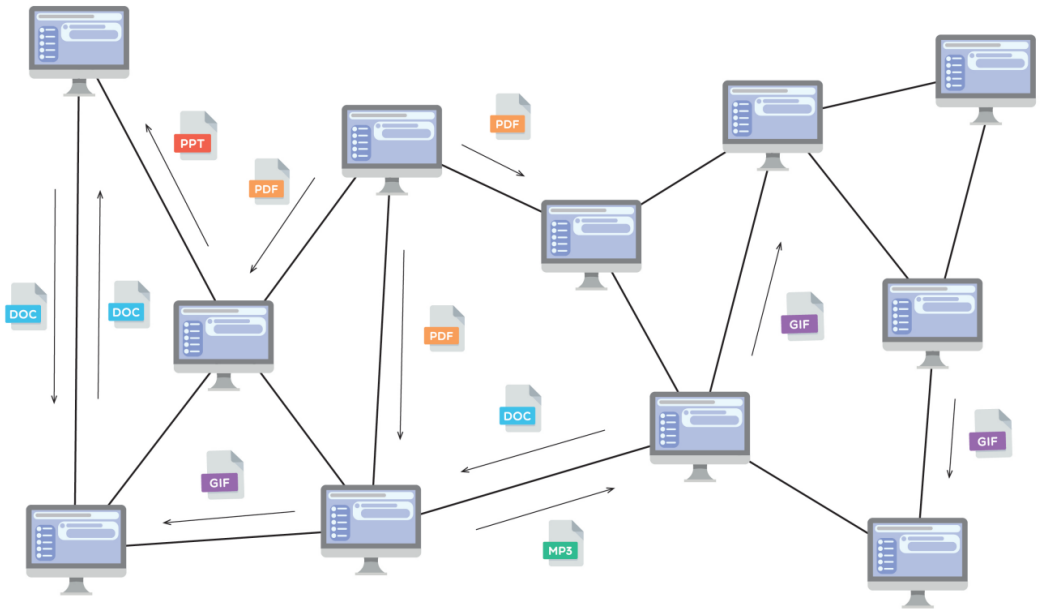

Рисунок 1.1 - Схема децентралізованої файлообмінної системи

Один з перших сервісів, Napster, надавав можливість обміну MP3-файлами. На той час музичні композиції були доступні людям переважно у вигляді касет та дисків, причому платно. Тому Napster став дуже популярним серед користувачів Інтернет. І хоча користувачі взаємодіяли за принципом peer-to-peer(P2P), база даних із файлами останньої версії все одно зберігалася на централізованому сервері. Пізніше це й послужило слабким місцем, тиск на який завершився закриттям сервісу.

Чим більше людей залучалося до роботи у глобальній мережі, тим гостріше відчувалася потреба у забезпеченні конфіденційності. На початку 2002 року був запущений проект під назвою Tor (The onion router) [4], що є системою проксі-

серверів, що дозволяють встановлювати анонімне мережне з'єднання, захищене від стеження передачі даних. Реалізація Tor дозволила користувачам з усього світу оминати блокування трафіку місцевих провайдерів та отримувати доступ до даних, зберігаючи свою конфіденційність [5].

Технології, що ґрунтуються на принципах децентралізації, отримали дуже сильний поштовх до розвитку в окремих сферах. Наприклад, у 2004 році було запущено перші проекти з використання бездротових mesh-мереж у Південній Африці. Принцип їхньої роботи полягає в тому, що користувачі самі підтримують канали передачі даних та виконують маршрутизацію пакетів даних по мережі. У такій мережі вузли «слухають» один одного, і якщо один із них виходить з ладу, то ті вузли, які були підключені до нього, шукають альтернативні вузли для підключення. Такий спосіб організації мережевої взаємодії зробив Інтернет більш доступним у тій місцевості, де централізовані провайдери не стали розміщувати своє устаткування з різних причин.

Децентралізовані обчислювальні системи (grid systems) – це системи, які використовують розподілені комп'ютерні ресурси задля досягнення спільної мети (рис. 1.2). Кількість вузлів у таких системах може коливатися від кількох машин до сотень і тисяч робочих станцій.

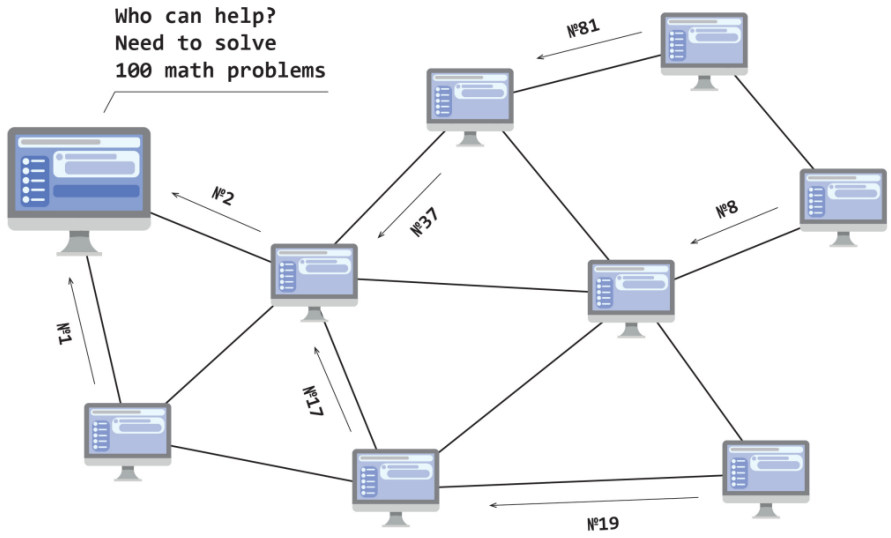

Рисунок 1.2 - Схема децентралізованої обчислювальної системи

Такий підхід вперше був запропонований у 1999 році у публікації "The Grid: Blueprint for a new computing infrastructure" [6]. У тому ж році було запущено перший проект, в якому реалізовано цей підхід під назвою SETI@home [7]. На даний момент існує безліч реалізацій подібних проектів, таких як BOINC, Folding@home, Einstein@Home, тощо. Вищезгаданий проект SETI@home, що з'явився раніше, досі є одним із найпотужніших розподілених суперкомп'ютерів.

Перераховані вище проекти дозволили зрозуміти, яким шляхом можна поліпшити існуючі системи зберігання даних.

Децентралізований підхід для побудови таких систем передбачає, що різні фрагменти файлів зберігаються різними вузлами мережі (рис. 1.3).

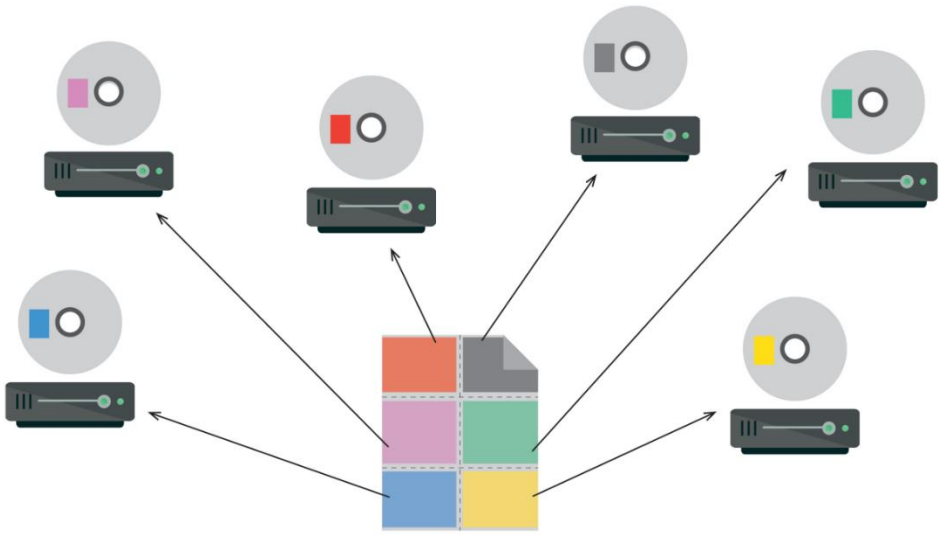

Рисунок 1.3 - Схема децентралізованої системи зберігання даних

У 2001 році з'явився BitTorrent – протокол, який дозволив працювати швидко, ефективно та був не тільки стійким до відмови, а й незалежним. Звичайно, спочатку для роботи був потрібен централізований клієнт, але пізніше з'явилися torrent-клієнти, що важко відслідковуються, а використання VPN дозволило підвищити рівень анонімності користувачів. І саме BitTorrent на сьогоднішній день є все ще функціонуючим продуктом, символом децентралізованого підходу – підходу, який успішно працює і досі.

Іншим способом застосування децентралізованого підходу є системи прийняття рішень. Працюють вони наступним чином, якщо 5 чоловік поклали в сейф торт і домовилися, що з'їдять його тільки якщо бажаючих буде більшість. Вони розділили секрет від кодового замку та розподілили частини секрету між собою. Тепер торт може бути з'їдений, але тільки якщо більшість учасників договору ухвалить рішення поділитися своєю частиною секретів та відкрити замок сейфу.

На сьогоднішній день дуже великі фірми не можуть керуватися однією людиною, а якщо такі й існують, то їхня ефективність перебуває під великим сумнівом. Тому практично у будь-якій великої компанії існує рада директорів та численна штат радників, а іноді для прийняття рішень враховуються і голоси працівників компанії. Практика показує, що такий підхід дійсно підвищує ефективність компанії завдяки співпраці людей з різними поглядами, з різними підходами до оцінки конкретної проблеми та її вирішення. Таким чином, кінцеве рішення можна вважати об'єктивнішим.

Наступним кроком стала децентралізація платіжних систем. Їх було найскладніше децентралізувати з цілком зрозумілої причини чутливості людей до всього, що безпосередньо пов'язане з безпекою їхніх грошей. Винахід грошей підняло поняття приватної власності на той рівень, на якому її стало набагато простіше оцінювати (можливість об'єктивної оцінки – одна з основних властивостей грошей). Гроші були історично прив'язані до товарів, таких як золото, корови, хутра, черепашки, сигарети тощо. Рівень добробуту людини обчислювався кількістю товару, яким він володів.

Сьогодні гроші набули цифрового вигляду і, по суті, стали числами в базі даних, що відображають ставлення між людьми, засобом оцінки можливостей, влади та статусів людей щодо один одного. Проблема з грошима такого роду полягає у непрозорості процесу випуску, який може бути обумовлений рішеннями окремих людей, а не загальною згодою. Це цілком логічно, оскільки

саме собою завдання досягнення загальної згоди щодо монетарної політики зовсім не із категорії тривіальних рішень.

У 2009 році поява Bitcoin, а саме першого дефіцитного цифрового активу, надихнула людей на ідею відокремити гроші від держави або банків (незалежно від її реалізації). Подібне сталося в деяких розвинених країнах сторіччя тому, коли релігія та преса стали існувати незалежно від держави. Тим не менш, на сьогоднішній день поняття єдиної національної валюти досі передбачено у конституціях більшості країн.

Головне питання полягає в тому, чи можливо створити ефективну платіжну систему із спочатку необмеженою емісією, здатну моделювати роботу фіатних грошей, але при цьому позбавлену впливу окремих людей. Напевно, можна сказати, що можливість створення цифрового дефіциту (обмеженої математикою емісії) та програмованих правил роботи (конституції, гарантованої криптографією) є революційною для багатьох аспектів життя і, без сумніву, продовжуватиме розвиватися. Тому розуміння принципів роботи Bitcoin необхідно, щоб успішно адаптуватися до реалій нового цифрового світу.

На прикладі Bitcoin у даній роботі описано механізм транзакцій та забезпечення їх безпеки при функціонуванні системи, оскільки багато принципів, згідно з якими він спроектований і реалізований, є фундаментальними для будь-якої децентралізованої системи.

2 ПОНЯТТЯ ТРАНЗАКЦІЇ

У цьому розділі здійснено аналіз основної концепції формування та обробки даних в децентралізованих системах, які стосуються: поняття транзакції (на прикладі Bitcoin): що таке біткоін-транзакція, як у розподіленій базі даних гарантується безпека даних, здійснюється перевірка їх цілісності, як користувачі забезпечують права та доступ до даних (монет), якими вони оперують, основний опис та призначення комісій у Bitcoin, поняття конфліктуючої транзакції та основні концепції забезпечення захисту даних у блокчейн системах.

2.1 Bitcoin транзакція

Транзакція – це набір цифрових даних, за допомогою якого відбувається оновлення бази даних (передача даних (монет) з однієї адреси на іншу). Власне, транзакція визначає як суму переказу та адресу одержувача, так і умови, які необхідно виконати для отримання доступу до монет.

Життєвий цикл транзакції складається з наступних етапів:

- створення;
- розповсюдження;
- верифікація;
- валідація (включення в блок);
- відторгнення.

До складу bitcoin-транзакції входить наступна інформація:

- походження монет, що витрачаються;
- доказ володіння монетами;
- адреса для переказу (умови витрати);
- сума переказу.

Насамперед, транзакція містить дані про походження монет, які витрачаються (тобто посилання на транзакції, де ці монети були отримані),

докази володіння монетами, адреси нових власників (у ширшому розумінні – умови, за якими монети можуть бути витрачені) та суми переказів.

У найпростішому випадку адреса прив'язана до однієї пари ключів (відкритий ключ та особистий ключ), яка використовується для формування та перевірки цифрового підпису. Особистий ключ використовується для засвідчення транзакцій. Важливо відзначити, що простір усіх можливих адрес величезна, а простір можливих особистих ключів ще більше - 2^{256}. При коректній генерації вгадати чи підібрати особистий ключ до чужої адреси практично неможливо. Важливо не плутати поняття адреси з поняттям облікового запису, оскільки в рамках протоколу Bitcoin облікових записів не існує (це стосується інших децентралізованих блокчейн систем).

Транзакція має задовольняти певним вимогам, щоб її можна було вважати коректною. По перше, вона формує та здійснює обмін даними (має переводити монети, що належать відправнику). По-друге, обробка цих даних (монет) проводиться однократно - можна витратити монети лише один раз (мається на увазі, що ті самі монети не можна перекласти одразу двом одержувачам, як і у випадку зі звичайною банкнотою). Це гарантується етапом верифікації.

Верифікація – це процес перевірки даних (транзакцій, блоків тощо) відповідно до правил протоколу. В процесі верифікації для кожної транзакції перевіряється доказ того, що відправник має монети, які витрачає. Зазвичай автор транзакції доводить володіння монетами за допомогою цифрового підпису. Також необхідно перевірити, що транзакція витрачає існуючі монети, один раз і вперше (як і було написано раніше, йдеться про випадок, коли людина намагається витратити одні й ті самі монети двічі).

Складновирішуваною проблемою даного підходу являється перевірка оригінальності транзакції, оскільки одну транзакцію, теоретично, можна виконати більше одного разу. При цьому необхідно бути впевненим, що транзакція правильно сформована і раніше не оброблена. Тому необхідно вирішити проблеми цього напрямку.

У Bitcoin передбачено об'єднання транзакцій у структурні одиниці під назвою блоків. Блок являє собою одиницю даних, яка складається з заголовка та тіла блоку, яке є набір транзакцій (зазвичай не порожній). Блоки зв'язуються між собою за допомогою хеш-значень і в такому вигляді зберігаються у розподіленій базі даних. Подібний підхід дозволяє забезпечити незмінність бази даних всіх транзакцій.

2.2 Блок транзакцій

Блок транзакцій - спеціальна структура для запису групи транзакцій у системі Біткойн та аналогічних їй. Транзакція вважається завершеною та достовірною («підтвердженою»), коли перевірено її формат та підписи, і коли сама транзакція об'єднана в групу з кількома іншими та записана у спеціальну структуру — блок.

Вміст блоків може бути перевірено, оскільки кожен блок містить інформацію про попередній блок. Всі блоки вибудовані в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції в базі. Найперший блок у ланцюжку — первинний блок (англ. genesis block) — сприймається як окремий випадок, оскільки він не має попереднього блоку. (рис 2.1)

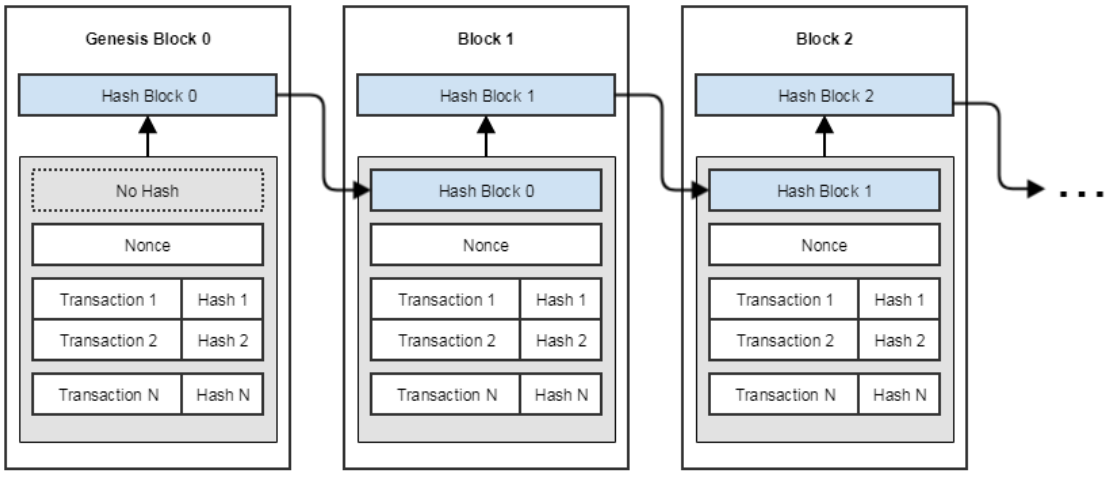

Рисунок 2.1 - Схема отримання хешу транзакцій

Блокчейн формується як ланцюжок блоків, що безперервно зростає, з записами про всі транзакції.

