Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут Технологія блокчейн та розподілені системи Лабораторна робота 1

«Розгортання систем Ethereum та криптовалют»

Виконав:

Студент групи ФЕ-41мп Забара Павло

Порівняльний аналіз систем Ethereum, Solana та Monero

Ethereum (ETH)

Ethereum є однією з найпопулярніших та найпоширеніших децентралізованих платформ, яка дозволяє створювати та запускати смарт-контракти та децентралізовані додатки (dApps). Центральним елементом Ethereum є Ethereum Virtual Machine (EVM) — спеціалізоване середовище виконання, яке забезпечує однакове виконання смарт-контрактів на всіх вузлах мережі.

Принцип роботи:

Ethereum використовує механізм консенсусу Proof-of-Stake (PoS), після переходу від Proof-of-Work (PoW), який був впроваджений у рамках оновлення Ethereum 2.0. Учасники мережі, які бажають бути валідаторами, блокують певну кількість токенів ЕТН як гарантію чесності та правильності своїх дій, отримуючи натомість винагороду за підтвердження транзакцій.

Ethereum пропонує потужні інструменти для створення різноманітних додатків, які охоплюють багато сфер — від фінансових послуг (децентралізовані фінанси, DeFi) до NFT та інтерактивних ігор. На Ethereum можна створювати токени за допомогою стандартів ERC-20 і ERC-721. ERC-20 є стандартом для створення взаємозамінних токенів, які можуть бути використані для різноманітних фінансових операцій, тоді як ERC-721 використовується для створення невзаємозамінних токенів (NFT), що дозволяють доводити право власності на унікальні цифрові об'єкти.

Однією з ключових проблем Ethereum є обмежена пропускна здатність мережі, яка складає близько 30 транзакцій за секунду. Ця обмеженість зумовлена особливостями архітектури блокчейну, що призводить до затримок та високих комісій під час пікових навантажень.

Газ і високі комісії:

У мережі Ethereum "газ" є умовною одиницею вимірювання витрат на обчислення та виконання транзакцій. Кожна транзакція або операція смарт-контракту вимагає певної кількості газу. Вартість газу визначається залежно від складності та навантаження на мережу, через що комісії можуть зростати у періоди високої активності, що робить транзакції дорогими.

Інфраструктура та спільнота:

Ethereum має одну з найбільших та найактивніших спільнот серед блокчейн-платформ. Розвинена інфраструктура включає численні бібліотеки, фреймворки (Truffle, Hardhat, Remix IDE), маркетплейси для NFT (OpenSea, Rarible), платформи DeFi (Uniswap, Compound, Aave) та різноманітні інструменти для аналітики та розгортання додатків.

Зручність Solidity, основної мови програмування Ethereum, полягає в її простоті, широкій документації та великій кількості навчальних матеріалів. Це дозволяє швидко почати розробку навіть новачкам у сфері блокчейну.

Децентралізовані фінанси (DeFi):

DeFi – це фінансові послуги, які реалізуються за допомогою смарт-контрактів без посередників, таких як банки. Ethereum став лідером у сфері DeFi завдяки можливості створення різноманітних фінансових інструментів – від кредитних платформ до децентралізованих бірж.

Переваги та недоліки:

Ethereum вирізняється потужною інфраструктурою, великою спільнотою та широкими можливостями для розробки додатків. Проте головними недоліками є висока вартість транзакцій та обмежена швидкість обробки, особливо у періоди високої активності.

Основні сфери використання:

Ethereum активно використовується для створення децентралізованих фінансових платформ (DeFi), NFT, інтерактивних ігор та соціальних додатків.

Solana (SOL)

Solana – це сучасна та високопродуктивна блокчейн-платформа, яка вирішує проблему «трилеми блокчейну» – забезпечує одночасно високу швидкість, масштабованість і безпеку. Завдяки використанню інноваційного механізму Proof-of-History (PoH) разом з Proof-of-Stake (PoS), Solana демонструє надзвичайно високу швидкість та ефективність обробки транзакцій.

Принцип роботи:

Solana використовує Proof-of-History як внутрішній годинник мережі, який дозволяє вузлам точно впорядковувати транзакції в часі без додаткових перевірок. Цей унікальний механізм суттєво зменшує час на валідацію та підтвердження транзакцій, а також значно покращує загальну пропускну здатність мережі.

Використовуючи Proof-of-Stake, учасники мережі (валідатори) підтверджують транзакції та створюють нові блоки, отримуючи за це винагороду у формі токенів SOL. Крім того, користувачі можуть делегувати свої токени валідаторам, посилюючи безпеку та стабільність мережі.

Solana також реалізує паралельну обробку смарт-контрактів завдяки технології Sealevel, що дозволяє значно підвищити ефективність та масштабованість роботи додатків.

