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

Звіт з виконання комп'ютерного практикуму №1

РОЗГОРТАННЯ СИСТЕМ ETHEREUM ТА КРИПТОВАЛЮТ

Виконали студенти
групи ФІ-32мн
Пелешенко Любов,
Панасюк Єгор,
Маринін Іван Павло

Перевірила:
Селюх П.В.

Київ — 2023

1

Мета роботи: Отримання навичок налаштування платформ виконання смартконтрактів та криптовалют

Постановка задачі: 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

1.1 Розгортання системи Ethereum

Перш ніж перейти до розгляду розгортання системи Ethereum, подивимося на визначення основних термінів.

Блокчейн — це ланцюжок блоків, який містить усю інформацію про всі транзакції, які відбуваються в мережі, у зашифрованому вигляді за допомогою відкритих і закритих ключів.

Технологія блокчейн може зміцнити базові послуги, необхідні для торговельного фінансування. Модель блокчейну працює на основі децентралізованої, оцифрованої та розподіленої моделі книги. Завдяки цим властивостям він є більш надійним і безпечним, ніж власний, централізований, який зараз використовується в торговій системі. Якщо говорити найпростіше, то блокчейн — це лише нова форма децентралізованої бази даних.

Ethereum — це децентралізована блокчейн-система з відкритим вихідним кодом, яка містить власну криптовалюту під назвою ефір (ETH). Це платформа, яку можна використовувати для різних програм, які можна розгортати за допомогою смарт-контрактів.

Мережа Ethereum є приватною, якщо вузли не підключені до основної мережі. Повністю контрольована приватна мережа Ethereum корисна як

серверна частина для основних розробників, які працюють над проблемами, пов'язаними з мережею/синхронізацією блокчейну тощо. Приватні мережі також корисні для розробників Dapp, які тестують багатоблокові та багатокористувацькі сценарії.

Розглянемо Geth, скорочення від Go Ethereum, - інтерфейс командного рядка, який дозволяє розробникам запускати повні вузли Ethereum, майнити криптовалюту та виконувати смарт-контракти, це найпростіший і найдоступніший спосіб запустити повний вузол Ethereum. Завдяки зручному інтерфейсу, Geth дозволяє розробникам швидко створювати облікові записи та починати редагувати та покращувати код мережі Ethereum. Будучи проєктом із повністю відкритим кодом, Geth дозволяє розробникам дістатися до самої основи блокчейну Ethereum та працювати над помилками та можливими вдосконаленнями. Усі вихідні коди для Ethereum доступні на Github, і розробники мають вільний доступ до них, а також дозволи на читання та запис. Наразі понад 400 людей зробили внесок у код блокчейну Ethereum. Звичайно, деякі з них беруть участь більше, ніж інші, тому такі люди, як Джеффрі Вілке (Jeffrey Wilcke) та Петер Сіляджі (Péter Szilágyi), які написали основні частини коду, вважаються топ учасниками.

Приватна мережа складається з кількох вузлів Ethereum, які можуть підключатися лише один до одного. Щоб запускати кілька вузлів локально, кожному з них потрібен окремий каталог даних (–datadir). Вузли також повинні знати один про одного і мати можливість обмінюватися інформацією, ділитися початковим станом і загальним консенсусним алгоритмом.

Розглянемо, як налаштувати Geth таким чином, щоб задовольнити основні вимоги, дозволивши запустити приватну мережу. І почати необхідно із вибору ідентифікатора мережі.

Основна мережа Ethereum має ідентифікатор мережі = 1. Існує також багато інших мереж, до яких Geth може підключатися, надаючи альтернативні ідентифікатори ланцюга, деякі з них є тестовими мережами,

а інші — альтернативними мережами, створеними з розгалужень вихідного коду Geth. Надання ідентифікатора мережі, який ще не використовується існуючою мережею або тестовою мережею, означає, що вузли, які використовують цей ідентифікатор мережі, можуть підключатися лише один до одного, створюючи приватну мережу. Список поточних ідентифікаторів мереж доступний на Chainlist.org. Ідентифікатор мережі контролюється за допомогою прапора networkid, наприклад (geth –networkid 12345).

Хоча основна мережа використовує proof-of-stake (PoS) для захисту блокчейну, Geth також підтримує алгоритм консенсусу «Clique» proof-of-authority (PoA) і алгоритм Ethash proof-of-work як альтернативи для приватних мереж. Clique наполегливо рекомендується для приватних тестових мереж, оскільки PoA вимагає набагато менше ресурсів, ніж PoW.