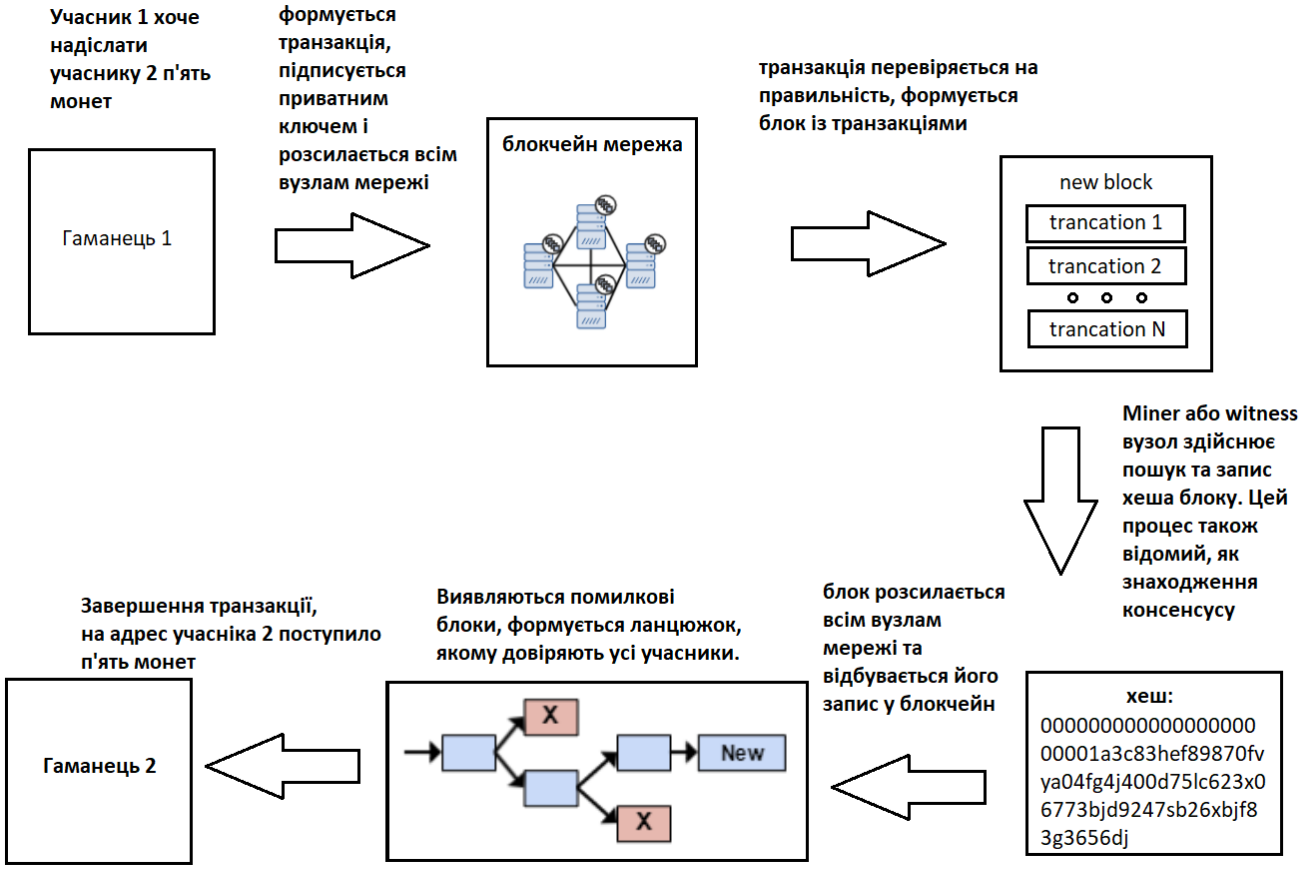

Рисунок 2.2 – Життєвий цикл транзакції

Копії бази або її частини одночасно зберігаються на багатьох комп'ютерах і синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блоках не шифрована і доступна у відкритому вигляді, але відсутність змін засвідчується криптографічно через хеш-ланцюжки. Повний життєвий цикл транзакції можна побачити на рисунку 2.2.

Щоб мати змогу обробляти велику кількість блоків за адекватний час, у блокчейн системах використовують дереве Меркла у якості структури збереження даних.

Концепцію побудови таких дерев уперше опублікував 1979 року Ральф Меркл [11]. Одним із перших застосувань дерев Меркла стало їх використання у протоколі BitTorrent. Дерева Меркла є структурою даних, яка дозволяє зв'язати

окремі фрагменти даних в єдине кореневе значення і після довести, що певний блок даних дійсно має відношення до конкретного кореневого значення.

Дерево Меркла містить такі компоненти (рис. 2.3):

– листя дерева (Merkle leaves);

– вузли дерева (Merkle nodes);

– корінь дерева (Merkle root).

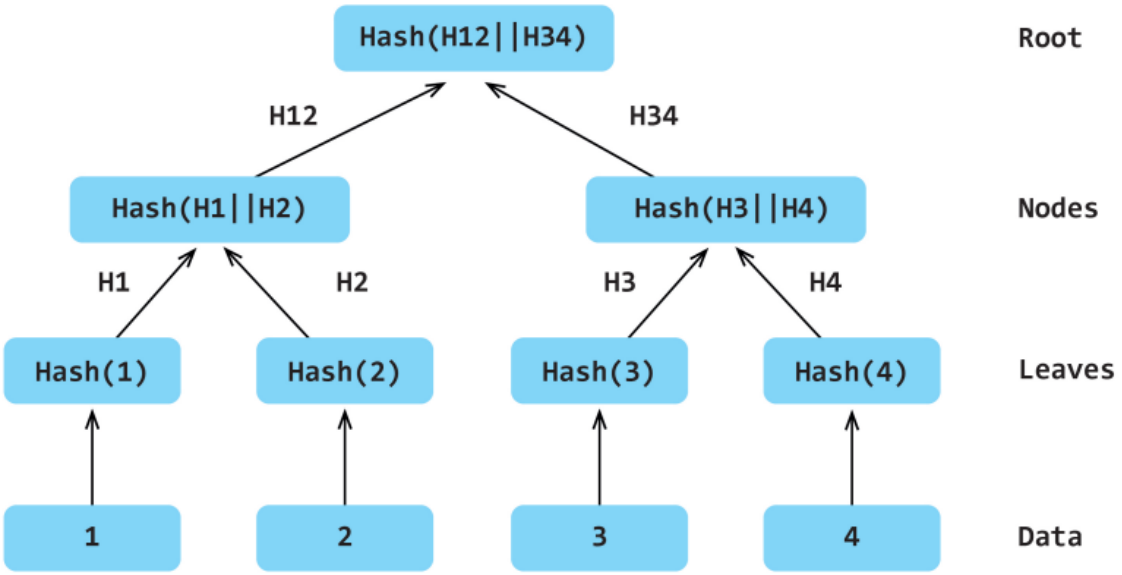

Рисунок 2.3 - Схема компонентів дерева Меркла.

Листя дерева Меркла є геш-значеннями для блоків даних, які необхідно зібрати в структуру. Вузол дерева є значенням, яке було отримано внаслідок конкатенації та подальшого гешування двох дочірніх вузлів або листя. Корінь дерева Меркла також є вузол, що знаходиться на вершині дерева.

Така технологія забезпечує можливість швидкої перевірки цілісності та незмінності великих даних завдяки наступним властивостям:

– зміна хоча б одного біта в одному з блоків даних спричинить повну зміну значення Merkle root;

– при порушенні одного з блоків можна досить швидко і точно визначити, який саме блок був модифікований;

– можна швидко перевірити, чи входить певний блок у структуру дерева Меркла.

2.3 Перевірка транзакцій

Відомо, що паперові чеки досі поширені у банковській сфері та люди отримують ними заробітну плату, сплачують оренду, переводять у готівку в банках тощо. На самому чеку можна побачити його серійний номер, у кожного чека він унікальний. Неможливо перевести в готівку два чека з однаковими серійними номерами (це вже шахрайство).

В чековій книжці унікальним ідентифікатором є порядковий номер чека. Але в децентралізованому середовищі, де функціонує Bitcoin, пронумерувати транзакції неможливо, оскільки усі учасники працюють асинхронно. Тому для того, щоб відрізняти одну транзакцію від іншої, вводиться глобальний унікальний ідентифікатор транзакції (txid/wtxid) – хеш-значення, розраховане від даних самої транзакції. Якщо зустрічається кілька транзакцій з однаковим хеш-значенням, враховується лише одна.

Цікава особливість Bitcoin полягає в тому, що існує можливість у будь-якій транзакції показати, звідки беруться монети, тобто виконується посилання на попередню транзакцію із зазначенням її хеш-значення. Таким чином, відбувається перевірка історії походження монет, що передаються.

Отже, можна виділити основні етапи верифікації транзакції:

– перевірка умови, що витрачаються монети, які існують в обліковій системі;

– перевірка умови, що конкретні монети не витрачаються двічі;

– перевірка доказів володіння монетами, які надав відправник (ініціатор транзакції).

Щоб витратити монети, користувач повинен показати, де він їх отримав, і довести, що саме він володіє ними. Якщо походження монет не викликає

додаткових питань, відсутня інша транзакція, яка витрачає ці монети, і користувач дійсно довів, що він є власником, то залишається лише дочекатися підтвердження цієї транзакції рештою учасників мережі.

Процес підтвердження транзакцій передбачає, що учасники попередньо перевіряють їх, після чого спільно узгоджують, які транзакції вважатимуться правильними. Для підтвердження транзакція має отримати згоду більшості активних учасників. В процесі підтвердження транзакцій у Bitcoin може взяти участь будь-хто.

Модель транзакцій у Bitcoin передбачає комісійні збори, що оплачуються монетами мережі. Комісію визначає сам відправник у момент створення транзакції, і за умовчанням вона повинна бути вищою за певне порогове значення. Хоча на практиці користувач може встановити її рівною нулю і така транзакція теоретично вважатиметься правильною. Цю комісію як додаткову винагороду отримує один із учасників, який підтверджує транзакцію (додає її до свого блоку).

Зі зростанням популярності Bitcoin значно збільшився потік нових транзакцій у мережі. При цьому відомо, що за протоколом розмір блоку суворо обмежений. У Bitcoin максимальний базовий розмір блоку становить 1 МБ. Відповідно, бувають такі ситуації, коли потік нових транзакцій перевершує пропускну здатність Bitcoin. При цьому кожен вузол мережі вибудовує всі непідтверджені транзакції в чергу таким чином, що спочатку підтверджуються ті транзакції, які сплачують комісію більшого розміру за одиницю своєї ваги. Ціна запису даних визначається як відношення встановленої у транзакції комісії до її розміру в байтах. Очевидно, що транзакції, які потрапляють у кінець черги, можуть довго залишатися непідтвердженими. Це не завжди зручно, тому що формується ринок, що важко передбачається, на ціну запису одиниці даних в базу Bitcoin.

Принципи децентралізації, які застосовуються для встановлення комісій у bitcoin-транзакціях, можна проілюструвати на наступному прикладі. Умовно

можна порівняти потенційно підтверджений блок із політичною партією, яка має шанси пройти до парламенту. Місця в прохідній частині партії дістануться тим депутатам, які запропонують найбільшу «компенсацію». Очевидно, що депутатів буде «відсортовано» за розміром компенсації, і ті, хто запропонував менше деякого значення, навіть не потраплять у прохідну частину списку. Швидше за все, їм доведеться чекати на наступні парламентські вибори і повторити спробу. Однак ця проблема може бути вирішена.

Отже, транзакції слідують наступним принципам:

– транзакція сплачує комісію за одиницю своєї ваги;

– максимальний базовий розмір блоку – 1 MB;

– валідатори сортують транзакції зі спадання ціни запису даних;

– транзакції з низькою ціною запису даних можуть залишитися непідтвердженими надовго (або назавжди).

В деяких випадках, можуть виникати конфліктуючі транзакції. Це такі транзакції, що посилаються на одні й ті самі дані, тобто транзакції у яких намагаються повторно витратити монети. Така ситуація може виникнути, якщо, після створення першої транзакції, пройшло не багато часу і вона ще не підтверджена, а вже створена інша транзакція, яка оперує тими самими монетами, що ще належать відправнику. Очевидно, що обидві транзакції не можуть бути включені в одну версію блокчейну. Тоді виникає питання, куди підуть витрачені монети - адресату з першої транзакції, або з другої. До моменту повного підтвердження однозначно відповісти на нього неможливо. Можна лише сказати, що з більшою ймовірністю підтвердиться саме та транзакція, яка раніше була поширена через мережу, або та, що сплачує комісію більшого розміру.

2.4 Підтвердження транзакцій

Будь-який користувач може вибрати серед непідтверджених транзакцій такі, які він вважає правильними, після чого об'єднати їх у блок та запропонувати цей блок решті всіх вузлів мережі. За рішенням більшості блок може бути прийнятий або відхилений. Якщо сам валідатор працював чесно, верифікував транзакції за правилами протоколу і першим запропонував наступний блок загального ланцюжка, інші чесні учасники приймуть цей блок.

По-перше, варто розглянути деталі створення транзакції.

Правильно сформований блок складається з непідтверджених у попередніх блоках транзакцій, які не конфліктують між собою. Кожен блок обов'язково містить хеш-значення попереднього блоку. Це означає, що блок підтверджує не лише свої транзакції, але й усі попередні, вже включені в ланцюжок, на який цей блок посилається. Ще одна особливість формування блоків полягає в тому, що протокол регулює складність ресурсомісткої задачі для формування блоків таким чином, щоб вони з'являлися в середньому один раз на 10 хвилин.

Отже, правильно сформований блок:

– містить коректні, ще не підтверджені транзакції, які не конфліктують один з одним;

– містить геш-значення попереднього блоку.

Щоб сформувати новий блок комп'ютер деякого користувача під керуванням програмного забезпечення (ПЗ) системи Bitcoin зберігає весь ланцюжок блоків, які були верифіковані цим комп'ютером і вважаються правильними. Однак у мережі постійно здійснюються перекази між користувачами та з'являються нові непідтверджені транзакції, які розповсюджуються по всіх вузлах. Комп'ютер даного користувача верифікує потік цих транзакцій і об'єднує в блок ті, які вважає правильними (рис. 2.2). Далі він обов'язково вказує посилання на попередній блок, щоб було зрозуміло, на підставі якої історії він працює, і щоб дотримувалася цілісність бази даних. Після

цього він пропонує іншим вузлам мережі свій блок як продовження загального ланцюжка.

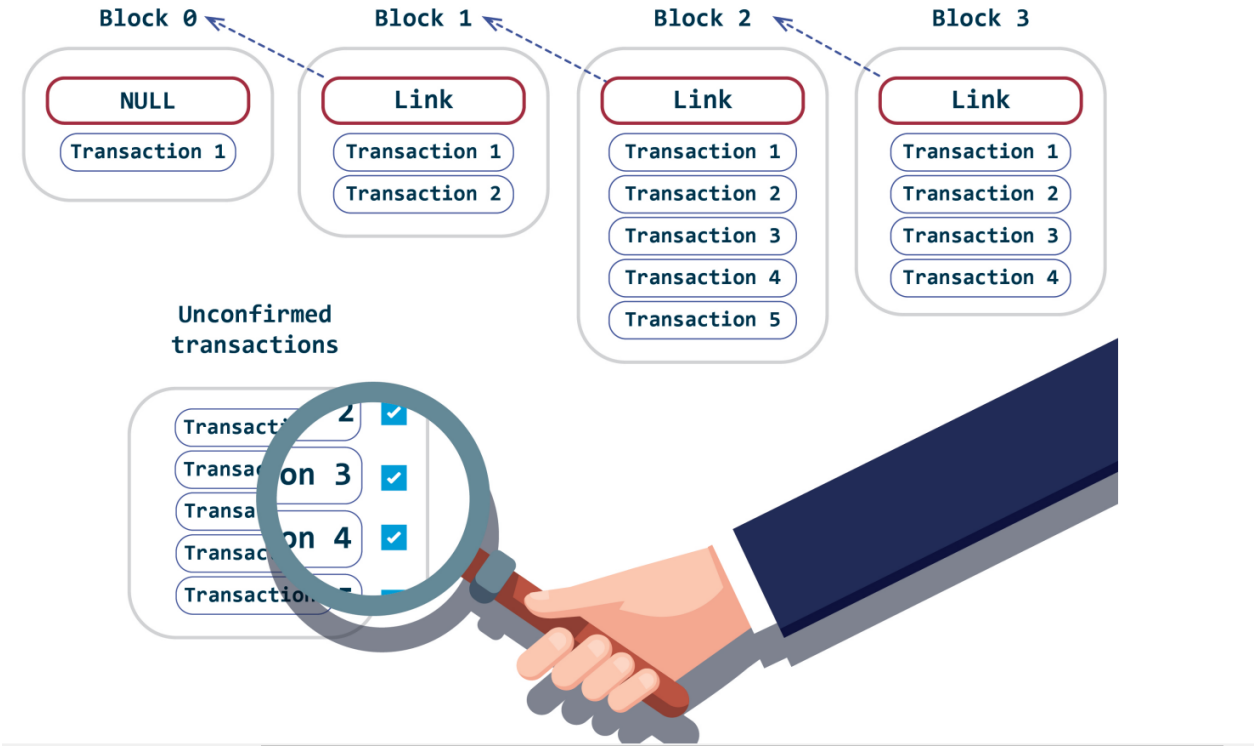

Рисунок 2.4 - Схема створення нового блоку користувачем

Але, у разі, якщо деякий користувач, запустить такий вузол мережі, який шахраюватиме, пропонуючи підроблені блоки іншим користувачам, або це може бути не один користувач, а організована група зловмисників, яка запустила цілу мережу ботів (botnet) із модифікованих вузлів мережі, які нехтують правилами протоколу. Для вирішення цієї задачі було висунуто певні вимоги до створення нових блоків:

– будь-який користувач може вибрати серед непідтверджених транзакцій правильні та об'єднати їх у блок;

– запропонований блок буде прийнято або відхилено за рішенням більшості валідаторів.

