ФБ-42 мп Омелянович Олександр, Сербіненко Олексій
Ethereum, Bitcoin, Monero

Ethereum — це децентралізована платформа для виконання смарт-контрактів і створення розподілених додатків (dApps), запущена в 2015 році групою розробників на чолі з Віталіком Бутеріним. На відміну від Bitcoin, який створений головним чином як система електронних платежів і зосереджений на передачі вартості, Ethereum відразу став своєрідним «світовим комп'ютером», що дозволяє будь-якому розробнику розгортати і виконувати програми без ризику цензури, простоючи чи втручання з боку третіх осіб.

У своїй основі Ethereum складається з блокчейну, у якому зберігаються не лише транзакції, а й стан виконуваних контрактів. Ключова ідея полягає в тому, що кожен вузол мережі одночасно зберігає копію всієї історії та поточного стану — це забезпечує високу стійкість і неприйнятність централізованого контролю.

Принцип роботи

Користувачі взаємодіють з мережею через транзакції — спеціальні повідомлення, підписані їхніми приватними ключами. Транзакції можуть передавати ефір (ETH) або викликати певний метод смарт-контракту. Кожна транзакція перед відправленням оцінюється за вартістю обчислень (газ), яку повинен сплатити відправник. Газова модель гарантує, що зловмисник не зможе завантажити мережу нескінченними або занадто важкими обчисленнями.

У липні 2022 року Ethereum завершив «The Merge» — перехід від механізму консенсусу Proof-of-Work (PoW) до Proof-of-Stake (PoS). Тепер замість майнерів створюють нові блоки валідатори, які вкладають ETH як заставу. Це значно знизило енергоспоживання мережі та змінило економіку винагород.

Архітектурні компоненти

1. Нода (клієнтська програма)

- Є кілька реалізацій клієнтів для виконання Ethereum: Geth (Go), OpenEthereum (Rust), Besu (Java) тощо.
- Кожна нода виконує дві ключові функції: обробку транзакцій та підтримку консенсусу.

2. Шар виконання (Execution Layer)

- Відповідає за зберігання стану (аккаунти, баланс, сховище контрактів) та виконання смарт-контрактів.
- Обчислює новий стан після кожного блоку.

3. Шар консенсусу (Consensus Layer)

- Після The Merge саме він вирішує, який блок вважати «правильним».
- Для PoS-валідаторів існують поняття «beacon chain» (ланцюг маяків), де зберігається інформація про валідаторів, їхні частки та результати голосування.

4. P2P-мережа

- Вузли з’єднуються між собою по протоколу DevP2P, обмінюються новими блоками і транзакціями через gossip-механізм.

5. JSON-RPC інтерфейс

- Забезпечує API для зовнішніх додатків: отримання балансу, надсилання транзакцій, виклику методів контрактів тощо.

6. Сховище даних

- Дані блокчейну зберігаються в базі LevelDB або RocksDB.
- Стан мережі організовано через Merkle Patricia Trie для ефективного доказу непідробності даних.

Ethereum Virtual Machine (EVM)

EVM — це віртуальна машина, призначена для детерміністичного виконання байткоду смарт-контрактів. Вона повністю ізольована від оточення, що гарантує, що смарт-контракти не зможуть непередбачувано вплинути на систему чи на інші контракти.

- Байткод та опкоди

Смарт-контракти компілюються з мов високого рівня (Solidity, Vyper) у низькорівневий байткод, який інтерпретується EVM. Байткод включає понад сотню опкодів (ADD, MUL, SSTORE тощо).

- Стекова архітектура

Виконання відбувається переважно через стекові операції: аргументи операцій завантажуються в стек, обчислюються, і результат повертається назад.

- Модель газу

Кожен опкод споживає певну кількість газу. Якщо на балансі відправника не вистачає газу — транзакція відхиляється, а мережа звільняється від занадто важких обчислень.

- Стан та зберігання

Контракти мають власне сховище (key–value), доступ до якого відбувається через відповідні опкоди (SLOAD, SSTORE).

Підсумок

Ethereum надає розширений набір інструментів для створення повноцінних децентралізованих застосунків. Його модульна архітектура — розділена на шари виконання та консенсусу, ізольована віртуальна машина (EVM), чітка модель газу та стандартизований API — роблять платформу одночасно гнучкою та надійною.

Bitcoin

Bitcoin — це перша у світі децентралізована цифрова валюта, створена у 2009 році невідомим розробником або групою розробників під псевдонімом Сатоші Накамото. Метою Bitcoin було створити систему, яка дозволяє користувачам безпечно передавати

вартість у мережі без необхідності довіряти центральному органу, банку або третій стороні.

Принцип роботи

У Bitcoin транзакції створюються користувачами, підписуються їх приватними ключами та поширюються мережею. Кожна транзакція — це передача певної кількості BTC від одного гаманця до іншого. Після збору транзакцій у мемпулі майнери конкурують за право включити їх у новий блок. Для цього вони повинні знайти такий хеш блоку, який відповідатиме заданому рівню складності — це і є **Proof of Work**.

