

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»**

**Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації**

**Звіт до лабораторної №1
за темою:
Розгортання систем Ethereum та криптовалют**

**Оформлення звіту:
Юрчук Олексій, ФІ-52мн**

16 лютого 2026 р.
м. Київ

ЗМІСТ

1	Невеличкий вступ	1
2	Огляд систем блокчейн і криптовалют	1
2.1	Bitcoin	1
2.2	Ethereum	1
2.3	Dash	2
2.4	NEO	2
2.5	Litecoin	3
3	Порівняльний аналіз архітектурних рішень та процедур розгортання	3
3.1	Механізми консенсусу	3
3.2	Архітектура мережі та P2P-взаємодія	3

1 Невеличкий вступ

Технологія блокчейн кардинально змінила наше уявлення про децентралізовані обчислення, фінансові транзакції та бездовірчі системи (trustless systems). З моменту публікації "Bitcoin whitepaper" [1] by Satoshi Nakamoto в 2008 році, з'явилося безліч платформ блокчейн, кожна з яких має свої архітектурні рішення, процедури розгортання та операційні характеристики.

У своїй лабораторній, я розглядав і порівнював, здебільшого зазначені в завданнях до лабораторної, особливості розгортання п'яти основних систем блокчейну/криптовалюти: **Ethereum** [2, 3], **Bitcoin** [1], **Dash** [4], **NEO** [5] та **Litecoin** [6]. Свій аналіз я спрямував більше на практичні аспекти реалізації, розгортання та конфігурації кожної системи, вивченні їх базової архітектури, механізмів консенсусу, мережних рівнів та можливості обміну модулями між ними.

Поки в планах наступне: у розділі 2 описати теоретичні основи кожної системи, далі в розділі 3 доволі детально порівняти їх за різними параметрами, розглянути їх взаємозамінність. А далі у розділі 4 планую навести покрокові, як я робитиму, практичне розгортання Ethereum (певно найпростіше, що можна взяти) у середовищі на базі WSL за setup-ами від [7, 8]. І відповідно в кінці підбити підсумки по отриманих результатах.

2 Огляд систем блокчейн і криптовалют

2.1 Bitcoin

Bitcoin – це певно перша і найвідоміша криптовалюта, опублікована в 2008 році анонімним девелопером з псевдонімом Сатоші Накамото. Вона використовує модель **UTXO (Unspent Transaction Output)** для відстеження балансів і механізм консенсусу **Proof-of-Work**, заснований на алгоритмі хешування SHA-256.

Ключові особливості Bitcoin включають в себе:

- **Жодних смарт-контрактів** (в традиційному сенсі) – Bitcoin Script навмисно є non-Turing-complete.
- **Block time** – генерація нового блоку ≈ 10 хвилин, **block size** обмежений $\approx 1\text{--}4$ MB (з SegWit).
- **Загальний обсяг** обмежений 21 мільйоном BTC.
- **Networking** – використовує особливий мережний P2P protocol через TCP (port 8333), розповсюдження інформації на основі gossip-based ("пліткування з сусідами").

2.2 Ethereum

Ethereum – відкрита розподілена обчислювальна платформа на основі блокчейну, яка підтримує функціональність смарт-контрактів. На відміну від Bitcoin, який був розроблений в першу чергу як цифрова валюта, Ethereum був задуманий як універсальний програмований блокчейн (!). Власна криптовалюта блокчейну Ethereum це **Ether (ETH)**.

Основні архітектурні особливості Ethereum включають:

- **Ethereum Virtual Machine (EVM)** – віртуальна машина, яка виконує смарт-контракти, з повною функціональністю Тюрінга (це такий а-ля емулятор для виконання програм за скінченний час і пам'ять);
- **State model** – модель на основі облікових записів діє як банківська книга, відстежуючи баланс і забезпечує можливість укладання складних смарт-контрактів. (в Bitcoin застосовується UTXO model, де рахунки ефективно управляються смарт-контрактами, і в якій забезпечується вищий рівень конфіденційності та здійснюється паралельна обробка даних);
- **Protocol of Consensus** – первісно застосовувався Proof-of-Work (Ethash), але у вересні 22 зробили трансфер на Proof-of-Stake (Casper/Beacon chain);
- **Smart Contracts** – пишуться мовами Solidity, Vyper та деякими іншими мовами і є EVM-compatible;
- **Gas system** – обчислювальні витрати вимірюються за допомогою так званих тарифів "gas fees".

