ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження децентралізованих фінансів на основі EVM-сумісних блокчейнів для їх безпечного зберігання»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

(підпис)	Владислав ЗУБЕНКО *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД- 41

Владислав ЗУБЕНКО

Ім'я, ПРІЗВИЩЕ

Керівник: *Д.т.н., професор* Каміла СТОРЧАК

науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____

науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти бакалавр
Спеціальність Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Зубенку Владислав Віталійовичу
(прізвище, ім'я, по батькові здобувача)

1.Тема кваліфікаційної роботи: Дослідження децентралізованих фінансів на основі EVM-сумісних блокчейнів для їх безпечного зберігання

керівник кваліфікаційної роботи Каміла СТОРЧАК д.т.н, професор
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи:

1. Науково-технічна література з теми бакалаврської роботи.
2. Принцип функціонування децентралізованих фінансів.
3. Основні принципи роботи EVM-сумісних блокчейнів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Дослідити основні властивості децентралізованих фінансів.

2. Проаналізувати EVM-сумісні платформи.
3. Дослідити методи захисту.

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання: «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз науково-технічної літератури	08.04 - 12.04.2024	виконано
2	Написання вступу та постановка проблеми	13.04 - 16.04.2024	виконано
3	Аналіз основних концепцій децентралізованих фінансів	17.04 - 20.04.2024	виконано
4	Аналіз EVM-сумісних блокчейнів	20.04 - 23.04.2024	виконано
5	Дослідження загроз у сфері децентралізованих фінансів	24.04 - 29.04.2024	виконано
6	Оцінка безпеки та розробка рекомендацій	30.04 - 03.05.2024	виконано
7	Написання висновків та рекомендацій	04.05 - 06.05.2024	виконано
8	Оформлення дипломної роботи	06.05 - 07.05.2024	виконано

Здобувач(ка) вищої освіти _____ Владислав ЗУБЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Каміла СТОРЧАК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 80 стор., 12 рис., 50 джерел.

Мета дослідження - дослідження можливостей та ефективності використання децентралізованих фінансів на EVM-сумісних блокчейнах. Проаналізувати основні виклики та знайти ефективні заходи для забезпечення безпеки користувачів платформ.

Об'єкт дослідження – процес забезпечення безпеки в децентралізованих фінансах на основі EVM- сумісних блокчейнів.

Предмет дослідження - безпека в децентралізованих фінансах, зокрема загрози, методи захисту та технології, що використовуються для забезпечення безпеки на EVM-сумісних блокчейнах.

У рамках дослідження було здійснено детальний аналіз теоретичних основ децентралізованих фінансів, включаючи визначення основних понять, основні принципи та механізми функціонування. Проведено огляд EVM-сумісних блокчейнів з аналізом їх технологічних аспектів та особливостей безпеки. Основна частина дослідження зосереджена на загрозах та викликах, що стоять перед децентралізованими фінансами. Розглянуто сучасні технології та методи захисту, а також проведено аналіз конкретних випадків, що ілюструють практичні приклади впровадження рішень для забезпечення безпеки. На основі аналізу отриманих даних було висвітлено основні проблеми та вразливості безпеки в децентралізованих фінансах, а також розроблено конкретні рекомендації для покращення безпеки на EVM-сумісних платформах.

КЛЮЧОВІ СЛОВА: КРИПТОВАЛЮТА, ДЕЦЕНТРАЛІЗОВАНІ ФІНАНСИ, БЛОКЧЕЙН, EVM, БЕЗПЕКА, ЗАГРОЗИ, ETHEREUM, МЕТОДИ ЗАХИСТУ.

ABSTRACT

Textual part of the qualification work for obtaining a bachelor's degree: 80 pages, 12 figures, 50 sources.

The purpose of the study is to examine the security of decentralized finance with a focus on analyzing threats, protection methods, and developing recommendations to improve security on EVM-compatible platforms. The study aims to analyze the main challenges and propose effective measures to ensure the safety of platform users.

Object of research - the process of ensuring security in decentralized finance based on EVM-compatible blockchains.

The subject of the study is the security in decentralized finance, specifically the threats, protection methods, and technologies used to ensure security on EVM-compatible blockchains.

As part of the study, a detailed analysis of the theoretical foundations of decentralized finance was conducted, including the definition of key concepts, main principles, and mechanisms of functioning. An overview of EVM-compatible blockchains was carried out, analyzing their technological aspects and security features. The main part of the study focuses on the threats and challenges faced by decentralized finance. Modern technologies and protection methods were reviewed, and specific cases illustrating practical examples of implementing security solutions were analyzed. Based on the analysis of the obtained data, the main problems and vulnerabilities in decentralized finance security were highlighted, and specific recommendations improving security on EVM-compatible platforms were developed.

KEYWORDS: CRYPTOCURRENCY, DECENTRALIZED FINANCE, BLOCKCHAIN, EVM, SECURITY, ETHEREUM, PROTECTION METHODS.

ЗМІСТ

ВСТУП

Актуальність теми. Тема бакалаврської роботи - “Безпека в децентралізованих фінансах на EVM-сумісних блокчейнах” є вкрай актуальною в сучасному світі цифрових технологій та фінансів. З поширенням технології блокчейн та зростанням популярності децентралізованих фінансових платформ (DeFi), питання безпеки стає першочерговим. DeFi платформи пропонують інноваційні фінансові послуги без посередників, що значно розширює доступ до фінансових інструментів для широкого кола користувачів.

Однак, зростання використання DeFi платформ супроводжується збільшенням кількості кіберзагроз та атак, що може призвести до значних фінансових втрат. У такому контексті розробка надійних методів забезпечення безпеки на EVM-сумісних блокчейнах, таких як Ethereum, Binance Smart Chain та Polygon, є критично важливою для сталого розвитку децентралізованих фінансів.

Аналіз існуючих загроз та розробка ефективних методів захисту не лише сприятимуть покращенню безпеки користувачів, але й підвищать довіру до DeFi платформ. Крім того, дослідження у цій сфері дозволять студенту глибше зрозуміти технічні аспекти функціонування блокчейнів та розвинути навички у сфері кібербезпеки. Таким чином, тема безпеки в децентралізованих фінансах на EVM-сумісних блокчейнах є надзвичайно важливою та перспективною як для академічного дослідження, так і для практичного застосування у сучасних фінансових системах.

Об’єкт дослідження - процес забезпечення безпеки в децентралізованих фінансах на основі EVM-сумісних блокчейнів.

Предмет дослідження - безпека децентралізованих фінансів на основі EVM-сумісних блокчейнів.

Мета дослідження - дослідження можливостей та ефективності використання децентралізованих фінансів на EVM-сумісних блокчейнах для підвищення безпеки та оптимізації фінансових операцій. Вивчення технологічних аспектів функціонування EVM-сумісних блокчейнів та їх застосування в контексті децентарлізованих фінансів. Аналіз типових загроз та розробка методів забезпечення безпеки в системах. Оцінка ефективності використання сучасних технологій захисту для мінімізації ризиків та підвищення надійності децентралізованих фінансових платформ.

Відповідно до мети було поставлено наступні **завдання:**

- Охарактеризувати явище та поняття децентралізованих фінансів;
- Дослідити процес розвитку EVM-сумісних блокчейнів;
- Проаналізувати ключові EVM-сумісні платформи
- Проаналізувати ключові загрози та виклики безпеки в децентралізованих фінансах;
- Проаналізувати випадки атак у децентралізованих фінансах;
- Розробити рекомендації для покращення безпеки в децентралізованих фінансах.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ERC-20 - Ethereum Request for Comment 20.

ETH - Ethereum.

DeFi – Decentralized Finance.

EVM – Ethereum Virtual Machine.

BSC – Binance Smart Chain.

PoW – Proof of Work.

PoS – Proof of Stake.

dApp – Decentralized Application.

DEX – Decentralized Exchange.

NFT – Non-Fungible Token.

DAO – Decentralized Autonomous Organization.

TVL – Total Value Locked.

AMM – Automated Market Maker.

DLT – Distributed Ledger Technology

PoA – Proof of Authority

PoSA – Proof of Staked Authority

BNB – Binance Coin

ERC – Ethereum Request for Comments

1. ТЕОРЕТИЧНІ ОСНОВИ ДЕЦЕНТРАЛІЗОВАНИХ ФІНАНСІВ

Децентралізовані фінанси - це інноваційний сектор у межах фінансових технологій, який використовує блокчейн-технології для створення фінансових інструментів у формі децентралізованих додатків. Ці системи працюють без централізованих посередників, таких як банки або традиційні фінансові інституції, забезпечуючи прямий доступ до широкого спектру фінансових послуг [1].

Перші блокчейн-застосування були в основному обмежені криптовалютами, як-от Bitcoin, який надавав переваги у вигляді цифрових грошей без потреби у централізованому регулюванні. З появою Ethereum та його можливостями смарт-контрактів, з'явилася можливість створення більш складних фінансових інструментів, що відкрило двері для DeFi. Ці розробки дозволили користувачам здійснювати такі дії, як позики, страхування, торгівлю активами та керування портфелем без посередників [5].

Однією з ключових переваг DeFi є використання блокчейну, який надає транзакції високий рівень безпеки, прозорості та незмінності. Всі операції записуються в загальнодоступну базу даних, що знижує ризик шахрайства та покращує довіру між учасниками [2].

Незважаючи на переваги, DeFi стикається з рядом викликів, включаючи проблеми масштабування, волатильність цін на активи, а також потенційні регулятивні обмеження. Тим не менш, потенціал для подальшого розвитку є значним. DeFi може зробити революцію у фінансовому секторі, забезпечуючи більшу інклюзивність і доступність фінансових послуг на глобальному рівні [2].

1.1 Історія та розвиток децентралізованих фінансів

Фінансова криза 2008 року стала однією з найгірших економічних катастроф в історії. Типові проблеми в традиційних фінансових ринках, такі як асиметрична інформація та конфлікт інтересів, призвели до кризи, що підірвало довіру громадськості до фінансових ринків. Виникла потреба в кращій системі [1].

У тому ж році автор або група під псевдонімом Сатоші Накамото опублікували статтю, що описувала нову систему електронних готівкових розрахунків між рівними (peer-to-peer), Bitcoin. Сатоші Накамото вирішив проблему подвійного витрачання коштів та запровадив новий, бездовірний спосіб транзакцій між рівними. Обіцянка Bitcoin полягала в можливості здійснення прямих платежів від однієї сторони до іншої без потреби у фінансовому посереднику. Раніше ці фінансові посередники були необхідні через відсутність довіри між окремими сторонами, але тепер довіра здобувалась за допомогою криптографічних засобів [4].

Основна технологія за Bitcoin називалася блокчейн. Блокчейн - це вид технології розподіленого реєстру (DLT), який не може бути підробленим та є відкритим для всіх. Замість довіри до одного посередника для управління реєстром, реєстр розподіляється між кількома акторами, які підтверджують транзакції та їх порядок у блокчейні [5].

Люди швидко почали усвідомлювати потенціал технології та уявляти інші варіанти використання блокчейну. Молодий програміст на ім'я Віталік Бутерін помітив проблему з Bitcoin: він не мав можливості, крім простих валютних транзакцій. Бутерін хотів створити універсальну, тюрінг-повну систему, яка б могла б наслідувати обіцянки технології блокчейну, але в той же час служити платформою для нових видів децентралізованих додатків [6]. Іншою основною інновацією, необхідною для цього, були розумні контракти, які спочатку

запропонував Нік Сзабо у 1994 році. Розумні контракти - це комп'ютерні програми, які автоматично виконують попередньо визначені дії, коли виконуються певні умови [7]. Розумні контракти дозволяли проводити складні, багатоступеневі процеси, які Bitcoin не міг виконати. У 2013 році Бутерін опублікував білий папір для своєї "дитини" під назвою Ethereum.

Ethereum відкрив нові можливості для блокчейну. Тепер інноватори могли розробляти складні, децентралізовані застосунки, dApps, які використовували безпеку, відкритість технології блокчейну та складні автоматизовані процеси розумних контрактів. Ці децентралізовані застосунки функціонували б без потреби в людському втручанні[8].

1.2 Блокчейн Ethereum

Станом на квітень 2024 року, Ethereum є другою за величиною криптовалютною платформою після Bitcoin за ринковою капіталізацією та першою платформою, якщо дивитись на щоденні комісійні збори за транзакції. Також це перша платформа для DApps та обмінів DeFi. Її перший блок з'явився у 2015 році, що є відносно молодшим, ніж блокчейн Bitcoin [12].

Ethereum спирається на публічний блокчейн, де після оновлення мережі консенсус підтримується за допомогою системи PoS, на відміну від Bitcoin, який використовує систему PoW. Система PoS базується на принципі, за яким право на додавання блоків до блокчейну пропорційне до кількості криптовалюти, яку володіє та заставляє учасник мережі[9].

Рисунок 1.1 – Загальна ринкова капіталізація Ethereum станом на квітень 2024 року становить близько 375 мільярдів доларів США.

У певному сенсі, Ethereum є наступним логічним розширенням Bitcoin. Хоча Bitcoin чудово підходить для зберігання активів, він не має складних функціональних можливостей. Ви можете відправляти та отримувати транзакції та виконувати деякі інші критичні функції, але немає підтримки розумних контрактів. Ось тут на сцену виходить Ethereum.

Він надає наступні функції на додаток до того, що пропонує Bitcoin:

- DApps
- Складні розумні контракти
- Створення цифрових токенів

Коротко кажучи, основна ідея системи блокчейну Ethereum полягає в тому, що розробники можуть створювати та запускати код, який функціонує в розподіленій мережі, а не на централізованому сервері. І теоретично ці застосунки не можна закрити або цензурувати – вони децентралізовані та автономні [12].

Як зазначено вище, Ethereum дозволяє використовувати розумні контракти. Розумний контракт — це просто код. Код не є ні розумним, ні контрактом у звичайному розумінні. Він називається розумним оскільки він виконується за певних умов, і його можна вважати контрактом, оскільки він забезпечує дотримання домовленостей між сторонами [10].

Розумні контракти — це коди, що існують на блокчейні, вони можуть керувати активами та даними та визначати взаємодії між активами, даними та учасниками мережі. Платформи розумних контрактів дали поштовх до створення децентралізованих застосунків або DApps. Ці DApps створені з взаємосумісними, прозорими розумними контрактами, які продовжують існувати, доки існує блокчейн, на якому вони розташовані. DApps дозволяють учасникам взаємодіяти безпосередньо та усувають будь-яких посередників або необхідність для компанії/інституції діяти як центральний керівний орган [11].

DeFi можна визначити як рух, що сприяє використанню децентралізованих мереж і програмного забезпечення з відкритим кодом для створення різних типів фінансових послуг та продуктів. Ідея полягає в розробці та використанні DApps на основі прозорої та надійної архітектури, такої як відкриті блокчейни та інші протоколи типу "рівний з рівним". DeFi швидко розвивається та поступово забирає більшу частку ринку від традиційної фінансової екосистеми [13].

Підсумовуючи, блокчейн Ethereum є наступним логічним еволюційним кроком від простішої технології блокчейну Bitcoin. Він дозволяє використовувати розумні контракти, які є кодами, що виконуються в певних умовах. Це дозволяє розробляти DApps, і DApps, які зосереджені на фінансових продуктах, називаються DeFi. Рух DeFi переносить традиційні фінансові продукти та послуги до світу з відкритим кодом і децентралізації. Це усуває потребу в посередниках, знижує загальні витрати та значно покращує взаємосумісність [13].

1.3 Основні компоненти та функціонування DeFi

DeFi складається з набору інструментів і технологій, що забезпечують широкий спектр фінансових послуг на основі блокчейн-платформ, таких як Ethereum. Основні елементи DeFi включають [14]:

- Децентралізовані обміни (DEX): На відміну від традиційних бірж, DEX дозволяють користувачам торгувати криптовалютами безпосередньо між собою без необхідності довіряти свої кошти третій стороні. Це знижує ризики, пов’язані з крадіжками та шахрайством.
- Платформи кредитування: Ці системи дозволяють користувачам виставляти свої криптовалюти як заставу для отримання позик або надавати свої кошти в позику під відсотки. Все це відбувається автоматично за допомогою смарт-контрактів, що гарантує дотримання умов угоди обома сторонами.
- Стабільні валюти: Ці криптовалюти прив'язані до стабільних активів, як-от долар США, євро або золото, що дозволяє уникнути великої волатильності ринку криптовалют. Стабільні валюти є ідеальним рішенням для транзакцій, де необхідна стабільність вартості.
- Інвестиційні пули та фонди: Користувачі можуть інвестувати свої активи в колективні інвестиційні фонди, які управляються смарт-контрактами. Це дає можливість диверсифікувати інвестиції та знизити ризики, а також збільшити потенційний прибуток.

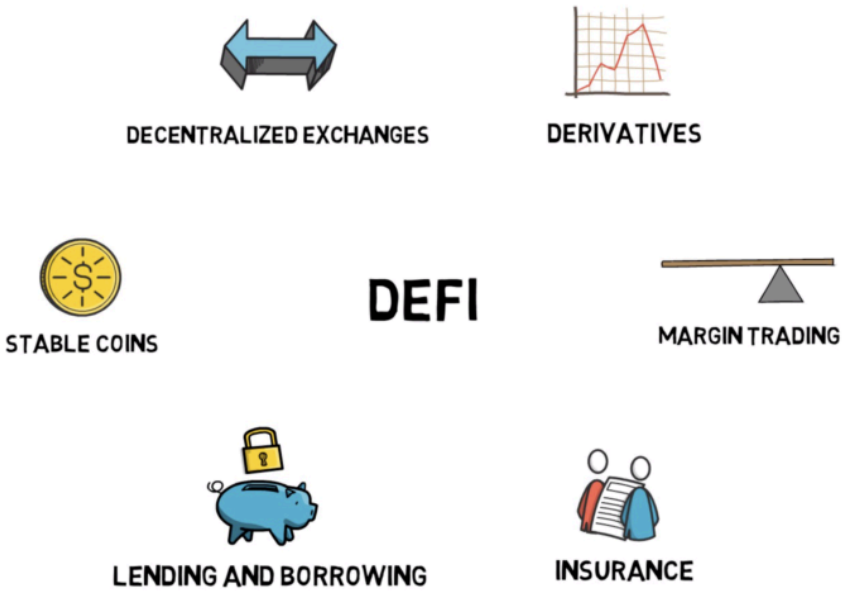


Рисунок 1.2 – Основні елементи DeFi

Децентралізовані фінанси працюють на основі блокчейну, де кожна транзакція або дія відбувається автоматично через смарт-контракти.

Смарт-контракти - це програми, які автоматично виконують угоди між сторонами на основі заданих умов. Вони забезпечують виконання фінансових операцій без необхідності залучення посередників, знижуючи вартість транзакцій та час на їх обробку.

Ці механізми та інструменти взаємодіють між собою, створюючи складну, але ефективну систему, яка може надавати фінансові послуги на новому рівні прозорості та доступності.

