НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп’ютерного практикума

Дослідження розгортання систем Etherium та криптовалют

Виконали студенти
групи ФЕ-31мп
Межуєв М.Д.
Альошкін В.А.

Перевірила:
Байденко П. В.

Київ — 2024

Зміст

1. Огляд реалізації приватної мережі в Bitcoin

Bitcoin (BTC) — це тип криптовалюти, яка була створена для анонімного та прямого обміну цінностями між користувачами за допомогою моделі однорангових транзакцій (P2P), яка усуває потребу у центральному посереднику, такому як банк або брокер. Термін P2P стосується децентралізованих мереж, в яких взаємодіють комп'ютерні системи, що містять однорангові вузли. Усі вузли рівноправні, і обмін даними відбувається без центрального сервера — тобто кожен комп'ютер або вузол може виступати як файловий сервер, так і клієнт. Наприклад, діючи як клієнт, вузол завантажує дані від інших учасників; і коли він діє як сервер, він може бути джерелом завантаження. Простіше кажучи, однорангові комп'ютери або комп'ютерні системи, що беруть участь у обміні, можуть одночасно споживати та надавати ресурси в одній мережі.

В якості основного елемента технології блокчейн, архітектура P2P керує транзакціями криптовалюти. Блокчейн публічно та безперервно зберігає транзакції. Нові "блоки", що містять відомості про відправників і одержувачів із міткою часу, постійно пов'язуються з раніше заповненими блоками, утворюючи ланцюжок блоків даних. У відсутності центрального органу управління мережею, лише вузли-учасники можуть перевіряти транзакції між собою. Система є "ненадійною", оскільки архітектура мережі сама по собі гарантує цілісність транзакцій.

Забезпечення приватності та безпеки - це складний процес, але не неможливий. Розробка інструментів, що допомагають зберігати приватність при використанні Bitcoin, продовжується, і, на щастя, взаємодія з більшістю цих інструментів стає все простішою. На жаль, панацеї не існує. Потрібно розуміти компроміси і дотримуватися кращих практик у процесі їх розвитку.

Основний метод, який використовується для збереження приватності користувачів BTC, полягає в відсутності ідентифікації власників відповідних монет та адрес. Іншими словами, хоча транзакції є відкритими, вкрай проблематично встановити осіб, які беруть участь у цьому процесі. Основні загрози для приватності виникають при покупці монет через KYC-сервіси

(тобто ті, що потребують документальне підтвердження особи) або використанні однієї адреси декілька разів.

У той самий час, придбання біткоїнів безпосередньо в інших власників (навіть із певним націненням) та використання нових адрес для різних транзакцій може забезпечити задовільну приватність у більшості випадків. Проте всі власники BTC повинні пам’ятати, що Bitcoin не є анонімним, і особиста дисципліна при його використанні відіграє ключову роль.

Використовуйте рішення, що дозволяють забезпечити власне зберігання приватної інформації. Якщо ви відправляєте кошти на біржу, які відомі ваші персональні дані, то вона зможе ідентифікувати вихідні транзакції як такі, що також належать вам. Далі вони зможуть проаналізувати транзакції, які передували їм. Цей цикл може бути подовжено, доки не вдасться ідентифікувати конкретну особу.

Один із способів підвищення конфіденційності — це проведення транзакцій таким чином, щоб мінімізувати ефективність аналізу блокчейну, заснованого на розрахунку ймовірностей. Існують різні підходи до розв'язання цієї проблеми, включаючи методи об'єднання учасників.

- Coinjoins - це складні транзакції, які дозволяють інтегрувати внески різних учасників у одну і ту ж транзакцію. JoinMarket створює вільний ринок для учасників для придбання входів, у той час, як WhirlPool та Wasabi є централізованими координаторами, що надають послуги за плату.
- CoinSwaps - це система, коли два користувачі обмінюються монетами, які виглядають як дві непов'язані транзакції в мережі. Такі реалізації, як Teleport Transaction, можуть за потреби зробити будь-яку звичайну транзакцію схожою на coinswap.

Для біткоїна існує чудовий клієнт для запуску вузла – Bitcoin Core. Він забезпечує повну валідацію, мережеву підтримку та безпеку конфіденційності. Основними мінімальними вимогами для запуску є: 7 ГБ на диску (хоча все ж рекомендовано близько 350 ГБ), 1 ГБ ОЗУ, стабільний інтернет та настільний комп'ютер чи ноутбук з чіпсетами ARM.

2. Огляд реалізації приватної мережі в Ethereum

Почнемо з визначення Ethereum і приватної мережі у контексті блокчейн-систем. Ethereum — це децентралізована мережа, де інформація передається безпосередньо між вузлами без посередництва центрального сервера. Кожні 12 секунд випадковим чином обирається один з вузлів для створення нового блоку, що містить перелік транзакцій, які повинні бути виконані вузлами, що отримують цей блок. Приватна мережа складається з кількох вузлів Ethereum, які можуть взаємодіяти лише між собою. Для локального запуску декількох вузлів кожен з них потребує окремого каталогу даних. Вузли також повинні бути обізнані один про одного, обмінюватися інформацією, поділяти початковий стан та загальний алгоритм консенсусу.

