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

Звіт з виконання комп'ютерного практикума

РОЗГОРТАННЯ СИСТЕМ ETHEREUM ТА КРИПТОВАЛЮТ

Виконали студентки
групи ФІ-32мн
Зацаренко А. Ю.
Футурська О. В.

Перевірила:
Селюх П. В.

Київ — 2024

ЗВІТ

1.1 Мета роботи

Отримання навичок налаштування платформ виконання смарт-контрактів та криптовалют.

1.2 Завдання на лабораторну роботу

Провести порівняльний аналіз особливостей розгортання систем криптовалют у порівнянні із системою Ethereum. Зробити висновок про можливість чи неможливість взаємозаміни модулів різних систем та пояснити причини.

1.3 Необхідні теоретичні відомості

Будь-який комп'ютер, який підключається до мережі, називається вузлом. Повні вузли завантажують кожен блок і транзакцію та перевіряють їх на відповідність правилам консенсусу.

Наприклад, для Bitcoin правила наступні:

1) Блоки можуть створювати лише певну кількість біткоїнів (наразі 6,25 BTC на блок, з 07.04.24 – 3,125 BTC);

2) Транзакції повинні мати правильні підписи для біткоїнів, що витрачаються;

3) Транзакції/блоки повинні бути в правильному форматі даних;

4) В межах одного ланцюжка блоків, вихідні дані транзакції не можуть бути витрачені двічі.

Якщо транзакція або блок порушує правила консенсусу, то вона абсолютно відхиляється, навіть якщо кожен інший вузол в мережі вважає її дійсною. Це одна з найважливіших характеристик повних вузлів: вони роблять те, що правильно, незважаючи ні на що. Для повних вузлів майнери насправді мають досить обмежену владу: вони можуть лише змінювати порядок або видаляти транзакції, і тільки витрачаючи багато

обчислювальної потужності. Потужний майнер здатен здійснити серйозні атаки, але оскільки повні вузли покладаються на майнерів лише в деяких питаннях, майнери не можуть повністю змінити або знищити Bitcoin.

Вузли, які мають різні правила консенсусу, фактично використовують дві різні мережі/валюти. Зміна будь-якого з правил консенсусу вимагає хардфорку, який можна уявити як створення нової валюти і переведення всіх на неї. Правила консенсусу відрізняються від правил політики, які визначають, як вузол або майнер надає пріоритет або не підтримує певні речі. Правила політики можна вільно змінювати, і різні вузли можуть мати різні правила політики. Оскільки всі повноцінні вузли повинні використовувати абсолютно однакові правила консенсусу, щоб залишатися сумісними один з одним, навіть дублюючи помилки і дивацтва в оригінальних правилах консенсусу, створення повноцінного вузла з нуля надзвичайно складно і небезпечно. Тому рекомендується, щоб кожен, хто бажає запустити повноцінний вузол, використовував програмне забезпечення, засноване на еталонному клієнті, який є єдиним клієнтом, що гарантовано поводиться коректно.

Вузли (nodes) відіграють вирішальну роль у функціонуванні та безпеці децентралізованих мереж блокчейн. Запуск криптовалютного вузла не тільки дозволяє людям брати активну участь у мережі, але й сприяє загальній цілісності та стійкості криптовалютної екосистеми.

Щодо програмного забезпечення вузла, то кожна криптовалютна мережа, як правило, має власне унікальне програмне забезпечення вузла, яке необхідно встановити і правильно налаштувати. Дуже важливо використовувати офіційне програмне забезпечення, надане командою розробників криптовалюти, або надійну альтернативу, що підтримується спільнотою. Найпоширеніше програмне забезпечення для вузлів включає Bitcoin Core для мережі Bitcoin, Geth для Ethereum, Litecoin Core для Litecoin та Dash Core для Dash.

Bitcoin Core - це еталонна реалізація протоколу Bitcoin, тобто це оригінальне і найбільш широко використовуване програмне забезпечення

для повноцінних вузлів. Забезпечує надійну перевірку дотримання всіх правил консенсусу біткоїна. Bitcoin Core можна використовувати як десктопний клієнт для регулярних платежів або як серверну утиліту для продавців та інших платіжних сервісів.

Запуск вузла Bitcoin Core дозволяє вам незалежно перевіряти транзакції з біткоїнами, сприяти безпеці та децентралізації мережі Bitcoin.

Litecoin Core, як і Dash Core – це найпопулярніший повний функціонал вузла; назва програмного забезпечення з відкритим вихідним кодом, яке дозволяє використовувати цю валюту. Litecoin Core і Dash Core – це реалізація протоколів Litecoin та Dash відповідно, подібна до Bitcoin Core для Bitcoin.

