

ДОСЛІДЖЕННЯ ТА РОЗРОБКА КРИПТОВАЛЮТНОГО ТЕРМІНАЛУ ДЛЯ МАСОВИХ ПЛАТЕЖІВ

Груша В. В., науковий керівник Болбот І. М.

У сучасних фінансових екосистемах швидкість та гнучкість платежів визначають конкурентну перевагу, а жорсткі тарифи і єдині моделі обробки транзакцій не відповідають динаміці навантажень та потребам бізнесу. Дослідження зосереджено на розробці моделі криптовалютного терміналу, що поєднує інструменти активного керування комісіями, децентралізовану ідентифікацію, розширені механізми безпеки та аналітики для адаптації до будь-яких змін технологічного й регуляторного ландшафту.

Платформа включатиме модуль динамічного аукціону, здатний аналізувати стан мемпулу в реальному часі, прогнозувати навантаження на мережу та розраховувати оптимальні комісії для бажаної швидкості підтвердження. Алгоритми, що спираються на систематизацію Layer 2-протоколів, дозволять балансувати між мінімальною вартістю транзакції та гарантованим часом її включення до блоку. Попередні розрахунки демонструють потенційне скорочення витрат на транзакцію до 37% порівняно зі статичними моделями комісій. Користувачі зможуть самостійно визначати пріоритет обробки своїх транзакцій, а система адаптуватиме параметри під поточне навантаження мережі.

Архітектура ідентифікації учасників базується на децентралізованих ідентичностях (DID) із селективним розкриттям атрибутів відповідно до стандартів W3C. Поєднання zk-Rollup технологій з модифікованою моделлю дочірніх ланцюгів Plasma формує двошаровий захист конфіденційності: транзакційна приватність для приховування деталей операцій та комплаєнс-аудит для регуляторної прозорості уповноваженим учасникам. Адаптація протоколу з авторськими модифікаціями може підвищити пропускну здатність системи на 42% при збереженні рівня конфіденційності, забезпечуючи ефективне масштабування зі зростанням користувацької бази.

Цілісність ключів забезпечуватимуть порогові BLS-підписи з параметрами m - 3 - n , оптимізовані для високонавантажених середовищ. Дизайн передбачає адаптивні мультипідписні схеми з автоматичним перерозподілом "квазістаф-ключів" при відмові учасників, підтримуючи безперервність функціонування. Система threat intelligence на основі нейромережових алгоритмів досягатиме точності виявлення аномалій понад 94%. Механізми запобігання fraud branching атакам збережуть роботоздатність навіть при компрометації до 30% вузлів мережі, перевершуючи існуючі комерційні рішення на 15-20%. Додаткові алгоритми аномальної детекції доповнять статичні засоби захисту моніторингом нехарактерних патернів взаємодії.

Архітектурний план включає DAO-смайт-контракт із поетапним голосуванням за критичні параметри системи, даючи стейкхолдерам можливість впливати на розвиток протоколу без форків. Розширені HTLC-протоколи з інтелектуальним маршрутизатором ліквідності забезпечать ефективну взаємодію між різними блокчейн-мережами. Оптимізовані Duplex Micropayment Channels з цільовим часом підтвердження менше 1.5 секунди забезпечать швидкі міжмережіві трансфери з мінімальними втратами на курсових різницях. Функціональність аналізу пулів автоматичних маркет-мейкерів дозволить обирати оптимальний шлях для проведення транзакцій у реальному часі.

Комплект розробника включатиме універсальні SDK з підтримкою 9 мов програмування та REST API з повною OpenAPI-специфікацією для спрощення інтеграції. Адміністративна панель відображатиме аналітичні дашборди реального часу та прогностичні моделі оптимізації потоків, візуалізуючи час підтвердження, обсяги, динаміку комісій і показники ризику. Нативна інтеграція з IoT-пристроями через енергоефективний протокол розширить можливості застосування системи в сфері

Інтернету речей. Інтерактивна аналітика з деталізацією до окремих транзакцій допоможе виявляти вузькі місця та оптимізувати параметри роботи платформи.

Інфраструктурний дизайн передбачає географічно розподілену Active-Active архітектуру з синхронною реплікацією для забезпечення безперервності при відмові цілих дата-центрів. Узгоджені ReplicaSet та PodDisruptionBudget політики забезпечать доступність на рівні 99.99%, гарантуючи функціональність критичної кількості інстансів. Цільові показники відновлення плануються на рівні RTO менше 2 хвилин та RPO менше 30 секунд, що перевищує галузеві стандарти. Автоматизовані процедури ескроу та ротації ключів із регулярною верифікацією захистять криптографічні матеріали та пришвидшать відновлення в критичних ситуаціях. Система регулярних знімків стану в захищених апаратних модулях (HSM) підвищить рівень захисту та забезпечить швидке відновлення після збоїв.

Запропонована модель криптовалютного терміналу формує концепцію універсальної, гнучкої та екологічно відповідальної платформи, здатної знизити середню вартість транзакцій на 35-40%, підвищити пропускну здатність до 10,000 TPS та забезпечити відповідність вимогам FATF та ISO 27001. Економічний аналіз демонструє можливе скорочення операційних витрат бізнесу до 28% порівняно з традиційними платіжними шлюзами. Соціальні переваги охоплюють розширення доступу до фінансових послуг для неохоплених банківським сектором верств населення та створення інклюзивної фінансової екосистеми з низьким порогом входу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Harvey C. R. DeFi and the Future of Finance / C. R. Harvey, A. Ramachandran, J. Santoro. – Wiley, 2021. – 288 с.
2. Bashir I. Mastering Blockchain: A Deep Dive into Distributed Ledgers, Consensus Protocols, Smart Contracts, DApps, Cryptocurrencies, Ethereum, and More / I. Bashir. – Packt Publishing, 2023. – 784 с.

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



**ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ
АСПЕКТИ РОЗРОБКИ
КОМП'ЮТЕРНИХ СИСТЕМ**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів