КОМП'ЮТЕРНИЙ ПРАКТИКУМ КРЕДИТНОГО МОДУЛЯ

"БЛОКЧЕЙН ТА ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ"

Лабораторна робота № 1

Виконали: студенти групи ФІ-32мн

Ємець Єлизавета

Карловський Володимир

Коваленко Дар'я

Тема: «Розгортання систем Etherium та криптовалют»

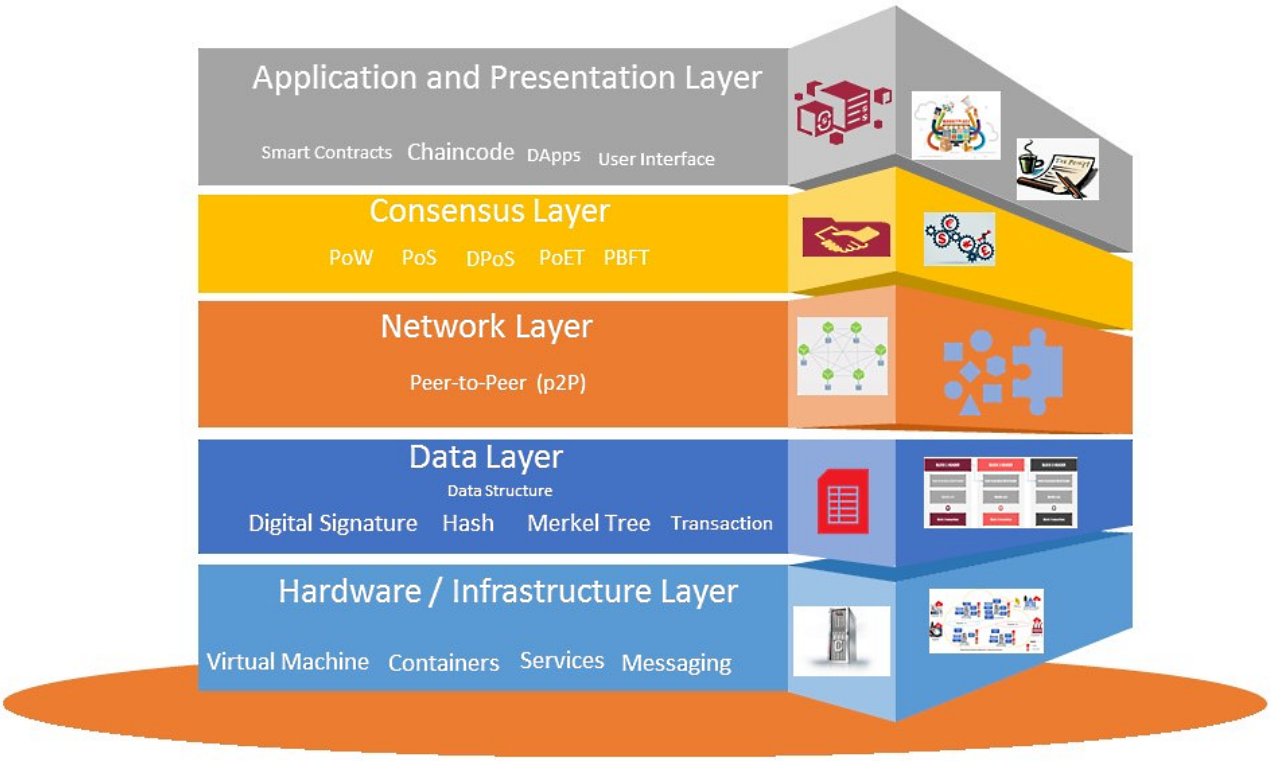
Мета роботи: «Отримання навичок налаштування платформ виконання смарт-контрактів та криптовалют».

Завдання на лабораторну роботу: 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.

Для проведення порівняльного аналізу особливостей розгортання систем криптовалют у порівнянні із системою Ethereum, важливо визначити ключові аспекти, на які ми будемо звертати увагу.