Вирішення проблеми з підробленими блоками полягає в наступному - блок вважається правильним, якщо на його створення було витрачено задану кількість

обчислювальних ресурсів. Це означає, що користувач повинен надати вирішення ресурсомісткої задачі, щоб всі інші учасники могли перевірити та прийняти його блок.

Завдяки цьому зловмисник не зможе відволікати решту учасників великою кількістю підроблених блоків. Попутно з цим вирішуються питання частоти появи нових блоків та черговості валідаторів у формуванні наступного блоку. Працює це в такий спосіб. Починають формувати новий блок всі, але право запропонувати свій блок решті отримує тільки той, хто вирішив ресурсомістке завдання першим.

Отже процес створення нового блоку складається з наступних кроків:

– вирішення ресурсомісткої задачі;

– розповсюдження нового блоку у мережі.

Імовірність стати першим залежить від частки ресурсів учасника у всіх обчислювальних ресурсах, задіяних у мережі, а також від затримок у каналах передачі даних.

Очевидно, що чим більше у користувача обчислювальних потужностей, тим частіше він стає першим серед решти бажаючих. Таким чином, можливість стати першим визначається відсотком обчислювальних ресурсів учасника від усіх ресурсів, задіяних у мережі.

Такий спосіб верифікації блоків називається майнінгом. Необхідно розуміти, що це завдання має однакову складність для всіх вузлів мережі. Майнінг дуже важливий для Bitcoin, і чесні користувачі займаються цим з метою підтримки надійності процесу підтвердження транзакцій. Справедливо, що той, хто контролює більше потужності, створює блоки найчастіше.

Основою блокчейн транзакцій є геш-значення, які використовуються як контрольні суми при передачі даних. Щоб перевірити, що повідомлення не було випадково порушено через якісь шуми в каналі передачі даних, сторона, що приймає, може повторно обчислити геш-значення від отриманих даних і порівняти його з уже наявним. Також такі функції використовуються для пошуку

дублікатів під час зберігання або для порівняння великих масивів даних. Щоб не порівнювати великі обсяги даних безпосередньо, можна зберігати відповідні значення геш-функцій і порівнювати тільки ці значення.

Якщо значення геш-функції для різних наборів даних збігаються, значить велика ймовірність, що і самі дані збігаються. Це значно прискорює процес, наприклад, для формування цифрового підпису. Зазвичай під час підписання документа підписуються не самі дані повідомлення, а їх геш-значення. При цьому вважається, що це геш-значення передається разом із повідомленням та підписом: так одержувач може перевірити і цілісність повідомлення, і коректність цифрового підпису.

Для перевірки цілісності використовується результат обчислення геш-коду по методу двійкового дерева Меркла (рис. 2.5). Таким чином, для верифікації цілісності і-го блоку даних на різних рівнях ієрархії даних використовується кортеж (2.1):

$$\langle (h_n^i, h_n^{i+1}), (h_{n-1}^i, h_{n-1}^{i+1}), \dots , (h_1^i, h_1^{i+1}), h_0 \rangle, \qquad (2.1)$$

де:

h - геш-код блоку даних;

i - номер поточного блоку;

n - кількі блоків у блокчейні.

Всього для верифікації блоку даних необхідно не більше O (log2 n) операцій та геш-кодів. Загальний принцип побудови конструкції «ланцюжка блоків транзакцій» із використанням дерева Меркла показаний на рисунку 2.5.

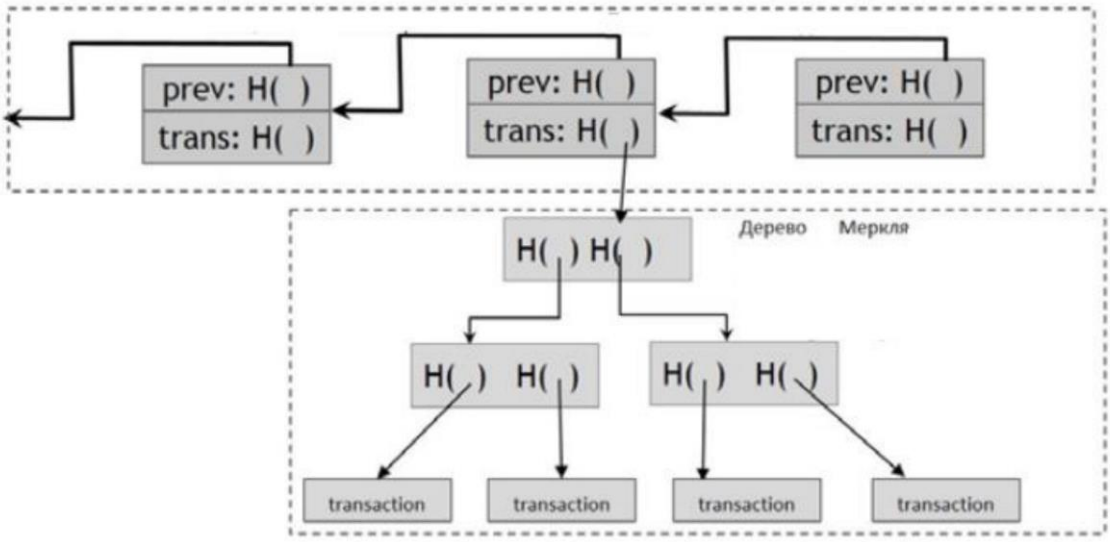

Рисунок 2.5 - Загальний принцип побудови конструкції «Ланцюжка блоків транзакцій»

Як зазначено раніше, кожен блок у Bitcoin складається з двох частин:

– заголовок блоку з ключовими параметрами, включаючи час створення блоку, посилання на попередній блок та корінь дерева Меркла [11] блоку транзакцій;

– перелік транзакцій.

Щоб посилатися на конкретний блок, його заголовок гешується двічі за допомогою функції SHA-256 [12], а підсумкове ціле число належить відрізку $[0, 2^{256} - 1]$.

Щоб врахувати різні можливі реалізації, загальна геш-функція позначається hash (дані) з різним числом аргументів та областю значень [0, M]. Наприклад, аргументи функції можуть розглядатися як бінарні рядки, які з'єднуються разом, формуючи один аргумент, який може бути переданий на вхід SHA-256 геш-функції.

Посилання на блок використовується у протоколі, який використовує доказ роботи; щоб блок вважався дійсним, його посилання має не перевищувати певний поріг (2.2):

$$hash(X) \leq \frac{M}{D}, \qquad (2.2)$$

де:

D є [1, M] - цільова складність;

X - вхідне значення;

M - верхня границя області значень.

Не існує відомого способу знайти X, задовільняючого нерівності (2.2), крім послідовного перебору за всією можливою областю значень заголовків блоку. Чим більше величина D, тим 6 більше ітерацій необхідно зробити, щоб знайти діючий блок; очікуване число операцій дорівнює D.

Час $T(r)$, який потрібен валідатору з обладнанням, здатним виконувати r операцій в секунду, щоб знайти новий блок, має експоненційне розподілення за параметром r/D (2.3):

$$P\{T(r) \leq t\} = 1 - \exp\left(-\frac{rt}{D}\right). \quad (2.3)$$

Стосовно майнерів Bitcoin (тих хто формує транзакції в вигляді блоків) з частками гешуючої потужності $r1, r2, \dots, rn$, час T – для формування блоку, дорівнює мінімальному зі значень випадкових величин T(r_i) в припущенні, що валідатор одразу ж розповсюджує новий блок і блок досягає інших вузлів (нод) без затримок. За власними властивостями експоненційного розподілу, T також розподілено експоненційно:

$$P\{T \stackrel{\text{def}}{=} \min(T_1, \dots, T_n) \leq t\} = 1 - \exp\left(-\frac{t}{D}\sum_{i=1}^{n} r_i\right), \quad (2.4)$$

$$P\{T = T_i\} = \frac{r_i}{\sum_{j=1}^{n} r_j}. \quad (2.5)$$

Згідно до формули 2.5 - валідатор з обчислювальною потужністю p має таку ж саму вірогідність p створити блок раніше інших.

Таким чином, можна зробити висновок про те, що технологія блокчейн може називатися безпечною, оскільки жоден користувач не може заплановано впливати на результати валідації з метою прискорення або компрометації процесу, а процеси формування та обробки даних виконуються за допомогою різних математичних (криптографічних) методів та алгоритмів.

2.5 Поширення блоку транзакцій

Після створення та валідації нового блоку транзакцій, цей блок поширюється в мережі. Це означає, що сформований блок, який містить у собі свідчення про вирішення ресурсомісткої задачі та посилання на попередній блок, отримують всі користувачі мережі з якими існує з'єднання. Після цього вузли, що прийняли блок, перевіряють його на відповідність до правил протоколу. Існує два варіанти розвитку подій. У першому випадку, якщо вузол погоджується, що прийнятий блок є коректним і може бути доданий в ланцюжок блоків, він зберігає собі копію блоку і поширює його далі по мережі. У іншому випадку, якщо один учасник не згоден із блоком іншого, то цілком нормальним вважається створити альтернативний блок на тій самій висоті ланцюжка блоків.

Висотою блоку називається порядковий номер блоку в ланцюжку щодо genesis block (рис. 2.6). Genesis block – блок, висота якого дорівнює нулю (перший блок в системі).

Рисунок 2.6 - Схема ланцюга блоків із зазначенням висоти кожного блоку

Таким чином, факт незгоди одного з учасників може спричинити ситуацію, коли буде сформовано два блоки, які посилаються на один попередній. Такі блоки можуть включати навіть однакові або конфліктні транзакції. При цьому вузли мережі можуть зберегти обидва запропоновані варіанти, якщо вважатимуть їх правильними, але кожен із цих вузлів повинен для себе визначити, на базі якого з альтернативних блоків створювати наступний. Таким чином, решта учасників робить свій вибір, формуючи блоки на основі одного з

існуючих блоків, вказуючи посилання на нього у новому блоці продовження конкретної версії ланцюжка. А правила протоколу вказують на те, що з двох правильних версій пріоритет слід віддавати тій, на створення якої було витрачено більше обчислювальних ресурсів.

Процес вирішення розбіжностей можна зобразити схематично (рис 2.7)

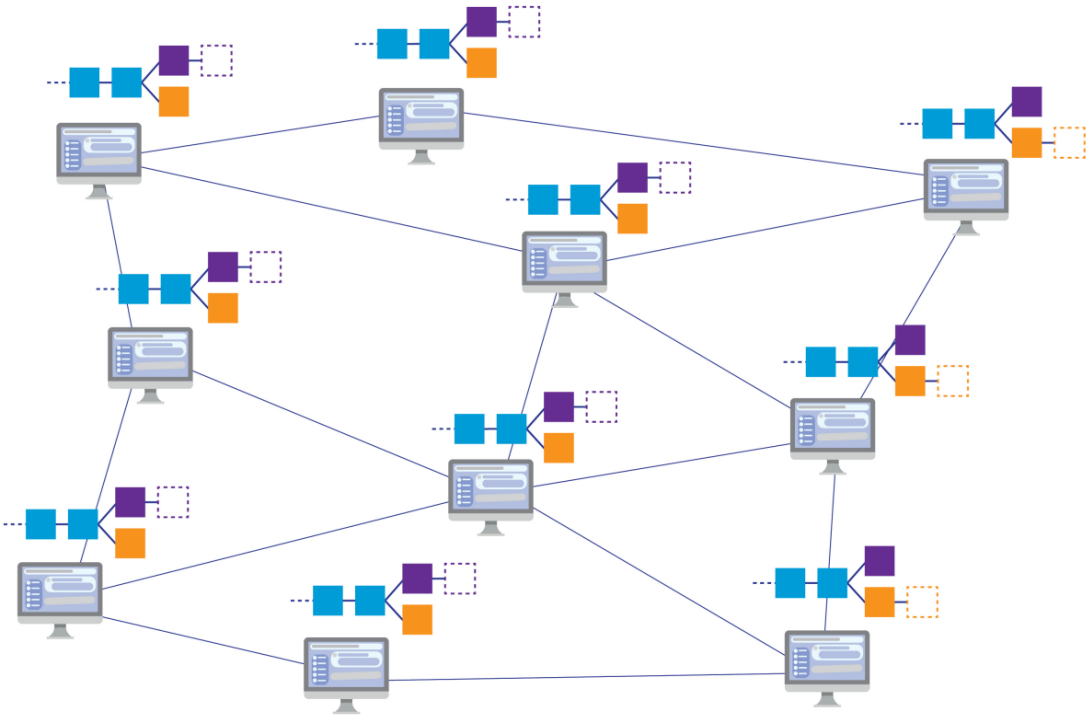

Рисунок 2.7 - Схема процесу вирішення розбіжностей

Існує мережа вузлів, у локальних копіях бази даних яких є два альтернативні блоки на одній висоті. Умовно, користувачі ліворуч вирішили вибрати верхній блок як основний, а користувачі праворуч – нижній. І, якщо всі продовжують працювати над створенням наступного блоку, підтримуючи різні версії, то в наступний момент часу якийсь користувач створив і запропонував новий блок, який посилається на верхній із двох альтернативних. При цьому його пропозиція була прийнята рештою учасників мережі. І навіть ті учасники, які спочатку обрали інший альтернативний блок, перевірили та прийняли довший ланцюжок (рис. 2.8).

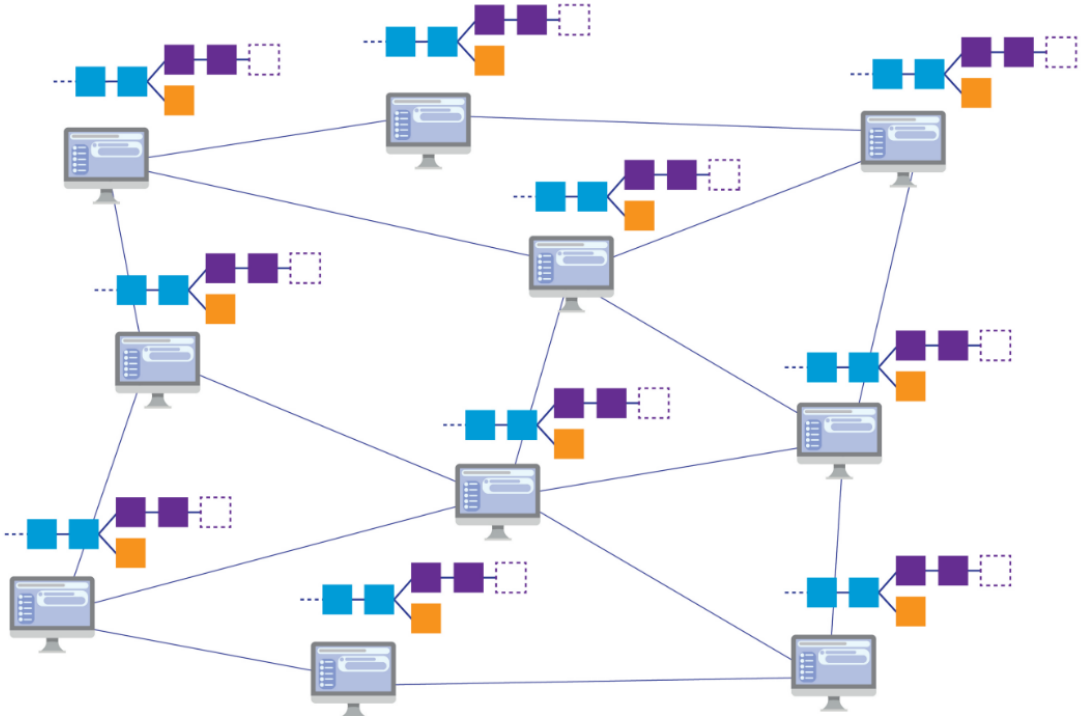

Рисунок 2.8 - Схема процесу вирішення розбіжностей після прийняття рішення учасниками щодо валідності блоків

Це правило найдовшого ланцюжка. Дане правило свідчить про те, що учасник повинен вибирати найдовший ланцюжок з усіх, які він вважає правильними, і вважати його основним. Іншими словами - вибирається той ланцюжок, для створення якого було виконано більше роботи. Причому важливо розуміти, що чесний учасник переключиться на найдовший ланцюжок лише в тому випадку, якщо він був побудований за правилами протоколу. Це не дозволяє зловмисникам порушити початкові правила Bitcoin, навіть якщо вони володітимуть великою обчислювальною потужністю.

Отже вирішення розбіжностей відбувається таким чином:

– незгодний учасник формує альтернативний блок;

– альтернативні блоки можуть містити однакові транзакції;

– вузли мережі зберігають обидва варіанти;

– інші учасники формують блоки, продовжуючи одну з версій ланцюжка;

– перемагає ланцюжок з найбільшою довжиною (найбільшою кількістю роботи, витраченої на її побудову).