Головним інструментом для створення приватної блокчейн-мережі є Geth. Geth, написаний мовою програмування Go, виступає клієнтом Ethereum, що перетворює комп'ютер на вузол мережі Ethereum. Кожен блок містить інформацію, яка використовується Geth для оновлення "стану" мережі, включаючи баланси ефіру на рахунках та дані смарт-контрактів. Існують два типи рахунків: рахунки зовнішньої власності (EOA) і контрактні рахунки. Контрактні рахунки виконують код смарт-контракту при отриманні транзакцій, тоді як EOA — це рахунки, якими користувачі керують локально для підписання та надсилання транзакцій. Кожен EOA складається з пари ключів: відкритого, який використовується для створення унікальної адреси, і закритого, який забезпечує безпеку рахунку та дозволяє підписувати повідомлення.

Головна мережа Ethereum має ідентифікатор ланцюга (ChainID) = 1. Також існує багато інших мереж, до яких Geth може підключатися, використовуючи альтернативні ідентифікатори ланцюгів. Деякі з цих мереж є тестовими, а інші — альтернативними мережами, створеними на основі форків вихідного коду Geth. Використання мережевого ідентифікатора, який не зайнятий жодною існуючою або тестовою мережею, дозволяє вузлам, що використовують цей ідентифікатор, підключатися лише між собою, створюючи

приватну мережу. Перелік поточних мережевих ідентифікаторів (ChainID) можна знайти на сайті Chainlist.org. ChainList містить список мереж EVM. Користувачі можуть використовувати цю інформацію для підключення своїх гаманців та Web3-провайдерів до відповідного ідентифікатора ланцюга та мережі. Всі вони базуються на Ethereum Virtual Machine, яка визначає правила обчислення нового стану мережі від блоку до блоку.

Апаратні вимоги для запуску вузла Geth змінюються залежно від конфігурації та оновлень мережі. Хоча вузли Ethereum можуть функціонувати на пристроях з низьким енергоспоживанням та обмеженими ресурсами, зазвичай використовують окремий комп'ютер, щоб уникнути перевантаження основного пристрою. Комп'ютер з високими технічними характеристиками дозволить відкласти необхідність обслуговування, оскільки блокчейн постійно збільшується, і рано чи пізно ця потреба виникне.

Щодо технічних вимог, мінімальні характеристики включають: 4-8 ГБ ОЗУ та 2 ТБ SSD (SSD рекомендується через високу швидкість запису). Рекомендовані параметри: Intel NUC 7-го покоління або вище, дротове інтернет-з'єднання (це не обов'язково, але забезпечує стабільнішу роботу з мережею), екран і клавіатура.

Існує кілька варіантів клієнтів для використання:

- **Geth** (описаний вище)
- **Besu** — клієнт Ethereum з відкритим вихідним кодом, розроблений за ліцензією Apache 2.0 і написаний на Java. Працює в публічних і приватних мережах.
- **Erigon** — реалізація Ethereum з рівнем виконання і вбудованим рівнем консенсусу, оптимізована для високої ефективності. Написана мовою Go.
- **OpenEthereum** — швидкий і багатофункціональний багатомережевий клієнт Ethereum, написаний на Rust. Важливо зазначити, що OpenEthereum вже застарів і більше не підтримується.
- **Nethermind** — вузол Ethereum з широкими можливостями налаштування, розроблений на платформі .NET.

Розглянемо систему Geth докладніше, розпочавши з її вимог і переходячи до

внутрішньої структури. Однією з головних складових будь-якої блокчейн мережі є алгоритм консенсусу, який вирішує завдання невизначеності щодо того, яким чином має працювати ланцюг. У той час як основна мережа використовує proof-of-stake (PoS) для захисту блокчейну, Geth також підтримує алгоритм консенсусу "Clique" proof-of-authority (PoA) і алгоритм доказу роботи Ethash як альтернативу приватним мережам.

2.1 Clique

Clique consensus — це система PoA, де нові блоки можуть створювати лише авторизовані "підписанти". Протокол консенсусу кліки описаний в EIP-225. Початковий набір авторизованих підписантів налаштовується в генезис-блоці. Підписанти можуть бути авторизовані та позбавлені авторизації за допомогою механізму голосування, що дозволяє змінювати набір підписантів під час роботи блокчейну. Clique можна налаштувати на будь-який час блоку, оскільки вона не прив'язана до налаштування складності.