1. Архітектура блокчейну є фундаментом для розуміння різниці між різними криптовалютними системами, включаючи Ethereum. Вона включає в себе кілька ключових компонентів, які визначають функціональність, безпеку, швидкість та

інші важливі аспекти системи. Ось детальний огляд основних елементів архітектури блокчейну:



Рівень інфраструктури

Вміст блокчейна зберігається десь на сервері в центрі обробки даних. Клієнти запитують контент або дані з серверів додатків під час перегляду веб-сторінок або використання будь-яких додатків.

Блокчейн - це однорангова мережа комп'ютерів, яка впорядковано обчислює, перевіряє і записує транзакції в загальний реєстр. У результаті створюється розподілена база даних, у якій зберігаються всі дані, транзакції та інші відповідні дані. Вузол - це комп'ютер у мережі P2P.

Рівень даних

Блокчейн - це структура даних, у якій транзакції упорядковані в пов'язаному списку блоків. Ця структура складається з покажчиків і пов'язаного списку. Пов'язаний список містить блоки з даними і покажчиками на попередній блок. Покажчики - це змінні, які посилаються на інші змінні, а пов'язаний список - це список блоків і покажчиків. Дерево Меркла - це бінарне дерево хешів, де кожен блок містить кореневий хеш дерева та інформацію про попередній блок, тимчасову мітку, номер блоку і поточну мету складності. Дерево Меркла

забезпечує безпеку, цілісність і неспростовність для систем блокчейну. Транзакції в блокчейні підписуються цифровим підписом для забезпечення безпеки, і будь-хто може перевірити підпис, якщо відкритий ключ доступний. У першому блоку, блоку генезису, немає покажчика.

Мережевий рівень

Мережевий рівень, який зазвичай називають рівнем P2P, відповідає за взаємодію між вузлами. Виявлення транзакцій, поширення блоків відбувається на мережевому рівні.

Цей рівень P2P гарантує, що вузли можуть знаходити один одного і взаємодіяти, розповсюджувати і синхронізувати інформацію, щоб підтримувати мережу блокчейна в законному стані. Мережа P2P - це комп'ютерна мережа, в якій вузли розподілені та розділяють робоче навантаження мережі для досягнення спільної мети. Транзакції блокчейна виконуються вузлами.

Рівень консенсусу

Рівень консенсусу - найнеобхідніший і найкритичніший рівень у будь-якому блокчейні. Він відповідає за перевірку блоків, їх упорядкування та гарантію того, що всі згодні з поточним станом блокчейна.

Прикладний рівень

Смарт-контракти, децентралізовані додатки (DApps) складають прикладний рівень. Протоколи прикладного рівня поділяються на прикладний і виконавчий рівні.

Рівень додатків містить програми, які кінцеві користувачі використовують для зв'язку з мережею блокчейна.Смарт-контракти - це частина рівня виконання.

Транзакція переміщується з рівня застосунку на рівень виконання. Додатки дають інструкції виконавчому шару, який виконує транзакції і забезпечує детермінований характер блокчейна.

2. Програмованість блокчейнів, особливо через смарт-контракти, стала однією з ключових особливостей, яка відрізняє сучасні блокчейни один від одного. Смарт-контракти дозволяють створювати складні логічні операції, автоматизувати виконання угод, створювати децентралізовані додатки (dApps) та автономні організації (DAOs), що забезпечує широкі можливості для інновацій у фінансовій, юридичній, логістичній та багатьох інших галузях.

Смарт-контракти — це програми, що виконуються на блокчейні при виконанні певних умов. Вони зберігаються в блокчейні та виконуються децентралізовано, без можливості зміни чи видалення після розгортання.

Особливості програмування на Ethereum

Ethereum був першим блокчейном, який запропонував повноцінну платформу для створення смарт-контрактів та dApps. Це стало можливим завдяки мові програмування Solidity, яка дозволяє розробникам створювати складні контракти з різноманітною логікою.

Порівняння з іншими блокчейнами

1. Cardano використовує мову програмування Plutus для смарт-контрактів, що заснована на Haskell. Cardano прагне до більшої безпеки та формальної верифікації коду смарт-контрактів, що робить їх потенційно більш надійними, але також може ускладнити розробку.