Транзакція вважається достатньо підтвердженою, якщо вона включена в найдовший ланцюжок і після блоку, в якому вона міститься, слідує ще 5 блоків. Інакше висловлюючись, потрібно дочекатися 6 підтверджень, замість 1. Якщо врахувати, що блок з'являється загалом 1 разів у 10 хвилин, неважко визначити, що повне підтвердження транзакції займає приблизно одну годину.

Відповідь на питання, чому необхідно саме 6 підтверджень, дає математичний розрахунок: якщо один ланцюжок випереджає інший на 5 блоків, при тому ж розподілі обчислювальної потужності ймовірність обігнати довший ланцюжок вкрай мала. Сатоші Накамото в своїй роботі [8] математично довів цей зв'язок на підставі такого виразу (2.6):

$$q_z = \begin{cases} 1, & p \le q \\ \left(\frac{q}{p}\right)^z, & p > q \end{cases} \qquad (2.6)$$

де:

p - ймовірність, що наступний блок буде знайдено чесним вузлом;

q - ймовірність, що наступний блок буде знайдений атакуючим;

q_z - ймовірність, що атакуючий колись наздожене основний ланцюжок, якщо він розпочав альтернативну z блоків назад.

Наприклад, якщо зловмисник має 10% обчислювальної потужності всіх валідаторів, а чесні вузли працюють у мережі зі швидкою доставкою повідомлень, то ця ймовірність після 1 підтвердження матиме значення близько 0.1, а після 6 – менше 0.000002.

Ще одне важливе питання – це мотивація користувачів вирішувати ресурсомісткі завдання, створювати нові блоки та підтверджувати транзакції, не залишаючи шансів зловмисникам.

В блокчейн системах (в перше чергу в Bitcoin) процеси формування блоків, емісії та підтвердження транзакцій дуже тісно пов'язані один з одним. Це пояснюється тим, що за правилами протоколу автор блоку може відправити на свою адресу певну кількість монет, взявши їх з нізвідки (це винагорода за формування блоку). Це і є емітовані монети. Підсумкова сума винагороди розраховується як емітовані монети плюс сума комісій усіх транзакцій, доданих до цього блоку.

Таким чином, у 2009 році винагорода за створення блоку була 50 монет, в 2012 — 25, в 2017 — 12.5, а починаючи з 2020 року — 6.25 монет плюс комісійні збори.

З міркувань організації безпеки в системі валідатор не отримує цієї винагороди відразу після створення блоку. Існує спеціальний параметр coinbase maturity [9]. Він вказує на мінімальну кількість підтверджень транзакції, у якій валідатор отримує винагороду. У Bitcoin цей параметр має значення 100, отже, після створення блоку необхідно дочекатися появи ще 99 блоків, які будуть підтверджувати цей, перш ніж винагорода стане доступною.

Як було зазначено раніше, блоки з'являються в середньому кожні 10 хвилин незалежно від сумарної обчислювальної потужності всієї мережі. Це досягається за рахунок використання параметра складності, який розраховується кожним вузлом незалежно за відомим алгоритмом і використовується для завдання вимог до вирішення ресурсомісткої задачі. Згодом цей параметр перераховується з урахуванням зміни обчислювальної потужності мережі.

Всі вузли мережі колективно знаходять новий блок за 10 хвилин. Кожен окремий учасник може шукати вирішення завдання для створення блоку годинами або навіть роками, але згідно з теорією ймовірностей хтось один знайде його в середньому за 10 хвилин за умови, що всі валідатори працюватимуть над одним ланцюжком блоків. Це також означає, що вимкнення половини потужності всієї мережі в один момент призведе до збільшення

середнього періоду формування блоку до 20 хвилин. І він залишатиметься збільшеним до моменту, коли параметр складності буде перерахований.

Впливати на обробку транзакцій може лише той, хто контролює понад 50% потужності. Щоб облікова система Bitcoin могла вважатися безпечною, необхідно, щоб більшість обчислювальної потужності всієї мережі контролювали саме чесні валідатори. Це означає, що довіряючи Bitcoin, кожен користувач упевнений у тому, що тисячі людей не зговоряться одночасно проти нього. Атака, за якої зловмисник контролює більше половини обчислювальних потужностей усієї мережі, зазвичай називається атакою 51%. Мережа Bitcoin жодного разу не піддавалася їй практично. Однак можна навести яскраві приклади з успішними double spending атаками в Bitcoin Gold та ZenCash, які сумарно завдали шкоди користувачам на суму більш ніж 18 мільйонів доларів США.

2.6 Вплив мережевих розривів на облікову систему

Більшість вузлів мережі Bitcoin використовують глобальну мережу для спілкування один з одним (на підставі внутрішнього протоколу), а майнери нерівномірно розподіляються на поверхні материкової частини Землі (рис. 2.9).

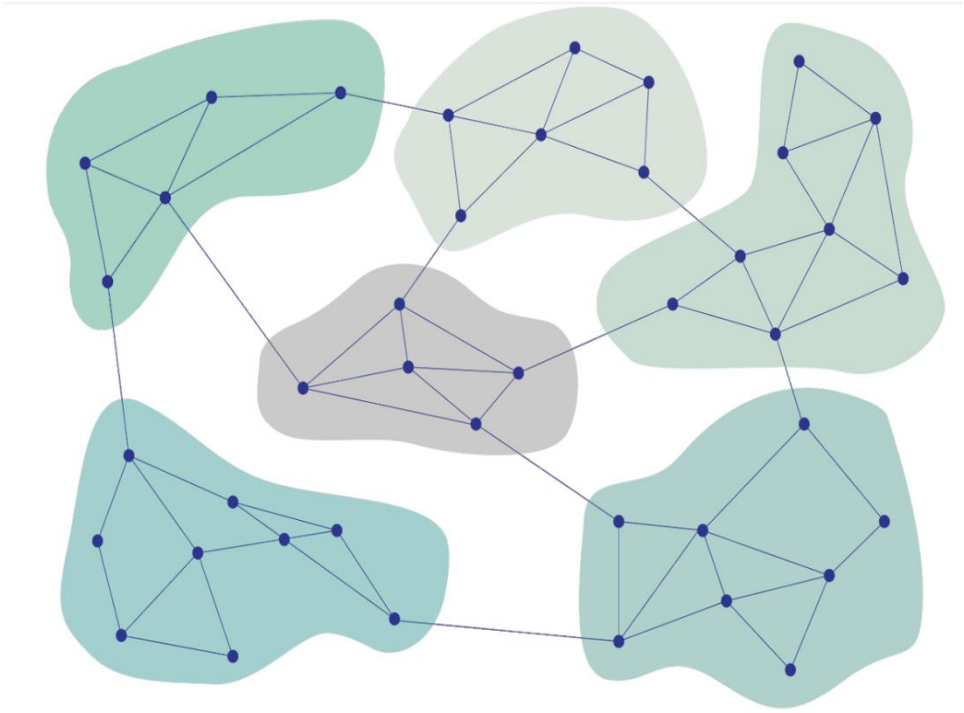

Рисунок 2.9 - Умовна схема розподілення майнерів

Якщо між континентами зображеними на рис 2.6 пропадає з’єднання, то вони будуть продовжувати коректно створювати нові блокі в своїх локальних підмережах. Однак користувачі різних підмереж не можуть синхронізуватися, щоб обмінюватися транзакціями та блоками, тому на кожному континенті валідатори формують різні версії ланцюжка блоків.

Оскільки групи валідаторів на різних континентах мають різну обчислювальну потужність, а параметр складності не оновлюється, період формування одного блоку набагато більше десяти хвилин для кожної з підмереж. Більше того, цей період є різним для кожного континенту, що призводить до формування альтернативних ланцюжків різної довжини (рис 2.10).

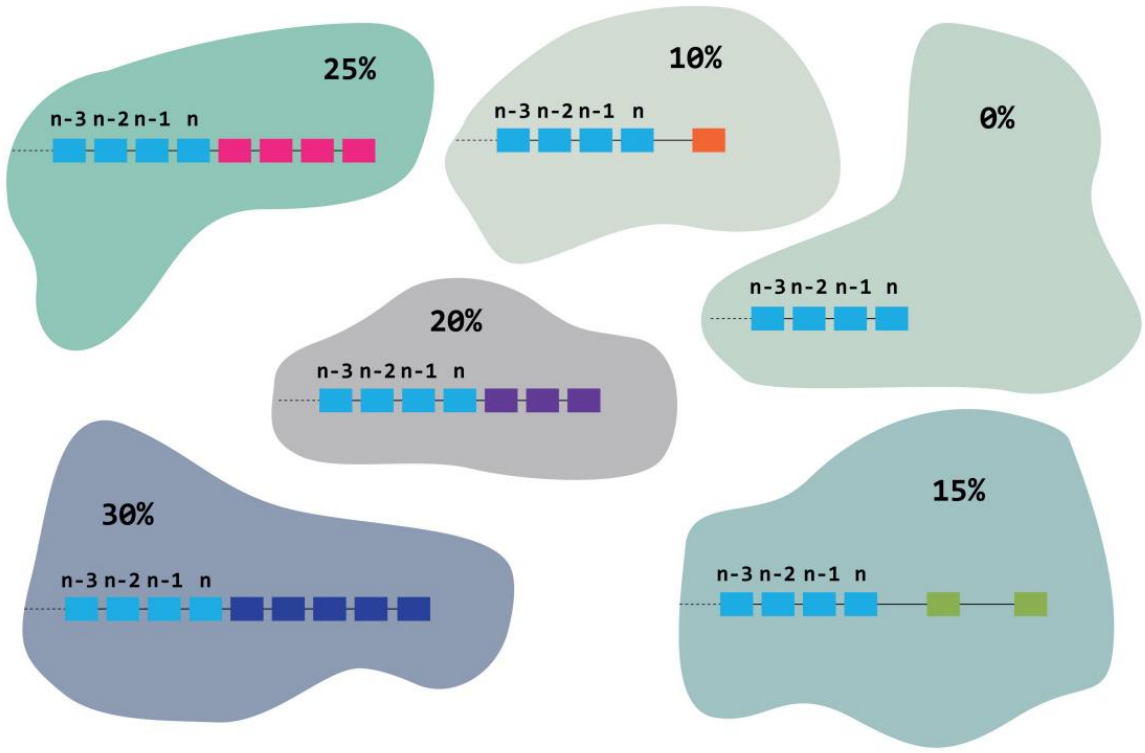

Рисунок 2.10 - Схема створених локальних ланцюжків блоків за умови відсутності з’єднання між континентами через деякий час.

Коли з’єднання буде відновлено, вузли мережі Bitcoin з різних континентів одночасно почнуть синхронізуватися один з одним.

В результаті чого виникає ситуація, коли є кілька різних версій ланцюжка блоків та всі вони мають різну довжину (рис. 2.10). Більше того, у різних ланцюжках знаходяться різні транзакції, підмножини яких можуть лише частково перетинатися.

Відповідно до вимог протоколу Bitcoin всі вузли виберуть найбільш довгий ланцюжок і будуть вважати його основним (mainchain). Але при цьому всі транзакції, які були включені лише до альтернативних ланцюжків, знову набувають статусу непідтверджених та включаються в подальшу обробку (тобто дані не зникають та не загублюються). Повні вузли мережі продовжують їх зберігати і синхронізувати, а вузли-валідатори, як і завжди, зацікавлені щодо їх включення в свої блоки з метою отримання винагороди (за умови, що ці транзакції не конфліктують із уже підтвердженими в mainchain).

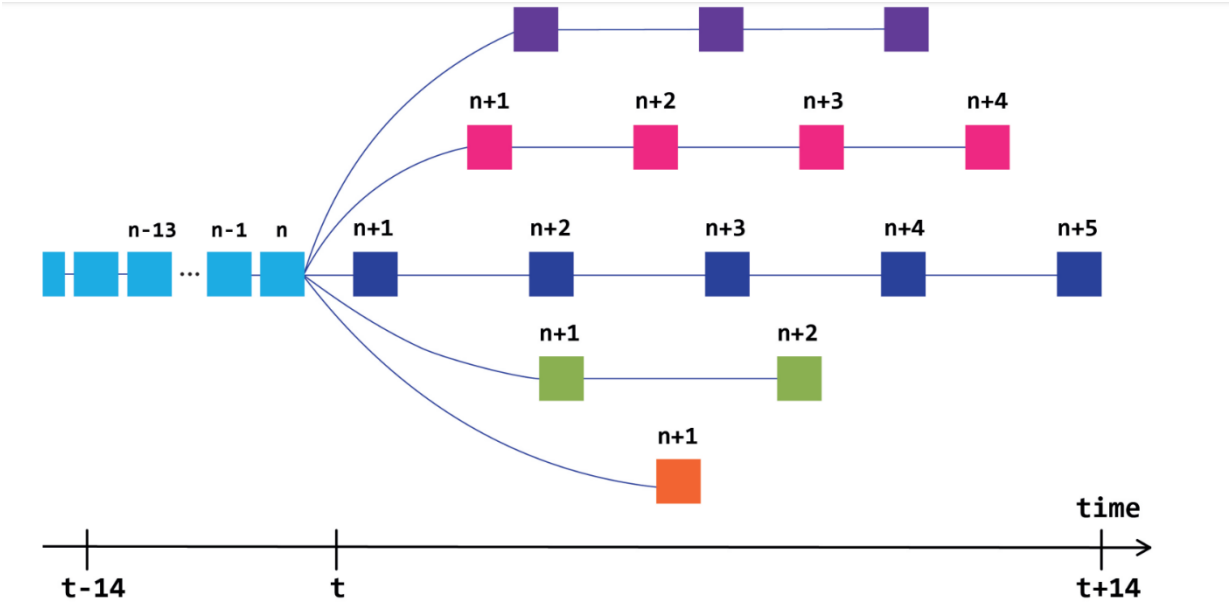

Рисунок 2.11 - Схема блокчейну після синхронізації локальних підмереж

Таким чином, транзакції з відкинутих блоків (orphan blocks) потраплять до списку непідтверджених і з високою ймовірністю будуть підтверджені пізніше. У результаті частина валідаторів не отримає винагороду за вирішення завдань, хоча всі вони працювали з колишньою старанністю.

В наведеній ситуації існують ризики щодо втрати даних (втрати монет) не тільки для валідаторів Bitcoin, але і для користувачів. Ці ризики обумовлені тим, що не вся обчислювальна потужність мережі Bitcoin використовувалася для підтримки безпеки даних, відсутностю єдиного центролю контролю даних та їх серверів щодо їх зберігання. При цьому користувачі можуть не помітити поділ глобальної мережі на підмережі та продовжувати обробку даних (здійснювати платежі у системі), ризикуючи пізніше не виявити прийняті монети на своєму балансі.

2.7 Об’єктивність протоколів узгодження

Одне із завдань протоколу – це узгодження даних та дій користувачів. Це завдання полягає в тому, щоб нові користувачі повині визначати стан системи

виходячи з інформації, що отримується від однорангових вузлів. Ця задача нетривіальна, оскільки деякі вузли можуть належати стороні, що здійснює атаку.

Протокол узгодження є об'єктивним, якщо новий вузол може незалежно прийти до того ж поточного стану, що і частина мережі, що грунтувалася тільки на правилах протоколу (таких, як визначення генезис-блоку) і повідомленнях, що поширюються системою. В основу це завдання методів та алгоритмів консенсусу.

Консенсус як доказ роботи є прикладом об'єктивного протоколу. Якщо новий вузол мережі має підключення хоча б до одного "чесного" користувача, він вибере дійсний блокчейн, оскільки той має велику сумарну обчислювальну складність. Підтвердження частки, з іншого боку, не є об'єктивним.

Розглядаючи зловмисника зі значною обчислювальною потужністю, у тому випадку, якщо гілка зловмисника досить довга, а складність всередині неї відрегульована, щоб відображати ситуацію, в якій тільки рахунки, контрольовані зловмисником, активні - це дозволяє зловмиснику побудувати ланцюжок, довший, ніж дійсний блокчейн. У той час як довгострокові розгалуження відкидаються існуючими користувачами системи (наприклад, введенням правила, яке обмежує довжину можливого розгалуження), нові ноди без попередніх відомостей про поточний стан оберуть блокчейн зловмисника.

Протокол узгодження є суб'єктивним - вузлу потрібен недавній стан у додаток до правил протоколу і повідомлень, що розповсюджуються системою з метою незалежно визначення поточного стану системи.

В разі підтвердження частки, якщо є правило, що забороняє розгалуження блоків довжиною більше N (тобто після точки розгалуження не може бути більше N блоків), достатньо аналізувати змістовність блоків глибиною N або менше, щоб надійно визначити поточний стан системи. Новий вузол (нода) може отримати доступ до блоку від довіреного джерела (наприклад, веб-сайту, присвячений аналізуванню валюти). У той час як цей метод може підірвати безпеку і децентралізацію системи підтвердження частки, в PoS системах

стверджується, що слабка суб'єктивність - це хороший спосіб об'єднати безпеку контрольовану комп’ютерними системами та соціально контрольовану [13].

Засновані на PoW системи в деякій мірі схильні до подвійного витрачання; тим не менш, можливість успішного подвійного витрачання поступово зменшується в міру зростання кількості підтверджень транзакції і сильно залежить від кількості потужностей, якими володіє атакуючий [16]. Щоб зменшити ризик подвійного витрачання, продавці зазвичай чекають певної кількості підтверджень (наприклад 6). Як доповнення існують механізми зменшення ризиків у швидких платежах [17].

