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

Звіт з виконання комп'ютерного практикуму

ДОСЛІДЖЕННЯ РОЗГОРТАННЯ СИСТЕМ ETHEREUM ТА КРИПТОВАЛЮТ

Виконали студенти
групи ФІ-32мн
Величко Олена,
Мельник Ілля,
Міснік Аліна

Перевірила:
Селюх П.В.

Київ — 2024

Мета роботи: Отримання навичок налаштування платформ виконання смартконтрактів та криптовалют.

Постановка задачі: Провести порівняльний аналіз особливостей розгортання систем криптовалют у порівнянні із системою Etherium.

1 ХІД РОБОТИ

1.1 Реалізація приватної мережі в Ethereum

Для початку варто зазначити, що таке Ethereum та приватна мережа в сфері блокчейн систем. Ethereum — це однорангова мережа, де інформація обмінюється безпосередньо між вузлами, а не керується центральним сервером. Кожні 12 секунд випадковим чином вибирається один вузол для генерації нового блоку, що містить список транзакцій, які вузли, що отримують блок, повинні виконати. Приватна мережа складається з кількох вузлів Ethereum, які можуть підключатися лише один до одного. Для того, щоб запускати кілька вузлів локально, для кожного з них потрібен окремий каталог даних. Вузли також повинні знати один про одного і вміти обмінюватися інформацією, розділяти початковий стан і загальний алгоритм консенсусу.

Основним інструментом для створення приватної мережі є Geth. Geth — це клієнт Ethereum, написаний на мові Go. Це означає, що запуск Geth перетворює комп'ютер на вузол Ethereum. Інформація, надана в кожному блоці, використовується Geth для оновлення його «стану» - ефірного балансу кожного облікового запису на Ethereum і даних, що зберігаються кожним смарт-контрактом. Існує два типи облікових записів: рахунки зовнішньої власності (EOA) і контрактні рахунки. Контрактні рахунки виконують код контракту, коли отримують транзакції. EOA – це облікові записи, якими користувачі керують локально, щоб підписувати та надсилати транзакції. Кожен EOA — це пара відкритих-закритих ключів, де відкритий ключ використовується для отримання унікальної адреси для користувача, а закритий ключ використовується для захисту облікового запису та безпечного підписання повідомлень.

Основна мережа Ethereum має ідентифікатор ланцюга (ChainID) = 1. Існує також багато інших мереж, до яких Geth може підключатися,

надаючи альтернативні ідентифікатори ланцюгів, деякі з них є тестовими мережами, а інші є альтернативними мережами, побудованими з форків вихідного коду Geth. Надання мережевого ідентифікатора, який ще не використовується існуючою мережею або тестовою мережею, означає, що вузли, які використовують цей мережевий ідентифікатор, можуть з'єднуватися лише один з одним, створюючи приватну мережу. Список поточних мережевих ідентифікаторів (ChainID) доступний на сторінці Chainlist.org. ChainList – це список мереж EVM. Користувачі можуть використовувати цю інформацію, щоб підключити свої гаманці та постачальників проміжного програмного забезпечення Web3 до відповідного ідентифікатора ланцюга та ідентифікатора мережі. По суті всі вони підпорядковуються Ethereum Virtual Machine — те, що визначає правила обчислення нового допустимого стану від блоку до блоку.

Апаратні вимоги для запуску вузла Geth залежать від конфігурації вузла і можуть змінюватися з часом у міру впровадження оновлень мережі. Ноди Ethereum можна запускати на пристроях з низьким енергоспоживанням і обмеженими ресурсами. Але зазвичай, для цього обирають простір (комп'ютер), щоб уникнути перевантаження вашого комп'ютера. Якщо ваш комп'ютер матиме чудові налаштування конфігурації, то це відтермінує час до потреби в обслуговуванні, оскільки ланцюг постійно зростає і потреба в цьому неминуче настане.

З приводу технічних вимог, то мінімальний набір: 4-8 ГБ ОЗУ та 2 ТБ SSD (Варто віддавати перевагу саме SSD для забезпечення швидкості запису). Рекомендовані: Intel NUC, 7-ме покоління чи вище, провідний інтернет (це є необов'язковою вимогою, але це забезпечує більш стабільну роботу з мережею), екран та клавіатура.