1.4 Властивості децентралізованих фінансів

DeFi пропонує набір ключових властивостей, які сьогодні не доступні в контексті традиційної фінансової економіки. У разі успіху, воно може мати

потенціал створити альтернативну фінансову систему, яка є більш децентралізованою, інноваційною, сумісною, прозорою та без кордонів. Більше того, цей рух підкреслює потенціал технології блокчейн у створенні нового набору бізнес-моделей, зосереджених на децентралізації [14].

1.4.1 Децентралізація

Одна з ключових властивостей DeFi вже закладена у самій назві – децентралізація. Коли централізовані фінансові інституції — такі як Citibank (або будь-який інший великий банк) чи онлайн-платіжні сервіси, як PayPal, домінують на ринку, вони накопичують непропорційну ринкову владу та великі прибутки. У централізованій фінансовій системі фінансові установи є основними посередниками, що ведуть переговори та контролюють фінансові транзакції.

На відміну від цього, у децентралізованій фінансовій системі транзакції здійснюються не централізованими установами, а децентралізованими мережами однорангових зв'язків по всьому світу - без необхідності втручання уряду або інституцій. Зменшуючи або повністю усуваючи участь централізованих установ, платформи DeFi можуть знижувати вартість транзакцій. Як тільки з'являються та набирають сили децентралізовані мережі однорангового зв'язку, кожен може взяти участь у системі для здійснення фінансових транзакцій. І все ж, жодна центральна особа не може монополізувати чи обмежувати мережу та виключати інших із участі. Децентралізація лежить в самому серці руху DeFi, на додаток до загальної технології блокчейну та декількох криптовалют [14].

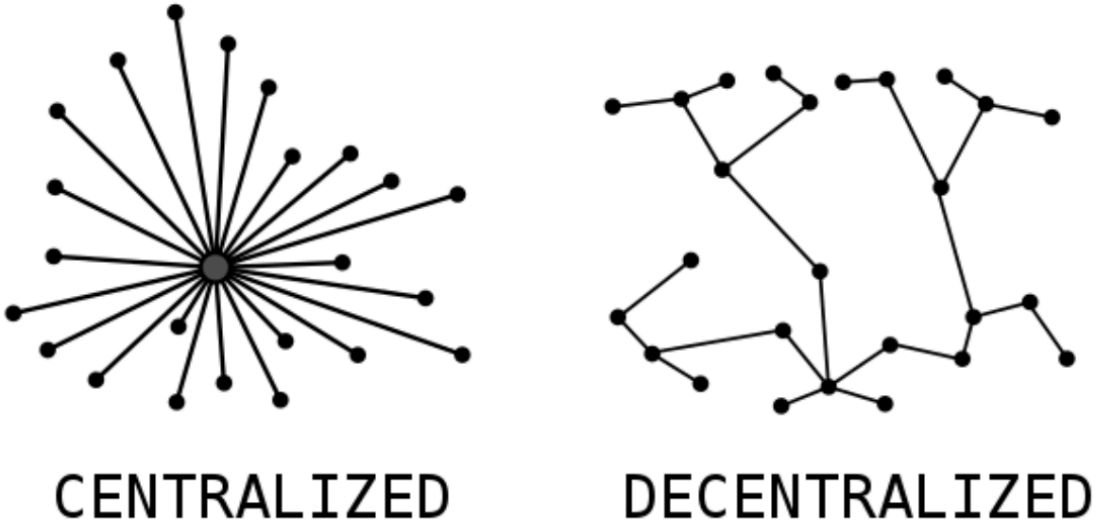


Рисунок 1.3 – Порівняння централізованих та децентралізованих мереж

1.4.2 Прозорість

Централізовані фінансові інституції не можуть мати повну прозорість, оскільки вони мають захищати свої централізовані активи. У контрасті до цього, DeFi забезпечує безпеку своїх публічних реєстрів через розподілений консенсус та фундаментальну прозорість. Воно використовує публічні записи, які легко переглянути та перевірити, і реєструє транзакції на публічних блокчейнах. Таким чином, сторони, що здійснюють транзакції, можуть взаємодіяти та довіряти один одному без попередніх відносин або посередника. Це може розширити масштаб та сферу потенційних транзакцій по всьому світу, оскільки розподілені реєстри створюють довіру.

Платформи DeFi також часто створюються з відкритим вихідним кодом. Це означає, що зовнішні сторони можуть перевіряти бізнес-логіку, виявляючи

приховані упередження, ризики та загрози. Крім того, прозорі публічні реєстри та відкритий вихідний код допомагають вести записи транзакцій [14].

1.4.3 Сумісність з іншими системами

Інституції в рамках традиційних фінансів схильні працювати на окремих, ізольованих платформах – це підвищує бар'єри для транзакцій. Різні фінансові інституції повинні підтримувати власні записи, тому одна фінансова послуга може не бути сумісною з іншою. Переміщення капіталу та активів між цими інституціями стає обтяжливим, трудомістким та дорогим. Натомість, DeFi побудовано на публічних блокчейнах з відкритими принципами, що збільшує сумісність між різними децентралізованими послугами. З високим рівнем сумісності фінансовий капітал та активи можуть безперешкодно пересуватися між різними сервісами та кордонами.

Хоча проекти, розроблені на одному публічному блокчейні, мають високий рівень сумісності, децентралізовані фінанси ще не досягли повної сумісності через відсутність сумісності між блокчейнами. Наразі багато проектів таких як Cosmos і Polkadot - працюють над перетинанням різних блокчейнів, щоб досягти повної сумісності в сфері децентралізованих фінансів [15].

1.5 Переваги та недоліки децентралізованих фінансових систем

Однією з основних революційних переваг, яку пропонує децентралізоване фінансування, є відкритий доступ до фінансових послуг. Цей аспект не просто розширює можливості традиційних фінансових систем, але й демократизує доступ до фінансових ресурсів на глобальному рівні.

Відкритий доступ у контексті DeFi означає, що будь-яка особа з інтернет-з'єднанням може взаємодіяти з фінансовими послугами без необхідності входу через традиційні фінансові інститути. Така система не

вимагає від користувачів проходження складних і часто дискримінаційних процедур перевірки, як це має місце у стандартних банківських системах. Вона не вимагає кредитної історії чи фізичної присутності для відкриття рахунку чи отримання кредиту[17].

Цей підхід має величезний вплив на фінансову інклюзивність, особливо в країнах, де доступ до традиційних банківських послуг є обмеженим. Люди в регіонах, що розвиваються, часто стикаються з відсутністю доступу до банківських послуг через відсутність необхідної інфраструктури або через неефективність фінансових установ. DeFi дозволяє таким особам взаємодіяти з економічними системами, інвестувати, зберігати заощадження та отримувати кредити без необхідності відвідування фізичного банку або іншої фінансової установи.

Центральним елементом, що дозволяє відкритий доступ, є використання блокчейн технологій та смарт-контрактів. Блокчейн забезпечує безпечну та незмінну базу даних транзакцій, тоді як смарт-контракти автоматизують фінансові угоди. Користувачі можуть виконувати транзакції, які автоматично обробляються на основі встановлених правил, без затримок або необхідності ручного втручання.

Незважаючи на значні переваги, відкритий доступ також має недоліки, зокрема забезпечення безпеки та приватності даних. Кібербезпека є критично важливою, оскільки системи, відкриті для широкого кола користувачів, можуть бути вразливими до атак. Також існує виклик у забезпеченні достатньої освіти та ресурсів для користувачів, які можуть бути не знайомі з технологією блокчейн.

Традиційні фінансові системи включають численні посередники, такі як банки, платіжні системи, брокери та інші фінансові установи, кожна з яких стягує комісію за свої послуги. В DeFi більшість цих операцій виконується автоматично за допомогою смарт-контрактів на блокчейні, що усуває

необхідність у таких посередниках. Це не тільки знижує комісійні витрати, але й прискорює виконання транзакцій[17].

Блокчейн-платформи забезпечують зниження операційних витрат завдяки своїм нативним характеристикам, таким як децентралізація та відсутність потреби в централізованих серверах або інфраструктурі. Вони вимагають значно менше ресурсів для обслуговування порівняно з традиційними фінансовими системами, де потрібна велика кількість персоналу, технологічної підтримки та інших ресурсів.

DeFi дозволяє розробникам легко створювати і запускати нові фінансові продукти через платформи, які підтримують смарт-контракти. Це включає інструменти які традиційні банки можуть вважати непрактичними або нерентабельними. Наприклад, автоматичні кредитні платформи, страхові продукти, засновані на криптовалютних індексах, та інвестиційні фонди, які користувачі можуть налаштовувати залежно від своїх ризиків і прибутковості[17].

DeFi розширює можливості для створення деривативів, які забезпечуються криптовалютами. Це включає ф'ючерси, опціони та інші комплексні фінансові інструменти, які дозволяють користувачам хеджувати ризики або спекулювати на змінах цін криптовалют. Ці інструменти допомагають розширити функціональність і ліквідність криптовалютного ринку.

DeFi сприяє створенню та управлінню децентралізованими автономними організаціями (DAO), які діють без централізованого керівництва. Ці організації можуть керувати активами, приймати управлінські рішення та автоматизувати операції через код, що забезпечує їхню діяльність в інтересах усіх учасників.

Хоча децентралізовані фінансові системи пропонують значні переваги, як і будь-яка інноваційна технологія, вони також мають ряд недоліків і викликів, які можуть вплинути на їхнє ширше прийняття та стабільність.

Один з основних недоліків DeFi пов'язаний з високою волатильністю криптовалют, які використовуються як основні активи в цих системах. Ціни на криптовалюти можуть дуже швидко змінюватися, що створює ризики для інвесторів та користувачів, особливо для тих, хто використовує DeFi для забезпечення кредитів або ведення бізнесу. Висока волатильність може призвести до раптових змін вартості застави та ліквідації позицій, що може виявитися катастрофічним для непідготовлених користувачів[17].

Смарт-контракти є фундаментальною частиною DeFi, дозволяючи автоматизувати виконання угод і управління активами без необхідності втручання третіх сторін. Однак, як і будь-яка технологія, смарт-контракти несуть в собі ризики, зокрема пов'язані з технічними помилками та вразливостями, які можуть мати серйозні наслідки[17].

Причини технічних помилок в смарт-контрактах:

- Помилки в коді: Смарт-контракти пишуться людьми, і помилки в програмуванні можуть призвести до серйозних вразливостей. Наприклад, неправильне використання змінних, логічні помилки, або неврахування певних умов може дозволити зловмисникам викрасти кошти або маніпулювати результатами контракту.
- Відсутність аудиту: Багато смарт-контрактів запускаються без належного аудиту коду, що збільшує ризик невиявлення помилок перед їх впровадженням у мережу. Аудит коду професійними фахівцями може значно знизити ризик вразливостей.
- Відсутність стандартів: Смарт-контракти розробляються різними командами, які можуть використовувати різні підходи та практики. Відсутність уніфікованих стандартів безпеки ускладнює перевірку та підтримку коду.

Забезпечення безпеки і надійності смарт-контрактів є ключовим для стабільного розвитку DeFi та збереження довіри користувачів і інвесторів у цю новітню і потенційно революційну технологію.

Регуляторна невизначеність є важливим викликом для сектора децентралізованих фінансів, оскільки швидкий розвиток цієї галузі часто випереджає можливості законодавчих та регуляторних органів реагувати на нові технології. Така невизначеність може створювати значні ризики для учасників ринку та обмежувати загальний потенціал розвитку DeFi[16].

У багатьох країнах ще не встановлені чіткі правила щодо використання криптовалют, проведення транзакцій через блокчейн, а також інших аспектів децентралізованих фінансових послуг. Це створює ряд проблем: від визначення правового статусу криптовалют і діяльності DeFi платформ до застосування податкових законів. Така правова невизначеність може змусити деяких інвесторів уникати участі в DeFi проектах, оскільки вони не можуть бути впевнені в юридичних наслідках своїх інвестицій.

Більше того, різні підходи до регуляції у різних юрисдикціях можуть призводити до конфліктів законодавства, що ускладнює міжнародну діяльність DeFi компаній. Наприклад, платформа, яка працює легально в одній країні, може порушувати закони іншої країни, що створює правові ризики для користувачів із різних держав.

Також, регуляторна невизначеність ускладнює захист прав споживачів. Без чітких регуляцій, користувачі DeFi можуть залишитися без захисту в разі шахрайства, втрати активів через хакерські атаки або невиконання обов'язків контрагентами. Це збільшує важливість наявності внутрішніх механізмів управління ризиками та процедур безпеки на DeFi платформах.

Нарешті, регуляторна невизначеність може обмежувати інновації. Хоча DeFi сприяє розвитку нових фінансових продуктів і технологій, відсутність чітких регулятивних рамок може стримувати інвестиції в дослідження і

розробку нових рішень, оскільки компанії та розробники не можуть бути впевнені, що їхні продукти будуть законними або залишатимуться законними в майбутньому.

Децентралізовані фінансові системи пропонують багато інноваційних можливостей, але водночас стикаються з кількома важливими бар'єрами, які можуть ускладнювати їх використання звичайними користувачами. Ці бар'єри включають технічні складнощі, високі вимоги до знань у сфері криптовалют та блокчейну, а також певні регуляторні та психологічні аспекти[17].

Децентралізовані фінансові продукти часто мають складні інтерфейси, що вимагають від користувачів глибокого розуміння того, як функціонують блокчейни та смарт-контракти. Наприклад, для використання DeFi платформ необхідно знати особливості гаманців для криптовалют, розуміти, що таке витрати на комісії, і як це може вплинути на вартість транзакцій.

Для ефективного використання DeFi необхідні специфічні знання в галузі криптовалют. Багатьом новим користувачам складно зрозуміти концепції підтвердження транзакцій, майнінгу, стейкінгу та інших аспектів блокчейн технологій. Навчальні ресурси часто розкидані або занадто технічні, що робить DeFi недоступним для широкої аудиторії.

Регуляторні вимоги можуть бути незрозумілими або змінними, особливо в міжнародному контексті, де різні країни мають різні правила щодо використання криптовалют і проведення фінансових операцій. Це створює правову невизначеність, яка може стримувати користувачів від участі у DeFi.

2. ОГЛЯД EVM-СУМІСНИХ БЛОКЧЕЙНІВ

2.1 Особливості та можливості EVM-платформ

Ethereum Virtual Machine є віртуальною машиною, створеною як центральний компонент архітектури Ethereum, що дозволяє виконувати смарт-контракти. Її ключова роль полягає у забезпеченні платформи для виконання коду смарт-контрактів незалежно від зовнішнього програмного та апаратного забезпечення, що забезпечує високий рівень безпеки та стандартизації у всій мережі.

EVM можна уявити як замкнену систему, яка має власний набір інструкцій та внутрішній стан. Вона працює аналогічно до фізичної комп'ютерної системи, але її виконання повністю ізольоване від хост-машини або інших віртуальних машин у мережі. Це гарантує, що дії смарт-контракту не можуть безпосередньо вплинути на оперативну систему або дані інших контрактів.

В EVM стек є ключовим компонентом для зберігання тимчасових даних під час виконання смарт-контрактів. Це структура даних, яка працює за принципом Last In, First Out, де останній елемент, доданий до стеку, буде першим елементом, що вилучається з нього.

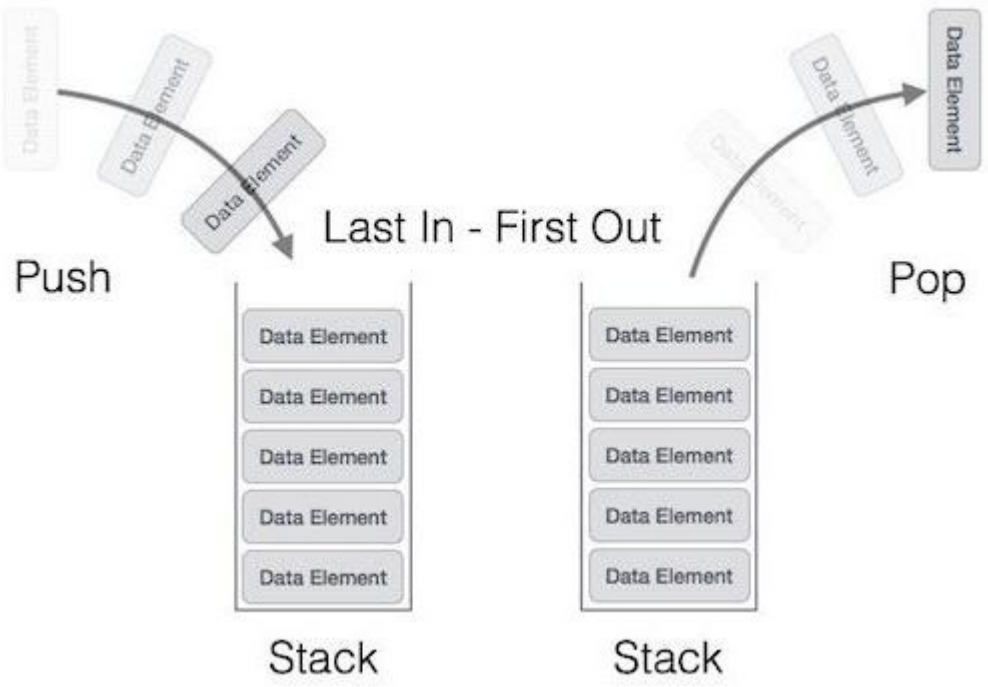


Рисунок 2.1 – Візуалізація роботи стеку

Під час виконання смарт-контрактів, стек використовується для зберігання та вилучення тимчасових даних, таких як значення для арифметичних операцій. Кожна операція використовує газ, тому оптимальне використання стеку може допомогти зменшити загальну вартість виконання смарт-контрактів.

Стек є важливим засобом для забезпечення безпеки та ефективності в EVM. Обмеження на розмір стеку допомагає запобігти переповненню буфера та іншим помилкам програмування, що можуть призвести до вразливостей безпеки. Розуміння та оптимальне використання стеку є критичними аспектами при розробці безпечних та ефективних смарт-контрактів на Ethereum [18].

Пам'ять у EVM виконує критичну функцію зберігання тимчасових даних під час виконання смарт-контрактів. Цей компонент є лінійним і динамічно розширюваним, що означає, що обсяг пам'яті може збільшуватися відповідно до потреб смарт-контракту. Пам'ять ініціалізується як порожня при кожному

запуску смарт-контракту і очищається після завершення його виконання, що забезпечує ізоляцію між окремими виконаннями.

Розширення пам'яті вимагає споживання газу, який є мірою вартості виконання операцій у Ethereum. Це обмеження сприяє оптимізації коду, оскільки розробники прагнуть мінімізувати використання пам'яті для зниження загальних витрат на газ. Тимчасовий характер пам'яті гарантує, що жодні дані не зберігаються довше, ніж необхідно для одного виконання, що підвищує безпеку шляхом усунення витоку або неправильного використання даних.

Пам'ять використовується для зберігання даних, які потрібно швидко обробляти, наприклад, для арифметичних операцій у контрактах. Таке використання забезпечує ефективність в порівнянні з операціями з постійним сховищем, які можуть бути дорожчими та повільнішими [18].

