Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-21-2
Зражевець К.П.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Куля Ю.Е.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Зражевцю Кирилу Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2023р.
3. Вихідні дані до роботи: розгляд відомих технологій роботи блокчейну, оцінка доцільности використання механізмів роботи блокчейну, розгляд безпечності зберігання ключів у різних гаманців та методи покращення безпечності їх зберігання
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз сучасних технологій роботи блокчейну
2) Розгляд методів забезпечення безпеки даних у блокчейні
3) Аналіз сучасних методів збереження безпеки ключів
4) Розробка власного програмного забезпечення взаємодії з блокчейном

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Куля Юлія Едуардівна		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	25.02.2023	Виконано
3	Розробка 1 розділу	05.03.2023	Виконано
4	Розробка 2 розділу	20.03.2023	Виконано
5	Розробка 3 розділу	05.04.2023	Виконано
6	Розробка 4 розділу	25.04.2023	Виконано
7	Оформлення кваліфікаційної роботи	15.05.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студента _____ Зражевець К.П.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Куля Ю.Е.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 29 рис., 1 додаток, 12 джерел.

БЛОКЧЕЙН, КОНСЕНСУС, ТРИЛЕМА БЛОКВЕЙНУ, СМАРТ-КОНТРАКТИ, ОРАКУЛИ, ТРАНЗАКЦІЇ, ХЕШУВАННЯ, ШИФРУВАННЯ, КЛЮЧІ, ГАМАНЦІ, КРИПТОГРАФІЧНІ ПІДПИСИ, БЕЗПЕКА.

Об'єкт дослідження – процес створення безпечного рішення для зберігання ключів у блокчейн-технологіях.

Предмет дослідження – методи та засоби збереження ключів у блокчейн-технологіях.

Мета роботи – аналіз шляхів досягнення максимального ступіню збереження ключів та зниження потенційних рисків щодо їх компрометації, розробка власного програмного забезпечення для роботи із блокчейном зі зменшенням ризику компрометації ключів.

Методи досліджень – емпіричний аналіз, формалізація та порівняння.

Протягом виконання роботи був виконан аналіз сучасних технологій блокчейнів, методів роботи та збереження безпеки ключів під час використання гаманців та взаємодії із блокчейном. Розглянуто сучасні методи шифрування, хешування та підвищення безпеки ключів. Було виконано аналіз існуючих рішень для збереження ключів. Було розробленого програмне забезпечення для взаємодії із блокчейном за допомогою гаманця.

ABSTRACT

The report contains: 73 p., 29 p., 1 application, 12 sources.

BLOCKCHAIN, CONSENSUS, BLOCKCHAIN TRILEMMA, SMART-CONTRACTS, ORACLES, TRANSACTIONS, HASHING, ENCRYPTION, KEYS, WALLETS, CRYPTOGRAPHIC SIGNATURES, SECURITY.

The object of research is the process of creating a secure solution for key storage in blockchain technologies.

The subject of research is methods and ways of keys storage in blockchain technologies.

An aim of work is to analyze the ways to achieve the maximum level of key preservation and reduce the potential risks of their compromise., developing of own sofrware to work with blockchain with reduced risk of keys compromise.

Methods of researches are empirical analysis, formalization and comparison.

During the execution of the work, an analysis of modern blockchain technologies, work methods and preservation of security of use was performed. Modern methods of encryption, hashing and increasing the security of keys are considered. An analysis of existing keys storages soultions was performed. Software has been developed to interact with the blockchain using a wallet.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AES – advanced encryption standard

DeFI – decentralized finance

DES – data encryption standard

DLT – distributed ledger technology

DPoS – delegated proof of stake

DSA – digital signature algorithm

dApp – decentralized application

ECC – elliptic curve cryptography

ERC – ethereum request for comments

EVM – ethereum virtual machine

IOTA – internet of things application

ISO – international organization for standardization

MPT – merkle patricia tree

NFT – non-fungible token

NIST – national institute of standards and technology

PoA – proof of authority

PoH – proof of history

PoI – proof of importance

PoS – proof of stake

PoW – proof of work

P2P – peer to peer

RSA – Rivest, Shamir, Adleman

TCP – transmission control protocol

ZKP – zero knowledge proof

ВСТУП

Блокчейн – це інноваційна технологія, що надає можливість зберігати, обмінювати та перевіряти дані в електронній формі з високим рівнем безпеки та прозорості. Він став чимось більшим, ніж просто технічним рішенням, і перетворився на новий метод управління та обміну даними, що відкриває безліч можливостей для бізнесу, науки та суспільства в цілому. У наш час блокчейн використовується в різних галузях, від фінансів та медицини до голосування та забезпечення безпеки мережі Інтернет речей.

У сучасному світі цифрових технологій та глобального інформаційного простору блокчейн відіграє все більш важливу роль в економіці, фінансах, управлінні та соціальній сфері. Він пропонує нові можливості для створення децентралізованих систем, відкриває перспективи розвитку сфери криптовалют та надійного зберігання даних. Отже, розуміння сучасних технологій роботи блокчейну є актуальним та важливим напрямом для впровадження нових рішень у різних галузях людської діяльності.

Розгляд сучасних технологій роботи блокчейну зосереджується на їх різновидів, принципів функціонування та впровадження. Основною метою є аналіз сучасних технологій роботи блокчейну та оцінка їх потенціалу та можливостей впровадження в різних сферах економіки та соціуму.

Блокчейн являє собою особливий вид бази даних, до якої можна вносити інформацію, але не можна видаляти чи змінювати. Структура блокчейну являє собою ланцюг із блоків з інформацією, що містять у собі посилання на попередні блоки, та також деяку інформацію про транзакції, часові мітки та інші метадані, що використовуються для підтвердження його достовірності. Через те що усі блоки взаємопов’язані між собою, записана інформація не може бути відредагована, змінена чи видалена, бо у такому випадку усі попередні блоки стануть недійсними.

Оскільки блокчейн підтримується багатьма пристроями, він функціонує як децентралізована база даних. Це означає, що кожен вузол зберігає у собі копію даних блокчейну та виконує взаємодію з іншими вузлами, для того щоб підтверджувати збіг інформації у блоках.

Блокчейн забезпечує транспарентність, оскільки всі транзакції та інформація доступні для перегляду всіма учасниками мережі. Це створює відкрите та прозоре середовище, яке важко підробити або змінити. Водночас, блокчейн може

забезпечувати анонімність, оскільки ідентифікаційні дані користувачів замінюються на унікальні криптографічні адреси.

Однією з проблем, яка виникає в контексті блокчейну, є масштабованість, оскільки розростання мережі може призвести до зниження швидкості обробки транзакцій. Різні технологічні рішення, такі як шарування, шардинг та створення бічних ланцюгів, розроблені для розв'язання проблеми масштабованості та підвищення ефективності мережі.

Енергоефективність стає дедалі більш актуальною темою у світі блокчейну. Традиційний алгоритм консенсусу Proof of Work вимагає значної кількості електроенергії для підтримки мережі, що викликає стурбованість щодо екологічного впливу. Відповідно, розробляються альтернативні алгоритми консенсусу, такі як Proof of Stake, Delegated Proof of Stake та Proof of Authority, які спрямовані на зниження енергоспоживання та підвищення екологічної стійкості блокчейн-технологій.