2. Polkadot пропонує інноваційну модель шардінгу через парачейни, дозволяючи кожному з них мати свою унікальну структуру даних та логіку. Це створює можливості для оптимізації під конкретні випадки використання та підвищення загальної шкалованості мережі.

3. Binance Smart Chain (BSC) спроектований для швидких транзакцій з низькими комісіями, використовуючи сумісність з Ethereum Virtual Machine (EVM), що дозволяє розробникам легко мігрувати додатки з Ethereum.

4. Tezos використовує мову Michelson для смарт-контрактів, надаючи інструменти для формальної верифікації коду, що забезпечує високий рівень безпеки та надійності контрактів. Особливість Tezos полягає також у механізмі вбудованого оновлення протоколу, який дозволяє мережі еволюціонувати без необхідності проведення хард-форків.

3. Шкалованість та продуктивність блокчейн-систем є ключовими параметрами, які впливають на їхню спроможність підтримувати велику кількість транзакцій і користувачів. Ці показники визначають, наскільки ефективно система може обробляти зростаючий обсяг даних і запитів без збільшення часу обробки транзакцій або вартості транзакцій. Давайте розглянемо детальніше.

Механізми, такі як Proof of Work (PoW), який використовується в Bitcoin, вимагають значної обчислювальної потужності та часу для обробки кожного блоку, що обмежує шкалованість і продуктивність. Механізми, як Proof of Stake (PoS), пропонують покращення за рахунок ефективнішого процесу валідації транзакцій.

Для порівняння Ethereum з іншими блокчейн-системами з точки зору шкалованості та продуктивності, розглянемо кілька ключових блокчейнів, які пропонують унікальні рішення для цих викликів.

	Механізм консенсусу	Шкалованість та продуктивність
Bitcoin	Використовує Proof of Work (PoW), який є досить безпечним, але вимагає значних обчислювальних ресурсів і часу для обробки транзакцій. Це обмежує продуктивність мережі приблизно 7 транзакціями в секунду (tps).	Шкалованість обмежена через механізм консенсусу та фіксований розмір блоку. Розглядалися різні рішення, такі як SegWit і Lightning Network, для покращення шкалованості без зміни основного протоколу.
Cardano	Використовує Proof of Stake (PoS) через свій унікальний алгоритм Ouroboros, який є енергоефективнішим та має кращу шкалованість порівняно з PoW.	Cardano прагне до вирішення проблем шкалованості та продуктивності через шардінг та оптимізацію алгоритму консенсусу, що дозволяє обробляти більшу кількість транзакцій.

Polkadot	Використовує варіант Nominated Proof of Stake (NPoS), що дозволяє досягнути високої продуктивності та шкалованості.	Polkadot реалізує інноваційну архітектуру, яка дозволяє мережам (парачейнам) працювати паралельно, значно збільшуючи загальну шкалованість і продуктивність мережі.
Binance Smart Chain (BSC)	Використовує Delegated Proof of Stake (DPoS), що дозволяє досягнути швидкості транзакцій та зменшити вартість транзакцій порівняно з Ethereum.	BSC досягає високої продуктивності, здатної обробляти тисячі транзакцій на секунду, завдяки своїй архітектурі та механізму консенсусу.

4. Безпека

В контексті безпеки блокчейн-систем, атака 51% є одним з найбільш критичних векторів атак, що може загрожувати інтегритету та довірі до мережі. Під час такої атаки атакувач, який контролює більшість хеш-рейту мережі або велику частину стейків, може переписувати транзакційні блоки, подвійно витрачати кошти або зупиняти підтвердження нових транзакцій. Давайте розглянемо, як різні блокчейни захищаються від таких атак і які мають переваги у плані безпеки.

Ethereum

- Перед Ethereum 2.0 (Proof of Work): Ethereum, подібно до Bitcoin, був схильний до потенційної атаки 51%, але високий рівень децентралізації та значний обсяг хеш-рейту ускладнювали реалізацію такої атаки.