Типи атак, загальні для PoW і PoS це відмова в обслуговуванні (англ. denial of servise, DoS) і атака Сибіли. DOS-атака спрямована на те, щоб перервати нормальне функціонування мережі шляхом переповнення вузлів. Наприклад, зловмисник може наповнити мережу транзакціями низької вартості. У разі атаки Сибіли зловмисник підриває функціонування мережі, створюючи значну кількість вузлів, що некоректно ведуть себе. Ступінь схильності мережі до DoS-атака і атак Сибіли залежить не тільки від типу погодження, що використовується в мережі, але і від деталей протоколу мережі. Не існує внутрішніх властивостей, які б зробили PoS менш чутливим до цих атак, ніж PoW.

Один з небагатьох векторів атаки, особливих для узгодження доказом роботи, є егоїстичний майнінг (англ. selfisn mining) [18]. При егоїстичному майнінгу зловмисник вибірково публікує блоки, щоб обчислювальні ресурси інших майнерів були витрачені впусту. Оскільки в разі узгодження дорогі ресурси не залучені у створенні блоків, ця атака не ефективна для PoS систем. З іншого боку, немає жодних доказів, що егоїстичний майнінг був коли-небудь успішно використаний у Bitcoin; деякі дослідження стверджують, що опис атаки ґрунтується на некоректних припущеннях [19].

Для узгодження з використанням PoW ступінь схильності до атак може бути передбачена, грунтуючись на сумарній гешуючій потужності системи. У випадку PoS-систем, немає еквівалентної міри «стану здоров'я» мережі:

– якщо валюта системи рівномірно розподілена між користувачами, система схильна до атак, заснованих на розгалуженні блокчейна;

– якщо є користувачі з великими частками, вони можуть підірвати роботу мережі (наприклад, застосовуючи до транзакцій цензуру).

В алгоритмах PoS-систем нерівність (2.2) модифікується таким чином, щоб вона залежала від кількості даних, що належать користувачу, а не від властивостей блоку. Зазвичай в алгоритмах підтвердження частки використовуються умови, аналогічні (2.7):

$$hash\big(hash\big(B_{prev}\big), A, t\big) \leq bal(A)\frac{M}{D}, \quad (2.7)$$

де:

B_{prev} - блок, над которим працює користувач;

T - поточний час (в форматі UTC);

A – адреса користувача;

$bal(A)$- баланс користувача.

На відміну від (2.2), єдина змінна, яку користувач може змінювати, це час T в лівій частині нерівності (2.7). Баланс адреси блокується протоколом; наприклад, протокол може розраховувати баланс, виходячи з кількості монет, які не рухалися протягом дня. В якості альтернативи, PoS-кріплювата може використовувати невикористані виходи транзакцій, як це робиться в Bitcoin; в такому випадку, баланс закритий природним чином. Протокол з підтвердженням частки ставить обмеження на можливі значения T. Наприклад, якщо T не може відрізнятися від UTC-часу вузлів мережі більше, чим на годину, то користувач може спробувати не більше 7200 значень T. Таким чином, в алгоритмах підтвердженні частки не використовуються інші складні обчислення.

Разом з адресою A і часом T, що задовільняють виразу (2.2), користувач повинен надати доказ володіння адресою. Щоб цього досягти, користувач може підписати новий блок за допомогою свого цифрового підпису; щоб створити дійсний підпис, необхідно мати секретний ключ, що відповідає адресі A.

Час, необхідний, щоб знайти блок для адреси A, розподілено експоненційно з параметром $\frac{\text{ва}l(A)}{D}$.

Отже, реалізація (2.7) підтвердження частки є надійною: ймовірність згенерувати блок дорівнює відношенню балансу адреси до загального обсягу монет в обороті. Час, який потрібно всій мережі, щоб знайти блок, розподілено експоненційно з параметром $\frac{\sum a\ bal(a)}{D}$.

Таким чином, якщо кількість валюти $\sum a\ bal(a)$ фіксована або зростає з передбачуваною швидкістю, складність D повинна бути відома заздалегідь:

$$D = \frac{1}{T_{ex}} \sum bal(a)\ , \tag{2.8}$$

де:

T_{ex} – очікуваний час між блоками.

На практиці, однак, складність D повинна налаштовуватися на підставі недавніх блоків, тому що не всі власники валюти беруть участь у валідації блоків.

У ході виконання даного етапу кваліфікаційної роботи було розглянуто основні етапи обробки даних (транзакцій): створення, валідація та поширення даних мережею, визначення та аналіз розгалужень блоків, вплив мережевих перешкод на стабільність роботи децентралізованих систем. Також проаналізовано технології та підходи, що забезпечують системі безпеку даних.

3 ОГЛЯД ПОТЕНЦІЙНИХ КІБЕРАТАК НА ДЕЦЕНТРАЛІЗОВАНІ МЕРЕЖІ

Даний розділ описує атаки, які можливі в кожній із PoS та PoW систем, а також деякі атаки, специфічні для конкретних реалізацій протоколу.

Більшість проблем з PoS-протоколами виникають через те, що протоколам не відомо нічого, крім відповідного блокчейна [14]. В системах доказу роботи присутня зовнішній фактор, а саме кількість обчислювальної роботи, яка потрібна, щоб знайти рішення. В системах з підтвердженням частки відсутні фактори, що закріплюють блокчейн у фізичному світі; тому інтуїтивно видно, що узгодження на основі PoS допускає більше видів атак.

3.1 Атака за допомогою переписання історії

В системі з PoS-узгодженням, зловмисник, що володіє достатньою обчислювальною потужністю, може спробувати побудувати альтернативний блокчейн, починаючи з самого першого блоку. В PoW-системі, подібній атаці перешкоджає величезна обчислювальна потужність, необхідна, щоб побудувати блокчейн з нуля; в той же час, це завдання реально вирішити в PoS-системі. Оскільки зловмисник може переміщати монети вільно в блокчейні, який він будує, у нього набагато більша розмірність простору пошуку; таким чином, цей тип атаки може бути кращим для побудови альтернативного блокчейна з недавньою точкою розгалуження.

Щоб запобігти подібній атаці, протокол може встановити максимальну дозволену глибину точки розгалуження. Наприклад, в NXT системах користувач не може приймати альтернативний блокчейн, якщо він відрізняється від існуючого більш ніж в останніх 720 блоках (що відповідає приблизно 12 годинам функціонування системи). Тим не менш, це обмеження не вирішує проблему нових користувачів. Коли користувач приєднується до мережі, він бачить кілька

блокчейнів, не маючи попередніх відомостей про їхню справжність. Якщо блокчейн атакуючого переважно дійсного в рамках протоколу, нові користувачі приймуть його. Один із способів дізнатися, який блокчейн правильний завантажити його з довіреного джерела; в той же час, це робить систему дещо централізованою і вносить фактор довіри. Тим не менше, завантаження блокчейна з довірених джерел використовуються фактично у всіх існуючих POS-системах.

Короткострокові атаки стають надто витратними в разі делегованого підтвердження частки, так що необхідно розглянути вартість атаки переписування історії. Для систем, що використовують доказ роботи, витрати на атаку за допомогою переписування історії надто великі. Наприклад, атака на Bitcoin тривалістю в 1 000 блоків потребує принаймні від зловмисників вкладення приблизно 21 млн. $ (але, на відміну від короткострокової атаки, вона буде легко виявлена, оскільки гешуюча потужність мережі, що спостерігається, впаде в два рази протягом тривалого проміжку часу).

В ранніх версіях протоколу (підтвердження частки), вартість атаки переписуванням історії набагато нижча; Вартість атаки тривалістю в один день може становити близько 10000 $ у випадку, коли коректний блокчейн вибирається на основі загального знищеного віку монет.

В делегованому POS (DPoS) алгоритмі консенсусу реалізація атаки в загальному випадку вимагає змови 2/3 користувачів (з правами делегатів). Її вартість складно оцінити, оскільки протоколи DPoS використовують істотно різні методи для вибору винагороди та покарання делегатів.

3.2 Атака за допомогою підкупу

При реалізації атаки за допомогою підкупу зловмисник намагається двічі витратити свої кошти наступним чином:

– купити будь-які товари або послуги;

– зачекати, поки транзакція, що містить платіж, буде вважатися підтвердженою продавцем;

– об'явити винагороду за продовження усіченого блокчейну, що не включає платіж, що розглядається. Наприклад, якщо продавець чекає шести підтверджень, зловмисник почне з блокчейна без останніх шести блоків. Зловмисник може запропонувати велику нагороду користувачам, які працюють тільки над блокчейном атакуючого, без цього блокчейн зловмисника ніколи не наздожене правильний;

– атакуючий може продовжувати підкупати валідаторів високими комісійними, навіть коли його блокчейн і правильний будуть мати однакову довжину, щоб отримати підтримку більшості власників криптовалюти;

– користувачі, які беруть участь в атаці, нічого не втрачають, якщо атака терпить невдачу; для атакуючого атака буде прибутковою, якщо загальна кількість монет витрачених на підкуп менша за вартість товару. Для порівняння, в PoW-системі подібна атака вимагає від зловмисника підкупу більшості майнерів. До того ж, у цьому випадку валідатори втрачають ресурси, витрачені на обчислення, якщо атака не вдається, сума підкупу, швидше за все, буде високою.

Теоретичний сценарій подвійної витрати:

– зловмисник витрачає кошти в транзакції, яку збирається пізніше звернути;

– одразу після транзакції, атакуючий починає будувати альтернативний ланцюг, ґрунтуючись на блоці, що передує тому, в якому міститься ця транзакція. Побудова альтернативного ланцюга відбувається у таємниці;

– після того, як транзакція отримує достатню кількість підтверджень (наприклад, 6) і ланцюг зловмисника стає довшим, ніж дійсний ланцюг, атакуючий поширює її мережею. Ланцюг атакуючого приймається за новий дійсний блокчейн, і транзакція стає зверненою, тобто недійсною.

Щоб провести успішну атаку зі стовідсотковою ймовірністю, зловмиснику потрібно контролювати більше 50% ресурсів, що використовуються для захисту системи (обчислювальна потужність у разі PoW, ліквідний капітал у випадку PoS) на час атаки.

Таким чином, у разі підтвердження частки атакуючому не потрібно володіти більш ніж половиною валюти, може лише отримати доступ більш, ніж до половини валюти в обороті на кілька годин, наприклад, заплативши високі комісійні. Сума підкупів пропорційна винагороді, яку приймаючі користувачі втрачають за роботу над недійсним блокчейном, якщо підкуплені користувачі працюватимуть над обома блокчейнами, блокчейн зловмисника ніколи не наздожене дійсний.

Для розрахунків припускається, що:

– нагороди за валідацію здійснюються з комісій за транзакції;

– кількість транзакцій на день 250 000 (приблизно дорівнює кількості підтверджених транзакцій на день у Bitcoin);

– комісія за транзакцію 2$ (вище ніж зараз у Bitcoin – 1,7$).

– тоді щоденна нагорода за валідацію буде 500000$; якщо атака триває годину, зловмиснику доведеться заплатити підкупів менш ніж на 21000$.

У Bitcoin нагорода за вирішення блоку становить 6.25 монет, або близько 312000$. У випадку економічної рівноваги, вартість майнінгу одного блоку близька до цього числа; Якщо атака повинна тривати 6 блоків, атакуючому знадобиться заплатити не менше ніж за 7 блоків, щоб обігнати дійсний блокчейн (сума становить 147000$). Це майже у 2 рази менше ніж сума підкупів у разі підтвердження частки. Існує інше міркування, яке робить атаку на підтвердження роботи менш надійною і більш дорогою. Атака стає очевидною, як тільки блокчейн атакуючого опублікований, тому що реорганізація останніх шести блоків статистично вкрай рідкісна подія. Оскільки в екосистемі Bitcoin досить небагато великих майнерів, участь в атаці негативно вплине на їхню репутацію. У випадку системи POS фактор репутації відіграє другорядну роль, так як більшість власників валюти, найімовірніше, анонімні.

POS-системи можуть представляти трохи інфляційну економіку для винагороди валідаторів. Розглядаючи систему з капіталізацією 3 мільярди доларів та інфляцією 1%. Щоденна нагорода за майнинг у системі складає (3.1):

$$3 * 10^9 * \frac{0.01}{365} \approx 82000\ . \quad (3.1)$$

Це число означає, що вартість атаки тривалістю 1 годину близька до 3400 доларів.

Щоб атака була прибутковою, атакуючому знадобиться двічі витратити велику суму грошей. Відповідно, контрагент може запросити більше підтверджень для транзакції зловмисника. Як у PoW, так і в PoS, пряма вартість атаки зростає лінійно з необхідною кількістю підтверджень; отже, відношення вартостей має бути приблизно тим самим. Тим не менше, в ході атаки на PoW-системи, вона стає все більш очевидною для учасників системи, тому що атака сильно зменшує хешрейт дійсного блокчейна. Якщо в системі відносно небагато майнерів, користувачі можуть ідентифікувати майнерів, що беруть участь в атаці, навіть до того, як вона закінчиться; якщо атакуючі являють собою майнінг пули, їх учасники будуть мати стимул приєднатися до інших пір або тимчасово призупинити свою діяльність. Таким чином в випадку, якщо атака на POS-систему проводиться кілька разів, курс обміну цієї валюти падає, в результаті зловмиснику стає простіше сформувати та зібрати ресурси для наступних атак. Останнє непрацює для систем, де впроваджується PoW алгоритми, так як витрати на майнінг (електрику, обладнання, тощо.) не залежать від курсу обміну аналізованої валюти.

3.3 Атака передобчислюванням

Нехай A валідатор деякого блоку B_h висоти h; тобто A задовільняє виразу (2.2) з параметрами відповідними B_h.

Якщо A має дійсну обчислювальну потужність, він може вплинути на геш блоку Bh, щоб мати можливість вирішити наступний блок $B_h + 1$, наприклад,

додаючи нову транзакцію в B_h. Щоб зарезервувати $B_h + 1$ для себе, A переглядає всі профілі користувачів і перевіряє, чи виконується умова виразу (2.2) для кожного з дозволених значень часу T. Якщо геш B_h не відповідає умовам («поганий»), тобто обчислення показують, що наступний блок буде сформовано іншим користувачем, зловмисник змінює параметри вставленої транзакції та пробує знову. Зловмисник, що здійснює атаку може побудувати довгий ланцюжок блоків, щоб зібрати більше комісій і спробувати провести подвійне витрачання (будуючи свій ланцюг в секреті і випустить потім всі блоки відразу, щоб обігнати правильний блокчейн з транзакцією, яку атакуючий хоче звернути).

Ефективність обчислювальної атаки залежить від частки зловмисника, а також від загальної кількості користувачів або UTXO в системі. В PoW-системі, ця атака фактично неможлива, оскільки згенерувати блок з "хорошим" гешем набагато складніше, ніж просто коректний блок. Аналогічно, в системі з делегованим PoS послідовність осіб, що підписують блоки, не залежить від властивостей останнього блоку; таким чином, DPoS-узгодження є стійким до передобчислювальних атак.

3.4 Атака Сибіли

Атака Сибіли - це атака, при якій зловмисник заповнює мережу безліччю підконтрольних вузлів зв'язку, і намагається «окружити» вузол жертви, тобто заволодіти всіма сусідніми вузлами мережі.

Контролюючи сусідні вузли жертви можна:

– блокувати транзакції від інших користувачів, від'єднавши окремо взятого користувача від спільної мережі;

– приєднувати жертву тільки до блоків, які створює він, в окремій мережі. В результаті цього будуть з'являтися транзакції, які будуть пересилати гроші повторно;

– атакуючий може бачити всі транзакції жертви за допомогою спеціальних програм.

Тому Атака Сібіли вважається однією з потенційно можливих атак і досить небезпечних, оскільки підірве не тільки довіру до системи, але і децентралізованість мережі.

Провести таку атаку досить складно, тому що коди децентралізованих систем написані таким чином, що вузол вибирає з'єднання з іншими вузлами практично випадково. І навіть якщо зловмисник контролює більше 70% всіх вузлів у мережі, ймовірність повністю огорнути вузол жертви менше 1%.

При першому підключенні до мережі сайт не знає IP-адрес довірених вузлів і не має іншого вибору, крім як запросити їх у інших вузлів.

Але навіть якщо список довірених вузлів відомий заздалегідь, неможливо підтримувати з'єднання тільки з ними - це порушує принципи децентралізованої організації мережі. Тому клієнт, намагаючись розширити свій круг контактів, підключається як до відомих вузлів, так і до тих, з якими ще не було з'єднань.

Це вразливість - зловмисник, маючи велику кількість вузлів може зробити так, щоб журнал жертви містив практично тільки адреси атакуючого.

За визначенням, повна нода — це підключений до мережі Bitcoin-клієнт, який містить нову версію блокчейна і налаштований на прийом вхідних запитів.

Для визначення вартості атаки Сібілли необхідно розрахувати, скільки буде коштувати запуск 1 ноди. Його можна зробити практично на будь-якому комп'ютері. І оскільки операційна система значення не має, для здешевлення вартості візьмемо безкоштовну операційну систему Linux, з відкритими програмними продуктами. Виходить, вартість запуску повної ноди в мережі формується тільки з ціни на комплектуючі для комп'ютера, на якому вона буде запущена.

Мінімальний набір комплектуючих та вимог до них, для коректної роботи ноди: основною вимогою є великий обсяг жорсткого диска, для завантаження всієї бази транзакцій, яка з кожним роком буде тільки збільшуватися. А

мінімальний набір комплектуючих складається з жорсткого диска, процесора, материнської плати та оперативної пам'яті. На сьогоднішній день мінімальна вартість подібного набору комплектуючих приблизно дорівнює 250$.