Оскільки на ринку з'являється все більше блокчейн-проектів та мереж, забезпечення взаємодії між ними стає однією з ключових проблем. Крос-ланцюгові рішення, такі як атомарні обміни, мости блокчейнів та інтероперабельні протоколи, спрямовані на спрощення обміну інформації та цінностей між різними блокчейн-мережами.

Регуляція блокчейн-технологій є актуальною проблемою, оскільки уряди та регулятори починають приділяти увагу забезпеченню легітимності цих технологій та їх використання. Стандартизація практик, термінології та процедур сприятиме розвитку та адаптації блокчейну в різних сферах діяльності та індустріях. Організації, такі як Enterprise Ethereum Alliance, Hyperledger Foundation та International Organization for Standardization активно працюють над створенням стандартів для блокчейн-індустрії.

1 РІЗНОВИДИ БЛОКЧЕЙНІВ, МЕТОДИ РОБОТИ, ОСНОВНІ ТЕХНОЛОГІЇ

1.1 Моделі консенсусу

Однією з ключових особливостей блокчейн-технологій є механізм консенсусу, який дозволяє учасникам мережі погоджуватися на одній версії історії транзакцій без необхідності довіри один одному. Найбільш розповсюдженими з них являються наступні.

1) Proof of Work – це одна з найбільш розповсюджених моделей консенсусу, яка використовується в більшості блокчейнів, таких як Bitcoin та Ethereum. У PoW майнери конкурують за право додати блок до ланцюжка, вирішуючи складні математичні задачі. Той, хто першим знаходить рішення, отримує винагороду в криптовалюті. До переваг можна віднести високу безпеку: атака на мережу вимагає великої обчислювальної потужності та витрат; запобігання подвійних витрат: атака на мережу нерентабельна, оскільки витрати на атаку перевищують можливу вигоду. До недоліків можна віднести високі енергетичні витрати: майнінг вимагає великої кількості електроенергії; централізацію майнінгу: великі майнери контролюють значну частину обчислювальної потужності мережі [1].

2) Proof of Stake – це альтернативний механізм консенсусу, в якому учасники мережі блокують (або ставлять) частину своїх криптовалютних активів на блокчейні, щоб отримати право створити наступний блок. Ймовірність створення блоку пропорційна кількості активів, заблокованих учасником. PoS-алгоритми використовуються у таких криптовалютах, як Cardano, Polkadot та Ethereum 2.0. До переваг можна віднести екологічну стійкість: менші енергетичні витрати порівняно з PoW; зниження ризику централізації: можливість для менших учасників мережі брати участь у створенні блоків. До недоліків можна віднести відсутність випробуваної безпеки: Pos-блокчейни є відносно новими та ще не пройшли випробування часом, як PoW; нерівність активів: учасники з більшими ставками мають більше шансів на створення блоків.

3) Delegated Proof of Stake (DPoS) – це варіант PoS, в якому власники криптовалют вибирають представників (делегатів) для створення блоків та підтримки мережі. DPoS використовується в таких блокчейн-проектах, як EOS, Lisk та Tezos. До переваг можна віднести швидкість та масштабування: делегати

можуть працювати над створенням блоків ефективніше, що підвищує пропускну здатність мережі; зниження енергетичних витрат: менші енергетичні витрати порівняно з PoW. До недоліків можна віднести ризик централізації: делегати з великими кількостями криптовалют можуть набути диспропорційно великого впливу на мережу; відсутність випробуваної безпеки: як і в PoS, DPoS-блокчейни відносно нові та ще не пройшли часового випробування.

4) Proof of Importance – це консенсусний алгоритм, запропонований у блокчейні NEM. Він базується на принципі, аналогічному Proof of Stake, проте враховує не лише кількість активів, що належать учасникам мережі, але й їх «важливість» або вклад у мережу. Важливість вимірюється на основі кількох факторів, таких як кількість здійснених транзакцій, зв'язків з іншими учасниками та інвестицій в мережу. Учасники з більшою важливістю мають більше шансів створити блок та отримати винагороду. До переваг можна віднести стимулювання активності: PoI заохочує учасників мережі до активного залучення в транзакції та співпрацю з іншими користувачами; екологічність: PoI використовує значно менше енергії порівняно з Proof of Work, що забезпечує більш сталий розвиток технології; відображення реального вкладу: важливість враховує дійсний внесок учасників у мережу, не залежачи від їх матеріальних ресурсів. До недоліків можна віднести комплексність: PoI вимагає складнішої системи визначення важливості та підрахунку відносних показників; обмежене застосування: PoI використовується переважно у мережі NEM, що обмежує його поширеність та адаптацію в інших проектах.

5) Proof of Authority – це консенсусний механізм, в якому відповідальність за створення блоків передається набору довірених валідаторів, обраних на основі їх репутації та відповідальності. PoA використовується в приватних та деяких публічних блокчейнах, таких як VeChain та xDai. До переваг можна віднести швидкість та масштабування: менший набір валідаторів працює ефективніше, забезпечуючи високу пропускну здатність; зниження енергетичних витрат: менші енергетичні витрати порівняно з PoW. До недоліків можна віднести централізацію: можливість контролю мережі невеликою кількістю валідаторів; залежність від репутації валідаторів: валідатори можуть стати мішенями для атак або корумпуватися, що може підривати довіру до мережі.

6) Proof of History – це консенсусний алгоритм, який вперше був запропонований для використання в блокчейн-мережі Solana. Основна ідея PoH полягає в створенні криптографічного часового журналу з відбитками часу, що

дозволяє учасникам мережі дійти згоди щодо послідовності транзакцій без необхідності використання складних алгоритмів консенсусу. До переваг можна віднести швидкість: PoH може забезпечити високу пропускну здатність та низькі затримки транзакцій; ефективність: PoH використовує менше ресурсів порівняно з PoW та PoS; синхронізацію: PoH дозволяє легко визначити порядок транзакцій в мережі. До недоліків можна віднести новизну: PoH є відносно новим алгоритмом консенсусу, що може створювати певні ризики та невизначеність; відсутність широкого застосування: наразі PoH використовується переважно в мережі Solana.

1.2 Рівні блокчейну

Рівні блокчейна можна розглядати як архітектурні компоненти, що складаються з різних протоколів, алгоритмів та механізмів, що спільно забезпечують функціонування мережі Блокчейн можна розділити на чотири рівня.

1) Нульовий рівень (Layer 0): протоколи передачі даних. Нульовий рівень відповідає за передачу даних між вузлами мережі. Він включає в себе протоколи комунікації, які забезпечують надійне та безпечне передавання інформації між учасниками блокчейну. На цьому рівні використовуються такі протоколи, як TCP, P2P та інші механізми передачі даних. Цей рівень забезпечує основу для побудови вищих рівнів блокчейну. Нульовий рівень відповідає за створення децентралізованої інфраструктури, яка усуває необхідність центрального органу або посередника. Також рівень забезпечує криптографічний захист даних, що допомагає зберігати інформацію безпечно та недоступною для сторонніх.

2) Перший рівень (Layer 1): протоколи блокчейну. Перший рівень блокчейну відповідає за створення та підтримку основної блокчейн-інфраструктури, зокрема блоків, транзакцій та консенсусу між вузлами мережі. Протоколи цього рівня визначають, яким чином блоки створюються, як вони зв’язуються між собою та як мережа досягає консенсусу щодо валідності транзакцій. Прикладами блокчейнів першого рівня є Bitcoin, Ethereum, Litecoin та інші. Перший рівень вирішує проблему визначення однозначного стану мережі, запобігаючи таким проблемам, як подвійні витрати, завдяки протоколам консенсусу. Протоколи консенсусу першого рівня допомагають забезпечити безпеку мережі від різноманітних атак, таких як атаки 51% або сибілів.