Ethash : Алгоритм PoW від Geth, Ethash, — це система, яка дозволяє відкриту участь будь-кому, хто бажає виділити ресурси для майнінгу. Хоча це критична властивість для загальнодоступної мережі, загальна безпека блокчейну суворо залежить від загального обсягу ресурсів, які використовуються для його захисту. Таким чином, PoW є поганим вибором для приватних мереж з невеликою кількістю майнерів. «Складність» майнінгу Ethash регулюється автоматично, щоб нові блоки створювалися приблизно з інтервалом у 12 секунд. Оскільки в мережі розгортається більше ресурсів майнінгу, створення нового блоку стає важчим, щоб середній час блоку відповідав цільовому часу блоку.

Clique : Clique consensus — це система PoA, де нові блоки можуть створювати лише авторизовані «підписувачі». Протокол консенсусу клавіатури визначено в EIP-225. Початковий набір авторизованих підписувачів налаштовується в блоці genesis. Підписантів можна авторизувати та скасувати авторизацію за допомогою механізму голосування, що дозволяє змінювати набір підписантів під час роботи блокчейну. Clique можна налаштувати на будь-який час блокування (в розумних межах), оскільки він не прив'язаний до налаштування складності.

Тож, розглянемо кроки для налаштування приватної мережі Ethereum.

1) Встановити Geth.

2) Створити папку для приватного Ethereum.

3) Створити блок Genesis.

4) Виконанb файл Genesis.

5) Створіть зовнішній обліковий запис (EOA).

6) Майнінг нашої приватної мережі Ethereum.

Детальніше про створення блоку Genesis: кожен блокчейн починається з такого блоку. Коли Geth запускається з параметрами за замовчуванням уперше, він передає генезис Mainnet до бази даних. Для приватної мережі, як правило, краще використовувати інший блок генезису. Блок genesis налаштовується за допомогою файлу genesis.json, шлях до якого необхідно надати Geth під час запуску. Під час створення блоку генезису необхідно визначити кілька початкових параметрів для приватного блокчейну:

– Функції платформи Ethereum увімкнено під час запуску (конфігурація). Щоб увімкнути та вимкнути функції після запуску блокчейну, потрібно запланувати хардфорк.

– Початковий блок обмеження газу (gasLimit). Це впливає на кількість обчислень EVM в межах одного блоку. Дзеркалювання основної мережі Ethereum, як правило, є хорошим вибором. Ліміт блокового газу можна налаштувати після запуску за допомогою параметра командного рядка –miner.gastarget.

– Початкове виділення ефіру (alloc). Це визначає, скільки ефіру доступно для адрес, перелічених у блоці генезису. Додатковий ефір можна створити за допомогою майнінгу в міру просування ланцюга.

– Ключі облікового запису підписувача можна згенерувати за допомогою команди geth account (цю команду можна запустити кілька разів, щоб створити більше одного ключа підписувача).

Що ж до завнішнього облікового запису (EOA), він має такі функції:

– Контролюється зовнішньою стороною або особою.

– Доступ через закриті ключі.

– Містить баланс ефіру.

– Може надсилати транзакції, а також «запускати» контрактні рахунки.

Якщо ми майнімо в основному ланцюжку Ethereum, для цього знадобиться дороге обладнання з потужними графічними процесорами. Зазвичай для цього використовуються ASIC, але в нашому ланцюжку висока продуктивність не потрібна, і ми можемо почати майнінг за допомогою такої команди – miner.start()

Якщо стан балансу перевіряється через пару секунд, рахунок поповнюється фейковим ефіром. Після цього можна припинити майнінг за допомогою команди – miner.stop()

1.2 Розгортання Bitcoin

Біткойн — це повністю децентралізована електронна валютна система, заснована на одноранговій мережі. Його історія починається в листопаді 2008 року, коли Сатоші Накомото опублікував статтю «Біткойн: однорангова електронна готівкова система». Біткойн базується на цифрових підписах, щоб підтвердити володіння біткойнами (валюта), а також на загальнодоступну історію транзакцій разом із криптографічним підтвердженням роботи.

Властивістю біткойна є відсутність центрального органу влади або емітента валюти. Натомість нові біткойни постійно випускаються за певним курсом за допомогою так званого «майнінгу». Крім того, виконання транзакцій контролюється та переглядається мережею P2P. Тому учасники мережі працюють над колективним консенсусом щодо дійсності транзакції та додають її до загальнодоступної історії вже підтверджених транзакцій (так званий «блокчейн»). Як розширення блокчейну, так і формування консенсусу щодо дійсних транзакцій досягається за допомогою системи підтвердження роботи. Учасники P2P-мережі Bitcoin збирають транзакції в блок даних і виконують хешування цього блоку, модифікованого один раз, доки не буде знайдено спеціально структурований ключ. Якщо шукане поле

знайдено, мережа P2P перевіряє результат і, нарешті, кожен клієнт додає транзакції до власної копії блокчейну. Таким чином, транзакція відбулася безповоротно, і відтепер найдовший блокчейн є доказом подій, що відбулися в точній послідовності.