Solana дозволяє створювати різноманітні застосунки — від складних децентралізованих фінансових платформ (DeFi) до швидких ігрових проектів та платформ для NFT. Завдяки високій швидкості та низьким комісіям, Solana ідеально підходить для високочастотної торгівлі, інтерактивних додатків та сервісів, що потребують швидкої взаємодії в реальному часі.

Однак через високу продуктивність Solana висуває значні вимоги до апаратних ресурсів. Для запуску повноцінного вузла потрібні потужні сервери з великим обсягом оперативної пам'яті (від 128 ГБ) та швидкі SSD-диски. Такі високі технічні вимоги створюють ризики певної централізації, оскільки кількість потенційних валідаторів є обмеженою.

Переваги:

Solana володіє надзвичайною швидкістю транзакцій, здатною досягати до 50,000 операцій за секунду, що робить її однією з найшвидших блокчейн-платформ у світі. Додатково, платформа пропонує дуже низькі транзакційні витрати, які часто складають менше одного цента.

Недоліки:

До недоліків Solana слід віднести високі початкові витрати на обладнання та потенційні ризики централізації управління мережею через значні ресурси, необхідні для підтримки вузлів.

Основні сфери використання:

Solana найбільше використовується у сферах децентралізованих фінансів (DeFi), платформах для NFT, ігровій індустрії та високочастотній торгівлі. Для використання у сфері NFT, Solana часто є більш вигідною та зручною альтернативою Ethereum завдяки значно нижчим комісіям і високій швидкості транзакцій, що суттєво зменшує витрати на створення та обіг токенів. Однак, Ethereum має більшу популярність та більш розвинену інфраструктуру і маркетплейси, що полегшує взаємодію з ширшою аудиторією.

Monero (XMR)

Monero є однією з провідних криптовалют, створених спеціально для забезпечення максимальної конфіденційності та анонімності транзакцій. Ця цифрова валюта відома завдяки використанню складних криптографічних технологій, таких як кільцеві підписи (Ring Signatures), приховані адреси (Stealth Addresses) і технологія Ring Confidential Transactions (RingCT). Ці технології забезпечують повну неможливість відстеження адрес відправника і одержувача, а також суми транзакцій.

Принцип роботи:

Монеро функціонує на алгоритмі Proof-of-Work (PoW), де майнери використовують обчислювальну потужність для підтвердження транзакцій та створення нових блоків. Цей процес майнінгу сприяє додатковому рівню безпеки та анонімності, оскільки участь у процесі доступна всім користувачам з відповідними апаратними ресурсами.

Монеро забезпечує абсолютну приватність завдяки унікальному процесу маскування, в якому реальні транзакції змішуються з іншими, створюючи додатковий шар захисту від потенційних спроб аналізу мережі.

Monero широко використовується у випадках, коли необхідно забезпечити абсолютну конфіденційність платежів, наприклад, у випадках приватних фінансових транзакцій або в операціях, де важливим є захист персональних даних.

Хоча Monero забезпечує відмінний рівень конфіденційності, він має меншу швидкість транзакцій порівняно з іншими блокчейнами, такими як Ethereum чи Solana. Також ця платформа не підтримує смарт-контракти і не дозволяє створювати децентралізовані додатки.

Переваги:

До переваг Monero належить надзвичайна конфіденційність і стійкість до аналізу транзакцій, а також широка доступність вузлів.

Недоліки:

Основними недоліками є низька швидкість обробки транзакцій та обмежені функціональні можливості щодо програмованості.

Основні сфери використання:

Monero частіше всього використовується у сферах, де анонімність є пріоритетом: приватні платежі, анонімні транзакції, захищені фінансові операції.

Характеристика	Ethereum	Solana	Monero
Консенсус	Proof-of-Stake (PoS)	Proof-of-Stake (PoS) + Proof-of-History (PoH)	Proof-of-Work (PoW)
Швидкість транзакцій	~30 транзакцій/сек	до 50,000 транзакцій/сек	нижча швидкість

Комісії	Високі (газ)	Дуже низькі	Помірні
Смарт-кон тракти	Solidity (ERC-20, ERC-721)	Rust, C++	Не підтримує
Конфіденційність	Середня	Низька	Висока (анонімні транзакції)
Сфери застосування	DeFi, NFT, dApps	DeFi, NFT, ігри	Анонімні платежі, фінансова конфіденційність
Вимоги до обладнання	Середні	Високі (128 ГБ RAM, SSD)	Низькі
Популярність для NFT	Висока, розвинені маркетплейси	Висока, швидко зростає	Не використовується

Взаємозаміна модулів

Модулі Ethereum, Solana та Monero не є взаємозамінними через такі причини:

- Різні механізми консенсусу (PoS, PoH, PoW).
- Різні мови програмування (Solidity, Rust, відсутність підтримки смарт-контрактів у Monero).
- Різна архітектура виконання смарт-контрактів (EVM у Ethereum, власна модель у Solana, відсутність у Monero).

Таким чином, кожна система має унікальні характеристики та цілі використання, що робить пряме перенесення модулів неможливим без суттєвої переробки.