Як тільки блок знайдено, він поширюється мережею і додається до локального ланцюга кожним вузлом. Новий блок визнається дійсним лише в тому випадку, якщо відповідає всім консенсусним правилам, і містить правильний хеш попереднього блоку, допустимі транзакції та відповідний PoW.

Архітектурні компоненти

Ноди (вузли мережі)
Усі учасники мережі можуть запускати вузол Bitcoin. Повні вузли (Bitcoin Core) зберігають повну копію блокчейну (наразі понад 500 ГБ), перевіряють усі транзакції та блоки відповідно до протоколу. Існують також полегшені клієнти, що працюють через SPV (Simplified Payment Verification), використовуючи лише заголовки блоків.

Блокчейн
Блокчейн Bitcoin — це незмінна послідовність блоків, де кожен блок містить:

- хеш попереднього блоку;
- список транзакцій;
- кореневий хеш дерева Меркла;

- час створення;
- nonce для PoW.

Новий блок створюється в середньому кожні 10 хвилин. Кожні 2016 блоків мережа автоматично перераховує складність задачі, щоб підтримувати сталий темп створення блоків. Блок має обмеження в 1 МБ (хоча після SegWit фактичний розмір збільшився), що обмежує кількість транзакцій у кожному блоці.

Proof of Work (PoW)
Це механізм консенсусу, який вимагає великих обчислювальних зусиль. Майнер повинен знайти такий nonce, щоб хеш заголовка блоку був меншим за встановлений поріг складності. Це гарантує, що додавання нового блоку є дорогим і трудомістким, а спроба зловживання мережею — економічно недоцільна.

Скриптова система (Bitcoin Script)
Bitcoin має вбудовану мову скриптів, яка дозволяє задавати прості умови витрат монет — наприклад, вимогу кількох підписів або обмеження за часом.

P2P-мережа
Усі вузли об’єднані в однорангову мережу, що працює за власним TCP-протоколом з обміном повідомленнями. Поширення транзакцій і блоків відбувається через flood- або gossip-механізми. Кожен вузол підтримує з’єднання з десятками інших.

API та інтерфейси
Bitcoin Core підтримує JSON-RPC API, який дозволяє зовнішнім програмам отримувати інформацію про стан мережі, надсилати транзакції, запитувати баланси тощо. Це основа для інтеграції бірж, гаманців і платіжних сервісів.

Економічна модель

У Bitcoin існує жорстка межа емісії — не більше 21 мільйона BTC. Цей ліміт забезпечується на рівні протоколу та є головною причиною дефляційного характеру системи. Щоб стимулювати початкову

участь майнерів, вони отримували винагороду за кожен блок. Ця винагорода автоматично зменшується вдвічі кожні приблизно чотири роки в результаті події, що називається **халвінгом**. Наприклад, у квітні 2024 року вона знизилася з 6.25 до 3.125 BTC.

Транзакції в Bitcoin супроводжуються комісіями, розмір яких залежить від обсягу даних у транзакції та завантаженості мережі. Комісії отримують майнери разом із базовою винагородою за блок.

Оновлення протоколу

У 2017 **Segregated Witness (SegWit)** — оновлення, що винесло цифрові підписи за межі основної структури транзакції, зменшивши її об'єм. Це дало змогу підвищити пропускну здатність.

У 2021 році з'явилося оновлення **Taproot**, яке об'єднало кілька покращень: підвищену конфіденційність, зменшення розміру мультипідписів і можливість складніших сценаріїв витрати монет.

Підсумок

Bitcoin — це фундаментальна технологія блокчейнів. Його архітектура проста, надійна і зосереджена на основній функції: безпечному зберіганні та передачі вартості. Відсутність повноцінної підтримки смарт-контрактів компенсується найвищою на ринку децентралізацією, передбачуваністю поведінки та репутацією найбезпечнішої мережі у криптосвіті. Bitcoin не намагається бути універсальним середовищем обчислень, як Ethereum, але натомість виконує свою вузькоспеціалізовану роль з неперевершеною ефективністю.

Monero

Monero — це децентралізована криптовалюта, сфокусована на приватності та неідентифікованості транзакцій. Створена в квітні 2014 року як форк протоколу CryptoNote, Monero (XMR) відрізняється від більшості інших криптовалют відмовою від прозорої публічної книжки: тут немає відкритих адрес відправника і отримувача, а суми платежів приховані. Основна мета проєкту —

забезпечити повну анонімність користувачів без залучення сторонніх послуг-міксерів, захищаючи їхню фінансову приватність від аналізу блокчейну та побічних витоків інформації.

Принцип роботи

У Monero кожна транзакція формується з використанням трьох ключових криптопримітивів: кільцевих підписів (ring signatures), прихованих адрес (stealth addresses) та конфіденційних транзакцій (RingCT). Кільцеві підписи дозволяють «змішати» справжній вхід транзакції з низкою фіктивних входів (декої), через що неможливо достовірно встановити, хто саме є відправником. Приховані адреси генерують для кожного платежу одноразовий ключ, навіть якщо отримувач дає лише свій публічний ідентифікатор, — це унеможливлює відстеження вхідних операцій. Ще одним шаром анонімності є RingCT: сума переказу шифрується, але завдяки нульовим доказам (Bulletproofs) вузли мережі перевіряють, що вхідна сума дорівнює вихідній без розкриття її конкретного значення.