2.2 Ethash

Алгоритм PoW від Geth, Ethash, — це система, що дозволяє відкрито брати участь будь-кому, хто бажає виділити ресурси на майнінг. Хоча це критично важлива властивість для загальнодоступної мережі, загальна безпека блокчейну суворо залежить від загальної кількості ресурсів, що використовуються для її захисту. Таким чином, PoW є поганим вибором для приватних мереж з невеликою кількістю майнерів. Складність майнінгу Ethash регулюється автоматично таким чином, що нові блоки створюються з інтервалом приблизно в 12 секунд. У міру того, як у мережі розгортається більше ресурсів для майнінгу, створення нового блоку стає складнішим, щоб середній час блоку збігався з цільовим часом блоку.

3. Огляд реалізації приватної мережі в Litecoin

Litecoin представляє собою цікаву криптовалюту, яка дуже схожа на Bitcoin, що навіть символізується її прізвиськом "срібло до золота біткоїна". Так само, як і біткоїн, Litecoin працює на блокчейні з відкритим вихідним кодом, який не контролюється жодним центральним органом влади. Кожен оператор вузла Litecoin має копію кожного блокчейну, щоб гарантувати, що нові транзакції не суперечать його історії транзакцій, а майнери допомагають обробляти нові транзакції, включаючи їх у щойно видобуті блоки.

Litecoin і Bitcoin мають кілька ключових відмінностей. Транзакції на Litecoin відбуваються швидше, а криптовалюта має більшу пропозицію. Він використовує інший алгоритм хешування, щоб майнінг був справедливим для всіх, і вважається, що ці відмінності допомогли LTC досягти успіху та залишатися однією з найкращих криптовалют протягом багатьох років.

Жоден центральний орган влади не може заморозити ваші гроші в Litecoin, оскільки це повністю децентралізована мережа. Тільки користувачі мають контроль і повноваження приймати рішення щодо своїх грошей. В результаті Litecoin можна використовувати як однорангову (P2P) платіжну систему для виплат людям у всьому світі без посередника. Також його можна використовувати як притулок або як частину диверсифікованого криптовалютного портфеля.

Крім того, Litecoin можна вважати безпечнішим за Bitcoin. Оскільки ніхто не створює форки Litecoin без надійного захисту, це, ймовірно, безпечніше, ніж Bitcoin. Проте ліквідність має велике значення для розвиваючихся установ, і Bitcoin набагато ліквідніший, ніж Litecoin. Litecoin відзначається серед інших альтернативних криптовалют своїми інноваціями, включаючи поєднання вищої швидкості поширення блоків і використання алгоритму хешування Scrypt. Також він значною мірою уникнув так званого премайнінгу, коли творці криптовалюти майнять монети до запуску проекту для громадськості.

Litecoin - це альткойн, що базується на майнінгу, і використовує метод консенсусу PoW для верифікації своїх транзакцій. Фактично, PoW вимагає, щоб

одна сторона продемонструвала всім іншим учасникам мережі, що було зроблено певні обчислювальні зусилля. На відміну від Bitcoin, який використовує метод хешування SHA-256 PoW, Litecoin використовує техніку Scrypt PoW, яка є менш вимогливою до ресурсів.

Початкові зусилля криптовалюти були підкріплені реалізацією кількох функцій, які також були запропоновані, а пізніше реалізовані в мережі Bitcoin. Ці поліпшення часто спрямовані на те, щоб гарантувати, що мережа може масштабуватися, щоб вміщати більше транзакцій на секунду, не жертвуючи децентралізацією, і забезпечувати конфіденційність під час транзакцій.

Технологія SegWit вперше була реалізована на блокчейні Litecoin, ще до її додавання у Bitcoin. Хоча вона була запропонована для Bitcoin у 2015 році, вперше вона була прийнята Litecoin. Після успішного впровадження на LTC, технологія була також додана до Bitcoin. Основна мета SegWit полягає у масштабуванні криптовалюти, відокремлюючи дані цифрового підпису для кожної транзакції (свідки) та ефективно використовуючи обмежений простір. Вона була розроблена для вирішення проблем масштабованості Bitcoin.

Lightning Network, з свого боку, це рішення для масштабування, яке створює додатковий рівень поверх блокчейну, де транзакції є швидкими і комісії невеликі. Цей додатковий рівень включає в себе платіжні канали, створені користувачами. Початково він був призначений для реалізації на блокчейні Bitcoin, і, подібно до SegWit, спочатку був реалізований на Litecoin, який багато хто використовував для тестування Lightning Network в реальних умовах. Однак впровадження Lightning Network на Litecoin було повільнішим, аніж на Bitcoin, величезній популярності якого воно набуло з різницею у часі. Це може бути пов'язано зі зниженим рівнем комісій за транзакції на Litecoin.

Висновок

У цій роботі ми досліджували можливість розгортання різних систем криптовалют і розглянули різноманітні функції та варіанти, що допомагають їм працювати більш ефективно. Порівнюючи їх, ми зазначили, що система Ethereum пропонує більше можливостей та варіацій для розгортання. Крім того,

ми навели мінімальні вимоги, за яких кожна система може працювати оптимально.