- Ethereum 2.0 (Proof of Stake): З переходом на PoS, атака 51% стає ще більш нереалістичною через механізми, які "спалюють" стейк атакувача у випадку детекції маніпуляцій, збільшуючи фінансові витрати та ризики для потенційних атакувачів.

Bitcoin

- Proof of Work: Як піонер блокчейну з найбільшим хеш-рейтом, Bitcoin є надзвичайно стійким до атаки 51% через величезну вартість та складність організації такої атаки. Однак теоретично атака все ще можлива.

Cardano

- Proof of Stake: Cardano використовує унікальний варіант PoS, Ouroboros, який включає ряд безпекових механізмів для запобігання атакам 51%. Система вимагає, щоб валідатори були вибрані на основі кількості стейка, але також і на випадковій основі, що ускладнює потенціал для маніпуляцій.

Polkadot

- Nominated Proof of Stake (NPoS): Polkadot використовує складний механізм консенсусу, який не тільки зменшує ймовірність атак 51%, але й забезпечує високу швидкість транзакцій. Система вимагає, щоб валідатори були обрані з пулу кандидатів, що забезпечує додатковий рівень безпеки.

Binance Smart Chain

- Delegated Proof of Stake (DPoS): BSC використовує DPoS, який дозволяє обраній групі валідаторів управляти блокчейном, значно знижуючи кількість учасників, необхідних для досягнення консенсусу. Це підвищує ефективність транзакцій, але також може збільшити централізацію та потенційну вразливість до атак 51%, оскільки атакувати потрібно меншу кількість валідаторів.

5. Децентралізація є одним із ключових аспектів, які визначають стійкість та безпеку блокчейн-мереж. Ступінь децентралізації може впливати на вразливість мережі до атак, її здатність обробляти транзакції, а також на довіру користувачів та розробників. Нижче представлена порівняльна характеристика децентралізації в різних блокчейн-системах.

	Децентралізація	Вплив на безпеку
Ethereum	Ethereum вважається високодецентралізованою мережею, з великою кількістю нод по всьому світу. Однак, перехід на Ethereum 2.0 і впровадження Proof of Stake можуть змінити динаміку децентралізації через зосередження стейка в руках великих власників.	Високий рівень децентралізації зменшує ризики атак 51% та інших векторів атак, одночасно збільшуючи відмовостійкість мережі.
Bitcoin	Bitcoin має одну з найвищих ступенів децентралізації серед всіх блокчейн-мереж, з тисячами нод по всьому світу та розподіленим майнінговим пулом.	Велика децентралізація робить Bitcoin дуже стійким до атак і маніпуляцій, в тому числі до атак 51%.
Cardano	Cardano прагне до високого рівня децентралізації через свою унікальну систему стейкінгу і валідації Ouroboros. Це включає розподілення впливу на мережу серед великої кількості стейкхолдерів.	Структура децентралізації в Cardano забезпечує додаткову безпеку і знижує ризик централізованих атак.
Polkadot	Polkadot реалізує унікальну мультичейн архітектуру, яка може підтримувати високий рівень децентралізації через розподілення впливу між різними блокчейнами (парачейнами).	Децентралізація в Polkadot сприяє збільшенню безпеки і ефективності мережі, забезпечуючи при цьому гнучкість і швидкість транзакцій між різними блокчейнами через свою інноваційну структуру, зменшуючи таким чином потенційні точки вразливості для атак.

Binance Smart Chain (BSC)	BSC оперує на моделі Delegated Proof of Stake (DPoS), яка забезпечує високу продуктивність за рахунок меншого рівня децентралізації, ніж у Bitcoin чи Ethereum. Це означає, що мережа залежить від обмеженої кількості валідаторів, що може створювати ризики централізації влади.	Хоча BSC пропонує швидкі та ефективні транзакції, менший рівень децентралізації може підвищити ризик атак і маніпуляцій, порівняно з більш децентралізованими мережами.

- Вплив децентралізації на безпеку: Вищий рівень децентралізації зазвичай забезпечує кращий захист від атак, оскільки це ускладнює контроль над мережею однією особою або групою.

