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

Звіт з виконання комп’ютерного практикуму “Розгортання систем Etherium та криптовалют”

Виконав:
студент групи ФБ-31мп
Варгіч Дмитро

Перевірила:
Селюх П.В.

Київ — 2024

Мета роботи: «Отримання навичок налаштування платформ виконання смарт-контрактів та криптовалют».

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

Особливості розгортання та призначення систем Bitcoin, Monero та Ethereum

Унікальні характеристики та можливі варіанти використання кожної блокчейн-платформи:

1. Мета та ключовий принцип

Bitcoin:

Основне призначення: цифрова валюта, створена як децентралізована однорангова електронна готівкова система.
Ключовий принцип: фокус на безпеці, децентралізації та незмінності.
Основна функція: Безпечна та незмінна платформа для транзакцій.

Monero:

Основне призначення: цифрова валюта, орієнтована на конфіденційність.
Ключовий принцип: покращена конфіденційність і анонімність транзакцій.
Основна функція: приватні, невідстежувані транзакції з використанням передових криптографічних методів.

Ethereum:

Основне призначення: платформа для децентралізованих програм (DApps) і смарт-контрактів.
Ключовий принцип: програмовані транзакції, що дозволяють використовувати різноманітні програми, окрім валюти.
Основна функція: повна функція смарт-контракту Turing.

2. Механізм консенсусу

Bitcoin:

Механізм консенсусу: підтвердження роботи (PoW).
Майнінг: вимагає вирішення криптографічних головоломок.
Енергоспоживання: високе через інтенсивність обчислень.
Безпека: надійний, але з обмеженнями масштабованості.
PoW із SHA-256: простий, але енергоємний, зосереджений на безпеці та децентралізації.

Monero:

Механізм консенсусу: підтвердження роботи (PoW), зокрема з використанням алгоритму RandomX.
Майнінг: розроблено для роботи з ЦП, щоб протистояти домінуванню ASIC.
Енергоспоживання: високе, хоча RandomX прагне демократизувати майнінг.
Безпека: Сильна, з акцентом на опір централізації майнінгу.
PoW з RandomX: розроблено для підтримки ЦП для сприяння децентралізації та протидії майнінгу ASIC.

Ethereum:

Механізм консенсусу: перехід від PoW до Proof of Stake (PoS) з Ethereum 2.0.
Майнінг/стійкинг: спочатку PoW, перехід до PoS, де валідатори роблять ставки ETH.
Енергоспоживання: очікується значне зниження з PoS.
Безпека: PoS має на меті покращити масштабованість і безпеку, одночасно зменшуючи споживання енергії.
Перехід від PoW (Ethash) до PoS (Casper): PoS має на меті покращити масштабованість і зменшити споживання енергії.

3. Функції конфіденційності

Bitcoin:

Конфіденційність: Псевдонім; усі транзакції є загальнодоступними, але не пов’язані безпосередньо з особами реального світу.
Методи: базова конфіденційність через уникнення повторного використання адреси, але піддається аналізу.

Monero:

Конфіденційність: велика увага до конфіденційності; транзакції є конфіденційними та не підлягають відстеженню.
Методи: використовує RingCT (конфіденційні транзакції кільця), приховані адреси та кільцеві підписи для приховування деталей.

Ethereum:

Конфіденційність: Псевдонім; схожий на біткойн, але дані транзакцій можуть бути складнішими через смарт-контракти.
Методи: базова конфіденційність із уникненням повторного використання адреси; деякі проекти, орієнтовані на конфіденційність (наприклад, Aztec Protocol), побудовані на Ethereum.

4. Можливість розумного контракту

Bitcoin:

Розумні контракти: обмежені можливості створення сценаріїв, переважно для простих сценаріїв транзакцій.
Випадки використання: переважно фінансові операції та базові контракти з кількома підписами.
Гнучкість: не розроблено для складних смарт-контрактів або DApps.

Monero:

Смарт-контракти: мінімальна підтримка складних сценаріїв; фокусується на безпечних і приватних транзакціях.
Випадки використання: переважно фінансові операції з сильним акцентом на конфіденційності.
Гнучкість: обмежено дизайном для підвищення конфіденційності та безпеки.

Ethereum:

Смарт-контракти: повна підтримка мови програмування Solidity.
Варіанти використання: широкий спектр, включаючи фінанси (DeFi), ігри, ланцюг поставок тощо.
Гнучкість: висока гнучкість, що дозволяє використовувати складні DApps і різні блокчейн-рішення.

5. Інструменти розгортання та розробки

Bitcoin:

Розгортання: передбачає налаштування вузлів і гаманців.
Інструменти розробки: обмежені інструменти, зосереджені на сценаріях Bitcoin (наприклад, Bitcoin Core, бібліотеки, такі як BitcoinJ).
Підтримка спільноти: сильна для фінансових операцій, менша для ширших програм.