Процес пошуку відповідного nonce є головним механізмом безпеки біткойна, оскільки передбачається, що він є дорогим з обчислювальної точки зору. Щоб мотивувати учасників долучатися до верифікації та додавання транзакцій, існує два механізми: комісії за транзакції та щойно «викарбовані» біткоіни. Кожен правильно хешований блок генерує біткойни, які належать майнеру.

Біткойн має свій власний спосіб реалізації. Найперший створений блок називається блоком Genesis. Поле «хеш попереднього блоку» — це 32-байтовий рядок нулів. Він має лише 1 транзакцію. Однак, оскільки блоки продовжують складатися один за одним, список транзакцій буде збільшуватися, поки не досягне максимального розміру в 1 МБ. Тоді всі блоки матимуть змінні транзакції, але приблизно розмір блоку становитиме 1 МБ. Кожного разу, коли створюється новий блок, він додається до останнього доданого блоку блокчейну.

У мережі завжди існує один і тільки один шлях від останнього доданого блоку до блоку генезису (першого блоку). Зворотне також вірно, але існує кілька шляхів, з яких лише 1 дійсний. Коли 2 блоки створюються приблизно в один і той самий час, мережа приймає лише 1. Наприклад блок з висотою 2 має 2 дітей. Але зрештою приймається лише 1. Таким чином, блок завжди матиме лише одного батька, але може мати кількох дітей (тимчасово). Зрештою блоки «сироти» виявляються, і їх транзакції підбираються для іншого блоку, і, отже, кожна транзакція отримує шанс бути включеною в мережу.

Одним із головних нововведень при створенні Bitcoin було вирішення проблеми, відомої як «подвійні витрати». Для будь-яких цифрових даних можна скопіювати дані та надіслати їх двом різним об'єктам, це може бути проблемою, якщо ці цифрові дані мають грошову вартість. Деталі рішення

будуть спиратися на криптографічний опис того, як працює протокол Bitcoin. Однак, кажучи простими словами, витрачаючи деякі біткойни як вхідні дані для транзакції, біткойн-гаманець повинен використовувати хеш тих вхідних даних, які вже є в блокчейні, коли він транслює цю транзакцію, він зберігатиметься в пам'яті всіх біткойн-вузли як непідтверджену транзакцію, поки майнер не включить її в блок. У цей проміжок часу можна використовувати той самий вхід в іншій транзакції та транслювати його в мережу тому, що цей вхід ще не був використаний у жодному блоці. Хоча лише одна з цих транзакцій може бути включена в новий блок, а інша буде недійсною та стерта з пам'яті. Через це платіжним процесорам біткойнів важко приймати транзакції підтвердження 0, оскільки їм не можна повністю довіряти.

Крім того, більшість банківських транзакцій можна відстежити та вони є оборотними, що ускладнює викрадення грошей та банківських облікових даних. Транзакції з біткойнами також можна відстежити, але вони не є оборотними. Таким чином, викрадені біткойни неможливо відновити централізовано або автоматично. Користувачі біткойнів зазвичай не мають правового захисту від втрати або крадіжки, і хоча вкрадені біткойни можна відстежити, коли вони змінюють власника, існує кілька механізмів для відмивання біткойнів і подібних цифрових валют.

Прагнучи вирішити деякі складності керування ключами, розробники програмного забезпечення для біткойнів створили ряд інноваційних технологій, починаючи від ключів, отриманих за допомогою пароля, до комп'ютерів із повітряним розривом і закінчуючи фізичними роздруківками особистих ключів у формі двовимірних штрих-кодів. Однак, оскільки жодна з цих пропозицій не була оцінена в контексті біткойнів, залишається незрозумілим, які методи мають переваги зручності використання.

Якщо користувачі не можуть безпечно керувати ключами Bitcoin, це може призвести до втрати ними коштів і/або поганої репутації Bitcoin, що може перешкодити подальшому прийняттю користувача.

ВИСНОВКИ

Bitcoin та Ethereum сьогодні є найвідомішими та цінними криптовалютами. Вони засновані на технології блокчейн, яка призначена для сприяння механізму довіри в одноранговій мережі на основі консенсусу більшості вузлів.

Спостереження показують, що біткойн має більшу місткість мережі, ніж Ethereum, але з більшою кількістю кластерних вузлів у центрах обробки даних. Крім того, біткойн і Ethereum мають досить централізовані процеси майнінгу, і необхідні подальші дослідження для подальшої децентралізації консенсусних протоколів без дозволу. В Ethereum винагороди за блоки мають меншу дисперсію, ніж у Bitcoin та Ethereum має нижче використання енергії для майнінгу, ніж Bitcoin, ймовірно, через високу частоту блоків.