Ethereum – це peer-to-peer надбудова над базою інтернет протоколів TCP/IP [9]. Кожен вузол запускає копію блокчейну та бере участь у валідації та розповсюдженні блоків. Офіційний клієнт **Geth** (Go-Ethereum) реалізує протокол RLC (Remote Procedure Call) Node Discovery Protocol, що базується на DHT (Distributed Hash Table) типу Kademlia для виявлення однорангових вузлів (peers) [9].

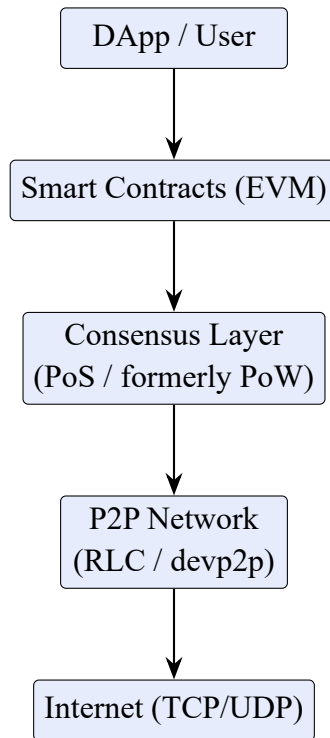


Рис. 1: Архітектура "шарів" Ethereum-a

2.3 Dash

Dash (originally "Darkcoin") являє собою fork від кодової бази Bitcoin, але з додатковими функціями конфіденційності та управління. В ньому було запроваджено:

- **Masternodes** – мережа другого рівня (second-tier network) з мотивованими (incentivized) вузлами, які забезпечують InstantSend і CoinJoin (PrivateSend).
- **Алгоритм гешування X11** – ланцюжкова послідовність із 11 криптографічних геш-функцій.
- **Система управління фінансами (Treasury system)** – 10% винагороди за блок виділяється на фінансування ідей щодо розвитку (за них голосуються masternodes).
- **Block time** – генерація нового блоку складає ≈ 2.5 хвилин.

2.4 NEO

NEO (колишня назва – AntShares) китайська блокчейн-платформа, яку частенько називають "китайським ефіром (Ethereum)". Вона також підтримує виконання смарт-контрактів, але має значні відмінності по своїй архітектурі:

- **Consensus** – делегована візантійська відмовостійкість (delegated Byzantine Fault Tolerance - dBFT), що забезпечує детермінованість виконання.
- **Dual token model** – NEO (токен управління, є неподільним) and GAS (токен-утиліта для виконання контрактів).
- **Multi-language support** – смарт-контракти можуть бути написані на різних мовах програмування, таких як: C#, Python, Java, Go (з подальшим виконанням у віртуальній машині NeoVM).
- **Інтеграція цифрової ідентичності** та орієнтація на сурове дотримання нормативних вимог.

2.5 Litecoin

Litecoin був створений Чарлі Лі в 2011 році як "полегшена" версія Bitcoin. Це один з найперших форків від Bitcoin, який і досі має багато спільного з кодом Bitcoin. Основні особливості:

- **Script hashing** – алгоритм, що вимагає великого обсягу пам'яті (первинно розроблявся для протидії майнінгу ASIC)
- **Block time** – генерування складає ≈ 2.5 хвилин (це у 4× швидше за Bitcoin).
- **Total supply** – 84 мільйони LTC (у 4× перевищує обсяг Bitcoin-a).
- **UTXO model** – така сама структура транзакцій, як у Bitcoin.
- **Test platform** – Часто стає тестовим майданчиком для функцій Bitcoin-a (наприклад, той же SegWit був активований спочатку на Litecoin).

3 Порівняльний аналіз архітектурних рішень та процедур розгортання

3.1 Механізми консенсусу

Механізм консенсусу є основним модулем, який визначає, як мережа блокчейну досягає згоди щодо стану реєстру. Кожен з названих нами п'яти блокчейнів використовують принципово різні підходи:

Блокчейн	Алгоритм гешування	Протокол	Остаточність
Ethereum	Gasper (PoS)	Proof-of-Stake	Probabilistic → deterministic (2 epochs)
Bitcoin	SHA-256	Proof-of-Work	Probabilistic (~ 6 confirmations blocks)
Dash	X11 + Masternodes	Hybrid: PoW + PoS	Instant (via ChainLocks)
NEO	dBFT 2.0	Delegated BFT	Deterministic (1 block, no forks)
Litecoin	Script	Proof-of-Work	Probabilistic (~ 6 confirmations blocks)

Таблиця 1: Порівняння протоколів консенсусу

3.2 Архітектура мережі та P2P-взаємодія