3) Другий рівень (Layer 2): протоколи оффчейну. Другий рівень блокчейну включає протоколи та рішення, які дозволяють розширити

масштабованість, швидкість та ефективність мережі, розробляючи рішення поза основним блокчейном. Ці протоколи дозволяють зменшити навантаження на основну мережу та покращити її продуктивність. Прикладами рішень другого рівня є Lightning Network для Bitcoin, Optimism та Arbitrum для Ethereum. Оффчейн рішення на другому рівні можуть знизити комісії за транзакції, оскільки вони можуть відбуватися поза основним блокчейном.

4) Третій рівень (Layer 3): додатки та сервіси. Третій рівень блокчейну відповідає за розробку додатків та сервісів, які використовуються користувачами та організаціями для взаємодії з мережею. Він включає смарт-контракти, децентралізовані додатки, організації, що працюють на основі блокчейну, та інші інструменти та сервіси, що використовуються для реалізації різноманітних функцій, таких як фінансові операції, управління активами, голосування, аутентифікація та інше. Третій рівень дозволяє розробникам створювати додатки, які можуть інтегруватися з існуючими системами, що полегшує прийняття та впровадження блокчейн-технологій у традиційних організаціях та бізнесах [2].

Отже, кожен рівень блокчейну відповідає за вирішення конкретних проблем, пов'язаних з розвитком технології та її впровадженням. Нульовий рівень забезпечує базову інфраструктуру для підтримки децентралізації, перший рівень використовує протоколи консенсусу для забезпечення безпеки та однозначності мережі, другий рівень покращує масштабність та ефективність мережі за допомогою оффчейн рішень, а третій рівень сприяє створенню та інтеграції різних додатків та сервісів на основі блокчейну. Завдяки цій багаторівневій архітектурі, блокчейн-технологія може бути адаптована для різних застосувань, від фінансових операцій та голосування до систем управління активами та децентралізованого управління організаціями.

Схематичне зображення загальної структури рівнів блокчейну зображене на рисунку 1.1.

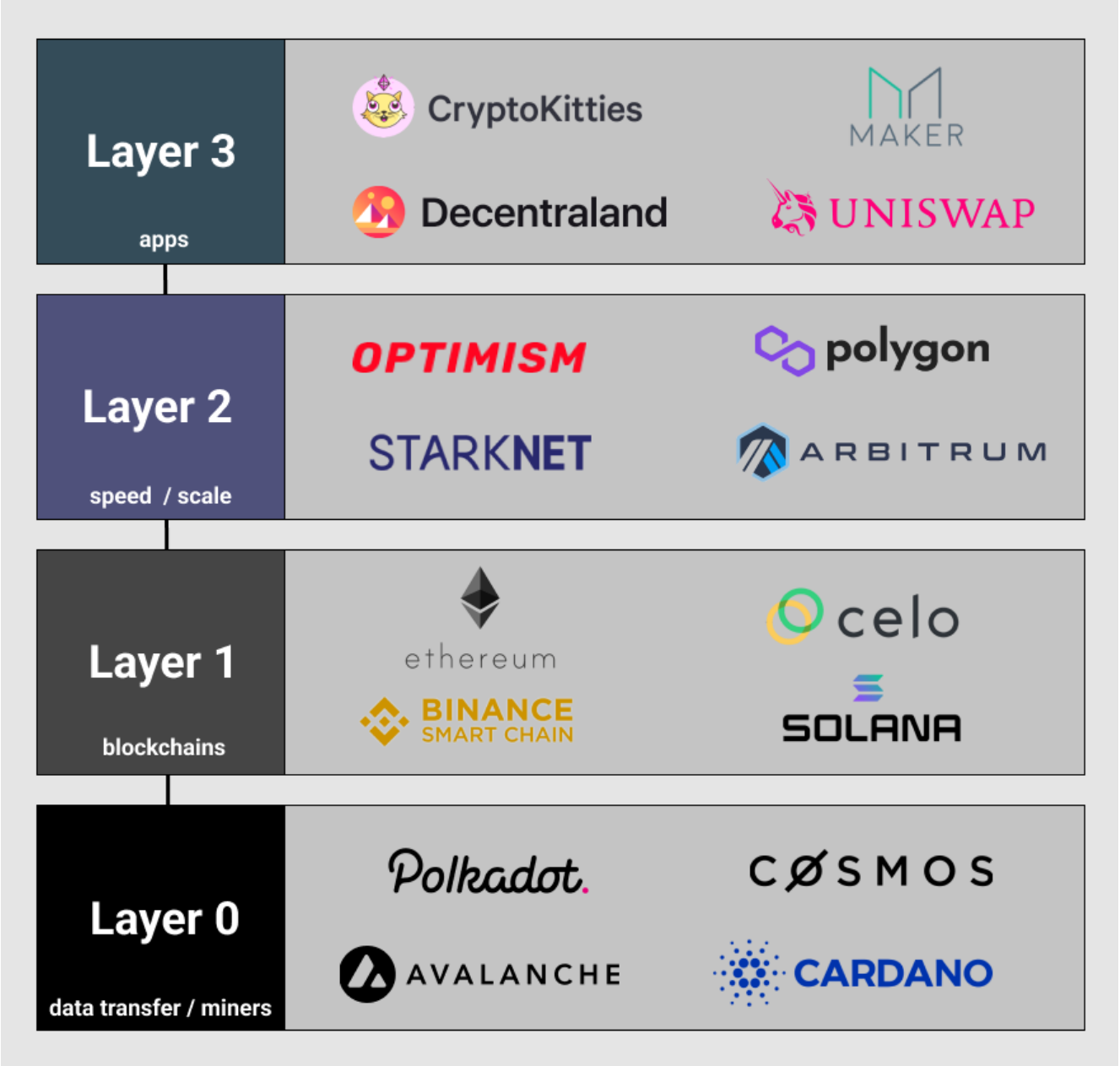

Рисунок 1.1 – Структура рівнів блокчейну

1.3 Типи блокчейнів за видами доступу

Типи блокчейнів можна класифікувати за ступенем доступу до мережі та контролю над ними. Загалом, існують три основні типи блокчейнів: відкриті (публічні), закриті (приватні) та консорціум блокчейни.

Відкриті блокчейни, такі як Bitcoin та Ethereum, є децентралізованими мережами, де будь-яка особа може приєднатися та взаємодіяти з мережею. Учасники мають можливість переглядати всі транзакції та взаємодіяти з мережею за допомогою криптографічних ключів. Відкриті блокчейни використовують різні моделі консенсусу для забезпечення безпеки та децентралізації.

Переваги відкритих блокчейнів.

1) Висока ступінь децентралізації та відсутність центрального контролю.
2) Вільний доступ для учасників з усього світу.
3) Забезпечення прозорості та незмінності даних.

До недоліків відкритих блокчейнів можна віднести те, що масштабування та швидкість транзакцій можуть бути обмежені та відносно високу витрату енергії в деяких моделях консенсусу.