Сховище в EVM відіграє важливу роль у зберіганні довгострокового стану смарт-контрактів. Відрізняючись від тимчасової пам'яті EVM, яка очищається після завершення виконання кожного контракту, сховище забезпечує постійне зберігання даних, що необхідні для функціонування децентралізованих додатків на Ethereum.

Сховище представляє собою структуру даних типу "ключ-значення", де кожен смарт-контракт має свою ізольовану область сховища. Ця область може бути використана для зберігання різноманітних типів даних, таких як баланси користувачів, результати обчислень та інші станові змінні, які мають зберігатися між транзакціями.

Кожна операція запису в сховище вимагає витрати певної кількості газу, що є внутрішньою валютою Ethereum для вимірювання вартості виконання операцій. Запис у сховище є значно дорожчим порівняно з читанням, що змушує розробників оптимізувати використання сховища, щоб мінімізувати вартість виконання контрактів.

Безпека сховища є важливим аспектом, адже воно містить чутливі та важливі дані. Ethereum використовує складні криптографічні механізми, включаючи хешування та шифрування, для забезпечення безпеки даних, збережених у сховищі. Це допомагає запобігти несанкціонованому доступу та маніпуляціям з даними [19].

Програмний лічильник (PC) в EVM відіграє важливу роль у керуванні послідовністю виконання інструкцій смарт-контрактів. Цей компонент EVM визначає, яка інструкція має виконуватися наступною, гарантуючи, що всі операції виконуються у правильному порядку та відповідно до логіки смарт-контракту.

Програмний лічильник ініціалізується на початку кожного виклику смарт-контракту, зазвичай на нуль, що вказує на першу інструкцію в байт-коді контракту. З кожною виконаною інструкцією, значення програмного лічильника збільшується на одиницю або більше, в залежності від того, чи включає інструкція перехід на іншу операцію в коді.

Цей механізм дозволяє EVM контролювати виконання складних операцій і гарантувати, що кожен крок у виконанні смарт-контракту є передбачуваним та відтворюваним. Завдяки програмному лічильнику, EVM може точно виконувати складні інструкції, що вимагають розгалужень або умовних переходів, що є основою для реалізації логіки смарт-контрактів.

Важливою особливістю програмного лічильника є його взаємодія з газом — кожна операція, що виконується EVM, витрачає певну кількість газу. Програмний лічильник допомагає визначити вартість виконання контракту, рахуючи кількість операцій, що були виконані [20].

Програмний лічильник в EVM керує потоком виконання, вказуючи на поточну інструкцію, яка має бути оброблена. Це дозволяє EVM послідовно переходити від однієї інструкції до іншої, виконуючи операції, які можуть

включати математичні обчислення, зміни стану, управління пам'яттю та багато іншого.

Операції під час виконання контракту маніпулюють даними в стеку та пам'яті для тимчасового зберігання даних, а також оновлюють стан сховища для збереження довгострокових змін. Всі ці компоненти тісно інтегровані та спільно працюють, щоб забезпечити надійне і безпечне виконання контрактів [20].

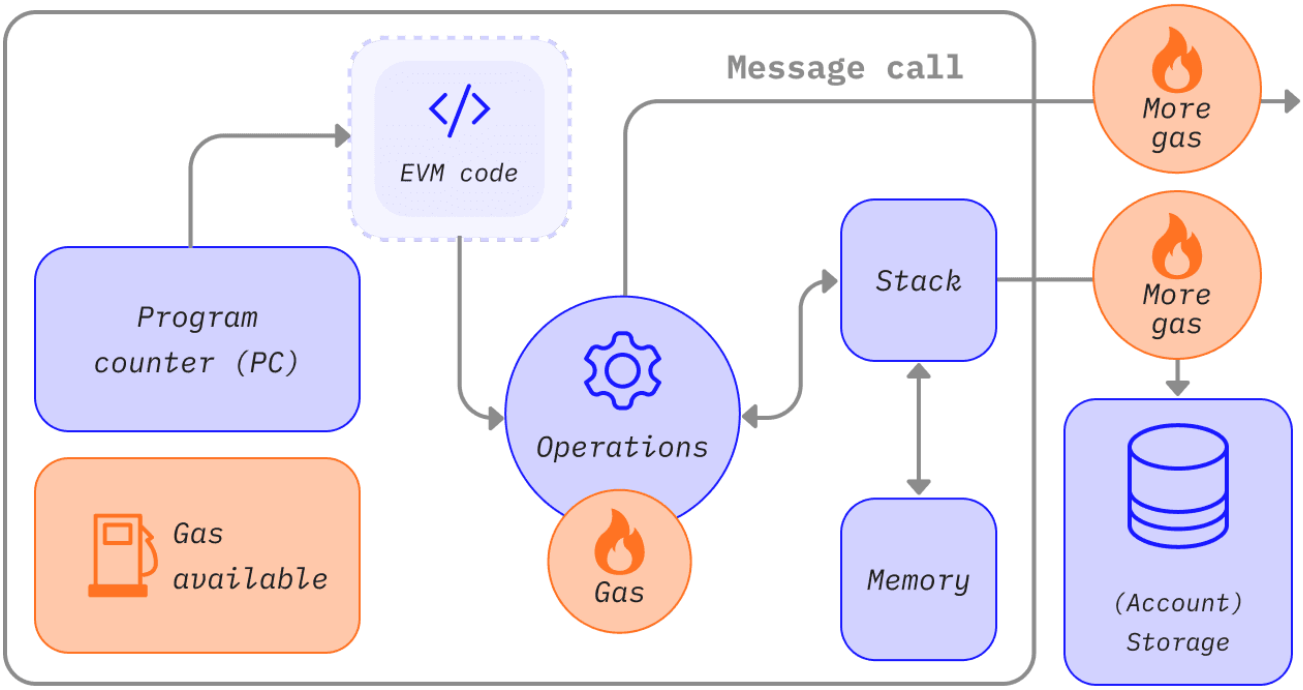


Рисунок 2.2 – Взаємодія основних компонентів EVM

EVM забезпечує ізоляцію виконання кожного смарт-контракту, використовуючи механізм віртуальної машини, який відділяє код та дані контракту від основної системи та інших контрактів. Це означає, що виконання одного контракту не може безпосередньо вплинути на виконання іншого контракту або на основний блокчейн, що запобігає можливим помилкам або атакам.

Кожен смарт-контракт має власне середовище виконання з ізольованими просторами пам'яті та сховища, що дозволяє контролювати доступ до чутливих даних та управління станами без ризику для інших компонентів системи. Ця модель ізоляції також сприяє безпеці, оскільки зловмисники не можуть прямо використовувати вразливості одного контракту для атак на інші контракти або на сам блокчейн [18].

Ці криптографічні методи не тільки забезпечують безпеку і цілісність даних в Ethereum, але й дозволяють підтримувати децентралізовану та прозору природу системи, яка є критичною для довіри та прийняття на ширшому ринку. Використання сучасних криптографічних технологій допомагає забезпечити, що Ethereum залишається однією з найбезпечніших та найнадійніших блокчейн-платформ [21].

Сумісність з мовами програмування в Ethereum Virtual Machine відіграє важливу роль у розширенні можливостей розробників та забезпеченні доступності платформи для широкої аудиторії. EVM підтримує кілька мов програмування, що робить її привабливою для різноманітних розробників з різними навичками і досвідом.

Основною мовою для написання смарт-контрактів на Ethereum є Solidity, яка є об'єктно-орієнтованою мовою, спеціально розробленою для створення та реалізації смарт-контрактів. Solidity має синтаксис, який нагадує JavaScript, що робить її доступною для широкого кола розробників. Крім того, Solidity дозволяє розробникам формулювати складні правила та виконувати їх автоматично через смарт-контракти, що виконуються на EVM [19].

Для більш широкої сумісності та гнучкості, EVM також підтримує інші мови, такі як Vyper, яка є більш спрямованою на безпеку та зрозумілість, забезпечуючи більш чистий і безпечний код для фінансових додатків. Vyper відмовляється від деяких аспектів Solidity в ім'я збільшення безпеки та простоти, що важливо для створення надійних і безпечних додатків [22].

Це є однією з ключових переваг, яку надає Ethereum Virtual Machine. Ця характеристика дозволяє розробникам легко переміщати та використовувати смарт-контракти на різних блокчейн-платформах, які сумісні з EVM, без необхідності вносити значні зміни в код.

Портабельність у EVM відкриває значні можливості для розробників, оскільки вони можуть розробляти додатки на одній платформі, наприклад Ethereum, а потім легко переносити їх на інші блокчейни, такі як Binance Smart Chain або Polygon, які також підтримують EVM. Це забезпечує значну економію часу та ресурсів, оскільки видаляє необхідність повторної розробки та тестування для кожної окремої платформи.

Крім того, портабельність сприяє більшій стандартизації в блокчейн-індустрії. Завдяки сумісності між різними платформами, розробники можуть використовувати загальноприйняті практики та інструменти, сприяючи розповсюдженню найкращих методів та підвищенню загальної якості додатків. Це також полегшує співпрацю між розробниками, оскільки код, розроблений для однієї платформи, може бути легко перевірений і адаптований колегами, які працюють на інших платформах.

Висока портабельність також важлива для забезпечення тривалої підтримки та обслуговування додатків. У світі, де технологічне середовище швидко змінюється, можливість адаптувати додатки до нових платформ або оновлених версій існуючих платформ без значних затрат є великою перевагою [19].

2.2 Аналіз ключових EVM-сумісних блокчейнів

2.2.1 Binance Smart Chain

Binance Smart Chain є високопродуктивною блокчейн-платформою, яка була запущена компанією Binance у вересні 2020 року. BSC забезпечує високу

швидкість транзакцій і низькі витрати, зберігаючи при цьому сумісність з EVM, що дозволяє легко переносити та запускати смарт-контракти, створені для Ethereum без необхідності значних змін у коді.

BSC працює паралельно з Binance Chain, основною блокчейн-платформою Binance, створеною для високошвидкісної торгівлі. Дволанцюгова структура дозволяє користувачам переміщати активи між двома блокчейнами з мінімальними затримками. Binance Chain забезпечує швидкі транзакції та низькі витрати, тоді як BSC підтримує складні смарт-контракти та dApps [24].

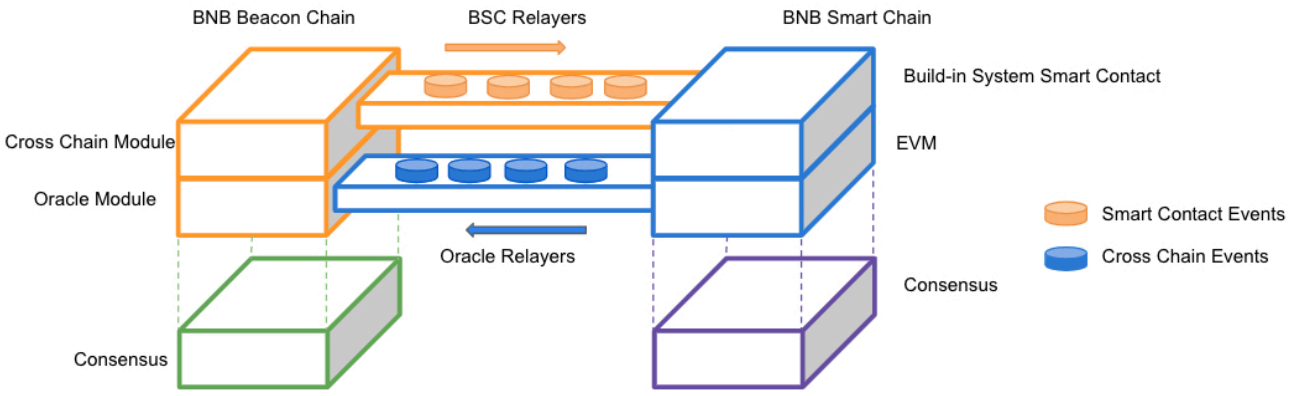


Рисунок 2.3 – Зображення дволанцюгової структури

BSC використовує гібридний консенсусний механізм Proof of Staked Authority, який поєднує елементи Proof of Stake і Proof of Authority. У цьому механізмі валідатори вибираються на основі кількості BNB, яку вони поставили, і їхньої репутації. PoSA забезпечує високу продуктивність і низькі витрати на транзакції, зберігаючи децентралізований характер мережі [25].

BSC досягає значно меншого часу створення блоку порівняно з Ethereum – приблизно 3 секунди на блок. Це забезпечує високу швидкість обробки транзакцій і швидкий час підтвердження. Завдяки швидкому створенню блоків і оптимізації консенсусного механізму, BSC здатна обробляти велику кількість транзакцій за секунду, що значно перевищує пропускну здатність Ethereum. Це

робить BSC привабливою платформою для децентралізованих фінансів (DeFi) та інших додатків, які потребують високої продуктивності.

Однією з найбільших переваг BSC є низькі витрати на газ для виконання транзакцій і смарт-контрактів. Це значно знижує витрати користувачів і розробників, роблячи платформу економічно вигідною для широкого кола застосувань.

У PoS консенсусному механізмі учасники мережі можуть ставити свої токени для участі у валідації транзакцій. Чим більше токенів користувач ставить, тим більше шансів він має бути обраним як валідатор для створення нового блоку. Цей підхід стимулює валідаторів діяти чесно, оскільки неправильна поведінка може призвести до втрати їхніх ставок [11].

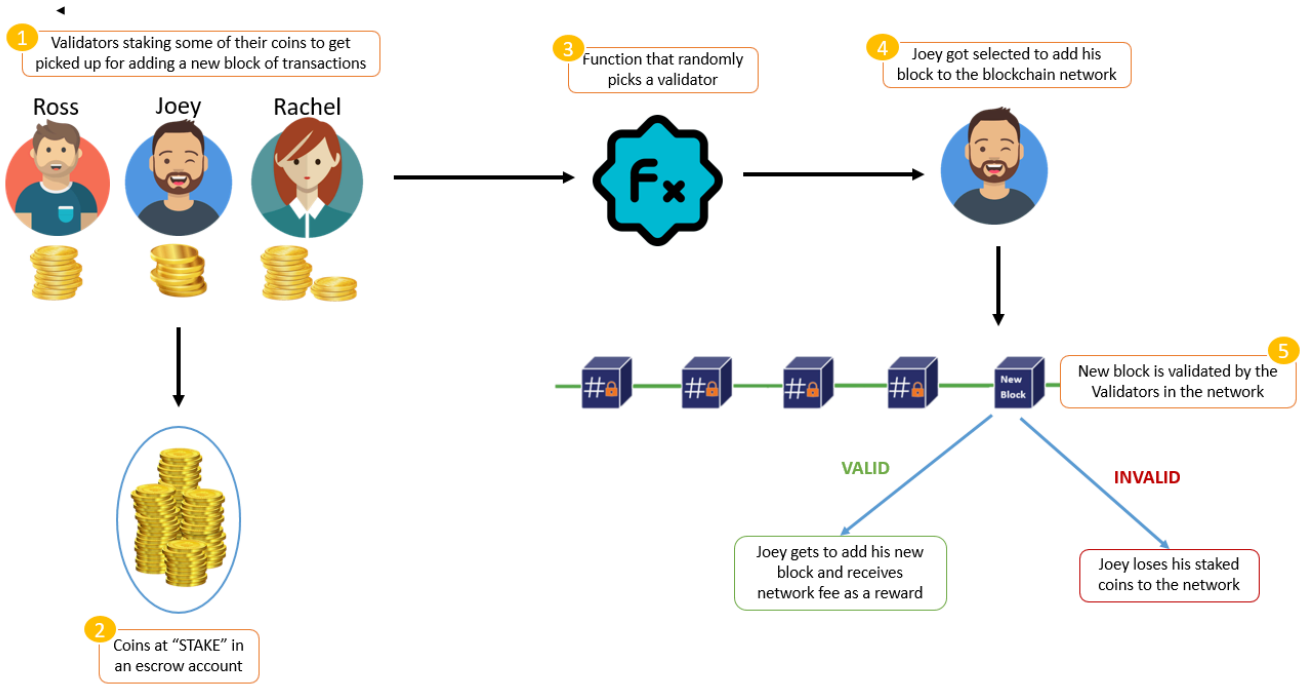


Рисунок 2.4 – Візуалізація роботи консенсусу PoS

PoA передбачає, що певні вузли в мережі отримують право валідувати транзакції та створювати нові блоки на основі їхньої репутації та довіри. Ці

вузли, відомі як авторитети, обираються на підставі суворих критеріїв і їхня ідентичність має бути підтверджена [26].

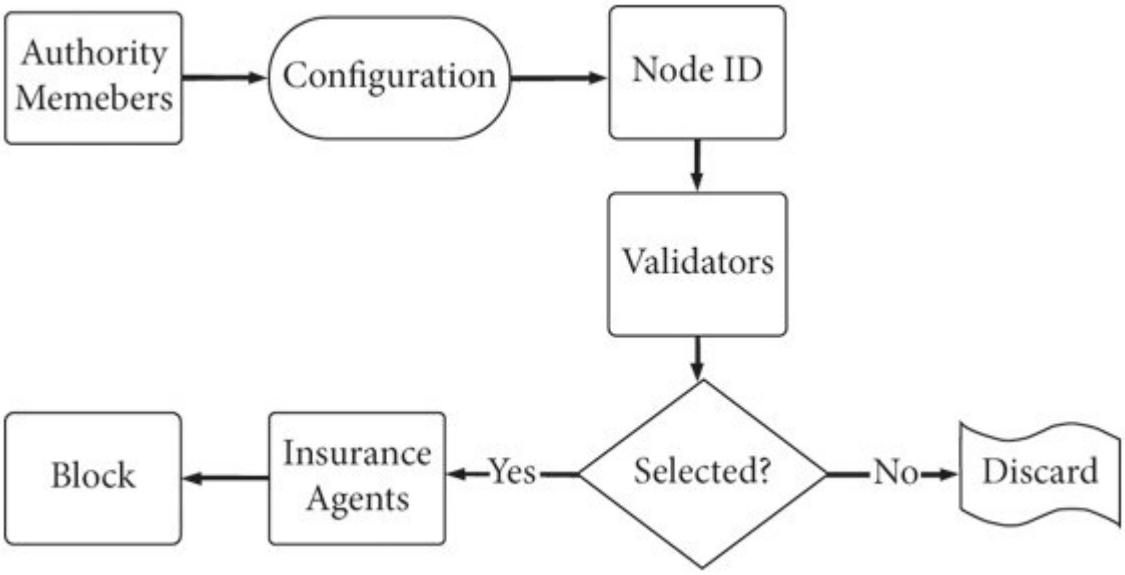


Рисунок 2.5 – Візуалізація роботи консенсусу PoA

BSC об'єднує ці два механізми, створюючи PoSA, який включає кращі риси обох методів. У PoSA, учасники можуть ставити свої токени BNB для участі у процесі валідації. Проте, замість відкритого вибору валідаторів, як у PoS, BSC використовує обмежену кількість валідаторів, що були обрані на підставі їхньої репутації та кількості поставлених токенів.