Окрім цього, зазначимо, що є декілька варіантів клієнтів для використання:

1) Geth (наведено вище)

2) Besu – це клієнт Ethereum з відкритим вихідним кодом, розроблений за ліцензією Apache 2.0 і написаний на Java. Він працює в

публічних і приватних мережах

3) Erigon – це реалізація Ethereum (рівень виконання з вбудованим рівнем консенсусу), на ефективність границя. Мова реалізації Go.

4) OpenEthereum – швидкий і багатофункціональний багатомережевий клієнт Ethereum. Працює OpenEthereum з використанням мови програмування Rust.

5) Nethermind – це вузол Ethereum із широкими можливостями налаштування, побудований на .NET.

Важливо вказати, що OpenEthereum вже застарів і більше не має оновлень та технічної підтримки, а тому варто звернути увагу на інші варіанти.

Пропонуємо розглянути систему Geth більш детально. Описавши її вимоги, перейдемо до внутрішньої роботи. Як відомо, однією з головних компонент будь-якої блокчейн мережі є алгоритм консенсусу. Це важливий механізм, що дозволяє вирішувати задачу невизначеності, як саме буде йти наш 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. Clique настійно рекомендується для приватних тестових мереж, оскільки PoA є набагато менш ресурсомістким, ніж PoW.

«Clique»

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

Ethash

Алгоритм PoW від Geth, Ethash, — це система, яка 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.

1.2 Реалізація приватної мережі в Bitcoin

Bitcoin (BTC) — це тип цифрової валюти, яка була створена для анонімного та прямого обміну цінностями між користувачами за допомогою моделі однорангових транзакцій (P2P), яка усуває потребу в центральному посереднику, такому як банк або брокер.

Термін P2P стосується децентралізованих мереж взаємопов'язаних комп'ютерних систем, що містять однорангові вузли. Усі вузли рівноправні, і обмін даними відбувається без центрального сервера — тобто кожен комп'ютер або вузол може виступати як файловим сервером, так і клієнтом. 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 в обміні, можуть одночасно споживати та надавати ресурси в одній мережі.

Будучи основним елементом 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. За 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.

Хоча Bitcoin часто описувався ранніми послідовниками та засобами масової інформації як анонімний спосіб оплати, це не так. Bitcoin у кращому випадку є псевдонімним, і на сьогоднішній день розрив зв'язку вашої реальної особистості з псевдонімними біткоін-аккаунтами для більшості не є найпростішим завданням. Оскільки Bitcoin - це прозора система, всі операції знаходяться у публічному доступі. Кожен може відслідкувати адреси, що беруть участь у транзакціях, та кількість BTC (або сатоші), що переказуються. Таким чином, кожна угода, відображена в ланцюжку підтвердження виконаної роботи (PoW), може бути розкрита доти, доки існує Bitcoin.

Досягнення приватності, як і безпека — це процес, і він досить складний, але не неможливий. Розробка інструментів, що допомагають зберегти приватність при використанні Bitcoin, триває, і, на щастя, взаємодіяти з більшістю цих інструментів стає все простіше. На жаль, панацеї як такої не існує. Потрібно усвідомлювати компроміси та слідувати кращим практикам у міру їх розвитку.

Головний підхід, що використовується для збереження приватності користувачів BTC полягає у відсутності ідентифікації власників відповідних коїнів та адрес. Тобто хоча й транзакції є у відкритому доступі, вкрай проблематично встановити осіб, які беруть участь у цьому процесі. Головні загрози для приватності полягають у купівлі монет через KYC-сервіси (тобто ті, що потребують документальне підтвердження особи) або використання однієї адреси декілька разів.

У той самий час купівля біткоїнів безпосередньо в інших власників (навіть з певною націнкою) та використання нових адрес для різних транзакцій може дозволити досягти задовільної приватності у більшості випадків. Але всі власники BTC мають пам'ятати, що Bitcoin не є анонімним, і власна дисципліна при його використанні грає ключову роль.

Використовуйте рішення, що дозволяють забезпечити власне зберігання приватної інформації. Якщо ви відправляєте кошти на біржу,

якій 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 методів підвищення конфіденційності є проведення транзакцій у такий спосіб, що дозволить мінімізувати ефективність аналізу блокчейну, заснованого на розрахунку ймовірностей. Є різні підходи до розв'язання цієї проблеми, включаючи методи об'єднання учасників.