Закриті блокчейни контролюються однією організацією або групою організацій, які вирішують, хто може приєднатися та взаємодіяти з мережею. Ці блокчейни можуть мати обмежений доступ до даних та зазвичай використовуються для внутрішніх корпоративних потреб. Як правило, закриті блокчейни використовують більш ефективні та енергозберігаючі моделі консенсусу

Переваги закритих блокчейнів.

1) Контрольований доступ до мережі, що дозволяє забезпечити конфіденційність даних.
2) Більш швидкі та масштабовані транзакції в порівнянні з відкритими блокчейнами.
3) Енергоефективність та нижчі витрати на обслуговування.

До недоліків закритих блокчейнів можна віднести те, що централізований контроль може призвести до зловживань або небажаних змін у мережі та те, що обмежений доступ може знизити рівень довіри до мережі з боку зовнішніх сторін.

Консорціум блокчейни є проміжним типом між відкритими та закритими блокчейнами. Вони контролюються групою організацій, які разом вирішують правила та умови доступу до мережі. Учасники консорціуму можуть використовувати спільну мережу для забезпечення ефективної обробки транзакцій та обміну даними між сторонами.

Переваги консорціум блокчейнів.

1) Співпраця між учасниками дозволяє забезпечити ефективне управління та контроль над мережею.
2) Висока прозорість та відстежуваність транзакцій між сторонами.
3) Енергоефективність та швидкість обробки транзакцій порівняно з відкритими блокчейнами.

До недоліків консорціум блокчейнів можна віднести те, що обмежений доступ до мережі та контроль над нею можуть створити певний рівень централізації.

Вибір найкращого типу блокчейну залежить від конкретних потреб та цілей організації або проекту. Відкриті блокчейни можуть бути найкращим варіантом для децентралізованих фінансових систем або глобальних додатків з відкритим доступом. Закриті блокчейни можуть бути відповідним вибором для корпоративних мереж, де контроль над даними та конфіденційність є пріоритетом. Консорціум блокчейни можуть бути корисними для спільних проектів та партнерств між різними організаціями, що шукають прозорість та ефективність у взаємодії.

1.4 Трилема блокчейну

Трилема блокчейну є ключовим поняттям у розумінні технології блокчейну та її обмежень. Трилема відображає взаємозв'язок трьох основних характеристик блокчейну: децентралізації, безпеки та масштабованості. Згідно з трилемою, система може одночасно мати тільки дві з цих трьох властивостей, але не всі три одночасно. Це є однією з головних проблем розвитку блокчейн-технологій, яка вимагає компромісів та рішень для підвищення ефективності та широкого застосування.

Децентралізація є одним з основних принципів блокчейну, який полягає в тому, що мережа не має центрального керуючого органу або одного сервера. Замість того, блокчейн-мережа складається з вузлів, кожен з яких зберігає та валідує всю інформацію в мережі. Децентралізація забезпечує відсутність контрольного органу, який може вплинути на рішення, прийняті в мережі, та забезпечує відсутність однієї точки відмови.

Безпека є важливою складовою блокчейн-технологій, оскільки вона забезпечує захист від зовнішніх атак та спроб злому. Безпека блокчейну забезпечується за допомогою криптографічних методів, таких як хешування та цифрові підписи, а також за допомогою різних протоколів консенсусу, які ускладнюють атаки на мережу.

Масштабованість є критичною властивістю для будь-якої технології, яка прагне до широкого застосування та прийняття. У контексті блокчейну масштабованість відноситься до здатності мережі обробляти велику кількість

транзакцій та запитів одночасно без значного зниження швидкості або стабільності. Відомо, що масштабованість є однією з ключових проблем, з якими зіштовхуються деякі блокчейни, такі як Bitcoin і Ethereum, через обмеження у розмірі блоків та часу між блоками.

Схематичне зображення трилеми блокчейну можна побачити на рисунку 1.2.

Рисунок 1.2 – Трилема блокчейну

Трилема блокчейну заявляє, що мережа може забезпечити тільки дві з трьох властивостей одночасно. Якщо мережа фокусується на децентралізації та безпеці, це може привести до обмеженої масштабності, що знижує швидкість та пропускну здатність мережі. З іншого боку, якщо мережа забезпечує високу масштабність, вона може стати більш централізованою або менш безпечною.

Для вирішення трилеми блокчейну розробники та дослідники постійно працюють над новими рішеннями та підходами. Однією з таких технологій є рішення другого рівня, такі як Lightning Network для Bitcoin і Arbitrum для

Ethereum, які дозволяють проводити транзакції поза основним блокчейном, що забезпечує відмінну масштабність без жертвування децентралізацією чи безпекою.

Іншим підходом до вирішення трилеми блокчейну є розробка нових алгоритмів консенсусу. Також досліджуються різні архітектурні рішення, такі як шардінг, який дозволяє розділяти мережу на декілька менших сегментів, що працюють паралельно, для підвищення пропускної здатності та загальної ефективності.

Всі ці рішення та підходи спрямовані на вирішення трилеми блокчейну, щоб забезпечити оптимальне співвідношення децентралізації, безпеки та масштабності для різних застосувань блокчейн-технологій. Однак на сьогодні ще не існує універсального рішення, яке б повністю вирішило трилему блокчейну для всіх сценаріїв застосування. Різні проекти та платформи блокчейну можуть вибирати різні компроміси, в залежності від своїх цілей та потреб користувачів. Наприклад, випадок застосування, який вимагає швидких транзакцій та високої пропускної здатності, може вибрати рішення з більшою масштабністю, але з меншою децентралізацією. З іншого боку, застосування, якому необхідна висока безпека та децентралізація, можуть прийняти компроміс з меншою масштабністю [3].

1.5 EVM-сумісні блокчейни

EVM-сумісні блокчейни – це альтернативні блокчейн-платформи, які були створені для сумісності з Ethereum Virtual Machine, що дозволяє їм виконувати ті ж смарт-контракти та додатки, які були розроблені для Ethereum. Ці блокчейни створені з метою вирішення певних проблем Ethereum, таких як масштабованість, швидкість транзакцій та високі комісії, не втрачаючи при цьому можливості взаємодії з екосистемою Ethereum.

Основні причини створення EVM-сумісних блокчейнів.

1) Масштабованість: Ethereum стикається з проблемами масштабування через обмежену пропускну здатність мережі. EVM-сумісні блокчейни зазвичай використовують власні протоколи консенсусу або альтернативні рішення для забезпечення вищої пропускної здатності.

2) Швидкість транзакцій: високий рівень завантаження Ethereum може призвести до повільних часів підтвердження транзакцій. EVM-сумісні блокчейни намагаються вирішити цю проблему, пропонуючи швидше підтвердження транзакцій.

3) Високі комісії: завантаження мережі Ethereum може призвести до високих комісій для користувачів. EVM-сумісні блокчейни прагнуть зменшити вартість транзакцій, пропонуючи низькі комісії.

Однак EVM-сумісні блокчейни також мають деякі недоліки.

1) Рівень децентралізації: деякі EVM-сумісні блокчейни можуть мати менший рівень децентралізації, ніж Ethereum, через свої механізми консенсусу або контроль з боку засновників.

2) Залежність від Ethereum: оскільки EVM-сумісні блокчейни базуються на Ethereum Virtual Machine, їх успіх та стабільність залежать від успіху Ethereum. У разі виникнення проблем із безпекою або стабільністю Ethereum, це може вплинути на всі EVM-сумісні блокчейни.