В блокчейні реалізована схема, за якою кожна нода вибирає 8 повних нод з мережі для поповнення і верифікації своєї бази даних. Оскільки ноди вибираються довільним чином, суть атаки Сибіли зводиться до того, щоб підключити до блокчейну таку кількість атакуючих нод, щоб кожна з 8 обраних користувачем повних нод була підконтрольна зловмисникам. Отже, кількість повних (чесних) нод, вибраних з блокчейна дорівнює 0. Для розрахунків ймовірності використовується метод гіпергеометричного розподілу. Це дискретний імовірнісний розподіл, який визначає кількість успіхів у вибірці без повернень довжини n над кінцевою сукупністю об'єктів. M – кількість нод, що належать множині дефектних (скомпрометованих) вузлів, m – кількість вузлів, до яких звертається користувач, зазвичай дорівнює 8. N – загальна кількість існуючих вузлів у системі, n – кількість обраних користувачем вузлів із загальної множини.

$$P(N;M;n;m) = \frac{C_M^m * C_{N-M}^{c-m}}{C_N^n}, \tag{3.2}$$

$$C_M^m = \frac{M!}{m!(M-m)!}, \tag{3.3}$$

де:

N — загальна множина об'єктів (удачних і дефектних) (N=6000);

M — множина повних нод, підконтрольних зловмисникам;

n — кількість повних вузлів (нод) із множини N, обраних користувачем з генеральної множини нод N+M;

m — кількість повних нод із множини M, обраних користувачем з генеральної множини нод $N + M$ $(m = 8)$;

C - Біноміальний коефіцієнт. $(C(N,n) = 1)$.

$$P = \frac{C_M^m}{C_{M+N}^m}, \tag{3.4}$$

$$P = \frac{M!}{m!(M-m)!} * \frac{m!(M+N-m)!}{(M+N)!}. \tag{3.5}$$

З формули (3.4), розписавши біноміальний коефіцієнт, отримали форму (3.5), а, скоротивши всі факторіали у формулі (3.3), отримали кінцеву (3.6) формулу.

$$P = \frac{(M-m+1)(M-m+2)\ldots(M-m+N)}{(M+1)(M+2)\ldots(M+N)}. \tag{3.6}$$

Розрахувавши імовірність успішної атаки Сибіли отримано таблицю 2.

Таблиця 3.1 - Ймовірність успішної атаки Сибіли – P за формулою (3.6)

M - необхідна кількість нод	P - імовірність успішної атаки Сибіли
38478	10%
42019	20%
47658	30%
56104	40%
68503	50%
82759	55%
95143	60%
112153	65%
138564	70%
168452	75%
222096	80%
304589	85%
472075	90%
981756	95%
5022464	99%

На підставі розрахованих даних пораховано приблизну суму атаки Сибілли в Bitcoin на поточний момент.

З ціни в 250$ за розгортання однієї ноди, таблиця 3.2.

Таблиця 3.2 - Вартість атаки для імовірності успішної атаки Сибіли

Вартість атаки, мільйонів доларів	Імовірність успішної атаки Сибіли

9,62	10%
10,5	20%
11,91	30%
14,02	40%
17,12	50%
20,69	55%
23,79	60%
28,03	65%
34,66	70%
42,11	75%
55,52	80%
76,15	85%
118,01	90%
245,44	95%
1255,62	99%

Для того, щоб атака Сибіли була максимально ефективною, необхідно значні фінансові витрати (витратити більше 1 мільярду доларів), що є досить великою сумою та ставить під сумнів впровадження такого типу атак на все систему.

Дана сума не включає в себе праці витрати на організацію всієї інфраструктури для атаки, але так як цей показник досить малий в порівнянні з сумою на програмно-апаратну складову, цим можна знехтувати. З таблиці 3 чудово видно залежність ціни атаки від ймовірності успішності атаки. Це дає підстави вважати, що захист, заснований на збільшенні кількості повних нод в мережі Біткоїн буде відносно недорога, оскільки кожна додаткова нода не тільки збільшує ціну атаки, але і залежність цієї ціни від ймовірності успішності самої атаки.

3.7 Атака подвійної витрати

Атака подвійної витрати (англ. Double-spending) це аатка на децентралізовані платіжні системи, коли зловмисник (або дійсний користувач) спробує повторно використати раніше передану кількість монет. Зазвичай

мережа не здійснить обробку такої транзакції як дійсної. Але в паралельних гілках блоків можуть бути транзакції, які по-різному розпоряджаються одним і тим же змістом. Імовірність існування паралельних ланцюжків блоків вкрай мала і експоненційно зменшується зі зростанням довжини ланцюжка та кількості незалежних валідаторів.

Коли здійснюється угода за криптовалютні монети, то очікується, що після перерахування монет відправник отримує у відповідь продукт або послугу, яку він сплатив. Але атака полягає в тому, що спочатку продавець переконується в тому, що транзакція на оплату була зроблена, після чого він передає свій товар, а після отримання товару покупцем створюється нова транзакція із зазначенням на переказ тих самих монет, яка і приймається мережею, замість першої. У продавця не залишиться ні товару, ні монет, тому що все буде у зловмисника.

Проблема полягає в синхронізації: потрібен якийсь універсальный сигнал, що вказує, що якась транзакція є кінцевою і ніяких інших конфліктуючих транзакцій прийнято не буде. Розробники захищають систему, стверджуючи, що подібна атака вимагає дуже високих обчислювальних ресурсів. Однак, якщо зловмисник все ж таки володіє дійсними обчислювальними ресурсами, то атака можлива.

Ланцюжок блоків можна представити у вигляді дерева, що починається з початкового блоку і йде послідовно. Гілки цього дерева є історією Bitcoin транзакцій. Гілка не може містити двох конфліктних транзакцій, однак може бути інша гілка, яка містить транзакцію, що їй суперечить. Це відповідає ситуації, коли одночасно згенерувалося 2 різних блоки і частина вузлів стало продовжувати працювати над першою гілкою, а інша частина - над другою. Зазвичай, така суперечність вирішується, як тільки знаходиться наступний блок. Справжньою гілкою вважається та, яка включає в себе більш довгий ланцюжок наступних блоків.

Для прикладу ланцюжок блоків, зображенио на рис.3.1.

Дерево починається знизу, стрілки вказують з якого блоку, на який йде посилання в заголовку блоку. Можливий варіант побудови дерева - a. Недійсна гілка позначена як - b, тому що її довжина становить лише 3 блоки, тоді як існує більш довга гілка. Темна гілка позначена як - c, має найбільшу довжину, тому деякими вузлами вважається дійсною. Коли знаходиться новий блок (позначено як d), який посилається тільки на один із попередніх блоків, то гілка стає довшою і приймається всіма вузлами, як дійсна.

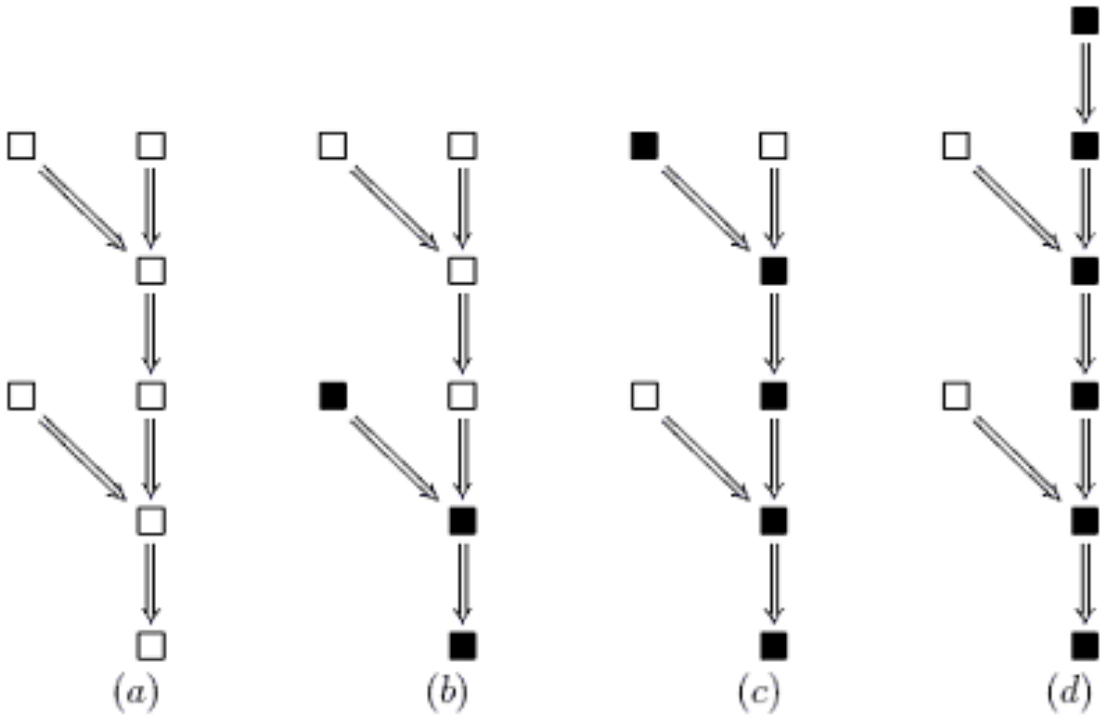

Рисунок 3.1 - Порядок вирішення розгалужень у блокчейні

Транзакція має n підтверджень, якщо вона включена в блок, який є частиною діючого ланцюжка, і існує n блоків, включаючи даний і всі наступні, що йдуть від нього. Вважається, що убезпечити транзакцію від double-spending може достатня кількість таких підтверджень.

Для проведення успішної атаки подвійної витрати потрібні наступні кроки:

– виконати транзакцію, яка атакує здійснену оплату;

– таємно валідувати, використовуючи той блок, який включає в себе цю останню транзакцію;

– дочекатися, поки транзакція, що відправляє гроші продавцю, отримає достатньо підтверджуючих блоків, і продавець передасть свій товар, впевнений, що гроші остаточно привласнені йому;

– продовжувати розробляти таємну альтернативну гілку, поки вона не стане більше, ніж публічна, після чого її поширити мережею. Оскільки нова гілка довша за всіх інших відомих, то вона буде вважатися дійсною, і переказ монет продавцю буде замінений відправкою монет зловмиснику.

На рисунку 3.2 зображені кроки проведення атаки подвійної витрати.

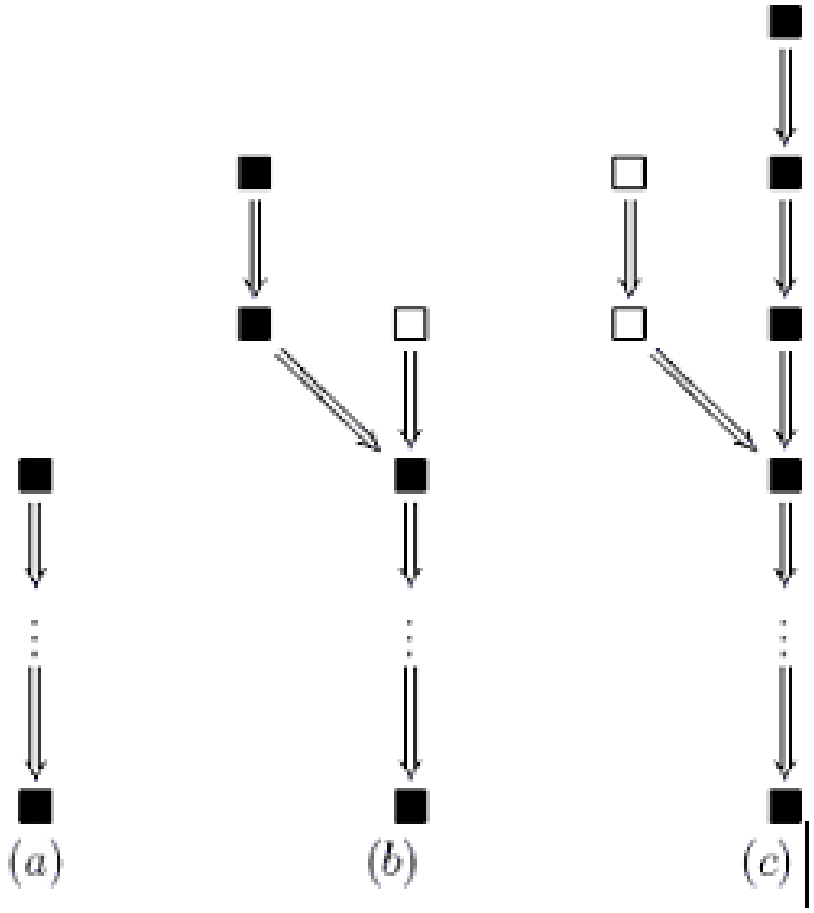

Рисунок 3.2 - Схема виконання атаки подвійної витрати

Стан мережі до дій зловмисника зображено під літерою - a. Зліва, під літерою (b) показана гілка, що включає транзакцію відправки монет продавцю. Має 2 підтвердження. У результаті чого продавець передав свій продукт. У цей час у зловмисника згенерований блок, що включає атакуючу транзакцію. Якщо

атакуючому вдається створити ланцюжок довше, то він поширює її мережею, і монети повертаються йому - c.

Стан мережі до дій зловмисника зображено під літерою (a). Зліва, під літерою (b) показана гілка, що включає транзакцію відправки монет продавцю. Має 2 підтвердження. У результаті чого продавець передав свій продукт. У цей час у зловмисника згенерований блок, що включає атакуючу транзакцію. (c) Якщо атакуючому вдається створити ланцюжок довше, то він поширює її мережею, і монети повертаються йому.

Для розрахування ймовірністі того, що зловмисник зможе згенерувати гілку, яка буде довшою, ніж гілка, яку визнали валідною всі інші, припускаються наступні спрощення:

– загальна швидкість створення блоку у спільній мережі та у атакуючого залишається постійною. Сумарна швидкість створення блоку буде H, з якої частина pH відноситься до чесних валідаторів, а qH - до зловмисника. При цьому: $\mathrm{p} + q = 1$. Тобто можливість, що блок знайде чесна мережа дорівнює p, а що зловмисник – q;

– складність знаходження нового блоку постійна.

$z = n - m$ - число блоків, в яких чесна мережа має перевагу перед атакуючим. Після кожного вияву нового блоку z змінюється, збільшуючись на 1, якщо його знайшла чесна мережа, і, зменшуючись на 1 - якщо зловмисник. Математично це є ланцюг Маркова.

Якщо z досягає значення -1, то атака вдається. Якщо цього ніколи не відбувається, то атака провалена. Оскільки нас цікавить, чи стане коли-небудь $z = -1$, і коли це трапиться, то можна використовувати для вирішення задачі теорію ланцюгів Маркова, де кожен крок є фактом знаходження блоку ким-небудь. $Z_i + 1$ може дорівнювати або $(Z_i + 1)$ з ймовірністю p, або $(Z_i - 1)$ з ймовірністю q.

Перший графік показує успішну спробу атаки подвійної витрати - після 13 виявлених блоків (рис 3.3).

Рисунок 3.3 - Успішна атака подвійної витрати

Другий графік показує провальну спробу атаки. Після 20 виявлених блоків мережа отримала настільки значну перевагу, що шанси атакуючого наздогнати незначні (рис. 3.4).

Рисунок 3.4 - Провальна спроба атаки подвійної витрати

Пропонується обчислення імовірності того, що зловмисник наздожене мережу при відставанні на z блоків здійснювати за формулою:

$$A_z = p * A_{z+1} + q * A_{z-1}, \quad (3.7)$$

де:

$A_z -$ імовірність того, що зловмисник наздожене мережу при відставанні на z блоків. Очевидно, що, якщо $z < 0$, то $A_z = 1$, тобто атака успішна;

$A_{z+1} -$ імовірність того, що зловмисник наздожене мережу на наступному кроці, після знаходження чесною мережею нового блоку, що можливо з імовірністю p;

$A_{z-1} -$ імовірність того, що зловмисник наздожене мережу на наступному кроці, після знаходження зловмисником нового блоку, що можливо з імовірністю q.

Враховуючи, що $p + q = 1$, імовірність того, що зловмисник наздожене мережу при відставанні на z блоків A_z дорівнює:

$$A_z = \min\left(\frac{q}{p}, 1\right)^{\max(z+1,0)} \begin{cases} 1, & z < 0, q > p \\ \left(\frac{q}{p}\right)^{z+1}, & z \geq 0, q \leq p \end{cases}. \quad (3.8)$$

Зрозуміло, що якщо зловмисник володіє більше ніж половиною потужності мережі, то його атака буде успішною. Шанси на успіх залежать від значення Z в момент часу, коли товар був передан, а значить, існує ланцюжок із n підтверджуючих блоків.

Функція імовірності від кількості успіхів при знаходженні нових блоків зловмисником перед тим як буде знайдено n блоків у чесній мережі може бути розраховано:

$$P(m) = \frac{m+n+1}{m} p^n q^m . \quad (3.9)$$

Гонка починається з $z = n - m - 1$ (за умови, що один блок був попередньо отриманий зловмисником, перш ніж він почав атаку).