Monero зберігає приблизно двохвилинний інтервал між блоками і використовує адаптивний розмір блоку: він динамічно підлаштовується під заповненість мережі, щоб забезпечити як низькі затримки, так і захист від потенційного спаму великими «важкими» блоками. Механізм консенсусу — Proof-of-Work на основі алгоритму RandomX, оптимізованого під виконання на звичайних CPU, що протидіє ASIC-централізації.

Архітектурні компоненти

1. Нода Monerod

Основна реалізація вузла на C++, яка підтримує зберігання та верифікацію блокчейну через LMDB; обмін транзакціями та блоками з однолітками; виконання PoW-обчислень.

2. Гаманці (monero-wallet-cli, monero-wallet-gui, monero-wallet-rpc)

CLI- і GUI-інтерфейси для керування ключами, створення й підпису транзакцій та перегляду балансу, а також JSON-RPC-сервер для інтеграції з додатками.

3. P2P-мережевий шар

Використовує Kademlia-подібний DHT для пошуку вузлів та gossip-протокол для розповсюдження нових блоків і транзакцій без централізованих точок контролю.

4. База даних і структура зберігання

Блокчейн і стан гаманців зберігаються в LMDB, а для доказів непідробності даних застосовується Merkle-дерево.

5. Криптографічний стек (CryptoNote Protocol)

Містить модулі для генерації кільцевих підписів, створення одноразових адрес, RingCT з Bulletproofs та алгоритм RandomX для PoW.

CryptoNote Protocol та технології приватності

У серці Monero лежить протокол CryptoNote, який задає набір правил для забезпечення конфіденційності й анонімності.

Кільцеві підписи (Ring Signatures) формують підпис, що підтверджує право витратити вхідні монети, але комбінує його з низкою «фальшивих» підписів інших користувачів, аби приховати справжнього власника.

Приховані адреси (Stealth Addresses): отримувач надає одним надлишковим публічним ключем, але відправник генерує одноразову адресу, що унеможливлює публічне зіставлення виплат із цим користувачем.

Конфіденційні транзакції (RingCT) приховують суми переказів, натомість вузли просто перевіряють математичну рівність входів і виходів за допомогою Bulletproofs — ефективних нульових доказів діапазону.

RandomX: персоніфікований PoW-алгоритм, що вимагає великого обсягу випадкових операцій з пам’яттю, роблячи майнінґ на

стандартних процесорах конкурентоспроможним і запобігаючи ASIC-монополізації.

Підсумок

Monero побудовано навколо приватності «за замовчуванням» через глибоку інтеграцію CryptoNote-модулів. На відміну від Ethereum, де ядро системи — EVM для універсального виконання смарт-контрактів — Monero не підтримує програмовані контракти, натомість концентрується на модульній побудові криптографічних технологій для анонімності. Оскільки архітектурні цілі та криптографічні основи цих двох мереж принципово відрізняються, взаємозаміна їхніх ключових компонентів (EVM ↔ RingCT, смарт-контракти ↔ stealth-адреси) технічно неможлива без повного переосмислення проєкту й компромісу в його основних цінностях. У подальшому порівняльному аналізі ми з’ясуємо, які модулі залишаються унікальними, а які можна концептуально адаптувати між системами.

	Ethereum	Bitcoin	Monero
Рік запуску	2015	2009	2014
Механізм Консенсусу	Proof-of-Stake (з липня 2022, раніше — Proof-of-Work)	Proof-of-Work (SHA-256)	Proof-of-Work (RandomX)
Час створення Блоку	≈12–14 секунд	≈10 хвилин	≈2 хвилини
Модель Транзакцій	Account-based (рахунок + контракти)	UTXO	CryptoNote-UTXO
Смарт-контракти	Так (Turing-complete через EVM)	Ні (лише скриптова мова, подібна до Forth, Обмежена)	Ні
Віртуальна Машина	Ethereum Virtual Machine (EVM)	Немає (лише вбудований скриптовий інтерпретатор)	Немає
Приватність	Публічні адреси й суми; можливі рішення Рівня 2 (zk-рішення)	Публічні адреси й суми; обмежена приватність Через CoinJoin	Анонімність «за замовчуванням»: кільцеві підписи,

			Приховані адреси, RingCT
Розмір блоку	Динамічний, орієнтований на навантаження Мережі	Жорсткий ліміт ~1 МБ (з SegWit — до 4 МБ «ваги»)	Динамічний, адаптивний до навантаження, Без жорсткого верхнього ліміту
Комісії	Газова модель: плата за обчислення + газовий ліміт	Плата за пріоритет включення в блок (на основі розміру)	Плаваюча комісія, залежить від розміру кільця Й розмірів блоків
Основне Призначення	Платформа для dApps, DeFi та Смарт-контрактів	Цифрове золото та однорангові платежі	Конфіденційні платежі та фінансова приватність