3) Розподіл ресурсів: інтеграція з Ethereum може мати свої недоліки, оскільки розробники та користувачі можуть бути розділені між Ethereum та EVM-сумісними блокчейнами. Це може призвести до меншої ліквідності, активності користувачів та ресурсів для розвитку додатків на кожній платформі.

4) Сумісність з майбутніми оновленнями Ethereum: EVM-сумісні блокчейни можуть стикатися з проблемами сумісності з майбутніми оновленнями Ethereum, які можуть змінити архітектуру EVM або внести інші значні зміни.

5) Безпека: використання EVM може перенести деякі аспекти безпеки Ethereum на EVM-сумісні блокчейни. Хоча це може бути перевагою, оскільки Ethereum досить безпечний, це також може створити ризики, пов'язані з потенційними проблемами безпеки EVM.

З усіх цих причин EVM-сумісні блокчейни можуть бути привабливим рішенням для розробників і користувачів, які шукають альтернативи Ethereum, що пропонують поліпшену масштабність, швидкість транзакцій та нижчі комісії. Проте, потрібно проаналізувати всі вище наведені важливі фактори, перш ніж вирішувати, який EVM-сумісний блокчейн найкраще підходить для конкретного проекту або додатку.

Декілька ключових EVM-сумісних блокчейнів та їх особливості.

1) Binance Smart Chain було створено криптовалютною біржею Binance, щоб забезпечити швидке та ефективне середовище для розробки та використання смарт-контрактів. Він пропонує низькі комісії та короткі часи підтвердження транзакцій, завдяки використанню консенсусу Proof of Staked Authority. Він забезпечує сумісність з Ethereum, дозволяючи розробникам легко переносити свої додатки та смарт-контракти на платформу. Він став популярним місцем для

розгортання децентралізованих фінансових додатків та NFT через свою високу продуктивність та низькі комісії. Однак, його рівень децентралізації є об'єктом критики, оскільки він в основному керується Binance та валідаторами, обраними Binance.

2) Polygon – це масштабована мережа, сумісна з Ethereum, яка має на меті підтримувати EVM-сумісні смарт-контракти та надавати високу пропускну здатність. Polygon використовує комбінацію шардінгу та платформи другого рівня для підтримки смарт-контрактів на своїй мережі. Це дозволяє знизити комісії та скоротити час підтвердження транзакцій у порівнянні з Ethereum. Polygon надає розробникам Ethereum можливість легко переносити свої додатки та смарт-контракти на свою платформу. Це створює місце для розвитку децентралізованих додатків та децентралізованих фінансових сервісів з високою пропускною здатністю та низькими комісіями. Polygon також підтримує токени ERC-20 та ERC-721, що робить його ідеальним місцем для розгортання NFT.

3) Avalanche – це високопродуктивний блокчейн, який використовує новий протокол консенсусу, Avalanche Consensus, і надає EVM-сумісне середовище для розробки та розгортання смарт-контрактів.

1.6 Смарт-контракти

Смарт-контракти – це самовиконувальні програми, які автоматично виконують умови контракту між сторонами без необхідності додаткового втручання. Вони вбудовані в блокчейн та виконуються автоматично після виконання певних умов. Смарт-контракти можуть використовуватися для автоматизації процесів, зменшення відсотка людської помилки та зниження вартості та часу виконання операцій [4].

Смарт-контракти стали особливо популярними завдяки платформі Ethereum, яка розробила мову програмування Solidity спеціально для створення та розгортання таких контрактів на її блокчейні. З того часу, інші блокчейн-платформи, такі як EOS, Cardano та Tezos, також розробили власні смарт-контракти та мови програмування, що забезпечують їх функціонування. Це відкрило нові можливості для створення децентралізованих додатків на базі смарт-контрактів, які можуть виконувати різноманітні функції, від децентралізованої фінансової системи до віртуальних організацій.

Схематичне зображеня виконання смарт-контракту можна побачити на рисунку 1.3.

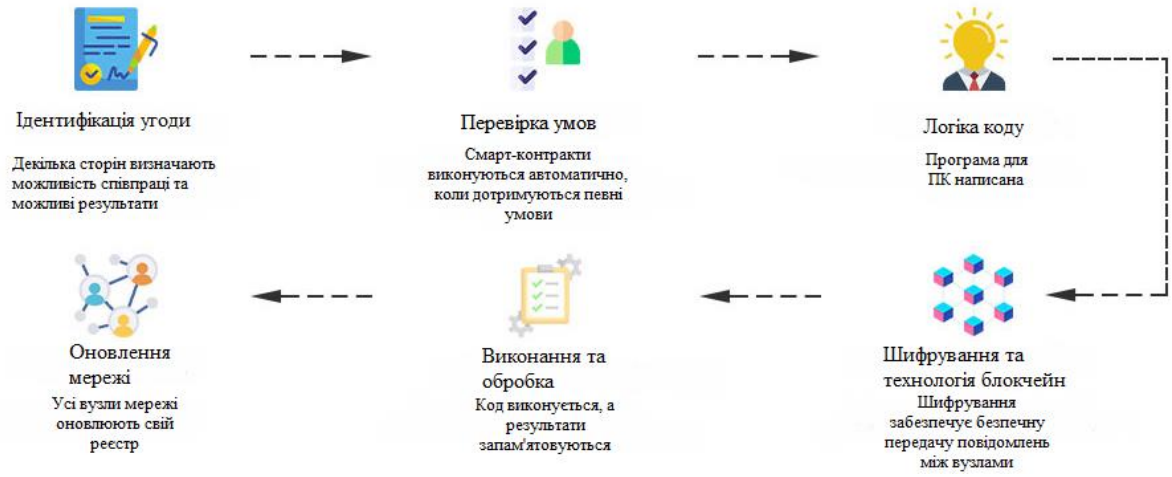

Рисунок 1.3 – Шлях виконання смарт-контракту

Однією з ключових переваг смарт-контрактів є відсутність потреби в посередниках, таких як юридичні або фінансові установи, для підтвердження та виконання угод між сторонами. Всі умови контракту записані в блокчейні в формі коду, і це гарантує прозорість та надійність угод. Крім того, це підвищує ефективність та знижує витрати на здійснення транзакцій, оскільки відсутність посередників забезпечує менші комісії та більш швидше виконання угод [5].

Однак, смарт-контракти також мають свої недоліки. Помилки у коді можуть призвести до втрати коштів або блокування активів, як це сталося з відомим випадком з The DAO у 2016 році, коли хакер використав помилку у коді смарт-контракту для крадіжки коштів. Крім того, масштабування та пропускна здатність блокчейнів, що використовують смарт-контракти, можуть бути обмеженими, що може призвести до зниження швидкості транзакцій та збільшення вартості газу. Це стало особливо помітним під час періодів пікової активності на платформі Ethereum, коли деякі користувачі зіткнулися зі збільшенням комісій та затримками у виконанні транзакцій.

Також, необхідно враховувати проблеми конфіденційності та захисту даних, пов'язані з використанням смарт-контрактів. Блокчейн, як правило, є прозорим та відкритим для перегляду, що може змусити сторони бути обережними щодо передачі та зберігання конфіденційної інформації в смарт-контрактах. Деякі платформи, такі як Monero та Zcash, розробляють технології конфіденційних

смарт-контрактів для захисту приватності користувачів та захисту їхньої інформації.