Кількість валідаторів у BSC зазвичай обмежена 21 валідатором, які обираються кожні 24 години з учасників, що ставлять свої BNB. Цей обмежений набір валідаторів забезпечує швидкий і ефективний процес валідації транзакцій.

Вибрані валідатори несуть відповідальність за створення нових блоків і валідацію транзакцій протягом визначеного періоду.

Система PoSA стимулює валідаторів діяти чесно за допомогою винагороди у вигляді транзакційних зборів та нових токенів. У разі виявлення шахрайства або неналежної поведінки валідатори можуть втратити частину або всю свою ставку, що служить додатковим запобіжним заходом для підтримання цілісності мережі [28].

BSC є однією з найпопулярніших блокчейн-платформ однак, як і будь-яка технологія, вона має свої переваги та недоліки. Переваги Binance Smart Chain:

- Низькі транзакційні витрати: BSC пропонує значно нижчі комісії за транзакції порівняно з Ethereum. Це досягається завдяки використанню механізму консенсусу PoSA.
- Висока продуктивність: завдяки короткому часу створення блоків, BSC може обробляти велику кількість транзакцій за одиницю часу.
- Сумісність з EVM: одна з ключових переваг BSC – це повна сумісність з EVM, що дозволяє розробникам легко переносити смарт-контракти з Ethereum на BSC без значних змін у коді.
- Широка підтримка та екосистема: BSC активно підтримується Binance, однією з найбільших криптовалютних бірж у світі. Це забезпечує стабільність та постійне вдосконалення платформи.

Недоліки Binance Smart Chain:

- Централізація: незважаючи на децентралізовану природу блокчейн-технології, BSC часто критикують за відносно високу ступінь централізації. Кількість валідаторів у мережі обмежена, і значна частина контролю належить Binance. Це може створювати ризики, пов'язані з концентрацією влади та впливом однієї організації на функціонування мережі.
- Залежність від Binance: BSC значною мірою залежить від інфраструктури та підтримки Binance. Хоча це забезпечує швидке впровадження нових

функцій та стабільність, будь-які проблеми або зміни у політиці Binance можуть мати значний вплив на функціонування та розвиток BSC.

На кінець 2023 року загальна вартість заблокованих активів на BSC досягла $4.6 мільярдів, що становить значне зростання у 33% квартал до кварталу. Це свідчить про стабільність і привабливість платформи для користувачів та розробників DeFi-додатків [29].

BSC продовжує демонструвати високу активність, досягаючи рекордних показників у 32 мільйони транзакцій на день і 2000 транзакцій за секунду. Це перевищує більшість інших блокчейнів за цими показниками, що підкреслює продуктивність і ефективність BSC [30].

Кількість активних користувачів на BSC залишається стабільно високою. У 2023 році BSC досягла 1 мільйона щоденних активних користувачів, що робить її однією з найпопулярніших блокчейн-платформ для децентралізованих додатків [31].

2.2.2 Polygon

Polygon (раніше відомий як Matic Network) є однією з провідних платформ, що надає рішення для масштабування та інфраструктури для розвитку на основі блокчейну Ethereum. У контексті швидкого зростання популярності DeFi, NFT та інших dApps, питання масштабування та ефективності стали надзвичайно важливими. Ethereum, як найбільш поширена платформа для розробки смарт-контрактів, зіштовхнулася з проблемами високих транзакційних витрат та низької пропускної спроможності [33].

Основна мережа Polygon використовує консенсусний механізм PoS, який є ефективнішою та екологічнішою альтернативою механізму PoW. В PoS, валідатори ставлять свої токени MATIC як заставу для підтвердження транзакцій і забезпечення безпеки мережі.

Основна мережа Polygon тісно пов'язана з основною мережею Ethereum, що забезпечує високу безпеку і стабільність системи. Це досягається через механізм контрольних точок, коли певні стани бічних ланцюгів та Layer 2 рішень періодично зберігаються в основній мережі Ethereum. Це дозволяє забезпечити відкат у разі виникнення проблем або атак на бічні ланцюги, захищаючи цілісність та безпеку мережі.

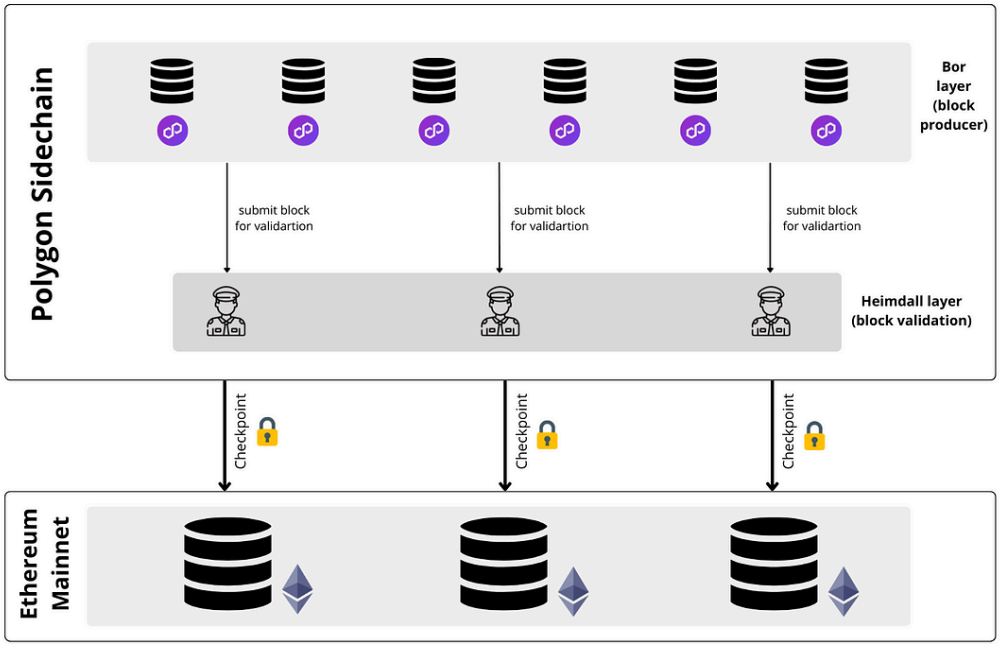


Рисунок 2.6 – Реалізація консенсусу PoS від Polygon

Система PoS в основній мережі Polygon дозволяє не тільки валідаторам, але й іншим учасникам мережі брати участь у процесі консенсусу через делегування. Користувачі можуть делегувати свої токени MATIC валідаторам, підтримуючи їхню ставку та підвищуючи шанси валідатора бути обраним для валідації блоків. У свою чергу, делегатори отримують частку винагороди валідатора, що стимулює їх брати участь у підтримці мережі.

Бічні ланцюги є однією з ключових технологій, що забезпечують масштабованість і ефективність блокчейн-платформи Polygon. Цей підхід

дозволяє обробляти транзакції поза основною мережею, що значно знижує навантаження на основний блокчейн і забезпечує високу швидкість транзакцій з мінімальними витратами.

Хоча бічні ланцюги функціонують незалежно, вони повністю інтегровані з основною мережею Ethereum через механізми мостів. Ці мости дозволяють безпечно пересилати активи, такі як токени або інші дані, між основною мережею та бічними ланцюгами. Така інтеграція забезпечує збереження цілісності і безпеки активів, а також забезпечує безперервність операцій між різними мережами [34].

Переваги бічних ланцюгів:

- Масштабованість: Бічні ланцюги забезпечують значне збільшення пропускної спроможності мережі, дозволяючи обробляти тисячі транзакцій за секунду.
- Зниження вартості транзакцій: Оскільки бічні ланцюги вимагають меншої кількості ресурсів для валідації транзакцій, вартість транзакцій на них суттєво нижча, ніж у основній мережі.
- Гнучкість: Розробники можуть створювати бічні ланцюги зі спеціалізованими правилами і логікою, що відповідають конкретним потребам їхніх додатків.

Використання бічних ланцюгів також пов'язане з деякими викликами. Зокрема, необхідність забезпечення безпеки мостів між ланцюгами може створювати потенційні вектори атак. Крім того, розробка і підтримка додаткових ланцюгів вимагає додаткових ресурсів і складностей у управлінні.

Загалом, бічні ланцюги Polygon відіграють критичну роль у вирішенні проблем масштабованості Ethereum, забезпечуючи ефективне та економічне рішення для розробників та користувачів блокчейн-додатків [35].

Polygon вирізняється серед блокчейн-платформ своїми передовими механізмами забезпечення безпеки. Це критично важливо, оскільки платформа

прагне надати масштабовані рішення для Ethereum без компромісів у безпеці. Наступні аспекти підкреслюють ключові елементи безпеки у Polygon.

Однією з основних переваг безпеки Polygon є те, що вона використовує основну мережу Ethereum для валідації транзакцій. Це означає, що хоча транзакції обробляються на бічних ланцюгах, вони також періодично забезпечуються та валідуються основною мережею Ethereum. Це використання дворівневої валідації допомагає забезпечити безпеку та цілісність даних у мережі Polygon.

Унікальною особливістю безпеки в Polygon є її здатність використовувати вторинні рівні перевірки, де валідатори на бічних ланцюгах і в Layer 2 рішеннях проводять додаткові перевірки транзакцій. Це додає ще один рівень захисту, перш ніж транзакції будуть остаточно підтверджені [34].

Переваги блокчейн-платформи Polygon:

- Висока масштабованість: Однією з найважливіших переваг Polygon є його здатність масштабувати додатки, що виконуються на Ethereum. Завдяки використанню бічних ланцюгів та технологій Layer 2, таких як zk-Rollups та Optimistic Rollups, Polygon забезпечує значне зменшення навантаження на основну мережу, що дозволяє обробляти значно більшу кількість транзакцій за секунду [36].
- Знижені витрати на транзакції: Використання бічних ланцюгів та рішень другого рівня дозволяє значно знизити вартість транзакцій у порівнянні з основною мережею Ethereum, що робить Polygon особливо привабливим для додатків з великою кількістю мікротранзакцій [36].
- Сумісність з EVM: Повна сумісність з EVM робить Polygon ідеальним вибором для розробників, які бажають використовувати існуючі інструменти, бібліотеки та рамки Ethereum без необхідності вносити зміни до коду своїх додатків.

- Швидкість транзакцій: Оптимізовані механізми консенсусу та обробки даних на бічних ланцюгах забезпечують швидке виконання транзакцій, що є критично важливим для додатків, які вимагають високої продуктивності, таких як ігри на блокчейні та децентралізовані біржі [36].

Недоліки блокчейн-платформи Polygon:

- Залежність від Ethereum: Незважаючи на свої переваги, Polygon все ще залежить від інфраструктури Ethereum, що означає, що будь-які проблеми або обмеження в основній мережі можуть негативно вплинути на продуктивність та стабільність додатків на Polygon.
- Складність інтеграції: Хоча Polygon забезпечує інструменти та фреймворки для спрощення розробки, інтеграція багаторівневої архітектури та управління бічними ланцюгами може бути складною для нових розробників або для проектів з обмеженими технічними ресурсами.
- Новизна технологій: Деякі з рішень, які використовує Polygon для масштабування, ще знаходяться на ранніх стадіях розвитку і можуть мати недосліджені ризики або потенційні вади, що може стати бар'єром для їх широкого прийняття [36].

2.3 Технічна інфраструктура EVM-сумісних платформ

У центрі розгляду EVM-сумісних блокчейнів лежить не лише їхня здатність підтримувати розподілені додатки через смарт-контракти, але й ефективність, з якою ці системи можуть обробляти та валідувати транзакції. Ключ до розуміння їх успіху та вразливостей криється в технічних аспектах їхньої архітектури. Важливість цих аспектів полягає не лише в забезпеченні безперервної роботи та безпеки, але й в можливості впровадження інновацій, які можуть розширити можливості та застосування блокчейн технологій.

2.3.1 Валідація транзакцій

Валідація транзакцій є критично важливим процесом у будь-якій блокчейн-мережі, оскільки вона забезпечує цілісність, безпеку та довіру до системи. Цей процес полягає у перевірці транзакцій перед їх додаванням до блоку, щоб переконатися, що вони відповідають всім встановленим правилам мережі. Валідація допомагає запобігти таким проблемам, як подвійні витрати, махінації або несанкціоновані зміни в ланцюжку [5].

Процес валідації включає кілька ключових етапів:

- Валідатори перевіряють, що цифровий підпис, який супроводжує кожну транзакцію, відповідає публічному ключу відправника, тим самим підтверджуючи, що відправник є законним власником коштів, які він намагається передати.
- Перевірка, що у відправника є достатньо коштів для здійснення транзакції. Це запобігає спробам подвійних витрат, коли одні і ті ж кошти намагаються витратити декілька разів.
- Транзакції повинні відповідати всім правилам мережі, включаючи структуру даних та валідність виконання смарт-контрактів, якщо такі існують.

Технічний процес валідації транзакцій у блокчейнах починається з ініціації транзакції користувачем. Користувач вводить необхідні параметри, такі як адреса отримувача, сума переказу і комісія за транзакцію. Він також може включати додаткові дані, особливо якщо транзакція включає виклик смарт-контракту. Після введення всієї необхідної інформації, користувач структурує транзакцію у відповідний формат та підписує її використовуючи свій приватний ключ. Цифровий підпис підтверджує, що ініціатор має право розпоряджатися зазначеними коштами.

Після формування, транзакція відправляється в мережу і потрапляє в пул транзакцій, де вона стає доступною для валідації майнерами або валідаторами.

Вони перевіряють цифровий підпис транзакції, щоб забезпечити його автентичність та відповідність публічному ключу ініціатора. Також перевіряється достатність коштів на рахунку відправника для покриття суми транзакції та комісії за майнінг. Якщо транзакція проходить усі перевірки, вона визнається валідною [38].

Валідні транзакції включаються до нового блоку, який формує майнер або валідатор, що має право створювати наступний блок. Крім транзакцій, блок включає додаткові метадані, такі як попередній хеш блоку, час створення, і сам хеш блоку. Після створення блок піддається процесу консенсусу в мережі, де інші учасники перевіряють його дійсність. Якщо консенсус досягнуто, блок додається до блокчейну [38].

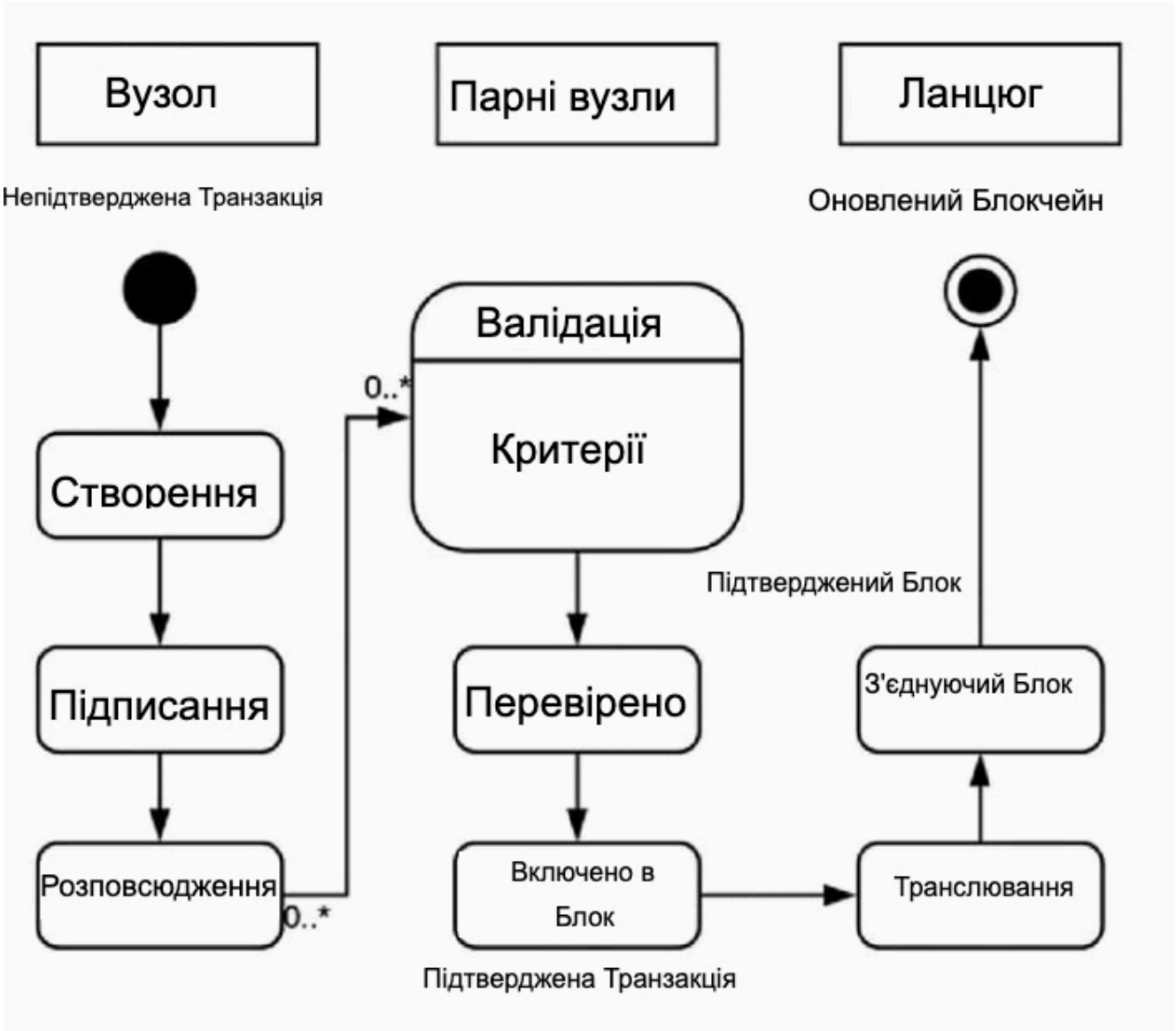


Рисунок 2.7 – Процес валідації транзакцій

Кожна транзакція у блокчейні записується в блоки, які з'єднані в ланцюг через хеші попередніх блоків, створюючи незмінну і послідовну історію всіх транзакцій. Це забезпечує відмінні можливості для відслідковування та аудиту, оскільки будь-яка транзакція може бути перевірена з точки зору її походження та шляху до поточного стану. Це критично важливо для фінансових аудитів, правозастосування та відновлення даних [18].

Прозорість транзакцій у блокчейні не лише підвищує довіру серед учасників, але й дозволяє користувачам верифікувати правильність обробки транзакцій. В більшості публічних блокчейнів, таких як Bitcoin чи Ethereum, будь-хто може переглядати транзакції в реальному часі за допомогою блокчейн експлорерів. Це забезпечує високий рівень прозорості та може сприяти більш відкритій та справедливій фінансовій системі.

Блокчейн технологія використовує розподілені вузли, які забезпечують, що дані завжди доступні з будь-якої точки світу, де є доступ до інтернету. Ця незалежність від централізованих джерел даних забезпечує більш високий рівень надійності та відмовостійкості у порівнянні з традиційними системами.