Відповідно ймовірність здійснення атаки double-spending, коли продавець отримав n підтверджень можливо розрахувати як:

$$r = \sum_{m=0}^{\infty} P(m) a_{n-m-1} = \sum_{m=0}^{n-1} \frac{m+n-1}{m} p^n q^m \left(\min\left(\frac{q}{p}, 1\right)\right)^{n-m} +$$

$$\sum_{m=n}^{\infty} \frac{m+n-1}{m} p^n q^m = \begin{cases} 1 - \sum_{m=0}^{n} \frac{m+n-1}{m} (p^n q^m - p^m q^n), & q < p \\ 1, & q \geq p \end{cases}. \quad (3.10)$$

За результатами розрахунків отримано графіки, які показує ймовірність успішності реалізації атаки (як функцію залежності від співвідношення рівня потужностей валідаторів і зловмисників) до всієї сумарної потужності мережі (рис. 3.5).

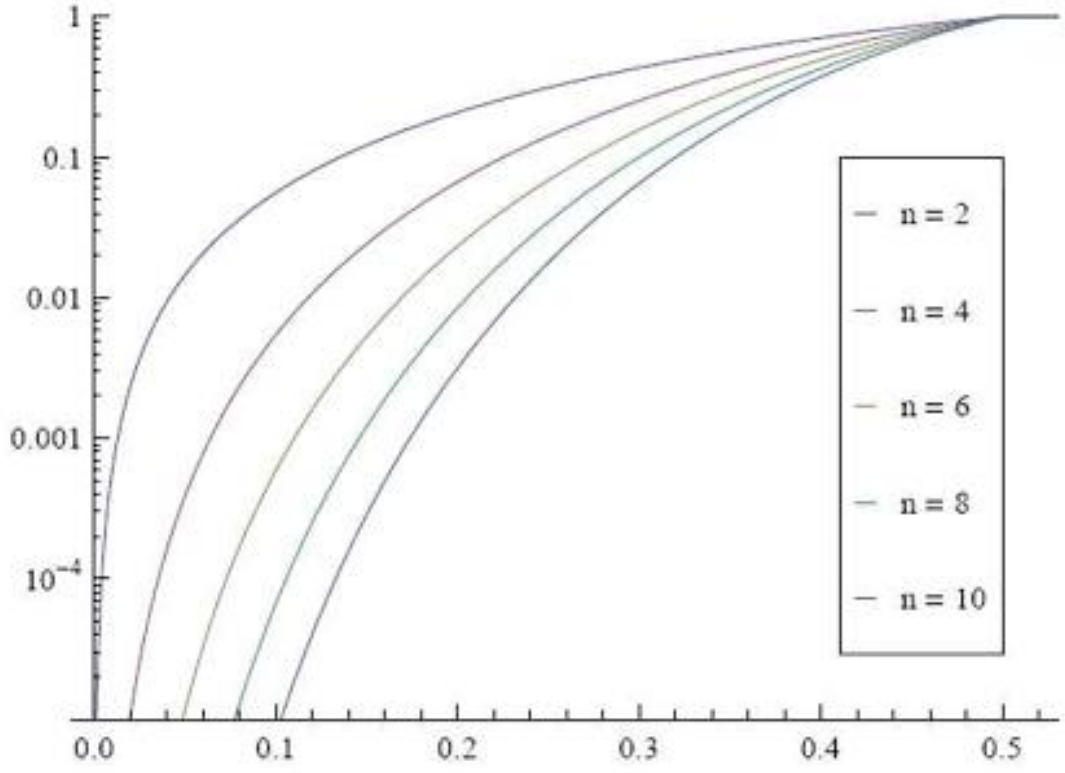

Рисунок 3.5 - Графік імовірності успішності атаки від співвідношення потужностей зловмисника до потужності мережі

На рисунку 3.5 наведено п'ять графіків для різного числа підтверджуючих блоків n. Більше підтверджень зменшує ймовірність успіху атаки. При наближенні співвідношення потужностей до 50%, ймовірність успіху наближається до 100%. Якщо потужність мережі зловмисника становить 10% від загальної потужності, то потрібно 2 підтвердження, щоб зробити ймовірність

атаки менше 10%, 4 підтвердження, щоб менше 1% та відповідно 6, щоб менше 0,1%.

В таблиці 3.3 представлено розрахункові значення ймовірності успіху атаки в залежності від співвідношення потужностей майнерів (q), що належать зловмиснику до всієї потужності мережі Bitcoin та числа підтверджень n.

Таблиця 3.3 - Імовірність успіху атаки в залежності від потужності зловмисника

	Кількість підтверджуючих блоків n									
q	1	2	3	4	5	6	7	8	9	10
2%	4	0,24	0,02	0,002	0	0	0	0	0	0
4%	8	0,93	0,12	0,02	0,002	0	0	0	0	0
6%	12	2,12	0,41	0,08	0,02	0,002	0,001	0	0	0
8%	16	3,63	0,91	0,24	0,06	0,02	0,005	0,001	0	0
10%	20	5,64	1,71	0,54	0,17	0,06	0,02	0,007	0,002	0,001
12%	24	7,52	2,86	1,07	0,41	0,16	0,06	0,02	0,01	0,004
14%	28	10,7	4,41	1,88	0,82	0,36	0,16	0,07	0,01	0,02
16%	32	13,7	6,35	3,15	1,49	0,74	0,37	0,19	0,03	0,05
18%	36	17,1	8,74	4,62	2,49	1,36	0,74	0,42	0,09	0,13
20%	40	20,8	11,58	6,69	3,91	2,33	1,41	0,84	0,23	0,31
22%	44	24,8	14,88	6,69	5,82	3,72	2,41	1,56	0,51	0,67
24%	48	29,1	18,65	9,22	8,31	5,66	3,89	2,69	1,02	1,31
26%	52	33,5	22,86	12,39	11,42	8,23	5,98	4,38	1,87	2,37
28%	56	38,2	27,53	16,03	15,23	11,53	8,81	6,76	3,22	4,12
30%	60	43,2	32,61	20,31	19,76	15,64	12,74	10,13	5,22	6,51
32%	64	48,3	38,15	25,21	25,03	20,61	17,18	14,26	8,01	9,98
34%	68	53,6	43,98	36,7	31,12	26,42	22,66	19,56	16,91	14,65
36%	72	59,1	50,18	43,33	37,84	33,22	29,35	26,14	23,17	20,74
38%	76	64,8	56,95	50,42	45,25	40,83	37,67	33,72	30,84	28,25
40%	80	70,4	63,53	57,94	23,36	49,33	45,79	42,66	39,83	37,21
42%	84	76,2	70,52	65,85	61,96	58,42	55,38	52,64	50,21	47,62
44%	88	82,4	77,72	74,13	71,24	68,28	65,85	63,55	61,45	59,41
46%	92	88,2	85,45	82,67	80,45	78,58	76,82	75,21	73,76	72,39
48%	96	94	92,27	91,22	90,12	89,29	88,31	87,51	86,74	85,97
50%	100	100	100	100	100	100	100	100	100	100
52%	100	100	100	100	100	100	100	100	100	100

Виходячи з аналізу результатів розрахунків:

– ймовірність успіху атаки є при будь-яких рівнях потужності атакуючого;

– чекання якомога більшої кількості підтверджуючих блоків збільшує ймовірність провалу атаки;

– можливість провалу атаки залежить від кількості підтверджуючих блоків, а не від часу очікування після здійснення транзакції. Альтернативні мережі, можуть дати більш високий рівень безпеки угоди, при однаковому часі очікування до видачі товару;

– ніяка кількість підтверджень не знизить ймовірність успіху до повного 0.

Економічний рівень прибутку для атакуючого при атаці double-spending:

– атака може бути здійснена проти більш ніж одного продавця. Альтернативні платежі можуть бути спрямовані одночасно проти k різних продавців;

– від кожного торговця будуть купуватися продукти із загальною вартістю v;

– незалежно від того, вдасться атака чи ні, зловмисник отримає товар на суму kv;

– якщо атака не вдасться, і зловмисник встигне знайти j блоків за час спроби, кожен за ціною B, всі вони будуть відхилені і зловмисник втратить суму рівну jB.

Можливість провалу атаки дорівнює $1 - r$ (функцію від n і q, знайдену раніше).

Для того, щоб атака була прибутковою, потрібно виконання умови:

$$v > \frac{(1-r)jB}{kr}. \quad (3.11)$$

де:

v – сумарна вартість товарів;

r – імовірність успішної атаки;

j – кількість товарів;

B – ціна одного товару;

k – кількість продавців, яким відсилаються одні й ті самі дані (монети).

Продавець у безпеці доти, поки вартість товару досить невисока, щоб було економічно невигідно здійснювати таку атаку.

Наприклад для наступних вихідних даних: при $j = 20$, тобто зловмисник згенерував 20 блоків, перш ніж припинив спроби генерації. B = 6.25BTC – нагорода за блок. А $k = 5$, можливо розрахувати умови доцільності проведення атаки (коли продавець, умовно буде захищений від атаки через її недоцільність доти):

$$v \leq \frac{100(1-r)}{r} BTC = 100(\frac{1}{r} - 1)BTC\ . \qquad (3.12)$$

Максимальні безпечні суми угод у BTC для різних значень числа підтверджуючих блоків n та рівнів потужності майнінгу у зловмисника представлені в таблиці 4.

Таблиця 3.4 – Економічні умови щодо доцільності реалізації атак (безпечні суми угод у BTC)

	Кількість підтверджуючих блоків n									
q	1	2	3	4	5	6	7	8	9	10
2%	600	10к	124к	1,2кк	∞	∞	∞	∞	∞	∞
4%	287	2.6к	20к	124к	1.2кк	∞	∞	∞	∞	∞
6%	183	1.1к	6к	31к	124к	1.2кк	2.4кк	∞	∞	∞
8%	131	663	2.7к	10к	41к	124к	499к	2,4кк	∞	∞
10%	100	418	1.4к	4.6к	14к	41к	124к	357к	1.2кк	2.5кк
12%	79	307	849	2.2к	6к	15к	41к	124к	250к	620к
14%	64	208	541	1.3к	3к	7к	15к	35к	250к	124к
16%	53	157	368	768	1.6к	3.3к	6к	13к	83к	50к
18%	44	120	261	516	979	1.8к	3к	5.9к	27к	19к
20%	37	94	190	348	614	1к	1.7к	2.9к	10к	8к
22%	31	75	143	348	404	647	1к	1.5к	5к	3.7к
24%	27	60	109	246	275	416	617	904	2.4к	1.8к
26%	23	49	84	176	193	278	393	545	1.3к	1к
28%	19	40	65	130	139	191	258	344	751	851
30%	16	32	51	98	101	134	171	221	453	359
32%	14	26	40	74	74	96	120	150	287	225
34%	11	21	31	43	55	69	85	102	122	145
36%	9	17	24	32	41	50	60	70	82	95
38%	7	13	18	24	30	36	41	49	56	63

40%	6	10	14	18	21	25	29	33	37	42
42%	4	7	10	12	15	17	20	22	24	27
44%	3	5	7	8	10	11	12	14	15	17
46%	2	3	4	5	6	6	7	8	8	9
48%	1	1	2	2	2	2	3	3	3	4
50%	0	0	0	0	0	0	0	0	0	0

У таблиці 3.4 літерами к та кк позначено тисячі та мільйони умовних одиниць, відповідно.

Отримані результати спростовують ті міфи, які існували раніше, пов'язані з атакою double-spending, а саме:

– дана атака вимагає більше половини всіх потужностей мережі Bitcoin;

– очікування підтверджуючих блоків значно захищає від атаки з великими потужностями майнінгу;

– 6 підтверджуючих блоків дають повний захист від атаки;

– важливо почекати якнайбільше часу після транзакції, не звертаючи уваги на те, скільки було в цей час згенеровано блоків.

3.7 DoS атака

DoS-атака (Denial of Servise - «відмова в обслуговуванні») — хакерська атака на обчислювальну систему з метою довести її до відмови.

DDoS (Distributed Denial of Service) — атака, що проводиться одночасно з великої кількості комп'ютерів, з метою викликати відмову в обслуговуванні сервера або мережі.

Зловмисник зламує велику кількість машин, вибираючи найбільш уразливі, і формує базу для розподілених мережевих атак типу «відмова в обслуговуванні».

Успіх DoS/DDos-атак заснований на обмеженні пропускної здатності, яка є однією з характеристик будь-якого мережевого ресурсу. Під час DDoS-атаки веб-ресурсу відправляється велика кількість запитів з метою вичерпати його можливості обробки даних і порушити його нормальне функціонування.

Якщо кількість запитів перевищує граничні можливості будь-якого компонента інфраструктури, можуть виникнути такі проблеми з рівнем обслуговування:

– формування відповіді на запити відбувається значно повільніше, ніж звичайно;

– деякі або навіть усі запити користувачів можуть бути залишені без відповіді.

Для відправки на ресурс надвеликої кількості запитів зловмисники часто створюють із заражених комп'ютерів так звану "Зомбі-мережу". Оскільки злочинці можуть повністю контролювати дії кожного зараженого комп'ютера зомбі-мережі, масштаб такої атаки може бути надмірним для атакованих веб-ресурсів [15].

Спам-атаки можуть проводитися не тільки з метою банальної відмови в доступі, з метою уповільнити або паралізувати нормальне функціонування мережі для її користувачів, але і з метою вимагання та шантажу.

Крім атак у своїх корисливих цілях, спам-атака так само може здійснюватися з метою допомогти «жертві», як би парадоксально це не звучало. Саме такий випадок і стався з мережею Bitcoin.

Основною проблемою мережі деяких систем і зокрема Bitcoin, є лімітований розмір блоку в 1Мб. Від максимального розміру залежить в першу чергу кількість транзакцій, які можуть бути включені в один блок. Оскільки блок в середньому формується кожні 10 хвилин, пропускна здатність всієї мережі Bitcoin напряму залежить від цього параметра. Існуючий зараз граничний розмір блоку в 1Мб дозволяє здійснювати до 7 простих транзакцій, які включає один або два входи і виходи, і не більше 3 штатних транзакцій в секунду.

Коли середній обсяг транзакцій перевищить величину в 1 Мб за 10 хвилин, блоки почнуть переповнюватися і черга транзакцій, що чекають на підтвердження, буде безупинно зростати. Користувачі мережі Біткоїн вимушені будуть перекупати один у одного право на транзакції, які повинні увійти в наступний блок, шляхом підвищення комісій. Багато експертів справедливо

побоюються, що процес так званої «гонки комісій» зробить транзакції надто дорогими, а сам Bitcoin втратить головну конкурентну перевагу перед традиційними платіжними системами.

У ході виконання даного етапу кваліфікаційної роботи було розглянуто потенційні атаки на децентралізовані мережі шляхом використання транзакцій як основного вразливого компоненту системи. В процесі аналізу було виявлено, що вартість атак у системах із різними підходами (PoS, PoW, DPoS) відрізняється і може бути недоцільною, оскільки вартість атаки буде перевищувати потенційний заробіток. Отримані результати використані для висунення рекомендацій щодо підвищення безпеки даних в блокчейн системах.

4 РОЗРОБКА ЗАХОДІВ ПІДВИЩЕННЯ БЕЗПЕКИ БЛОКЧЕЙН СИСТЕМ

З урахуванням проведеного аналізу щодо визначених загроз та вектору атак на транзакції використовується наступна ідеологія щодо удосконалення захисту даних в блокчейн системах:

– застосування алгоритмів, які дозволяють перевіряти чи є новий сформований блок продовженням існуючого блокчейну, що дозволить запобігти ситуації, коли зловмисник працює над побудовою альтернативного блокчейну і намагається провести атаку подвійної витрати;

– застосування гібридної моделі погодження, яка дозволить зменшити множину можливих атак на систему завдяки тому, що використовує переваги обох підходів;

– застосування протоколу узгодження Tendermint, основною метою якого є ідея обмежити вагу рішення зловмисника у процесі валідації шляхом використання моделі заставної транзакції;

– використання гібридного алгоритму узгодження Slasher, головною ідеєю якого є блокування нагороди за валідацію на деякий час, що набагато збільшує вартість проведення атак типу атаки підкупом або подвійної витрати, оскільки змушує зловмисника витрачати більше ресурсів на підтримання життєдіяльності альтернативного блокчейну;

– збільшення кількості повних нод та заохочення фінансових організацій до розвитку блокчейн систем, насамперед, щоб зменшити відсоток успішності проведення атаки Сибіли та збільшити її вартість;

– розробку та впровадження активних захисних систем проти спам-атак, які використовують мінімальну вартість транзакції для заповнення черги транзакцій і виклику відказу системи чи простою.

4.1 Посилання на блоки в транзакціях

В деяких PoS-системах, кожна транзакція може включати геш попереднього останнього відомого її винахіднику блоку. Ця модифікація робить неможливим включення транзакції в блокчейн, який не містить блоку, на який посилається транзакція. Таким чином, атакуючий, створює альтернативний блокчейн і користувачі системи, які його підтримують, створюючи блоки поверх ланцюга блоків атакуючого, не можуть зібрати комісію за більшість транзакцій.

Удосконалення покладається на дещо оптимістичні припущення, що користувачі системи можуть за будь-яких умов визначити, який блокчейн є коректним; воно не є ефективним, якщо нагорода за створення блоків не визначається комісією за транзакції.

4.2 Використання гібридного погодження PoW/PoS

Деякі системи, що використовують підтвердження частки, вирішують проблему початкового розподілу коштів, застосовуючи обмежену версію доказу роботи для збільшення монетарної маси; Прикладами таких валют є Peercoin і Novacoin. Гібридне погодження працює за рахунок створення двох типів коректних блоків:

Основна альтернатива гібридному узгодженню - повністю заздалегідь створений запас валюти. Рішення з PoW і PoS-блоками, розділеними в часі, використовується в Etnereum. У 2021 році Etnereum випустили версію Etnereum 2.0 у якій використовується PoS-підхід.

Гібридне PoW / PoS-узгодження стійке проти атак переписуванням історії за умови, що безпека системи забезпечується достатніми гешуючими потужностями. Включення PoW-блоків в блокчейн також допомагає захистити систему проти інших видів атак. Тому що підтвердження частки зазвичай вводиться як альтернатива доказу роботи, комбіновані системи з часом

відмовляються від PoW повністю або принаймні знижують його роль у системі, як це зробили у Etnereum 2.0.

4.3 Tendermint

Tendermint [21] запропонована концепція блокчейна, в якому безпека забезпечується модифікованим протоколом узгодження на основі підтвердження частки. В Tendermint кожен блок має бути криптографічно підписаний валідаторами. Валідатор це користувач системи, який підтверджує свою зацікавленість у забезпеченні безпеки, замикаючи свої кошти за допомогою заставної транзакції (англ. bonding transaction); вага думки кожного валідатора пропорційна до обсягу замкнених засобів. Після закінчення служби в якості валідатора, користувач отримує доступ до замкнених коштів за рахунок повернення застави (англ. unbonding transastion); кошти повертаються з певною затримкою (англ. unbonding period).

Блок вважається коректним, якщо він підписаний валідаторами, які в сумі мають не менше ніж 2/3 загальної ваги голосів. Таким чином, форк блокчейна можливий тільки в разі, якщо існує група валідаторів з не менше ніж 1/3 вагою голосів, яка підписує блоки в обох конкуруючих блокчейнах. У випадку форка валідаторів, що підписують кілька блокчейнів, можна покарати за рахунок публікації довільним користувачем транзакції свідоцтва (англ. evidence transstation), що містить доказ їх злого умислу, наприклад, їх цифрових підписів блоків однакової висоти з обох ланцюжків.

Транзакція-свідоцтво знищує всі закладені кошти валідаторів, що діють поза протоколом. Ця логіка запобігає короткочасним атакам. У той же час, атаки переписуванням історії все ще можливі: валідатори з 2/3 загальної ваги голосів можуть змовитися і опублікувати форк блокчейна після того, як їх кошти розблоковані. Для запобігання довгостроковим атакам можна використовувати механізм, що забороняє довгі форки блокчейна.

4.4 Slasher

Slasher гібридний PoS/PoW-алгоритм узгодження, описаний Віталіком Бутериним, одним з архітекторів Ethereum [22]. На відміну від інших гібридних алгоритмів, для генерації блоків у Slasher використовується виключно доказ роботи; але при цьому кожен блок валідується як PoW, так і PoS.

Блоки створюються за допомогою підтвердження роботи. Замість того, щоб включати coin-base-транзакцію для отримання винагороди за вирішений блок, валідатор включає в блок число $hash(n)$ для деякого великого натурального числа n. Це число є доказом валідації; валідатор може забрати положену йому винагороду за блок, створивши спеціальну транзакцію, що відкриває n. Нагорода за валідацію замкнута на 100 блоків і обмежена в часі: винагороду за блок на висоті h можна отримати за рахунок транзакції, записаної в одному з блоків з висотою $h + 100, h + 101, \dots, h + 900$. Середній час між створенням блоків дорівнює 30 секунд.

Щоб створити коректний блок, він має бути підписаний криптографічно. Підписуючі користувачі вибираються випадково з використанням умови:

$$Signers(h) = \left\{A: hash(n(h-2000), n(h-1999), \dots, n(h-1901), A) \leq 64M\ bal(\frac{A}{B})\right\}, \quad (4.1)$$

де:

$B = \Sigma$а ваl(а) загальна кількість монет у обігу;

$n(i)$ - доказ майнінгу, використаний у блоці i.

Рівняння (4.1) означає, що в середньому кожен блок може підписати 64 користувача, а можливість стати передплатником пропорційна обсягу коштів, якими володіє користувач. Для визначення коректного блокчейна при форці використовується сумарна кількість підписів. Підписавши блок, користувач отримує нагороду, замкнуту протягом наступних 100 блоків.

Нагорода за підпис вище, ніж нагорода за майнінг, з метою запобігти гонку озброєнь серед майнерів.

Для боротьби з форками блокчейну Slasher використовує механізм, аналогічний Tendermint. Якщо користувач системи бачить кілька блоків однакової висоти, підписані одним і тим самим валідатором, користувач може опублікувати транзакцію з цими двома підписами. Якщо ця транзакція буде включена в блок перш ніж нагорода за блок стане доступна для використання несумлінним валідатором, 33% нагороди виплачується користувачеві, що виявив відступ від протоколу, а решта коштів знищується.

Імплементація підтвердження частки, що використовується в Slasher, великою мірою запобігає короткостроковим форкам блокчейна. Насправді, вразливість POS до короткострокових атак виникає з наступного спостереження.

В моделі PoS, ймовірності створити блок для кожної з конкуруючих ланцюгів незалежні один від одного, оскільки вони залежать від геша останнього блоку ланцюга. Для користувачів системи має сенс намагатися створити блоки на основі кожного з ланцюгів, оскільки це збільшує очікувану винагороду. З іншого боку, у Slasher ймовірність стати валідатором блоку визначається з великим тимчасовим інтервалом і однакова для всіх ланцюгів, якщо вони відносно малі. Таким чином, у користувачів немає підстав підтримувати форк блокчейна, оскільки вони заздалегідь знають, чи будуть вони підписувати блоки в майбутньому. Для користувачів не має сенсу підтримувати кілька гілок блокчейна, якщо у них немає впевненості, що форк має більше 2000 блоків. Оскільки Slasher використовує доказ роботи для створення блоків, атака переписуванням історії вимагає існуючих обчислювальних потужностей. Це дає Slashep істотно перевагу в порівнянні з моделями делегованого PoS, які не використовують доказ роботи.

4.5 Основні концепції захисту від атаки Сибіли

Атака Сибіли представляє фактичну загрозу безпеці мережі будь-якої системи і Bitcoin зокрема. Одним із способів захисту від атаки Сибілли - спробувати зробити її дорожчою. Кількість повних нод, підконтрольних

зловмисникам залежить від безпосередньої кількості повних нод в мережі, а значить, щоб зробити атаку дорожчою, необхідно збільшити кількість повних вузлів (нод).

Збільшити кількість повних нод можна двома способами:

– створити прямий фінансовий інтерес для розгортання повної ноди для самих користувачів;

– організувати розгортання повних нод силами організацій, що використовують децентралізовані системи для проведення фінансових операцій.

Перший спосіб уже успішно застосований в інших системах. На сьогоднішній день система заохочує майнерів за те, що вони здобувають монети і підтверджують транзакції, але можна ввести правило, в рамках якого будуть заохочуватися власники повних нод на підставі кількості часу безперервного перебування в мережі або кількості підключень, в рамках яких повна нода працювала на поширення інформації про транзакції іншим учасникам мережі.

Другий спосіб - це організоване розгортання повних нод силами організацій, що використовують криптовалюту для проведення фінансових операцій. Організації, які надають можливість використовувати Bitcoin для оплати своїх товарів і послуг, валютні біржі та інші організації, які безпосередньо зацікавлені в безпеці системи можуть, у приватному порядку, використовуючи свої фінансові можливості посилити безпеку мережі шляхом розгортання повних нод.

4.6 Протидія DoS/DDoS-атакам

Для ефективної протидії DoS-атакам необхідно знати тип, характер і інші їх характеристики, а оперативно отримати ці відомості дозволяють послуги забезпечення безпеки. Вони допомагають зробити деякі налаштування системи, але визначити, чи була ця атака зроблена зловмисником, або відмова в обслуговуванні була наслідком позаштатної події, вони не можуть. У відповідності з правилами політики забезпечення безпеки, при виявленні DOS

або DDoS-атаки буде потрібна її реєстрація для подальшого аудиту. Для виявлення DDoS-атаки можуть також використовуватися служби, не пов'язані з безпекою, наприклад, перенаправлення трафіку по інших каналах зв'язку, включення резервних серверів для копіювання інформації. Таким чином, засоби для виявлення і запобігання DDoS-атак можуть сильно відрізнятися в залежності від виду системи, що захищається.

Методи вияву DoS-атак можна розділити на кілька великих груп:

– сигнатурні - засновані на якісному аналізу трафіку;

– статистичні – засновані на кількісному аналізу трафіку;

– гібридні (комбіновані) - які поєднують у собі переваги обох вищеназваних методів.

Заходи протидії DDoS-атакам можна розділити на пасивні та активні, а також на превентивні та реакційні атаки.

Запобігання — профілактика причин, що спонукають тих чи інших осіб організовувати та вживати DDoS-атаки.

Заходи у відповідь — застосовуючи технічні та правові заходи, потрібно якомога активніше впливати на джерело DDoS-атаки та його організатора.

Програмне забезпечення - на сьогоднішній день існують спеціальні розробки, найчастіше сервери, здатні захистити від слабких DDoS-атак.

Зворотний DDoS - перенаправлення трафіку, що використовується для атаки, на атакуючого. При достатній потужності сервера, що атакується, дозволяє не тільки успішно відбити атаку, але і вивести з ладу сервер атакуючого.

Усунення вразливостей - міра, спрямована на усунення помилок в системах і службах. Однак такий метод не працює проти флуд-атак, для яких вразливістю є кінцівка тих чи інших системних ресурсів.

Нарощування ресурсів - є хорошим фоном для застосування інших видів захисту від DDoS-атак.

Розосередження - побудова розподілених систем, а також їх дублювання, які не припинять обслуговувати користувачів, навіть якщо деякі їх елементи стануть недоступні через DOS-атаки.

Ухилення - уведення безпосередньої мети атаки подалі від інших ресурсів, які часто також піддаються впливу разом з безпосередньою метою атаки.

Активні заходи у відповідь — вплив на джерела, організатора або центр управління атакою, як техногенними, так і організаційно-правовими засобами.

У даному розділі кваліфікаційної роботи було висунуто діючі засоби та заходи для забезпечення безпеки децентралізованих систем при роботі з даними. Більшість запропонованих рекомендацій грунтуються на необхідності маштабування існуючих систем задля збільшення часу або вартості проведення атак і, відповідно, щоб зробити атаки недоцільними.

ВИСНОВКИ

Метою даного дослідження був аналіз методів забезпечення безпеки даних (транзакцій) у блокчейн системах, аналіз можливих атак, обчислення вартості їх реалізації, з метою їх запобігання та моделювання стратегій захисту. Були виконані такі завдання: описано та проаналізовано принцип роботи блокчейну, принцип побудови блоків транзакцій, описано криптографічні алгоритми які забезпечують децентралізованість мережі, складено список потенційних кібератак, проведено їх огляд, розраховано приблизну вартість реалізації атак та розроблено стратегію захисту від них.

Для атаки Сибіли був сформований список мінімальних технічних вимог комплектуючих комп'ютера для створення однієї ноди. На прикладі Bitcoin був зроблений приблизний розрахунок вартості атаки Сибілли на мережу. За розрахунковими даними, за якими було обчислено вартість атаки, було запропоновано метод реалізації захисту — зробити атаку дорожчою. Кількість повних нод, підконтрольних зловмисникам залежить від безпосередньої кількості повних нод в мережі, а значить, щоб зробити атаку дорожчою, необхідно збільшити кількість повних нод.

Збільшити кількість повних вузлів (нод) можна двома способами:

– створити прямий фінансовий інтерес для розгортання повної ноди для самих користувачів;

– організувати розгортання повних нод силами організацій, що використовують децетралізовані системи для проведення фінансових операцій.

На теперішній час мінімальна вартість атаки Сибіли становить близько 10 мільйонів доларів. З аналізу результатів розрахунків можливо зробити висновки, що, збільшивши кількість повних вузлів (нод) у кілька разів, вартість атаки буде набагато більша за суму витрачену на відкриття нод. Таким чином, підтримка фінансової зацікавленості користувачів для розгортання повних вузлів (нод) призведе до їх збільшення в мережі. Внаслідок цього зробить реалізація атак Сибіли буде занадто дорогою для зловмисників.

Для атак подвійної витрати були визначені етапи їх реалізації та змодельована (розраховано) необхідні умови їх успішного впровадження. На прикладі Bitcoin був проведений розрахунок ймовірності успіху атаки в залежності від потужностей майнера та за отриманими даними були обчислені максимальні безпечні суми угод в BTC для різних значень кількості підтверджуючих блоків n і рівнів потужності майнінгу у зловмисника від загальної потужності мережі.

За результатами аналізу методів безпеки та розрахунків можливо зробити наступні висновки:

– є ймовірність успіху атаки при будь-яких рівнях потужності атакуючого;

– можливість провалу атаки залежить від кількості підтверджуючих блоків, а не від часу очікування після здійснення транзакції, тобто очікування якомога більшої кількості підтверджуючих блоків збільшує ймовірність провалу атаки.

Для DDoS-атаки було проведено аналіз методів захисту від атак, визначені (розраховані) умови за яких проведення цього типу атак є економічно невигідними. Однією з популярних DDoS-атак є відправка мікротранзакцій. Зробити таку атаку невигідною можливо кількома способами:

– стягувати комісію за кожен малий вихід, який створює відправник. Цей спосіб збільшить кількість витрат зловмисника вп'ятеро;

– не включати в блокчейн, тобто. у міру накопичення мінімальних транзакцій, формувати в одну більшу, після чого відправляти в мережу. Такий спосіб може практично повністю позбавити мережу від атак міктротранзакціями;

– збільшити розмір блоку на 1 Мбайт, що збільшить комісію спам-атак в 3 рази, що є вкрай невигідно для атакуючого.

Основною ідеєю впровадження запропонованих заходів забезпечення безпеки є подальше маштабування існуючих систем з метою збільшення часу або вартості проведення атак, підвищення складності їх впровадження, а відповідно створення комплексних умов недоцільності їх проведення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Usenet: A Bulletin Board for Unix Users // BYTE. – 8(10) January 1983. – P. 219–236.

2. Bhushan A. A File Transfer Protocol [Електроний ресурс] / A. Bhushan. – April 1971. – Режим доступу: https://www.rfc-editor.org/rfc/pdfrfc/rfc114.txt.pdf.

3. Huckle S. Internet of Things, Blockchain and Shared Economy Applications / S. Huckle, R. Bhattacharya, M. White, N. Beloff // Procedia Comput. Science. – Oct. 2016. – Vol. 98. – P. 461–466.

4. Dingledine R. Tor: The second-generation onion router [Електроний ресурс] / Roger Dingledine, Nick Mathewson, Paul Syverson. – Режим доступу: https://www.freehaven.net/ anonbib/cache/draft-tor-design2004.pdf.

5. Dingledine R. Tor: The second-generation onion router [Електроний ресурс] / Roger Dingledine, Nick Mathewson, Paul Syverson // Naval Research Lab Washington DC, 2004. – Режим доступу: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

6. Foster I. The Grid: Blueprint for a new computing infrastructure / Foster Ian, Kesselman Carl. – San Francisco, CA, USA : Morgan Kaufmann Publishers Inc., 1999. – 677 p.

7. SETI@home [Электронный ресурс]. – Режим доступа: https://setiathome.berkeley.edu/.

8. Baran P. On distributed communications: I. Introduction to distributed communications networks [Електроний ресурс] / Paul Baran. – Aug. 1964. – Режим доступу:https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.

9. Coinbase maturity of 100 transactions [duplicate] [Електроний ресурс]. – Режим доступу: https://bitcoin.stackexchange.com/ questions/ 22548/coinbase-maturity-of-100-transactions.

10. Entropy (computing) [Електроний ресурс] // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/Entropy_(computing).

11. Ralph C. Merkle. A Digital Signature Based on a Conventional Encryption Function. In Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science. Vol. 293. https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkle.pdf.

12. SHA-2 [Електроний ресурс] // Wikipedia. - Режим доступу: https://ru.wikipedia.ord/wiki/SHA-2.

13. Proof of stake: How I learned to love weak subjectivity // Ethereum Blog.2014 [Електроний ресурс] — Режим доступу: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity.

14. Vitalik Buterin .On stake// Ethereum Blog.2014 [Електроний ресурс] — Режим доступу: https://blog.ethereum.org/2014/07/05/stake.

15. Khaled Baqer, Danny Yuxing Huang, Damon McCoy, Nicholas Weaver “Stressing out: Bitcoin Stress Testing”. [Електроний ресурс] Режим доступу: https://www.cl.cam.ac.uk/~kabnb2/papers.

16. Rosenfeld. Analysis of hashrate-based double-spending [Електроний ресурс] Режим доступу: https://bitcoil.co.il/Doublespend.pdf.

17. Ghassan O.Karame, Elli Androulaki. Double-spending attacks on fast payments in Bitcoin. 2012. [Електроний ресурс] Режим доступу:https://eprint.iacr.ord/2012/248.pdf.

18. Ittay Eyal, Emil Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable [Електроний ресурс] Режим доступу: https://arxiv.org/pdf/1311.0243v5.

19. Ed Felten. Game of theory and Bitcoin // Freedom to Tinker.2013 [Електроний ресурс] - Режим доступу: https://freedom-to-tinker.com/blog/felten/game-theory-and-bitcoin.

20. Bitcoin days destroyed [Електроний ресурс] - Режим доступу: https://blockchain.info/charts/bitcoin-days-destroyed.

21. Daniel Larimer. Transactions as proof-of-stake [Електроний ресурс] – Режимдоступу:https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf.

22. Jae Kwon. Tendermint: consensus without mining. [Електроний ресурс]: — Режим доступу: http://tendermint.com/docs/tendermint.pdf.

23. Сайт статистики мережі Bitcoin [Електроний ресурс] — Режим доступу: https://blockchain.info.