Незважаючи на зазначені вище недоліки, смарт-контракти продовжують набувати популярності та розвиватися, і майбутнє блокчейн-технологій великою мірою залежить від успіху смарт-контрактів. На сьогоднішній день вже існує велика кількість децентралізованих додатків, які базуються на смарт-контрактах, і надалі очікується їх поширення в різних галузях та сферах діяльності.

Виходячи з цього можна зазначити, що смарт-контракти представляють величезний потенціал для автоматизації та забезпечення безпеки транзакцій у ряді сфер, від фінансів до логістики. Незважаючи на їх недоліки, такі як помилки в коді, обмеження масштабування та проблеми конфіденційності, інновації в сфері блокчейн та смарт-контрактів продовжують розвиватися. Відповідно, можна очікувати постійного вдосконалення технологій, забезпечення більшої пропускної здатності та відпрацювання методів захисту конфіденційної інформації.

Також варто зазначити, що смарт-контракти можуть стати основою для створення децентралізованих автономних організацій та децентралізованого управління. Це може призвести до створення нових моделей бізнесу, які будуть набагато менш залежні від посередників та відповідних витрат.

Враховуючи вище наведене, смарт-контракти мають потенціал стати ключовою технологією, що революціонізує багато галузей нашого життя. Завдяки непер ервному розвитку та вдосконаленню блокчейн-технологій, ми можемо очікувати, що смарт-контракти зможуть вирішувати поточні проблеми, такі як швидкість, масштабування та безпека, а також допомагати у вирішенні глобальних викликів, таких як кліматичні зміни, бідність та економічна нерівність.

З погляду регуляторної політики та законодавства, смарт-контракти можуть також вплинути на юридичну сферу, сприяючи змінам у понятті контрактів та їх виконання. Регулятори повинні враховувати вплив смарт-контрактів на правові системи та розробляти відповідні законодавчі акти, які б дозволили їм функціонувати в рамках існуючих правових систем.

Також важливо підкреслити вплив смарт-контрактів на освіту та професійний розвиток. Оскільки попит на спеціалістів у галузі блокчейн та смарт-контрактів продовжує зростати, навчальні заклади та організації повинні пристосуватися до цього тренду, розробляючи програми навчання та надаючи можливості для здобуття відповідних навичок.

Аудит безпеки смарт-контрактів – це процес незалежного аналізу коду смарт-контракту з метою виявлення потенційних слабких місць, помилок та зловживань. Це важливий крок для забезпечення безпеки, прозорості та надійності роботи смарт-контрактів в рамках блокчейн-екосистеми.

Основні етапи аудиту безпеки смарт-контрактів.

1) Збір інформації: аудитори збирають всю необхідну інформацію про смарт-контракт, включаючи його специфікації, код, документацію та інші матеріали.

2) Розбір коду: аудитори проводять детальний аналіз коду смарт-контракту, шукаючи потенційні вразливості, помилки або некоректну реалізацію функцій.

3) Статичний аналіз: використовуються спеціальні інструменти та програмне забезпечення для автоматичного аналізу коду смарт-контракту на наявність вразливостей та небезпечних патернів.

4) Динамічний аналіз: аудитори проводять тести на живому контракті, спробуючи відтворити різні атаки або зловживання, щоб перевірити реакцію контракту та ідентифікувати потенційні ризики.

5) Відповідність стандартам: смарт-контракт аналізується на відповідність загальноприйнятим стандартам безпеки, як-от стандартам Ethereum або іншим платформам блокчейну.

6) Підготовка звіту: після завершення аудиту аудитори підготовлюють детальний звіт, який описує знайдені проблеми, вразливості та рекомендації щодо їх вирішення. Звіт включає у себе загальну оцінку, вразливості та проблеми, рекомендації та заключні зауваження [6].

Аудит безпеки смарт-контрактів допомагає виявити та виправити потенційні проблеми, забезпечуючи надійність та безпеку функціонування контракту. Він відіграє важливу роль у впровадженні та розвитку блокчейн-технологій, оскільки сприяє підвищенню довіри користувачів до системи та забезпечує їхню захищеність від можливих зловживань.

У цілому, смарт-контракти є перспективною технологією, яка може мати значний вплив на різні аспекти нашого життя. Проте, для досягнення свого повного потенціалу, смарт-контракти потребують подальшого розвитку та інтеграції з існуючими системами та законодавством. Це вимагає співпраці між урядами, приватним сектором, академічними та дослідницькими установами.

Приклад звіту з виконаним аудитом можна побачити на рисунку 1.4.