Основна проблема полягає в тому, що швидкість та ефективність валідації можуть бути обмежені залежно від вибраного алгоритму консенсусу та від механізмів безпеки, що використовуються.

2.3.2 Особливості інтеграції та розгортання

EVM-сумісність важлива для міжопераційності, оскільки вона дозволяє розробникам створювати додатки, які можуть легко взаємодіяти з різними блокчейнами, не переписуючи код для кожної нової платформи. Це сприяє більш широкому прийняттю та використанню смарт-контрактів, оскільки вони можуть бути розгорнуті в різних екосистемах без значних змін [41].

EVM забезпечує єдиний стандарт для написання та виконання смарт-контрактів. Розробники можуть використовувати високорівневі мови програмування, такі як Solidity, для написання контрактів, які потім компілюються у байткод EVM.

Стандартизація коду смарт-контрактів важлива для забезпечення того, що вони можуть легко взаємодіяти з іншими контрактами і компонентами в блокчейні без ризику помилок чи непередбачених взаємодій. Стандартизація також спрощує розробку, оскільки розробники можуть використовувати

загальноприйняті шаблони та використовувати існуючі бібліотеки та інструменти.

Один із способів стандартизації у світі Ethereum і EVM-сумісних блокчейнів — використання стандартів ERC. Наприклад, ERC-20 стандарт для токенів зробив створення та взаємодію токенів дуже передбачуваними, що допомогло широкому прийняттю токенізованих активів [40].

Стандартизація також знижує потенціал безпекових ризиків, оскільки зменшує кількість унікального коду, який потрібно перевіряти на вразливості. Використання перевірених шаблонів та бібліотек може допомогти уникнути поширених помилок, що часто призводять до втрати коштів або інших серйозних проблем [42].

Ключовим елементом оптимізації є ідентифікація і видалення непотрібних або надмірних операцій у коді. Розробники повинні перевіряти кожен рядок коду, щоб забезпечити, що він виконує необхідні дії без зайвих обчислень. Зменшення кількості операцій не тільки знижує витрати на газ, але і прискорює виконання транзакцій.

Управління пам'яттю є важливим аспектом при написанні смарт-контрактів. Використання пам'яті для зберігання тимчасових даних може значно знизити витрати на газ [43].

Кожен зовнішній виклик до іншого контракту або до зовнішніх функцій може бути дорогим з точки зору витрат на газ. Оптимізація смарт-контрактів може включати мінімізацію цих викликів, замінюючи їх більш ефективними внутрішніми операціями, де це можливо [43].

Методи та інструменти перевірки безпеки смарт-контрактів є ключовими для гарантування їх надійності та безпечності перед впровадженням у блокчейн. Основні методи та інструменти:

- Статичний аналіз. Це метод перевірки коду смарт-контрактів, який виконується без реального запуску коду. Цей метод дозволяє розробникам

ідентифікувати потенційні проблеми безпеки, помилки в коді, та неефективні практики програмування до того, як код буде запущено чи розгорнуто [47].

Основна перевага статичного аналізу полягає в його здатності швидко переглядати великі обсяги коду та виявляти широкий спектр потенційних проблем. Ці проблеми можуть включати неправильне управління пам'яттю, вразливості пов'язані з переповненням даних, проблеми пов'язані з доступом до змінних або атаки повторного входу (reentrancy attacks), які можуть дозволити зловмисникам втручатися в логіку контрактів.

Однак статичний аналіз не може виявити всі можливі помилки або проблеми безпеки, оскільки він не може імітувати всі можливі сценарії виконання або взаємодію з іншими контрактами чи зовнішніми впливами. Тому він зазвичай використовується в комбінації з іншими методами перевірки, такими як динамічний аналіз і ручний аудит коду [47].

- Динамічний аналіз смарт-контрактів. Метод, що включає виконання коду смарт-контракту в контрольованому середовищі, з метою виявлення вразливостей, помилок та непередбачуваної поведінки, які можуть не бути виявлені під час статичного аналізу. Цей процес допомагає перевірити поведінку смарт-контрактів у реальних умовах, забезпечуючи більш глибоке розуміння потенційних ризиків та проблем, які можуть виникнути під час їх використання в блокчейні [48].

Під час динамічного аналізу розробники використовують інструменти для тестування, які можуть імітувати різні умови мережі та взаємодії користувачів. Це включає в себе тестування на витривалість, де смарт-контракти піддаються стресу з високою кількістю запитів або атак, щоб перевірити їхню здатність витримувати навантаження та реагувати на нештатні ситуації.

Один з ключових аспектів динамічного аналізу — це виявлення таких вразливостей, як повторний вхід (reentrancy), переповнення цілочисельних

змінних, а також інші проблеми з управлінням станами та логікою транзакцій. Цей метод дозволяє також перевірити, наскільки добре смарт-контракти відповідають своїм вимогам та чи не містять вони логічних помилок, які можуть бути використані зловмисниками [48].

- Фаззинг. Ефективний метод динамічного тестування, який широко використовується для виявлення помилок і вразливостей у програмному забезпеченні, включаючи смарт-контракти. Він полягає у генерації великої кількості випадкових вхідних даних, які подаються на вхід програми або смарт-контракту для виклику помилок або непередбачуваної поведінки. Цей процес допомагає виявити вразливості, які можуть залишитися непоміченими під час статичного аналізу або звичайного тестування [49].

Основна ідея фаззингу полягає в тому, що шляхом автоматичного введення несподіваних, неправильних або випадкових даних до програми можна спровокувати помилки, такі як переповнення буфера, виключення або інші критичні збої, які потенційно можуть бути використані зловмисниками [49].

Фаззинг особливо важливий для смарт-контрактів, оскільки вони часто управляють значними фінансовими активами і використовуються в середовищах, де помилки можуть призвести до серйозних фінансових втрат [49].

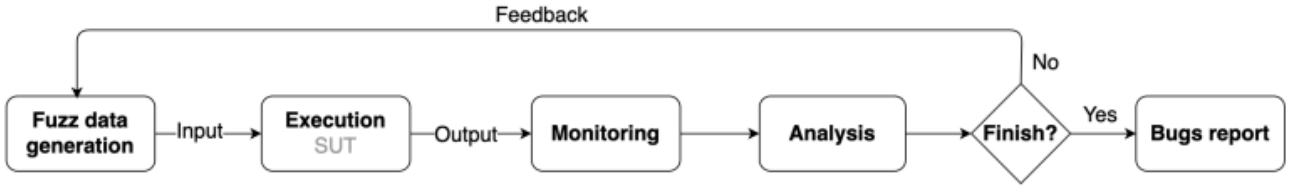


Рисунок 2.8 – Виявлення помилок методом фаззинг

- Формальна верифікація. Включає використання математичних методів для доведення відповідності коду до його формальних специфікацій, що дозволяє переконатися у відсутності помилок і вразливостей до запуску контрактів у мережі. Цей процес передбачає визначення математичної моделі контракту та використання спеціалізованих інструментів для доведення коректності його логіки відносно визначених властивостей безпеки [50].

Види вразливостей у смарт-контрактах:

- Reentrancy. Ця вразливість дозволяє атакуючому здійснити повторний виклик функції контракту в рамках одного виклику транзакції, що може призвести до небажаних побічних ефектів, таких як крадіжка коштів. Найвідоміший приклад атаки з використанням reentrancy - це атака на DAO (Decentralized Autonomous Organization), де зловмисники витягли мільйони доларів у ефірі [45].
- Integer overflow/underflow. Ці вразливості виникають, коли значення, яке зберігається в змінній, перевищує максимально або мінімально можливе значення, яке вона може зберігати. Наприклад, якщо змінна типу uint8 (яка може зберігати значення від 0 до 255) досягає значення 255 і до неї додають одиницю, вона повернеться до 0 (overflow), що може призвести до неправильних обчислень і потенційних фінансових втрат [45].
- Timestamp dependency. Деякі смарт-контракти використовують таймстемпи блоків як частину своєї логіки, наприклад, для визначення часу закінчення аукціону або лотереї. Оскільки майнери визначають, який блок є наступним у ланцюзі, вони можуть маніпулювати таймстемпом блоку, щоб вплинути на результати виконання контракту [45].
- External call to untrusted contract. Коли смарт-контракт викликає зовнішній контракт, він відкривається для ризиків, оскільки зовнішній контракт може бути зловмисним або містити помилки. Це може призвести до

непередбачених викликів або дій, які можуть шкодити логіці оригінального контракту [43].

- Gas limit and loops. Смарт-контракти обмежені кількістю газу, яке може бути використано для обробки транзакції. Цикли, які виконують багато операцій, можуть вичерпати весь доступний газ і не завершитися, що може заблокувати функціональність контракту [45].
- Short address/parameter attack. Цей тип атаки використовує недоліки в способі обробки вхідних даних, як-от довжина адреси етереуму, що може бути використано зловмисником для маніпуляції вхідними даними, спричиняючи некоректну валідацію і відповідні дії [46].

3. ДОСЛІДЖЕННЯ БЕЗПЕКИ В DEFI

У міру того, як децентралізовані фінанси продовжують впроваджуватися в глобальну фінансову інфраструктуру, питання безпеки стають все більш актуальними. Безпека в DeFi — це не тільки захист активів, але й забезпечення довіри та стабільності всієї системи. Враховуючи значні суми, які обертаються в DeFi-проектах, необхідність високого рівня захисту не може бути переоцінена.

3.1 Загрози та виклики в DeFi

Безпека в DeFi має вирішальне значення, оскільки вся система базується на коді смарт-контрактів, які можуть містити уразливості. Ці уразливості можуть призвести до значних фінансових втрат користувачів та підриву довіри до системи DeFi в цілому. Більш того, децентралізація означає відсутність єдиного контрольного органу, що ускладнює швидке реагування на атаки та управління ризиками.

3.1.1 Експлуатація контрактних вразливостей

Експлуатація контрактних уразливостей є однією з найбільших загроз для систем DeFi, оскільки децентралізовані фінанси практично повністю залежать від смарт-контрактів для виконання фінансових операцій. Уразливості в смарт-контрактах можуть призвести до величезних фінансових втрат та підірвати довіру до всієї системи DeFi.

Атаки повторного входу (Reentrancy attacks) - це один з найвідоміших типів атак, який був використаний в знаменитій атаці на DAO. Атака полягає в тому, що зловмисник виконує непередбачений додатковий виклик смарт-контракту під час його виконання. Наприклад, якщо контракт передбачає відправлення ефірів до користувача і не оновлює відповідний стан до

завершення транзакції, атакуючий може викликати контракт знову перед завершенням першого виклику, змусивши контракт відправити кошти повторно.

Проблеми з довірою до зовнішніх джерел інформації (Oracle Manipulation). DeFi-контракти часто залежать від зовнішніх джерел даних (оракулів) для отримання інформації про ціни активів, індекси тощо. Якщо зловмисник може маніпулювати даними, які контракт отримує від оракула, вони можуть змусити контракт виконувати несправедливі або збиткові транзакції.

Проблеми з цілісністю даних (Data Integrity Issues). Це стосується вразливостей, коли зловмисники можуть змінювати, видаляти або пошкоджувати дані всередині контракту. Це може включати зміну параметрів контракту, як-от розмір ставок, ліміти виведення коштів, або навіть умови виконання контрактів.

Переповнення та нестача (Overflow and Underflow). Ці помилки стаються, коли виконується арифметична операція, що виходить за межі обмеження числових типів даних, що використовуються в контракті. Наприклад, якщо змінна має максимально можливе значення і до неї додають щось, відбувається переповнення, і змінна повертається до надзвичайно малого значення або нуля. Зловмисники можуть використовувати такі помилки для неправомірного збільшення балансів або інших маніпуляцій.

Неавторизований доступ або зміни в контрактах. У разі коли контракти не мають належних перевірок на автентифікацію чи авторизацію, зловмисники можуть здійснювати несанкціоновані зміни в контрактах, включаючи зміну логіки виконання або параметрів.

3.1.2 Фронтраннінг та мінінг уразливостей в DeFi

Фронтраннінг — це вид атаки в мережах DeFi, який використовується учасниками з привілейованим доступом до мережевої інформації. Зокрема, мова

йде про тих, хто може бачити непідтверджені транзакції в мемпулі — тобто в пулі пам'яті, де транзакції чекають на підтвердження та включення до блоку.

Учасники, які здійснюють фронтраннінг, моніторять мемпул, щоб виявити потенційно прибуткові транзакції (наприклад, великі торговельні замовлення на біржах DeFi). Вони подають свою власну транзакцію з вищою комісією за газ, щоб майнери обрали саме їхню транзакцію до включення в блок перед оригінальною транзакцією. Таким чином, вони використовують інформацію про майбутні транзакції, щоб заробити на змінах ціни, викликаних великими ордерами.

Цей термін відноситься до експлуатації уразливостей в алгоритмах консенсусу або в імплементації смарт-контрактів, які можуть бути використані для набуття переваг або нечесного збагачення. Це включає, наприклад, використання вразливостей для подвійного витрачання або створення нових монет без належного підтвердження транзакцій.

Для боротьби з фронтраннінгом та мінінгом уразливостей, розробники DeFi та блокчейн спільноти впроваджують ряд технічних рішень:

- Використання приватних мемпулів: Це обмежує доступ до непідтверджених транзакцій, зменшуючи можливість фронтраннінгу.
- Розумні контракти без можливості зміни стану через зовнішні виклики: Такі контракти унеможливлюють фронтраннінг, оскільки зовнішні дії не можуть впливати на результати транзакцій.

3.1.3 Аналіз типових інцидентів

Вивчення конкретних випадків зламів та втрат активів є важливим у формуванні загального розуміння потенційних слабких місць та методів атаки, що використовують зловмисники. Такий аналіз не тільки підсвічує типові помилки та уразливості у смарт-контрактах та протоколах, але й допомагає розробити рекомендації щодо посилення захисту і зниження ризиків у

майбутньому. На прикладах конкретних інцидентів можна детально розглянути, як реагувала спільнота, які заходи були прийняті для відновлення втрачених коштів та як це вплинуло на розвиток та довіру до децентралізованих фінансів.

Ось п'ять значущих випадків зломів у секторі DeFi, кожен з яких ілюструє різні типи недоліків безпеки, які можуть виникати у децентралізованих фінансових системах:

- The DAO Attack. Це був інноваційний проект на платформі Ethereum, що функціонував як децентралізована автономна організація для венчурного фінансування проектів блокчейну. Інвестори вносили ETH і отримували взамін DAO токени, що давали їм право голосу в управлінні капіталом, інвестованим в різні проекти. Внаслідок великого інтересу та захоплення ідеєю, DAO швидко залучив значну суму інвестицій, що перетворило його на один з найбільших краудфандингових проектів у світі.

У випадку The DAO, вразливість повторного входу проявилася через спосіб обробки функції виведення коштів (splitDAO). Коли користувач вирішив вийти з DAO і створити новий "дочірній" DAO, він міг забрати частину своїх внесків у формі ETH. Користувач ініціював splitDAO, і DAO передавав зазначену суму на адресу нового DAO контракту. Однак, зменшення балансу користувача в DAO відбувалося після переказу коштів, а не до нього.

Зловмисник, створивши зловмисний смарт-контракт, міг ініціювати splitDAO та під час переказу коштів знову викликати splitDAO зі свого контракту. Оскільки первісна транзакція ще не завершилася та не зменшила баланс користувача, DAO знову переказувала кошти. Це дозволяло зловмиснику повторювати процес, забираючи більше коштів, ніж належало йому насправді.

Ця атака призвела до втрати понад 60 мільйонів доларів в ETH, що становило приблизно третину всіх коштів, зібраних проектом. Ця значна втрата фінансових ресурсів не тільки зруйнувала довіру інвесторів до проекту DAO,

але й поставила під сумнів загальну безпеку та стійкість смарт-контрактів на платформі Ethereum в той час.

Атака спровокувала серйозні дебати всередині спільноти Ethereum щодо кращого шляху реагування на кризу. Спільнота стояла перед вибором: залишити все як є та визнати втрату коштів, або провести "хард форк" блокчейну, що дозволить повернути вкрадені кошти інвесторам. Рішення про проведення "хард форка" було прийнято, але це рішення не знайшло підтримки всієї спільноти, що призвело до розколу і створення нової версії блокчейну Ethereum Classic, яка зберегла оригінальний ланцюг без змін.

- Poly Network Hack. Є одним з найбільших зломів у сфері DeFi, де зловмисник експлуатував вразливості в механізмах міжблокчейнових транзакцій. Poly Network - це протокол, що дозволяє здійснювати міжблокчейнові перекази активів, спрямований на покращення взаємодії між різними блокчейнами.

Вразливість, яка була використана під час злому Poly Network, виникла через недоліки в реалізації смарт-контрактів, які керують міжблокчейновими переказами активів. Специфіка цієї вразливості полягала у недостатньо строгій перевірці даних, що передаються між блокчейнами, та використанні певних методів доступу до даних і їх зміни, які не були належним чином захищені.

В основі проблеми лежала неправильна реалізація механізмів верифікації підписів у транзакціях між блокчейнами. Підписи, які мають забезпечити автентичність і валідність транзакцій, не проходили повноцінну перевірку. Це дало змогу зловмиснику створити транзакцію, яка здавалася легітимною, але насправді була маніпульована.

Вразливість у смарт-контрактах дозволила зловмиснику маніпулювати вхідними даними транзакцій. Зокрема, зловмисник зміг змінити "payload" транзакції, що включає інформацію про кінцевого одержувача коштів. В

результаті, активи були переказані не на офіційні адреси, а на контрольовані хакером.

Злом призвів до втрати понад 600 мільйонів доларів у різних криптовалютах, що робить його одним із найбільших в історії криптовалютних зломів.

- bZx Attacks. У лютому 2020 року bZx зазнав двох великих атак, які експлуатували як флеш-позики, так і реентрансивні вразливості в їхніх смарт-контрактах. Ці атаки показали високий рівень креативності та технічної спроможності зловмисників в експлуатації комплексних інтеракцій між різними протоколами та інструментами в DeFi.

В цих атаках зловмисники використовували два типи вразливостей, а саме: флеш-позики, які дозволяють користувачам позичати велику кількість активів без забезпечення, але з умовою їх повернення в тому ж транзакційному блоку та реентрансивні вразливості, що дозволяли атакуючим рекурсивно викликати функції в контракті, дозволяючи їм кілька разів знімати кошти до того, як початковий внесок був відмінений або змінений.

В першій атаці 14 лютого зловмисник використав флеш-позику для позики великої кількості ETH, які він потім обміняв на токени sUSD на біржі KyberSwap. Ця операція штучно підвищила ціну sUSD. Наступно, зловмисник використав ці високо оцінені sUSD як заставу для отримання інших позик на bZx, а потім обміняв отримані активи назад на ETH, отримуючи прибуток і повертаючи флеш-позику.