- Баланс між децентралізацією, продуктивністю та безпекою: Блокчейни, які прагнуть до високої продуктивності за рахунок зменшення децентралізації (наприклад, BSC), можуть пропонувати користувачам швидші та дешевші транзакції, але за рахунок потенційно збільшеного ризику безпеки.

6. Інтероперабельність блокчейн-систем відіграє критичну роль в створенні єдиного цифрового екосистеми, де різні блокчейни можуть взаємодіяти між собою без посередників. Ця характеристика дозволяє користувачам та розробникам використовувати різні блокчейни для різноманітних потреб, виходячи з їхніх унікальних переваг, не будучи при цьому обмеженими однією системою.

Ethereum

- Інтероперабельність: Хоча Ethereum сам по собі не має вбудованих інструментів для інтероперабельності з іншими блокчейнами, його широка підтримка та велика екосистема додатків сприяють розвитку багатьох сторонніх рішень для міжланцюгової взаємодії.

- Приклади: Мости, такі як Polygon Bridge, дозволяють переміщення активів між Ethereum та іншими блокчейнами, зокрема Polygon і Binance Smart Chain.

	Інтероперабельність	Переваги
Polkadot	Polkadot був спеціально розроблений для забезпечення інтероперабельності між різними блокчейнами через свою унікальну мультичейн архітектуру. Він дозволяє блокчейнам (парачейнам) взаємодіяти між собою безпосередньо та безпечно.	Висока інтероперабельність Polkadot сприяє створенню складних міжланцюгових додатків, збільшуючи можливості використання блокчейн-технологій.
Cosmos	Cosmos також зосереджений на інтероперабельності та пропонує IBC (Inter-Blockchain Communication) протокол, який дозволяє безпечний обмін даними та активами між незалежними блокчейнами.	Cosmos спрощує створення та підключення нових блокчейнів, що дозволяє їм ефективно співпрацювати між собою, підвищуючи загальну утилітарність і досяжність блокчейн-екосистеми.
Binance Smart Chain (BSC)	BSC спроектований для сумісності з Ethereum, що дозволяє легко переміщати додатки та активи між цими двома мережами. Однак, для міжланцюгової взаємодії з іншими блокчейнами, необхідні сторонні рішення та мости, подібні до тих, що використовуються в Ethereum.	BSC надає швидкі та економічно вигідні транзакції з високою сумісністю з екосистемою Ethereum, що сприяє легкому переміщенню активів та додатків між цими мережами.

Cardano	Cardano розробляє свої рішення для інтероперабельності, включаючи Sidechains і мости, які дозволять йому взаємодіяти з іншими блокчейнами. Проте, наразі ці можливості ще знаходяться на етапі розробки або тестування.	Впровадження інтероперабельності в Cardano дозволить йому взаємодіяти з ширшим спектром блокчейн-мереж, підвищуючи універсальність і доступність його екосистеми для розробників та користувачів.

Інтероперабельність між різними блокчейнами відіграє ключову роль у розвитку та адаптації блокчейн-технологій, оскільки вона відкриває нові можливості для їх використання та інтеграції у різноманітні галузі. Кожен блокчейн має свій підхід до забезпечення інтероперабельності, від прямої підтримки в архітектурі до розробки сторонніх рішень і мостів.

7. Екосистема та розвиток блокчейну включають у себе не лише розмір та активність розробницької спільноти, а й наявність додатків, сервісів, інструментів розробки, а також підтримку з боку інвесторів та партнерів. Ці аспекти визначають, наскільки швидко та ефективно може розвиватися платформа, а також її здатність адаптуватися до нових викликів та потреб користувачів.