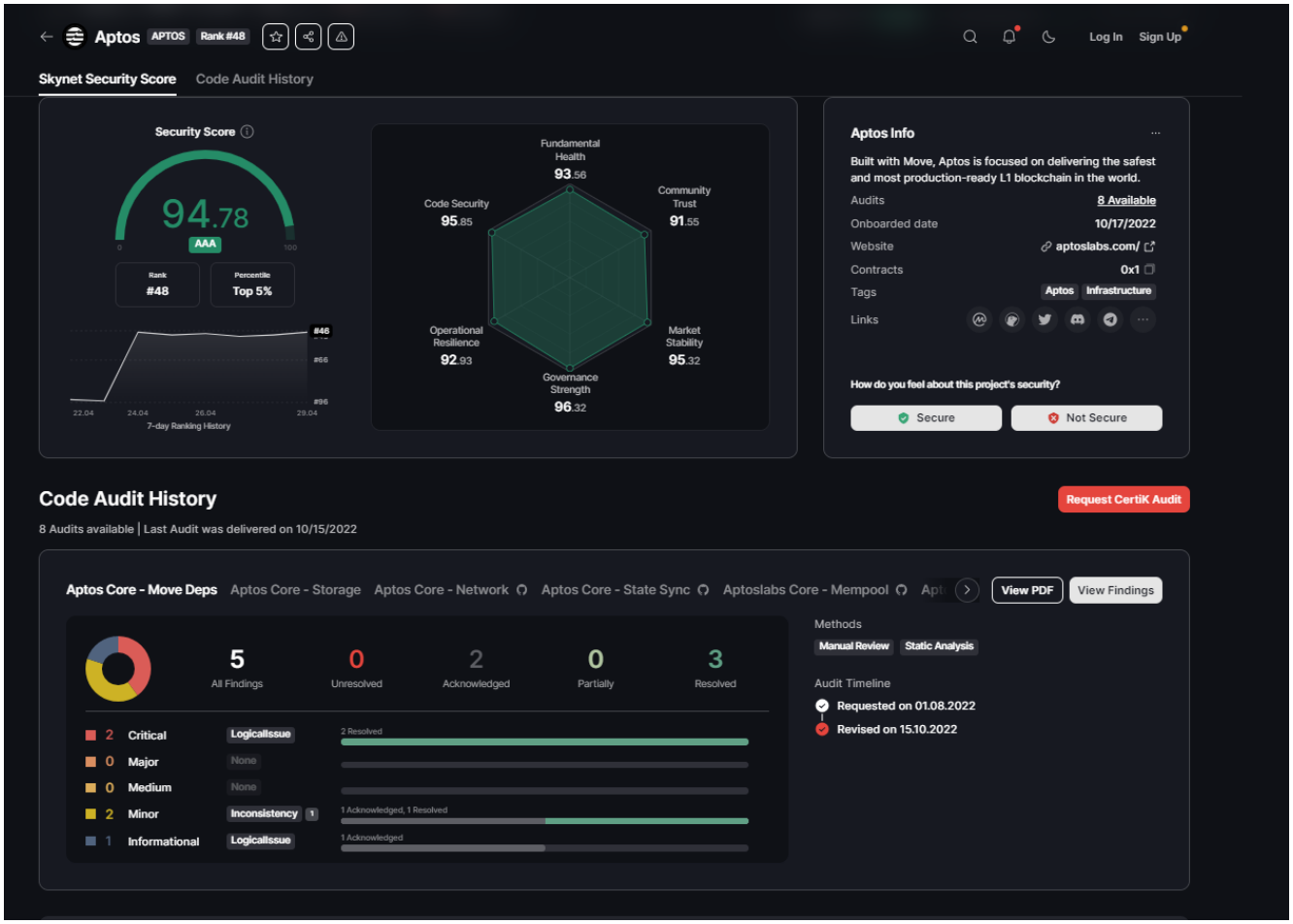

Рисунок 1.4 – Результати звіту після аудиту Aptos від Certik

1.7 Доказ із нульовим розголошенням

Zero-knowledge proof – це криптографічна технологія, яка дозволяє одній стороні довести іншій стороні, що певна інформація або знання є правдивими, не розкриваючи саму інформацію. У контексті блокчейну ZKP може використовуватися для підтримки приватності та безпеки транзакцій, водночас забезпечуючи достовірність та аудитованість даних.

Ключові характеристики та переваги технології Zero-knowledge proof.

1) Приватність: ZKP може забезпечити приватність транзакцій у блокчейні, дозволяючи користувачам доводити валідність своїх транзакцій без розкриття деталей, таких як суми або ідентифікаційні дані. Це робить ZKP особливо привабливим для блокчейнів, які прагнуть підтримувати високий рівень приватності для своїх користувачів.

2) Легкість аудиту: незважаючи на приватність, ZKP дозволяє провести аудит транзакцій та переконатися, що вони відповідають певним критеріям, не

порушуючи приватності учасників. Це може бути корисним для регуляторів або інших сторін, які хочуть перевірити відповідність транзакцій без доступу до чутливої інформації.

3) Безпека: ZKP використовує складні криптографічні протоколи, що робить його важким для зловмисників, які намагаються порушити приватність або маніпулювати даними. Це забезпечує високий рівень безпеки транзакцій у блокчейні.

4) Сумісність: Технологія Zero-knowledge proof може бути інтегрована в різні блокчейн-системи та платформи. Вона може бути використана як в публічних блокчейнах, де приватність та анонімність є важливими, так і в приватних блокчейнах, де контроль доступу та відповідність регулятивним нормам є важливими факторами.

5) Ефективність: незважаючи на складність криптографічних протоколів, сучасні реалізації ZKP можуть пропонувати високу ефективність та масштабованість. Це означає, що вони можуть бути використані в різноманітних застосуваннях та індустріях, не створюючи значного навантаження на мережу або інфраструктуру блокчейну.

Схематичне зображення схеми роботи доказу із нульовим розголошенням можна побачити на рисунку 1.5.

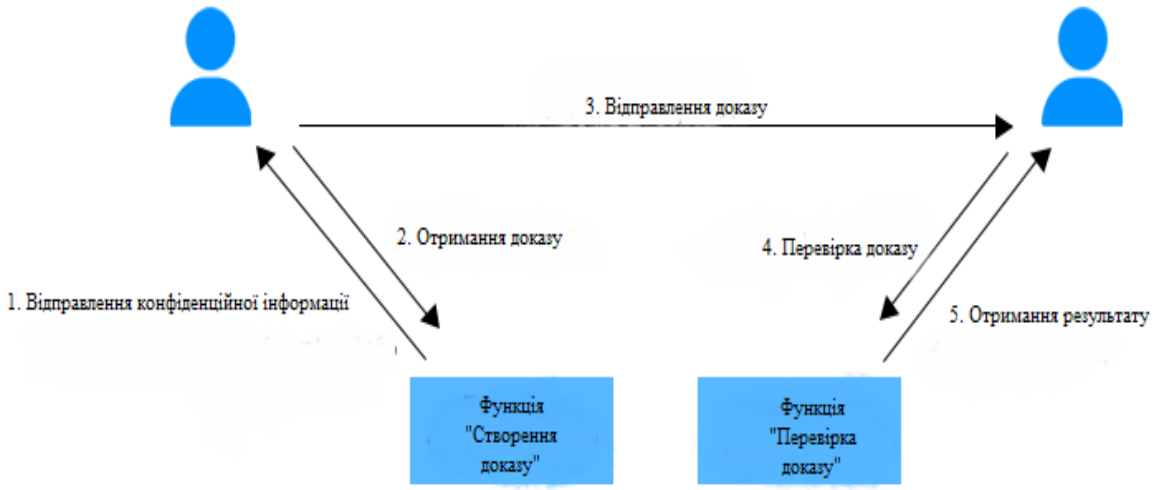

Рисунок 1.5 – Схема роботи доказу із нульовим розголошенням

Технологія Zero-knowledge proof продовжує розвиватися та знаходити нові застосування в різних сферах, таких як фінанси, охорона здоров'я, постачання, вибори та інше. У майбутньому можна очікувати бачити ще більше інновацій та

покращень, пов'язаних з ZKP, що сприятиме широкому впровадженню цієї технології в блокчейн-системах та за їх межами.

1.8 Розподілені технології обліку

Розподілені технології обліку – це сімейство технологій, які дозволяють створювати та управляти децентралізованими базами даних. Блокчейн є одним з видів Distributed Ledger Technology (DLT), що використовує ланцюг блоків для збереження інформації. Інші види DLT включають протоколи, як-от IOTA, Hashgraph та Holochain.

IOTA використовує унікальний тип DLT, відомий як Tangle. Tangle – це ациклічний спрямований граф, який дозволяє забезпечити масштабування та високу швидкість транзакцій без потреби в майнерах. Замість блоків, Tangle використовує взаємопов'язані транзакції, які перевіряються іншими транзакціями. Ця структура дозволяє зменшити витрати на обробку транзакцій та забезпечити високу пропускну здатність, особливо актуально для інтернету речей.

Hashgraph є альтернативною DLT, яка використовує консенсусний алгоритм, заснований на віртуальному голосуванні, замість майнінгу або стейкінгу. Hashgraph використовує ациклічний спрямований граф для зберігання інформації та забезпечення узгодження в мережі. Цей підхід дозволяє досягти високої пропускної здатності та надійності без великих витрат на енергію, які властиві традиційному майнінгу.

Holochain – це інноваційна DLT, яка відрізняється від блокчейну за своєю архітектурою та підходами до зберігання даних. Вона використовує розподілений граф, замість ланцюжка блоків, і дозволяє користувачам мати власні незалежні ланцюги, які синхронізуються з іншими ланцюгами за потреби. Holochain покликана створити масштабовану, енергоефективну та децентралізовану інфраструктуру для розробки різноманітних додатків та сервісів.

Radix є ще одним прикладом DLT, який намагається вирішити проблеми масштабування та пропускної здатності, властиві традиційним блокчейн-технологіям. Radix використовує темпоральний ациклічний граф та комбінує його з консенсусним алгоритмом, заснованим на коміті. Це дозволяє досягти високої швидкості транзакцій та зменшити затримки в обробці транзакцій. Окрім того, Radix пропонує власну платформу для смарт-контрактів, яка може бути використана для розробки децентралізованих додатків.