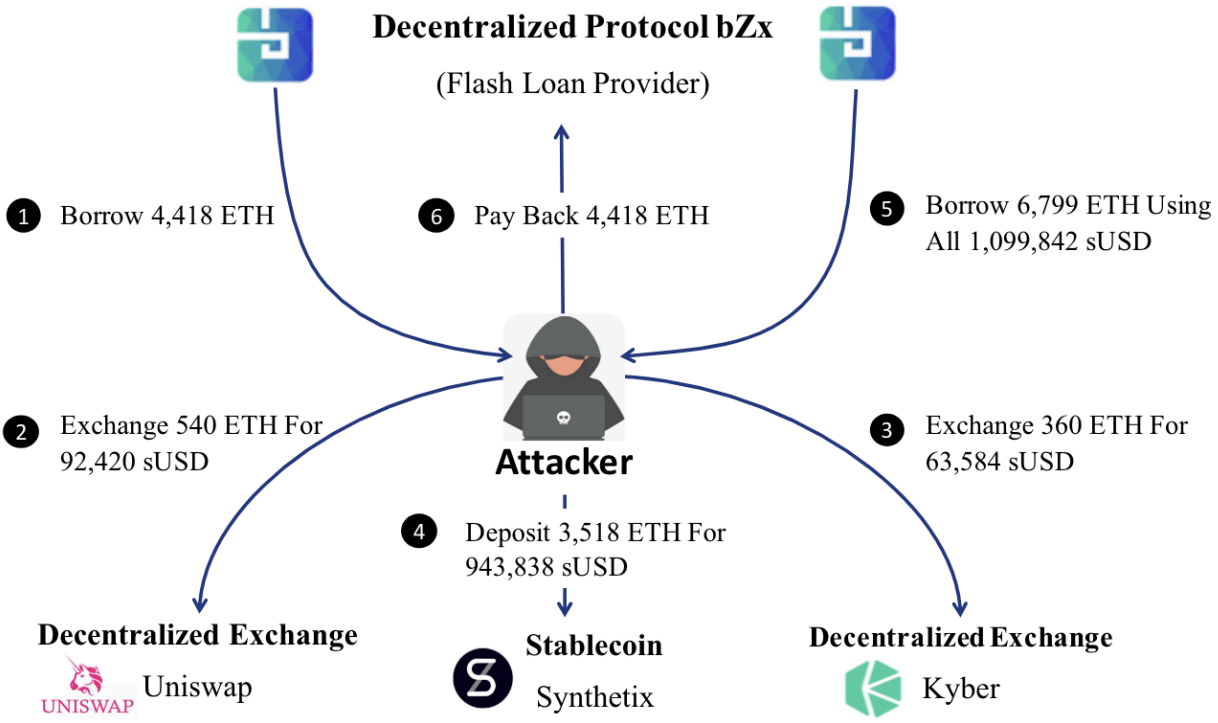


Рисунок 3.1 – Схема атаки на bZx

Після серії атак bZx залучила кілька зовнішніх фірм для проведення глибоких аудитів їхніх смарт-контрактів: розробила і впровадила додаткові шари контролю за транзакціями, що забезпечують моніторинг у реальному часі з метою виявлення та запобігання підозрілим або потенційно шкідливим операціям. Також були вдосконалені інструменти моніторингу, які використовують машинне навчання для аналізу патернів транзакцій та виявлення аномалій, що можуть вказувати на атаку або іншу небезпечну активність.

- Harvest Finance Exploit. Атака на один з популярних протоколів DeFi, який дозволяє користувачам оптимізувати свої інвестиції в різні пули ліквідності. Зловмисник використав техніку, відому як арбітраж, для

маніпуляції цінами в одному з пулів ліквідності протоколу, що призвело до значних втрат коштів.

Протокол Harvest Finance використовує кілька оракулів для отримання інформації про ціни активів, які входять до складу пулів ліквідності. Зловмисник скористався вразливістю у механізмі ціноутворення, що залежав від оракулів, які надавали оновлення цін в реальному часі. Вони використали техніку "flash loan", щоб штучно надути ціну одного з активів в пулі перед виконанням транзакцій з виведення коштів.

Зловмисник розпочав атаку на Harvest Finance, використовуючи флеш-позику для отримання значної суми криптовалюти без забезпечення на дуже короткий термін. Після отримання цих коштів, він використав їх для купівлі великої кількості певного активу в одному з пулів ліквідності на платформі. Швидке закуповування великої кількості активу штучно підняло його ціну на ринку через раптове збільшення попиту.

Оскільки ціна активу на платформі Harvest Finance була тимчасово інфльована, зловмисник скористався цим і переходив до іншого пулу, де цей актив використовувався як забезпечення. Він здійснив транзакції з виведення коштів, що значно перевищували вартість отриманої флеш-позики. Завершальний крок полягав у поверненні флеш-позики, використовуючи частину неправомірно отриманих коштів для погашення позики в межах того самого блоку транзакцій.

Зловмисник успішно вивів понад 24 мільйони доларів, ефективно використовуючи недоліки в механізмі оцінки активів протоколом.

Інцидент наголосив на необхідності підвищення безпеки оракулів. Протоколи мають включати додаткові заходи захисту, такі як використання декількох джерел даних та затримки в оновленні цін, щоб запобігти потенційним маніпуляціям.

3.2 Технології та методи захисту

У сучасному світі DeFi безпека виступає як один з найбільш критичних аспектів, що впливає на довіру та прийняття користувачами цих технологій. Розвиток технологій блокчейну відкрив нові можливості для фінансових операцій, але водночас він привернув увагу шахраїв та хакерів, що намагаються використати будь-які вразливості в системах.

3.2.1 Смарт-контракти та їхнє безпечне програмування

Смарт-контракти — це самовиконувані контракти з визначеними умовами угоди, засновані на програмному коді, які зберігаються на блокчейні. Вони автоматично виконують, контролюють або документують юридично значимі події та дії відповідно до умов контракту. Ключові властивості смарт-контрактів, які роблять їх унікальним інструментом в DeFi:

- Автономність: смарт-контракти є автономними тому, що вони автоматично виконують умови угоди без необхідності втручання ззовні або участі посередників. Це досягається завдяки тому, що код смарт-контракту заздалегідь програмує всі необхідні дії, які повинні відбуватися при заданих умовах.
- Незмінність: однією з фундаментальних властивостей блокчейну є незмінність даних, яка передається і на смарт-контракти. Як тільки смарт-контракт розгорнуто на блокчейні, його не можна змінити чи видалити.
- Розподіленість: смарт-контракти виконуються на блокчейні, що є розподіленою базою даних, контрольованою багатьма вузлами по всьому світу. Це забезпечує велику стійкість до цензури та зовнішніх атак, а також сприяє прозорості виконання угод.

- Безпосередність: смарт-контракти можуть автоматично і миттєво виконувати транзакції та інші дії, як тільки виконані встановлені умови, забезпечуючи швидке та ефективне виконання угод. Це істотно прискорює багато процесів у сфері фінансів, що раніше потребували значно більше часу для ручної обробки та затвердження.

Захист смарт-контрактів в DeFi є критично важливим, оскільки ці контракти виконують ключові фінансові операції і зберігають значні активи. Важливість розробки та впровадження ефективних захисних механізмів обумовлена потенційними ризиками втрати коштів через помилки у коді, атаки або шахрайство. Ось кілька основних захисних механізмів:

- Перевірка та аудит коду: перш за все, смарт-контракти повинні проходити ретельну перевірку і аудит з боку досвідчених розробників блокчейну та безпеки. Це включає в себе статичний аналіз коду, динамічне тестування, а також формальну верифікацію, яка підтверджує логічну коректність коду смарт-контракту за допомогою математичних методів.
- Модульні тести: Розробка модульних тестів для кожної функції смарт-контракту допомагає забезпечити, що вся бізнес-логіка працює належним чином і без помилок. Модульні тести також дозволяють виявити потенційні вразливості перед впровадженням контракту в мережу.
- Обмеження прав доступу: Важливо чітко регулювати, хто може виконувати певні дії з контрактом. Це може включати механізми, які обмежують доступ до виконання ключових функцій тільки для певних адрес або використання шаблонів ролей для керування доступом.
- Використання шаблонів безпеки: Є ряд шаблонів і практик, які довели свою ефективність у забезпеченні безпеки смарт-контрактів. Це включає такі підходи, як: "Check-Effects-Interactions" для запобігання повторного входу (reentrancy attacks), "Circuit breakers" для тимчасового призупинення

контрактів у разі виявлення помилок або атак та обмеження газу для певних транзакцій, щоб запобігти несподіваним витратам.

- Часові затримки: Впровадження часових замків для здійснення великих транзакцій або змін у ключових параметрах системи може допомогти запобігти раптовим змінам і дозволити час для відповіді спільноти.

3.2.2 Шифрування

В DeFi захист інформації та транзакцій користувачів є критично важливим. З розвитком технологій блокчейн і збільшенням обсягів даних, які передаються та зберігаються в DeFi платформах, важливість надійних методів шифрування та забезпечення приватності зростає.

Шифрування не тільки захищає важливі фінансові дані від несанкціонованого доступу, але й допомагає забезпечити конфіденційність транзакцій, що є невід'ємною частиною приватності користувачів. Це стає ще більш актуальним у світлі глобальних нормативних вимог, таких як GDPR у Європі, які вимагають від організацій забезпечувати високий рівень захисту персональних даних.

Основні типи шифрування, які широко застосовуються в DeFi та інших блокчейн-додатках:

- Симетричне шифрування: це метод криптографії, де один і той самий ключ використовується для шифрування та розшифрування даних. Цей метод є одним з найбільш ефективних з точки зору швидкості обробки, що робить його ідеальним для використання в ситуаціях, де потрібно швидко обробляти великі обсяги інформації. У контексті децентралізованих фінансів, симетричне шифрування може використовуватися для захисту даних, зберіганих на блокчейн-платформах, а також для шифрування транзакційних повідомлень. Важливість захисту ключів у таких системах

не може бути недооціненою, оскільки втрата або крадіжка ключів може призвести до значних фінансових втрат.

- Асиметричне шифрування: відоме також як шифрування з відкритим ключем, використовує пару ключів для захисту даних — публічний і приватний. Ця методика є основою для багатьох криптографічних систем і відіграє критичну роль в захисті цифрової інформації та в обміні даними. Асиметричне шифрування у децентралізованих фінансах (DeFi) застосовується для захисту транзакцій, створення цифрових підписів, що гарантують автентичність та цілісність даних, а також для контролю доступу до смарт-контрактів.
- Хешування: процес перетворення вхідної інформації будь-якого розміру в стисле, фіксоване хеш-значення, яке діє як унікальний відбиток вхідних даних. Ключовими властивостями хеш-функцій є їх детермінізм, швидкість, необоротність і відсутність колізій. Хеш-функції застосовуються у блокчейні для зв'язування блоків, де кожен блок містить хеш попереднього, створюючи таким чином ланцюг, який важко змінити без перерахунку всіх наступних хешів.

3.2.3 Оракули в DeFi: вразливості та методи захисту

Оракул — це сервіс або протокол, який дістає та верифікує зовнішні дані та передає їх у блокчейн для використання у смарт-контрактах. Він діє як посередник, що забезпечує смарт-контракти необхідною інформацією, яка не може бути безпосередньо отримана смарт-контрактами через ізольовану природу блокчейнів. Основні функції оракулів:

- Доставка даних: оракули забезпечують смарт-контракти доступом до даних із зовнішніх джерел, таких як курси валют, ціни акцій, погодні умови або навіть результати спортивних ігор. Ця інформація може

використовуватися для автоматизації виконання контрактів на основі попередньо визначених умов.

- Верифікація даних: оракули не тільки збирають дані, але й перевіряють їхню достовірність перед тим, як передати їх у блокчейн. Це забезпечує надійність і точність даних, які використовуються у смарт-контрактах.
- Зворотний зв’язок зі смарт-контрактами: деякі оракули можуть отримувати інформацію від смарт-контрактів та виконувати певні дії у зовнішньому світі, наприклад, відправляти платежі, активувати механізми або навіть взаємодіяти з іншими системами.

Типи оракулів:

- Централізовані оракули: оперують під контролем одного оператора або організації, що створює ризик "єдиної точки відмови".
- Децентралізовані оракули: використовують декілька джерел та вузлів для збору та верифікації даних, значно знижуючи ризики централізації.
- Гібридні оракули: комбінують елементи централізованих та децентралізованих підходів для оптимізації точності та надійності даних.

Оракули також забезпечують смарт-контракти необхідними зовнішніми даними. Проте, ця ж важлива роль робить оракули потенційно вразливими до різних видів атак, які можуть мати серйозні наслідки для безпеки всієї DeFi платформи. Основні вразливості, які часто зустрічаються в оракулах:

- Атаки “Man-in-the-Middle”: оракули, які передають дані між зовнішніми джерелами і блокчейном, можуть бути піддані MiTM атакам, де зловмисник перехоплює або альтерує дані перед їхнім досягненням смарт-контракту. Це може призвести до того, що смарт-контракт отримає хибну інформацію та виконає невірні дії.
- Залежність від одного джерела даних: якщо оракул використовує дані з одного джерела, це створює ризик, що дані можуть бути недостовірними

або маніпульованими. Залежність від одного джерела робить систему уразливою до збоїв або зловмисних втручань у це джерело.

- Таймінг атаки: оракули можуть стати об'єктом таймінг атак, де зловмисник намагається вплинути на таймінг подачі даних. Це може бути зроблено для того, щоб викликати несправедливі умови торгівлі або вплинути на виконання смарт-контрактів у певний момент часу.
- Контрольовані атаки: оскільки оракули часто залежать від зовнішніх джерел, вони можуть стати мішенню для контрольованих атак, де зловмисник спеціально маніпулює джерелом даних для впливу на результати смарт-контрактів.

Децентралізація джерел даних є фундаментальним методом для зниження ризику маніпуляцій. Це включає використання даних з кількох незалежних джерел, щоб жодне одне джерело не мало вирішального впливу на результати смарт-контрактів.

Аудит і моніторинг виконують критичну роль у виявленні та реагуванні на ненормальні дії. Це включає постійний нагляд за діяльністю оракулів, що дозволяє швидко виявляти та реагувати на підозрілі зміни або спроби маніпуляції.

Один із яскравих прикладів маніпуляції ціновим оракулом стався у липні 2019 року, коли протокол Synthetix зазнав атаки, що призвело до втрати активів на суму близько $1 млн. Зловмисник скористався вразливістю у механізмі оновлення цінового оракула, щоб маніпулювати цінами на синтетичні активи. Це дозволило йому отримати значні прибутки за рахунок використання підроблених даних про ціни. Цей випадок продемонстрував, як централізоване джерело даних може бути маніпульоване, що має серйозні наслідки для роботи протоколу.

На противагу цим прикладам, є успішні стратегії захисту, такі як використання децентралізованих оракулів Chainlink. Chainlink використовує

мережу децентралізованих оракулів для забезпечення надійних і захищених даних. Вони застосовують множинні незалежні джерела даних, криптографічні підписи та алгоритми консенсусу для перевірки достовірності інформації. Це дозволило Chainlink успішно запобігати атакам, забезпечуючи більш високу стійкість і надійність даних.

Ще один приклад ефективної стратегії захисту надано компанією MakerDAO, яка використовує систему мульти-оракулів. У цій системі дані надходять з декількох незалежних джерел, що зменшує ризик маніпуляцій та підвищує надійність цінових даних. Використання децентралізації джерел даних, регулярний аудит і моніторинг роботи оракулів дозволили MakerDAO зменшити ризик маніпуляцій і підвищити безпеку своєї платформи.

3.2.4 Приклади впровадження технологій безпеки

Uniswap є одним з найвідоміших та найбільш використовуваних децентралізованих обмінників у секторі DeFi. Платформа дозволяє користувачам торгувати криптовалютами без необхідності посередника, використовуючи технологію смарт-контрактів на блокчейні Ethereum. Ключовим елементом Uniswap є автоматизовані маркет-мейкери (AMM), які дозволяють ліквідність на ринку зберігатися за допомогою алгоритмічного ціноутворення.

В одному з інцидентів, смарт-контракти Uniswap були вразливими до атаки повторного входу. Після виявлення атаки команда Uniswap негайно провела аудит своїх смарт-контрактів. В рамках відповіді на інцидент було впроваджено наступні заходи:

- Оновлення смарт-контрактів: Запровадження оновлених версій контрактів з покращеними механізмами безпеки, що запобігають подібним атакам.
- Аудити коду: Регулярні аудити коду проводились як внутрішніми командами, так і залученими зовні експертами у сфері кібербезпеки.

- Використання зовнішніх аудиторських компаній: Для забезпечення незалежної перевірки смарт-контрактів та впевненості у їх безпеці.
- Формальна верифікація: Впровадження формальної верифікації коду, яка дозволяє математично переконатися у відсутності певних класів уразливостей.

Synthetix - це децентралізований протокол для випуску синтетичних активів, які можуть відображати вартість реальних активів, таких як валюти, акції або товари. Важливим компонентом роботи платформи є точність та надійність даних, що використовуються для оцінки вартості синтетичних активів.

Проблеми, з якими стикалась Synthetix, включали можливість маніпуляції даними оракулів. Наприклад, зловмисники можуть подавати хибні дані, що призводить до некоректних розрахунків вартості синтетичних активів. Для усунення цих вразливостей були вжиті наступні заходи:

- Використання мультиоракулів: замість одного джерела даних, Synthetix почала використовувати декілька ореклів, що надають дані з різних джерел. Це знижує ризик маніпуляції даними з одного джерела.
- Децентралізована перевірка даних: дані, що надходять від ореклів, перевіряються незалежними учасниками мережі, що додає додатковий рівень захисту.
- Аудит та моніторинг: Постійний аудит даних і моніторинг роботи ореклів дозволяє швидко виявляти і реагувати на будь-які аномалії.

MakerDAO є однією з провідних децентралізованих платформ, що надає послуги зі створення стабільної криптовалюти DAI. DAI є стейблкоїном, прив’язаним до вартості долара США, і забезпечує стабільність шляхом використання системи забезпечених боргових позицій. Успішна робота цієї платформи вимагає високого рівня безпеки, зокрема через складність і важливість її смарт-контрактів.

У випадку MakerDAO були використані такі ключові методи:

- Моделювання логічної правильності: Перевірка логіки смарт-контрактів на предмет коректності та відповідності заявленим функціональним вимогам.
- Аналіз безпеки: Виявлення можливих шляхів експлуатації через автоматизоване тестування та симуляції.
- Верифікація інваріантів: Перевірка того, що певні умови залишаються істинними протягом всього виконання смарт-контракту.

Формальна верифікація дозволила виявити кілька потенційних вразливостей в смарт-контрактах MakerDAO до їхнього впровадження. Ось деякі з основних висновків цього аналізу:

- Попередження помилок логіки: було виявлено та виправлено кілька помилок логіки, які могли призвести до некоректного функціонування платформи та втрати активів користувачів.
- Захист від атак типу повторного входу: верифікація виявила можливість атак reentrancy (повторного входу), що дозволило команді вжити додаткових заходів для запобігання таких атак.
- Оптимізація кодової бази: процес формальної верифікації також сприяв оптимізації коду, роблячи його більш ефективним та безпечним.