Платформа	**Екосистема**	**Розвиток**	**Особливості**
Ethereum	Найбільша, тисячі dApps	Перехід на Eth2.0, шардінг, PoS	Велика розробницька спільнота, широке використання
Polkadot	Унікальна мультичейн архітектура, спеціалізовані блокчейни	Активне залучення проєктів, розвиток парачейнів	Інноваційна інтероперабельність, гнучкість
BSC	Сумісна з EVM, швидке зростання	Швидке прийняття, збільшення кількості dApps	Низькі комісії, висока продуктивність
Cardano	Розвивається, науковий підхід	Запуск смарт-контрактів, розширення екосистеми	Висока безпека, масштабованість

Ethereum продовжує бути лідером за кількістю та різноманітністю додатків у своїй екосистемі, а перехід на Ethereum 2.0 має зміцнити його позиції щодо масштабованості та ефективності.
Polkadot пропонує унікальну модель інтероперабельності, що дозволяє створювати спеціалізовані блокчейни з можливістю взаємодії, відкриваючи нові можливості для розробників.
Binance Smart Chain зосереджується на високій продуктивності та низьких комісіях, що робить його привабливим для проєктів DeFi та транзакцій з NFT.
Cardano прагне до розвитку високоякісної, безпечної та масштабованої екосистеми, підкріпленої науковими дослідженнями та формальною верифікацією.

Висновки
Провівши порівняльний аналіз різних аспектів блокчейн-платформ, ми можемо зробити декілька ключових висновків щодо їх архітектури, інтероперабельності, екосистеми, а також потенціалу для майбутнього розвитку та взаємодії між ними.

Архітектура та Механізми Консенсусу
Різноманітність архітектур та механізмів консенсусу (Proof of Work, Proof of Stake, Delegated Proof of Stake, та інші) відображає широкий спектр підходів до забезпечення безпеки, шкалованості, та ефективності блокчейн-мереж. Ethereum переходить на Proof of Stake у рамках оновлення Ethereum 2.0 для покращення шкалованості та ефективності. Водночас, платформи як Polkadot та Cosmos розробляють унікальні рішення для інтероперабельності між блокчейнами.

Інтероперабельність
Інтероперабельність є ключовим фактором для майбутнього блокчейну, дозволяючи різним мережам спілкуватися та взаємодіяти між собою. Polkadot та Cosmos виокремлюються своїми передовими рішеннями для підтримки міжланцюгової взаємодії, в той час як Ethereum та Binance Smart Chain зосереджуються на розробці мостів та інших сторонніх рішень для підтримки інтероперабельності.

Екосистема та Розвиток
Ethereum продовжує лідирувати за розміром та активністю своєї екосистеми, пропонуючи найбільшу кількість додатків та сервісів. В той же час, новіші платформи, як Polkadot, Cardano, та BSC, швидко розвиваються, пропонуючи інновації та спеціалізовані можливості, що може сприяти розширенню та диверсифікації блокчейн-екосистеми в цілому.

Майбутній Розвиток

Потенціал для майбутнього розвитку в багатьох блокчейн-платформах величезний, особливо з урахуванням активного впровадження технологічних інновацій, таких як шардінг, удосконалені механізми консенсусу, та розширення інструментів для розробників. Очікується, що з часом платформи стануть більш масштабованими, безпечними, та корисними для широкого спектра застосувань, від фінансових послуг до логістики та ідентифікації.

Розвиток децентралізованих фінансів (DeFi), незамінних токенів (NFT), та інших інноваційних додатків на блокчейні продовжує відкривати нові можливості для користувачів, інвесторів, та розробників. Платформи, що пропонують вдосконалену функціональність, вищу швидкість транзакцій, нижчі комісії, або кращі інструменти для створення додатків, можуть отримати конкурентну перевагу в цьому швидко зростаючому ринку.

Співпраця та стандартизація в блокчейн-індустрії можуть сприяти ще більшому розширенню інтероперабельності та взаємодії між різними платформами, спрощуючи інтеграцію блокчейн-технологій у традиційні індустрії та системи. Це може призвести до створення єдиної глобальної блокчейн-інфраструктури, яка забезпечуватиме безпечний, прозорий та ефективний обмін даними та активами.

Регулятивні виклики та ухвалення залишаються ключовими факторами, які впливають на подальший розвиток блокчейн-екосистем. Адаптація регулятивних рамок та створення сприятливого правового середовища можуть значно прискорити прийняття блокчейну в широкому масштабі, дозволяючи повною мірою реалізувати його потенціал у різних секторах.