Geth – це інтерфейс командного рядка для одного з трьох основних компонентів коду блокчейну Ethereum. Go, мова програмування, розроблена Google, є однією з мов, які були використані для створення мережі Ethereum, а Go Ethereum – це інтерфейс, який використовується для написання, редагування та керування кодом Go для блокчейну. Крім Go, блокчейн та протокол Ethereum також значною мірою базуються на Python та C++.

Geth – це найпростіший і найдоступніший спосіб для розробника чи інвестора запустити повний вузол Ethereum. Завдяки зручному інтерфейсу, Geth дозволяє розробникам швидко створювати облікові записи та починати редагувати та покращувати код мережі Ethereum.

Запуск криптовалютного вузла вимагає відповідних апаратних ресурсів для забезпечення безперебійної роботи. Вимоги до апаратного забезпечення можуть відрізнятися в залежності від конкретної криптовалютної мережі, але існують деякі загальні специфікації:

1) Достатня обчислювальна потужність (CPU) і пам'ять (RAM) для виконання обчислювальних вимог програмного забезпечення вузла;

2) Значна ємність сховища для зберігання даних блокчейну, яка може значно зростати з часом;

3) Стабільне та високошвидкісне інтернет-з'єднання для безперебійної

синхронізації даних з мережею блокчейн.

Мінімальні вимоги, встановлені Ethereum: для процесора вам потрібен багатоядерний процесор з принаймні 4 ядрами, що працюють на частоті 2 ГГц або вище. Крім того, система повинна мати мінімум 8 ГБ оперативної пам'яті і SSD-накопичувач об'ємом не менше 250 ГБ. Рекомендована мінімальна швидкість мережевого підключення становить близько 10 Мбіт/с на завантаження і відправлення.

Для Bitcoin Core: 7 ГБ вільного дискового простору, доступного зі швидкістю читання/запису не менше 100 МБ/с, 2 ГБ пам'яті (RAM). Зазвичай повноцінні вузли на високошвидкісних з'єднаннях використовують 200 і більше ГБ на місяць. Завантаження становить близько 20 ГБ на місяць, плюс ще близько 340 ГБ при першому запуску вашого вузла.

Криптовалютні вузли потребують надійного і безперебійного підключення до мережі, щоб залишатися синхронізованими з мережею блокчейн. Стабільне інтернет-з'єднання з достатньою пропускною здатністю необхідне для полегшення зв'язку і передачі даних з іншими вузлами мережі. Рекомендується також мати статичну IP-адресу або динамічний DNS-сервіс для полегшення доступу.

При створенні нового криптовалютного вузла важливим є процес початкової синхронізації, також відомий як початкове завантаження блоків (Initial Block Download, IBD). Цей процес включає в себе завантаження всієї історії блокчейну і перевірку його автентичності, що може зайняти багато часу і ресурсів. Користувачі повинні переконатися, що їхнє обладнання та мережеві можливості можуть ефективно обробляти процес IBD.

Початкове завантаження блоків – це процес, під час якого вузли синхронізуються з мережею, завантажуючи нові для них блоки. Це відбувається, коли вузол знаходиться далеко позаду вершини ланцюжка блоків. В процесі IBD вузол не приймає вхідні транзакції і не запитує транзакції.

Якщо створюється новий вузол, процес IBD відбувається при першому запуску, і це може зайняти значну кількість часу, оскільки новий вузол

повинен завантажити весь ланцюжок блоків.

Дані блокчейну, що зберігаються на криптовалютному вузлі, з часом можуть займати значний обсяг дискового простору. Оператори вузлів повинні мати достатній обсяг пам'яті і надійну стратегію резервного копіювання, щоб захистити дані блокчейну від випадкової втрати або пошкодження. Регулярне резервне копіювання, як локальне, так і віддалене, гарантує, що вузол зможе відновитися в разі апаратних збоїв або пошкодження даних.

Запуск криптовалютного вузла вимагає уваги до практик безпеки для захисту як оператора вузла, так і мережі. Деякі з найважливіших заходів безпеки включають наступне:

1) Регулярне оновлення програмного забезпечення вузла для забезпечення сумісності, покращення продуктивності та виправлень безпеки;

2) Впровадження брандмауерів і протоколів мережевої безпеки для запобігання несанкціонованому доступу до вузла;

3) Увімкнення шифрування каналів зв'язку для захисту конфіденційних даних;

4) Використання надійних та унікальних паролів для доступу до вузла та ключів шифрування;

5) Моніторинг вузла на предмет будь-яких підозрілих дій або потенційних порушень безпеки.