3.3 Оцінка безпеки та рекомендації

У цьому підрозділі буде здійснено комплексний аналіз безпеки EVM-сумісних блокчейнів та платформ DeFi. Основною метою є ідентифікація ключових вразливостей та оцінка ефективності поточних методів захисту. На основі отриманих даних будуть розроблені рекомендації щодо покращення безпеки, які включатимуть оптимізацію смарт-контрактів, підвищення безпеки консенсусу, а також проактивний моніторинг та навчання користувачів. Це

дозволить створити більш надійні та захищені DeFi-системи, сприяючи їх подальшому розвитку та впровадженню.

3.3.1 Аналіз отриманих даних

Основні вразливості в смарт-контрактах:

- Reentrancy Attacks: атака, яка виникає, коли зловмисник викликає функцію смарт-контракту, яка знову викликає іншу функцію до завершення початкової транзакції.
- Integer Overflow/Underflow: ці вразливості виникають, коли арифметичні операції призводять до переповнення або недоповнення змінної, що може використовуватися для маніпуляцій зі значеннями.
- Unprotected Functions: відсутність доступу до контролю або перевірок дозволяє зловмисникам викликати критичні функції смарт-контракту.
- Logical Errors: логічні помилки у коді смарт-контракту, які можуть бути використані зловмисниками для зміни поведінки контракту.

Основні недоліки в механізмах консенсусу:

- Front-running: зловмисники маніпулюють порядком транзакцій, щоб отримати вигоду від майбутніх транзакцій, наприклад, шляхом купівлі токенів до виконання великого ордеру.

У період з 2020 по 2023 рік було зафіксовано 250 значних атак на платформи DeFi. Найпоширенішими типами атак були reentrancy (40%), flash loan (25%), rug pull (20%) та інші (15%).

Загальні фінансові втрати склали 3,5 мільярда доларів США. Середній розмір втрат на одну атаку становив 14 мільйонів доларів. Найбільші втрати були пов'язані з reentrancy атаками, які спричинили загальні втрати у 1,4 мільярда доларів. Flash loan атаки призвели до втрат у 875 мільйонів доларів, а rug pull - до втрат у 700 мільйонів доларів.

Розподіл атак за платформами показав, що найбільше постраждали Ethereum, Binance Smart Chain та Polygon. Ethereum зазнав 150 атак, що становить 60% від загальної кількості, з загальними втратами у 2,1 мільярда доларів. Binance Smart Chain мав 70 атак (28%) з втратами у 980 мільйонів доларів, а Polygon - 30 атак (12%) з втратами у 420 мільйонів доларів.

Аналіз часових трендів показав, що кількість атак зросла з 2020 по 2022 рік, а у 2023 році спостерігалося незначне зниження. У 2020 році було зафіксовано 50 атак з загальними втратами у 700 мільйонів доларів, у 2021 році - 80 атак з втратами у 1,2 мільярда доларів, у 2022 році - 90 атак з втратами у 1,4 мільярда доларів, а у 2023 році - 30 атак з втратами у 210 мільйонів доларів.

Дескриптивний аналіз показав, що середнє значення атак на рік становило 62.5, медіана - 70 атак на рік, а стандартне відхилення - 26 атак. Кореляційний аналіз виявив сильний позитивний зв'язок між кількістю атак та обсягом активів на платформі, з коефіцієнтом кореляції 0.85. Це вказує на те, що більші платформи з великим обсягом активів є більш привабливими для зловмисників.

На основі проведеного статистичного огляду були зроблені такі висновки: reentrancy атаки залишаються найпоширенішими, Ethereum є найбільш уразливою платформою, що пояснюється її домінуючою роллю на ринку DeFi, кількість атак зросла у 2020-2022 роках, але у 2023 році спостерігалося зниження, а фінансові втрати на одну атаку залишаються високими.

Розглянемо безпеку основних платформ DeFi, таких як Ethereum, Binance Smart Chain, та Polygon, зосереджуючись на механізмах консенсусу, управлінні смарт-контрактами, захисті приватних ключів, та проактивному моніторингу.

В управлінні смарт-контрактами Ethereum має добре розвинену екосистему інструментів для розробки та аудиту, таких як Truffle, Hardhat, та OpenZeppelin, і часто проводить аудити та баг-баунті програми. BSC використовує подібні інструменти та стандарти, що забезпечує сумісність, але має менше аудитів та менш поширені баг-баунті програми. Polygon також

використовує інструменти Ethereum, додаючи рішення для безпеки через Plasma та інші технології.

Щодо захисту приватних ключів, всі три платформи підтримують апаратні гаманці та багатофакторну автентифікацію. Ethereum і BSC мають схожу інфраструктуру завдяки сумісності, тоді як Polygon додатково забезпечує безпеку через багаторівневу архітектуру.

Проактивний моніторинг та реагування на загрози на Ethereum забезпечується активною спільнотою розробників та дослідників, що сприяє частим оновленням та вдосконаленням мережі. BSC також має активну підтримку з боку Binance та часті оновлення безпеки, але менш активну спільноту розробників. Polygon має активну спільноту та часті оновлення, додатково забезпечуючи моніторинг через багаторівневу архітектуру.

Загалом, Ethereum залишається лідером за рівнем безпеки завдяки широкій підтримці спільноти, частим аудитам та багатій екосистемі інструментів. Binance Smart Chain пропонує високошвидкісні транзакції та низькі витрати, але менш захищений через централізацію валідаторів. Polygon забезпечує додаткову безпеку та масштабованість завдяки багаторівневій архітектурі, але має складнішу інфраструктуру, що може створювати додаткові ризики.

3.3.2 Розробка рекомендацій

Внаслідок проведеного аналізу отриманих даних щодо безпеки в децентралізованих фінансах, виявлено низку критичних вразливостей та недоліків у функціонуванні EVM-сумісних блокчейнів. Для забезпечення високого рівня безпеки та надійності платформ DeFi необхідно вжити комплексних заходів, які будуть спрямовані на усунення існуючих загроз та мінімізацію ризиків у майбутньому.

Розробка рекомендацій базується на аналізі досліджень у сфері кібербезпеки, успішних кейсів впровадження захисних технологій, а також на специфічних потребах децентралізованих платформ. Представлені рекомендації включають оптимізацію процесів написання та валідації смарт-контрактів, підвищення безпеки консенсусу, зміцнення механізмів автентифікації та управління ключами, а також впровадження проактивних заходів моніторингу та реагування на загрози.

Рекомендації для покращення смарт-контрактів:

- Регулярні аудити: залучення команди внутрішніх аудиторів для регулярного перегляду та перевірки коду смарт-контрактів.
- Аналіз статичним кодом: використання інструментів для статичного аналізу коду, які можуть виявити потенційні вразливості та помилки на ранніх стадіях розробки.
- Впровадження стандартів: дотримання встановлених стандартів написання смарт-контрактів, таких як ERC-20, ERC-721, які забезпечують базову безпеку та функціональність. Використання перевірених бібліотек дозволяє зменшити ризик помилок, а регулярне оновлення цих бібліотек гарантує захист від нових вразливостей.
- Використання перевірених бібліотек: таких як OpenZeppelin, які містять готові рішення для захисту смарт-контрактів. Регулярне оновлення бібліотек для врахування нових версій та виправлення вразливостей.
- Контрактне програмування: впровадження контрактного програмування з використанням інваріантів, перед- та постумов для забезпечення правильності виконання смарт-контрактів.
- Модульне тестування: тестування всіх функцій смарт-контрактів за допомогою таких інструментів, як Truffle або Hardhat, дозволяє автоматизувати процес тестування.

- Симуляції та стрес-тести: проведення симуляцій різних сценаріїв використання смарт-контрактів для виявлення можливих проблем та вразливостей. Використання стрес-тестів для перевірки роботи смарт-контрактів під високим навантаженням та в умовах високої кількості транзакцій.
- Захист від reentrancy атак: використання шаблонів розробки, таких як "check-effects-interactions", для запобігання повторному виклику функцій.
- Обмеження використання зовнішніх викликів: мінімізація використання зовнішніх викликів до інших смарт-контрактів для зменшення ризику зовнішніх атак. Впровадження тайм-аутів та лімітів на виконання критичних функцій.
- Децентралізована аудиторська система: система, де незалежні учасники перевіряють смарт-контракти на наявність вразливостей. Аудитори реєструються на платформі, яка розподіляє контракти для перевірки. Винагороди стимулюють якісний аудит, а рейтингова система оцінює роботу аудиторів. Процес аудиту включає подання контрактів, їх розподіл між аудиторами, проведення перевірки та подання звітів з результатами. Платформа може інтегруватися з різними блокчейн-екосистемами.
- Інтеграція ШІ для аналізу, оптимізації та симуляції атак: впровадження штучного інтелекту для комплексного аналізу, оптимізації та симуляції атак на смарт-контракти забезпечить виявлення вразливостей та допоможе створювати більш стійкі системи. ШІ може аналізувати історичні дані, прогнозувати потенційні загрози та моделювати можливі сценарії атак для підвищення рівня безпеки.
- Вбудовані контрольні точки відновлення: дозволяє створювати певні стани контракту, до яких можна повернутися у разі виявлення проблем або аномалій. Це забезпечить можливість швидкого відновлення контракту після збою або атаки, мінімізуючи втрати та знижуючи ризики.

Оптимізація алгоритмів консенсусу є ключовим елементом для підвищення безпеки та ефективності блокчейн-мереж. Від вибору та налаштування консенсусного алгоритму залежить стійкість мережі до атак, її масштабованість та енергетична ефективність. Існує кілька основних напрямків, за якими можна оптимізувати алгоритми консенсусу.

Одним із найбільш популярних та перспективних методів оптимізації є перехід від PoW до PoS та його варіацій. У PoS валідатори обираються для підтвердження транзакцій та створення нових блоків на основі кількості криптовалюти, яку вони утримують та ставлять як заставу. Це значно знижує енергоспоживання в порівнянні з PoW та робить атаки менш вигідними, оскільки потенційний зловмисник має ризикувати власними активами.

Гібридні моделі консенсусу комбінують переваги різних алгоритмів для підвищення безпеки та ефективності. Наприклад, комбінація PoW та PoS дозволяє використовувати переваги обох підходів. У таких моделях PoW забезпечує безпеку та стійкість до атак, тоді як PoS підвищує енергоефективність та швидкість підтвердження транзакцій.

Для підвищення відповідальності валідаторів та запобігання зловживань використовуються механізми слешингу (slashing). Вони передбачають штрафи або втрату застави валідатором у разі виявлення неправомірних дій, таких як подвійне витрачання або підтвердження неправильних транзакцій. Це створює додаткову мотивацію для валідаторів діяти чесно та дотримуватися правил мережі.

Стратегії проактивного моніторингу та реагування на загрози, які можуть бути використані для забезпечення більш ефективного захисту платформ DeFi:

- Цілодобовий моніторинг транзакцій: впровадження інструментів для безперервного відстеження транзакцій на платформі. Це включає використання аналітичних інструментів для виявлення підозрілої активності в реальному часі.

- Аналіз логів: використання програмних рішень для збирання та аналізу логів дій користувачів і системи. Це допомагає швидко виявляти аномалії або невідповідності у поведінці системи.
- Каталогізація загроз та інцидентів: ведення бази даних відомих загроз, атак та їхніх наслідків. Це допоможе швидко ідентифікувати нові загрози, порівнюючи їх з попередніми випадками.
- Системи автоматичного відключення: впровадження механізмів, які автоматично зупиняють підозрілі транзакції або блокують доступ до системи у разі виявлення загрози. Наприклад, при виявленні незвичайного обсягу транзакцій за короткий час система може тимчасово призупинити ці транзакції для перевірки.
- Оповіщення та сповіщення: налаштування системи сповіщень для негайного інформування адміністраторів та розробників про виявлені загрози.

ВИСНОВКИ

Тема дослідження безпеки в децентралізованих фінансах на EVM-сумісних блокчейнах є надзвичайно актуальною в сучасному світі, де DeFi стають все більш популярними як інструмент фінансових операцій та інвестування. Основними перевагами DeFi є доступність, прозорість і відсутність посередників у порівнянні з традиційними фінансовими системами. Проте, існують значні виклики, пов'язані з безпекою та ризиками використання децентралізованих платформ.

Відповідно до визначених завдань, у першому розділі було охарактеризовано явище та поняття децентралізованих фінансів, розглянуто основні концепції блокчейн технологій та EVM-сумісних блокчейнів. Було вивчено історію та розвиток DeFi, а також основні принципи та механізми їх функціонування, включаючи аналіз переваг та недоліків.

У другому розділі було проаналізовано ключові EVM-сумісні платформи, такі як Ethereum, Binance Smart Chain та Polygon. Окрім загальної характеристики, були розглянуті технологічні аспекти функціонування цих платформ, зокрема консенсус, валідація транзакцій та особливості безпеки.

У третьому об'єднаному розділі було проведено аналіз типових загроз та інцидентів, що трапляються у децентралізованих фінансах, а також розглянуто сучасні технології та методи забезпечення безпеки. Зокрема, були розглянуті кейс-стадії зламів та втрат активів, що дозволило глибше зрозуміти реальні ризики.

Також було здійснено вибір методів та інструментів для дослідження безпеки на EVM-сумісних платформах. Було оброблено та проаналізовано дані про безпеку, що дозволило виявити основні вразливості. На основі цього аналізу були розроблені рекомендації для покращення безпеки в децентралізованих

фінансах, що включають технічні рішення та практичні поради для користувачів та розробників.

У даній бакалаврській роботі було проведено комплексне дослідження безпеки в DeFi, що включає аналіз загроз, методів захисту та випадків зловживань. Розроблені рекомендації спрямовані на покращення безпеки, а саме: вбудовані точки відновлення, використання штучного інтелекту для аналізу, оптимізації та симуляції атак та децентралізована аудиторська мережа. Впровадження запропонованих рішень дозволить знизити ризики та забезпечити більш надійну і захищену платформу для користувачів, сприяючи таким чином розширенню застосування DeFi у фінансових операціях та інвестиціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chen, Y., & Bellavitis, C. (2019). Decentralized finance: Blockchain technology and the quest for an open financial system. *Stevens Institute of Technology School of Business Research Paper*. 1-10
2. Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review*. 1-4
3. Sapienza, P., & Zingales, L. (2012). A trust crisis. *International Review of Finance*, 123-131.
4. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf.
5. Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, 92-95.
6. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37), 2-1.
7. Raskin, M. (2016). The law and legality of smart contracts. *Geo. L. Tech. Rev.*, *1*, 305.
8. Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE access*, *6*, 53019-53033.
9. Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, *6*, 1151724.
10. Metcalfe, W. (2020). Ethereum, smart contracts, DApps. *Blockchain and Cryptocurrency*, *77*, 77-93.
11. Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance*. John Wiley & Sons.

12. Coinmarketcap.com. Ethereum, 2024. URL: https://coinmarketcap.com/currencies/ethereum/
13. Binance Academy. The Complete Beginner's Guide to Decentralized Finance (DeFi), 2021. URL: https://academy.binance.com/en/articles/the-complete-beginners-guide-todecentralized-finance-defi.
14. Aquilina, M., Frost, J., & Schrimpf, A. (2024). Decentralized finance (DeFi): A functional approach. *Journal of Financial Regulation*, 1-27.
15. Meyer, E., Welpe, I. M., & Sandner, P. G. (2022). Decentralized finance—A systematic literature review and research directions. ECIS. 8-11
16. Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and decentralized finance (DeFi)*. National Bureau of Economic Research.
17. Kirvesoja, V. (2022). *Advantages and disadvantages of decentralized financial (DeFi) services* (Master's thesis).
18. Antonopoulos, A. M., & Wood, G. (2018). *Mastering ethereum: building smart contracts and dapps*. O'reilly Media.
19. Solidity Team. (n.d.). *Solidity Documentation.* URL: https://docs.soliditylang.org/en/v0.8.25/
20. *Ethereum Virtual Machine (EVM)*. Ethereum.org. URL: https://ethereum.org/en/developers/docs/evm/
21. Badruddoja, S., Dantu, R., He, Y., Upadhayay, K., & Thompson, M. (2021, May). Making smart contracts smarter. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-3). IEEE.
22. *Vyper Documentation*. URL: https://docs.soliditylang.org/en/v0.8.25/
23. Mungoli, N. (2023). HybridCoin: Unifying the Advantages of Bitcoin and Ethereum in a Next-Generation Cryptocurrency. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY*, 235-250.

24. Binance. (n.d.). *Binance Smart Chain Whitepaper*. URL: https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md
25. Safi, O., & Atabeyli, M. (2023). Blockchains and Smart Contracts for Cryptocurrency: An Analysis of Their Functionality and Performance.
26. Singh, S., & Sharma, R. (2021). *Secured Insurance Framework Using Blockchain and Smart Contract.* ResearchGate
27. *Proof of Staked Authority (PoSA) on Binance Smart Chain*. URL: https://academy.binance.com/en/glossary/proof-of-staked-authority-posa
28. *BNB Chain Documentation. URL: https://docs.bnbchain.org*
29. *BNB Chain: The Web3 blueprint. URL: https://www.bnbchain.org/en/blog/bnb-chain-the-web3-blueprint*
30. BNB Chain Team. *Building DeFi on BNB Smart Chain (BSC): The World's Number One Layer 1 by DAU*. BNB Chain Blog. URL: https://www.bnbchain.org/en/blog/building-defi-on-bnb-smart-chain-bsc-the-worlds-number-one-layer-1-by-dau
31. *BNB Chain 2024 tech roadmap*. BNB Chain Blog. URL: https://www.bnbchain.org/en/blog/bnb-chain-2024-tech-roadmap
32. DeFi Llama. *DeFi metrics on Binance Smart Chain*. URL: https://defillama.com/chain/BSC
33. Senta, R., Sawant, A., & Jain, S. (2024). Enhancing Food Safety and Transparency in the Supply Chain through Polygon Blockchain and Cloud Integration. *International Journal of Computing and Digital Systems*, *16*(1), 189-202.
34. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. *URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 201-224.

35. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). Sok: Layer-two blockchain protocols. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24* (pp. 201-226). Springer International Publishing.
36. Polygon Technology. *Polygon: Ethereum's Internet of Blockchains*. URL: https://docs.polygon.technology/pos/
37. Jia, R., & Yin, S. (2022, November). To EVM or not to EVM: Blockchain compatibility and network effects. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (pp. 23-29).
38. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.
39. Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2016). Secure multiparty computations on bitcoin. *Communications of the ACM*, *59*(4), 76-84.
40. Buterin, V. Ethereum white paper: A next generation smart contract & decentralized application platform. URL: https://ethereum.org/en/whitepaper/
41. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.
42. Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., ... & Zanella-Béguelin, S. (2016, October). Formal verification of smart contracts: Short paper. In *Proceedings of the 2016 ACM workshop on programming languages and analysis for security* (pp. 91-96).
43. Brandstätter, T., Schulte, S., Cito, J., & Borkowski, M. (2020, November). Characterizing efficiency optimizations in solidity smart contracts. In *2020*

IEEE International Conference on Blockchain (Blockchain) (pp. 281-290). IEEE.