Monero:

Розгортання: передбачає налаштування вузлів, гаманців і, можливо, програмного забезпечення для майнінгу.
Інструменти розробки: такі інструменти, як Monero Wallet CLI/GUI, і бібліотеки (наприклад, Monero Integrations).
Підтримка спільноти: зосереджено на покращенні конфіденційності та підтримці безпеки мережі.

Ethereum:

Розгортання: передбачає налаштування вузлів, гаманців і середовищ розробки для смарт-контрактів.
Інструменти розробки: багата екосистема з такими інструментами, як Truffle Suite, Remix IDE та фреймворками для тестування та розгортання (наприклад, Hardhat).
Підтримка спільноти: широка як для розробки смарт-контрактів, так і для DApps.

6. Швидкість транзакцій і масштабованість

Bitcoin:

Швидкість транзакцій: приблизно 7 транзакцій на секунду (TPS).
Рішення масштабованості: рішення рівня 2, такі як Lightning Network.
Час блоку: 10 хвилин.

Monero:

Швидкість транзакції: близько 4-5 TPS.
Рішення масштабованості: Постійне дослідження вдосконалення масштабованості; ще немає широко прийнятих рішень рівня 2.
Час блоку: 2 хвилини.

Ethereum:

Швидкість транзакції: змінюється; спочатку приблизно 15-30 TPS, очікується покращення з Ethereum 2.0.
Рішення для масштабованості: рішення рівня 2, такі як Optimistic Rollups, Plasma та шардинг в Ethereum 2.0.
Час блоку: 12-14 секунд.

7. Екосистема та спільнота

Bitcoin:

Екосистема: зосереджена на фінансових послугах із сильним наголосом на тому, щоб бути засобом збереження вартості («цифрове золото»).
Спільнота: велика, з консервативним підходом до змін для забезпечення стабільності та безпеки мережі.

Monero:

Екосистема: зосереджено на конфіденційності та безпечних транзакціях.
Спільнота: сильний акцент на конфіденційності та безпеці; активний у розвитку криптографічних методів.

Ethereum:

Екосистема: різноманітна, включаючи фінанси, ігри, ланцюги поставок і соціальні мережі.

Спільнота: інноваційна та ініціативна, що сприяє швидкому розвитку та впровадженню нових функцій і вдосконалень.

8. Управління

Bitcoin:

Управління: децентралізоване з сильним наголосом на консенсусі та обережності у прийнятті змін.
Пропозиції щодо розвитку: керуються за допомогою пропозицій щодо вдосконалення біткойнів (BIP).

Monero:

Управління: децентралізоване, з розвитком і прийняттям рішень, керованих ком'юніті.
Пропозиції щодо розвитку: керуються за допомогою пропозицій щодо вдосконалення Monero (MRP).

Ethereum:

Управління: більш гнучке та кероване розробниками, з активною участю спільноти.
Пропозиції щодо розвитку: керуються за допомогою пропозицій щодо вдосконалення Ethereum (EIP).

Аналіз можливості заміни модулів

Механізми консенсусу принципово відрізняються за принципом роботи і призначенням. PoW SHA-256 Bitcoin не можна легко замінити RandomX PoW Monero або PoS Ethereum через відмінності в припущеннях безпеки, вимогах до енергії та апаратній сумісності.

Функції конфіденційності Monero (RingCT, приховані адреси) глибоко інтегровані в його протокол. Реалізація їх у Bitcoin або Ethereum вимагала б суттєвих змін у їхніх основних протоколах, що вплинуло б на їх моделі транзакцій та існуючі стани мережі.

Біткойн і Monero не розроблені для підтримки повних смарт-контрактів Тьюрінга. Включення можливостей смарт-контрактів Ethereum вимагатиме повного перегляду їхніх мов сценаріїв і моделей транзакцій.

Біткойн використовує модель UTXO, тоді як Ethereum використовує модель на основі облікового запису. Хоча Monero використовує модифіковану модель UTXO, все ще несумісний через модифікації, орієнтовані на конфіденційність. Обмін цими моделями вимагав би фундаментальних змін у тому, як транзакції реєструються та підтверджуються.

Висновок

Обмін модулями між Bitcoin, Monero та Ethereum значною мірою неможливий через фундаментальні відмінності в їхній архітектурі, принципах проектування, механізмах консенсусу, функціях конфіденційності та моделях транзакцій. Кожна система оптимізована для конкретного випадку використання, і інтеграція функцій однієї в іншу вимагатиме суттєвих змін, які можуть поставити під загрозу цілісність і функціональність оригінальних систем.