Ethereum відрізняється від Bitcoin, Litecoin та Dash тим, що пропонує більш широкий спектр можливостей для створення додатків на основі блокчейну. Bitcoin, Litecoin та Dash, з іншого боку, більше спрямовані на роль цифрових валют і мають свої власні унікальні особливості, такі як приватність (у випадку Dash) та швидкість транзакцій (у випадку Litecoin).

«Смарт-контракт» – це набір коду (його функцій) і даних (його стан), який знаходиться за певною адресою в блокчейні Ethereum.

Це само-виконувані контракти, в яких умови угоди між покупцем і продавцем записані в рядках коду. Ці контракти працюють на блокчейні Ethereum, децентралізованій та безпечній платформі. Код смарт-контракту

автоматично виконується при виконанні певних умов, що усуває потребу в посередниках і підвищує ефективність і безпеку транзакції.

Смарт-контракти Ethereum написані на мові Solidity – комп'ютерній мові, яку можна порівняти з JavaScript. Код визначає обставини, за яких контракт буде виконуватися, і дії, які будуть виконані, якщо ці вимоги будуть виконані.

Децентралізовані додатки, також відомі як DApps, - це оцифровані бездозвільні програми, що встановлюються та працюють у мережі блокчейн. Хоча DApps - це додатки, що працюють на мережі блокчейн, смарт-контракти є джерелом живлення для цих DApps. Смарт-контракти виступають інтерфейсом між DApps та мережею блокчейн. Смарт-контракти - це просто код, який діє як внутрішній механізм. Тоді як DApp - це інтерфейс користувача, який взаємодіє безпосередньо з користувачем.

Протокол Proof-of-Work є надійним механізмом консенсусу, який використовується найпопулярнішими мережами криптовалют, такими як Bitcoin, Litecoin, Dogecoin, Monero, тощо. Протокол вимагає, щоб вузли в мережі надали докази того, що вони витратили обчислювальну потужність, щоб досягти консенсусу децентралізованим способом.

Варто також зазначити, що доволі часто можна зустріти механізм Proof-of-Work об'єднаним з іншим протоколом консенсусу. Наприклад, у криптовалюті Dash дворівнева мережа: блокчейн та набір головних вузлів (masternodes). Аналогічно Bitcoin, сам блокчейн захищений протоколом консенсусу Proof-of-Work. Цей рівень відповідає за проведення всіх транзакцій та захист від атаки подвійних витрат. Рівень головних вузлів відповідає за фінансову конфіденційність, миттєві транзакції та децентралізацію і керується протоколом консенсусу Proof-of-Service (PoSe). Головні вузли та майнери ділять винагороду між собою згідно з певними правилами.

Окрім Proof-of-Work іншим найпоширенішим механізмом консенсусу є Proof-of-Stake. Даний протокол покладається на метод, відомий як ставка,

а не майнінг. Можна сказати, що це більш енергоефективна альтернатива оригінальній моделі Proof-of-Work.

Згідно з цим протоколом, учасники мережі, які хочуть підтримувати блокчейн шляхом перевірки нових транзакцій і додавання нових блоків, повинні «закласти» встановлені суми криптовалюти. Якщо вони неналежним чином підтвердять помилкові або шахрайські дані, вони можуть втратити частину або всю свою частку як штраф. Але, якщо вони підтверджують правильні, законні транзакції та дані, то вони зароблять більше криптовалюти як винагороду.

У 2022 році, а точніше 15 вересня 2022 року, криптовалюта Ethereum змінила свій протокол консенсусу з Proof-of-Work на Proof-of-Stake. Дана подія набула широкого резонансу у світі криптовалют та отримала назву «the Merge» або «the Ethereum Merge». Простіше кажучи, «the Merge» — це термін, який придумали розробники Ethereum для опису злиття поточної основної мережі, яка використовує Proof-of-Work і окремий блокчейн Proof-of-Stake, відомий як Beacon Chain, які зараз співіснують як єдиний ланцюг. Як зазначалося, таке рішення було прийнято, оскільки Proof-of-Stake є більш безпечним, менш енергомістким і кращим для реалізації нових рішень масштабування порівняно з попередньою архітектурою Proof-of-Work. Дана подія спровокувала до значних змін та серйозних оновлень в мережі.

Однак варто зазначити, що окремий блокчейн Proof-of-Work (у дійсності це старий Ethereum до злиття) став активним. Ця розгалужена версія Ethereum спрямована на підтримку процесу майнінгу в Proof-of-Work для майнерів Ethereum.

ВИСНОВКИ

У даній лабораторній роботі було детально досліджено принцип роботи та запуску функціоналів повних вузлів для систем Etherium та криптовалют Bitcoin, Litecoin, Dash. Було зазначено основні мінімально дозволені вимоги для розгортання мережі та надано основні правила, яким тьреба слідувати, аби система працювала без помилок.