Coinjoins

Це комплексні транзакції, які дозволяють інтегрувати внески різних учасників у одну й ту саму транзакцію. JoinMarket створює вільний ринок для учасників для придбання входів, у той час, як WhirlPool та Wasabi є централізованими координаторами, які надають послуги за плату.

CoinSwaps

Це система, коли два користувачі обмінюються коїнами, 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 запуска 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.

1.3 Реалізація приватної мережі в Litecoin

Litecoin є досить цікавою криптовалютою, що є дуже подібною до Bitcoin, що навіть символізує її прозвище «срібло до золота біткойна». Так само, як і біткойн, Litecoin працює на блокчейні з відкритим вихідним кодом, який не контролюється жодним центральним органом влади. Кожен оператор ноди 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 над своїми грошима. В результаті Litecoin можна використовувати як однорангову (P2P) платіжну систему для виплат людям у всьому світі без посередника. Його також можна використовувати як притулок або як частину диверсифікованого криптовалютного портфеля.

Також, Litecoin є привід вважати безпечнішим за Bitcoin. Оскільки ніхто не робить форки Litecoin без релейного захисту, це, ймовірно, безпечніше, ніж Bitcoin. Однак ліквідність має важливе значення для установ, що розвиваються, і Bitcoin набагато ліквідніший, ніж Litecoin. Litecoin виділявся серед інших альтернативних криптовалют своїми інноваціями, включаючи поєднання більш високої швидкості поширення блоків і використання алгоритму хешування Scrypt. Він також значною мірою уникнув так званого премайнінгу, який дозволяє творцям криптовалюти на основі блокчейну майнити монети до того, як проект буде запущений для громадськості.

Litecoin - це альткойн, заснований на майнінгу, і такі монети використовують метод консенсусу PoW для перевірки своїх транзакцій.По суті, PoW вимагає, щоб одна сторона продемонструвала всім іншим учасникам мережі, що було докладено певних обчислювальних зусиль. На відміну від Bitcoin, який використовує метод хешування SHA-256 PoW, Litecoin використовує техніку Scrypt PoW, яка є менш ресурсомісткою.

Початкові зусилля криптовалюти були підкріплені реалізацією кількох

функцій, які також були запропоновані, а пізніше реалізовані в мережі Bitcoin. Ці вдосконалення часто спрямовані на те, щоб гарантувати, що мережа може масштабуватися, щоб вмістити більше транзакцій на секунду, не жертвуючи децентралізацією, і забезпечити конфіденційність під час транзакцій.

SegWit

Однією з перших функцій, реалізованих на блокчейні Litecoin до додавання в Bitcoin, була Segregated Witness. Хоча SegWit був вперше запропонований для Bitcoin у 2015 році, Litecoin спочатку прийняв цю технологію. Після того, як на LTC не було помічено серйозних інцидентів, технологія була додана до Bitcoin. По суті, SegWit допомагає масштабувати криптовалюту, «відокремлюючи» дані цифрового підпису для кожної транзакції (свідка) за її межами, краще використовуючи обмежений простір. Він був розроблений для вирішення проблем масштабованості Bitcoin.

Lightning Network

Lightning Network — це рішення для масштабування, яке, по суті, створює додатковий рівень поверх блокчейну криптовалюти, в якому транзакції є швидкими, а комісії незначними. Цей додатковий рівень складається з платіжних каналів, створених користувачами. Спочатку він був розроблений для реалізації на блокчейні Bitcoin. Як і SegWit, мережа була вперше реалізована на Litecoin, який багато хто використовував для тестування Lightning Network в реальному економічному середовищі. Рішення для масштабування рівня 2 є суперечливим. На думку критиків, це підштовхує користувачів до некастодіальних гаманців, на яких користувачам довелося б запускати свій вузол. Впровадження Lightning Network у Litecoin було дещо повільним, тоді як прийняття Bitcoin Lightning Network зросло в геометричній прогресії в перші місяці. Причиною уповільнення LTC можуть бути і без того низькі комісії за транзакції базового рівня.

ВИСНОВКИ

У даній роботі ми дослідили можливість розгортання систем криптовалют та розглянули різні допоміжні їх функції та варіації. В контексті порівняння, можна зазначити, що система Etherium має більше можливостей та варіацій для розгортання. Також були наведені мінімальні вимоги, за яких система працювала б найкраще.