44. Praitheeshan, P., Pan, L., Yu, J., Liu, J., & Doss, R. (2019). Security analysis methods on ethereum smart contract vulnerabilities: a survey. *arXiv preprint arXiv:1908.08605*.
45. Saveetha, D., & Maragatham, G. (2023). Detection of Re-Entrancy, Timestamp Dependence and Infinite Loop Attack in Smart Contracts Using Graph Convolution Network. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(11s), 285-292.
46. Ferreira Torres, C., Iannillo, A. K., Gervais, A., & State, R. (2021, March). The eye of horus: Spotting and analyzing attacks on ethereum smart contracts. In *International Conference on Financial Cryptography and Data Security* (pp. 33-52). Berlin, Heidelberg: Springer Berlin Heidelberg.
47. Feist, J., Grieco, G., & Groce, A. (2019, May). Slither: a static analysis framework for smart contracts. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)* (pp. 8-15). IEEE.
48. Qin, K., Ye, Z., Wang, Z., Li, W., Zhou, L., Zhang, C., ... & Gervais, A. (2023). Towards automated security analysis of smart contracts based on execution property graph. *arXiv preprint arXiv:2305.14046*.
49. Wu, S., Li, Z., Yan, L., Chen, W., Jiang, M., Wang, C., ... & Zhou, H. (2024, April). Are We There Yet? Unraveling the State-of-the-Art Smart Contract Fuzzers. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (pp. 1-13).
50. Tolmach, P., Li, Y., Lin, S. W., Liu, Y., & Li, Z. (2021). A survey of smart contract formal specification and verification. *ACM Computing Surveys (CSUR)*, *54*(7), 1-38.

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Дослідження децентралізованих фінансів на основі EVM-сумісних блокчейнів для їх безпечного зберігання»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав(ла): Зубенко В.В., ІСД-41
Науковий керівник роботи:
д.т.н., професор Сторчак К.П.

Київ - 2024

Актуальність теми: безпека в децентралізованих фініансах є вкрай актуальною через зростання використання DeFi платформ, збільшення кіберзагроз та необхідність розробки надійних методів захисту для забезпечення сталого розвитку фінансових технологій.

Об`єкт дослідження: Процес забезпечення безпеки в децентралізованих фінансах на основі EVM-сумісних блокчейнів.

Предмет дослідження: безпека децентралізованих фінансів на основі EVM-сумісних блокчейнів.

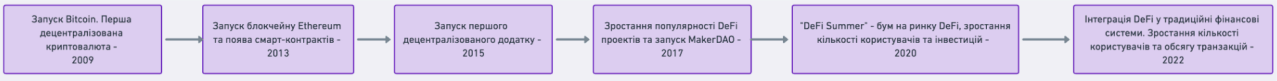
Мета дослідження: Дослідження можливостей та ефективності використання децентралізованих фінансів на EVM-сумісних блокчейнах для підвищення безпеки.

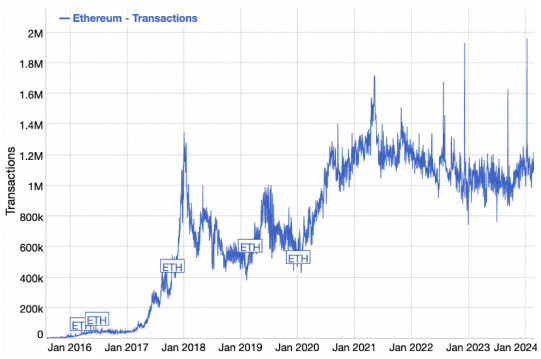
Завдання дослідження:

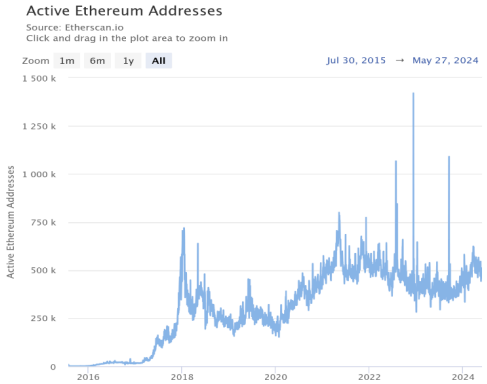
1. Дослідити процес розвитку EVM-сумісних блокчейнів;
2. Проаналізувати ключові EVM-сумісні платформи;
3. Проаналізувати ключові загрози та виклики безпеки в децентралізованих фінансах;
4. Проаналізувати випадки атак у децентралізованих фінансах;
5. Розробити рекомендації для покращення безпеки в децентралізованих фінансах;

Історія та розвиток DeFi

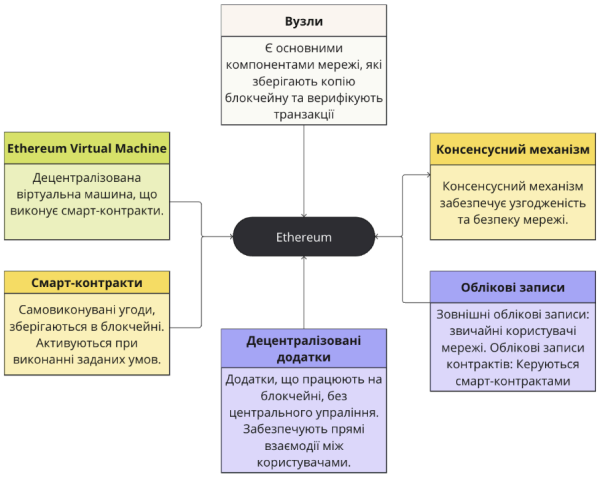
Децентралізовані фінанси виникли як альтернатива традиційним фінансовим системам, використовуючи технології блокчейн та смарт-контракти для забезпечення фінансових послуг без посередників.

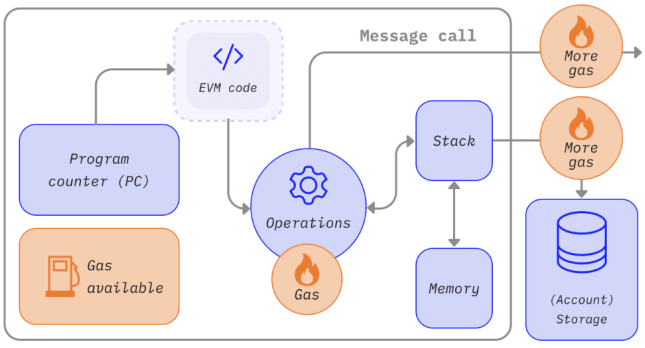






Блокчейн Ethereum. Візуалізація Архітектури та Функціонування



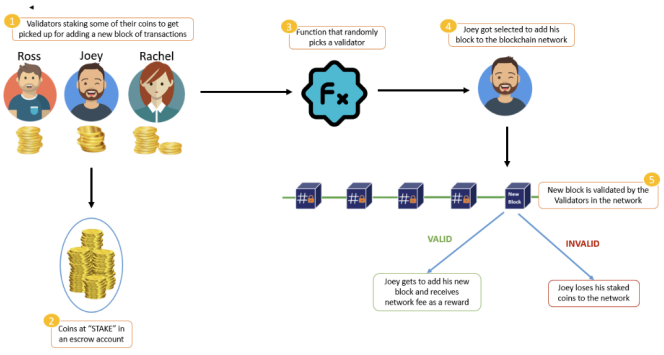


Властивості децентралізованих фінансів

Критерії	Централізовані фінанси	Децентралізовані фінанси
Контроль	Централізовані організації	Мережа вузлів
Прозорість	Обмежена	Висока
Доступність	Залежить від юрисдикції	Глобальна
Анонімність	Обмежена	Висока
Програмованість	Обмежена	Висока
Швидкість транзакцій	Від хвилин до днів	Від миттєво до хвилин
Вартість транзакцій	Висока	Низька
Безпека	Залежить від організацій	Базується на криптографії
Регулювання	Національне та міжнародне	Мало регульована
Доступ до фінансових послуг	Обмежений	Відкритий

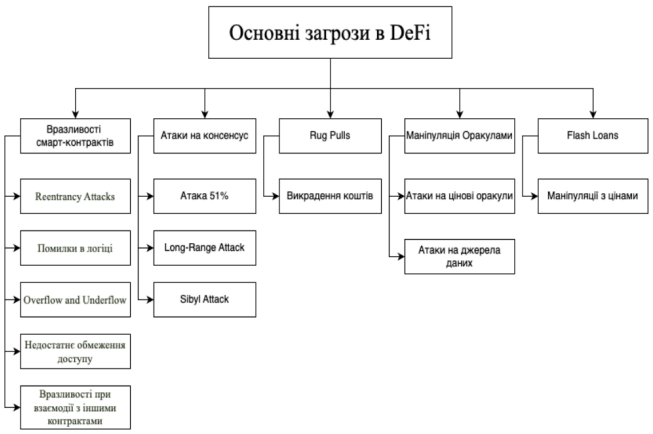
Огляд EVM-сумісних блокчейнів

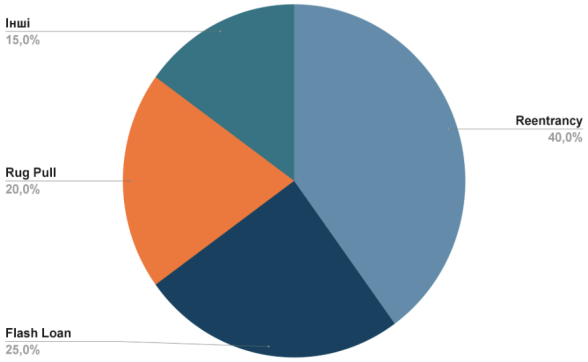
Платформа	Ethereum	Binance Smart Chain	Polygon
Запуск	2015	2020	2017
Пропускна здатність	15тр/с	55тр/с	65тр/с
Комісія за транзакцію	Висока	Низька	Дуже низька
Консенсусний механізм	Proof of Stake (PoS)	PoS Authority (PoSA)	Proof of Stake (PoS)
Особливості	Найбільш поширена платформа	Висока сумісність з Ethereum, низькі комісії	Механізм контрольних точок, низькі комісії
TVL (млрд $)	65	5	2
Децентралізація	Висока	Низька	Середня
Масштабованість	Низька	Середня	Висока



Візуалізація роботи консенсусу PoS

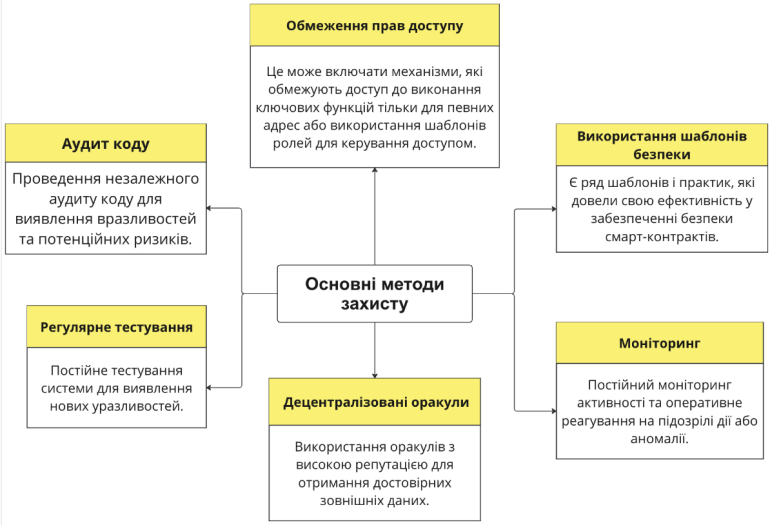
Загрози в DeFi





Найпоширеніші типи атак

Методи захисту DeFi



Таблиця ефективності методів захисту

Метод захисту	Складність реалізації	Вартість	Надійність
Аудит коду	Висока	Висока	Висока
Обмеження прав доступу	Низька	Низька	Середня
Використання шаблонів	Низька	Низька	Середня
Моніторинг	Середня	Середня	Висока
Децентралізовані оракули	Середня	Середня	Висока
Регулярне тестування	Середня	Середня	Висока

Аналіз типових інцидентів

The Dao Attack

Масштабна хакерська атака, яка сталася у червні 2016 року і була спрямована на DAO. Внаслідок вразливості, відомої як "reentrancy", в коді смарт-контракту хакери змогли вивести близько 60 мільйонів доларів США. Ця атака призвела до розколу в спільноті Ethereum і створення двох окремих блокчейнів: Ethereum і Ethereum Classic.

bZx Attack

При атаці на bZx використовували тип атаки "flash loan attack". Хакери скористалися вразливостями в протоколі bZx, отримуючи миттєві кредити без застави та маніпулюючи ринковими цінами, що дозволило їм викрасти значні суми криптовалюти. Після атаки впровадили додаткові шари контролю за транзакціями.

Poly Network Hack

Стався у серпні 2021 року і є одним з найбільших хакерських нападів у сфері децентралізованих фінансів. Хакери скористалися вразливістю у міжланцюговому протоколі Poly Network, що дозволило їм викрасти криптовалюту на суму понад $600 мільйонів. Згодом більшість коштів було повернуто після переговорів з хакерами.

Harvest Finance Exploit

У жовтні 2020 року платформа Harvest Finance зазнала експлойту, що призвів до втрати приблизно $24 мільйонів. Зловмисник скористався вразливістю у механізмі ціноутворення, що залежав від оракулів та метод флеш-позик для маніпуляції цінами активів у пулі ліквідності, що дозволило їм вивести значні суми коштів.

Огляд рекомендацій

1 Регулярні аудити

Залучення команди внутрішніх та зовнішніх аудиторів для регулярного перегляду та перевірки коду смарт-контрактів.

2 Впровадження стандартів

Дотримання встановлених стандартів написання смарт-контрактів, які забезпечують базову безпеку та функціональність.

3 Проактивний моніторинг

Постійне відстеження та аналіз діяльності системи з метою передбачення та попередження потенційних загроз до того, як вони завдадуть шкоди.

4 Інтеграція ШІ

Впровадження ШІ для комплексного аналізу, оптимізації та симуляції атак на смарт-контракти забезпечить виявлення вразливостей та допоможе створювати більш стійкі системи.

5 Точки відновлення

Дозволяє створювати певні стани контракту, до яких можна повернутися у разі виявлення проблем або аномалій.

6 Децентралізована аудиторська система

Система, де незалежні учасники перевіряють смарт-контракти на наявність вразливостей. Винагороди стимулюють якісний аудит, а рейтингова система оцінює роботу аудиторів.

Розробка рекомендацій

Інтеграція ШІ

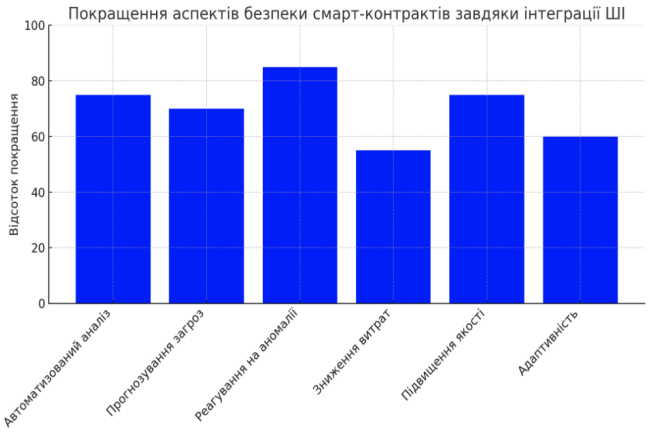
Інтеграція штучного інтелекту у смарт-контракти може покращити їх безпеку, ефективність та надійність на 60-75%. ШІ забезпечує автоматизований аналіз та виявлення вразливостей, прогнозує потенційні загрози, реагує на аномалії в реальному часі, знижує витрати на аудит, підвищує якість та надійність контрактів та адаптується до нових загроз. Це робить ШІ ключовим інструментом для розвитку безпечних децентралізованих систем.

Точки відновлення

Точки відновлення значно підвищують безпеку DeFi-систем, дозволяючи створювати регулярні знімки стану смарт-контрактів. У випадку виявлення аномалій або атак, ці знімки можуть бути використані для швидкого відновлення до попереднього безпечного стану, мінімізуючи втрати та збитки. Такий підхід підвищує стійкість до атак. Крім того, механізм точок відновлення забезпечує резервне копіювання критичних даних і дозволяє гнучко налаштовувати частоту створення знімків та умови їх активації.

Децентралізована аудиторська система

Забезпечує прозорість та незалежність процесу аудиту, зменшуючи ризик корупції та упередженості. Дозволяє залучити велику кількість аудиторів, стимулюючи їх винагородами, що підвищує якість перевірок. Результати аудиту доступні для всіх учасників мережі, що сприяє довірі користувачів до смарт-контрактів. Система легко масштабується і інтегрується з іншими децентралізованими технологіями, створюючи надійну екосистему.



Перевага	Опис
Підвищена прозорість	Забезпечення доступності результатів перевірок для всіх учасників мережі.
Незалежність і неупередженість	Зменшення ризику упередженості або змови.
Висока стійкість до корупції	Менша схильність до корупційних дій завдяки децентралізації.
Масова перевірка і верифікація	Ефективне виявлення вразливостей завдяки великій кількості учасників.
Гнучкість і масштабованість	Легке масштабування з ростом кількості смарт-контрактів і користувачів.
Стимулювання якості аудиту	Винагорода за якісне виконання аудиту.
Довіра і репутація	Підвищення довіри користувачів до смарт-контрактів.
Синергія з іншими децентралізованими технологіями	Добра інтеграція з іншими децентралізованими технологіями.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Зубенко В.В. Дослідження децентралізованих фінансів на основі EVM-сумісних блокчейнів для їх безпечного зберігання. Матеріали IV Всеукраїнська науково-практичної конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті». Збірник тез, ДУІКТ, м. Київ - К.: ДУІКТ, 2024. - С. 49.

Висновки

У рамках дослідження було досліджено процес розвитку EVM-сумісних блокчейнів, що дозволило виявити основні тенденції та напрями еволюції цієї технології, включаючи впровадження нових функціональностей та оптимізацію продуктивності. Проаналізовано ключові EVM-сумісні платформи, такі як Ethereum, Binance Smart Chain та Polygon.

Визначено ключові загрози та виклики безпеки в децентралізованих фінансах, зокрема вразливості смарт-контрактів, що можуть бути експлуатовані хакерами, та ризики, пов’язані з атаками. Проаналізовано випадки атак у децентралізованих фінансах, що дозволило виявити основні причини та механізми цих атак, а також окреслити наслідки для користувачів та екосистеми в цілому, підкресливши необхідність підвищення рівня безпеки.

Розроблено рекомендації для покращення безпеки в децентралізованих фінансах, які включають удосконалення процедур аудиту смарт-контрактів для виявлення потенційних вразливостей до їх запуску, інтеграції штучного інтелекту для аналізу та оптимізації, впровадження контрольних точок відновлення, модульного тестування, системи автоматичного відключення та децентралізованої аудиторської системи.