Конфіденційні розподілені технології обліку – це сімейство DLT, які фокусуються на забезпеченні конфіденційності та приватності. Ці технології використовують криптографічні методи, такі як нуль-довідкові докази (Zero-Knowledge Proofs) або гомоморфні шифрування, для захисту даних та забезпечення приватності користувачів. Прикладами є Zcash, Monero та Beam, які розроблені з метою забезпечення анонімності транзакцій та захисту фінансової приватності користувачів.

Розподілені технології обліку продовжують розвиватися та пропонувати нові та інноваційні підходи до зберігання та обробки даних. Вони забезпечують можливості для реалізації децентралізованих, масштабованих та безпечних систем, які можуть відповідати різним потребам та вимогам ринку. У майбутньому можна очікувати появу нових видів DLT, які зосереджуються на вирішенні конкретних проблем, таких як енергоефективність, конфіденційність, швидкість обробки транзакцій та інше.

Одним з ключових аспектів розвитку розподілених технологій обліку є можливість взаємодії та інтеграції різних DLT. Це включає розробку механізмів для безпечного та ефективного обміну даними та активами між різними блокчейн-платформами та DLT. Інтероперабельність може допомогти досягти більшої адаптації технології та поширення її використання в різних галузях та серед користувачів [7].

1.9 Оракули

Оракули в блокчейн-технологіях відіграють важливу роль, оскільки вони дозволяють доповнювати дані відтворюваної, децентралізованої мережі даними з зовнішніх джерел. Оракули є сторонніми сервісами, які надають інформацію з-поза блокчейна для використання в смарт-контрактах та інших додатках.

Ключові аспекти оракулів у блокчейн-технологіях.

1) Зовнішня інформація: оскільки блокчейни є замкненими системами, вони не мають прямого доступу до зовнішньої інформації, такої як ціни на активи, погода або інші дані, що змінюються. Оракули дозволяють розумним контрактам та іншим додаткам на блокчейні отримати доступ до цієї інформації.

2) Довіра: оракули повинні бути надійними джерелами інформації, оскільки рішення, прийняті на основі їх даних, можуть мати значні наслідки для

користувачів блокчейна. Це може створювати потенційні проблеми з централізацією та довірою, які блокчейн намагається вирішити.

3) Децентралізація: щоб зменшити ризик маніпуляції та збоїв, деякі оракули використовують децентралізовані мережі для надання інформації. В таких системах кілька незалежних джерел збирають дані з різних джерел і досягають консенсусу перед тим, як передавати інформацію розумному контракту.

4) Захист приватності: оскільки деякі дані, які надають оракули, можуть бути конфіденеційними або чутливими, важливо використовувати методи захисту приватності для забезпечення безпеки та непорушності цієї інформації. Один із способів захисту приватності полягає в використанні технологій шифрування або технік, які гарантують, що лише уповноважені сторони можуть отримати доступ до даних.

5) Оновлення та розширення: оракули повинні забезпечувати своєчасне та точне оновлення зовнішніх даних, щоб додатки на блокчейні могли працювати ефективно та відповідати змінам у зовнішніх умовах. Це може включати регулярні оновлення, підтримку нових джерел інформації та покращення протоколів безпеки.

6) Інтеграція: оракули повинні бути сумісними з різними блокчейн-технологіями та додатками. Вони повинні мати зручні та гнучкі інтерфейси для інтеграції з смарт-контрактами, а також можливість працювати з різними блокчейн-платформами.

Схематичне зображення методу роботи оракулу можна побачити на рисунку 1.6.

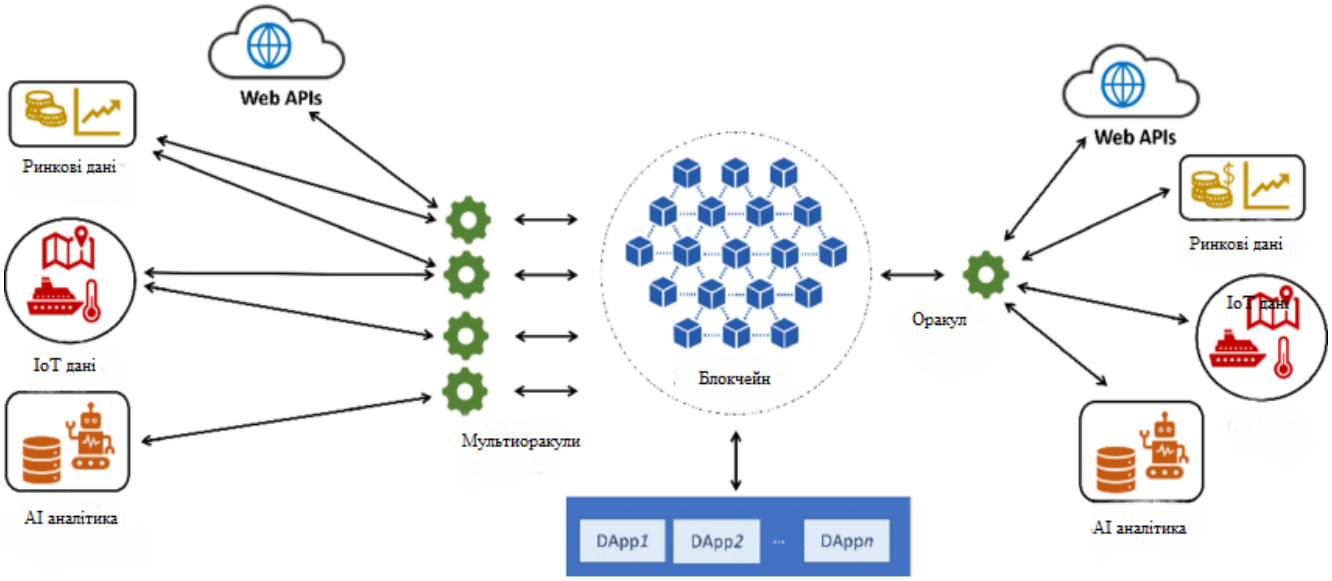

Рисунок 1.6 – Метод роботи оракулу

Оракули є життєво важливим компонентом у блокчейн-технологіях, які дозволяють смарт-контрактам та іншим додаткам отримувати інформацію зі світу поза блокчейном. Вони відіграють важливу роль у вирішенні проблеми доступу до зовнішніх даних та довіри, а також допомагають забезпечити безпеку та приватність користувачів.

1.10 Семантична мережа

Web3, також відомий як Web 3.0 або семантичний веб, є наступним етапом розвитку Інтернету. Це новий підхід до створення, структурування та взаємодії веб-додатків з метою децентралізації, безпеки та приватності. Web3 включає в себе використання блокчейн-технологій, розумних контрактів, децентралізованих додатків та інших технологій для досягнення своїх цілей.

Основні характеристики Web3.

1) Децентралізація: на відміну від традиційного Інтернету, де дані та сервіси контролюються централізованими організаціями, Web3 пропонує децентралізований підхід, який забезпечує більшу рівність та забезпечує, що жодна окрема сторона не може контролювати всю екосистему.

2) Безпека та приватність: Web3 прагне забезпечити безпеку та приватність користувачів за допомогою криптографічних методів, таких як шифрування, та інших протоколів безпеки. Це дозволяє користувачам контролювати свої дані та відомості про транзакції.

3) Взаємодія між різними блокчейнами: Web3 прагне до створення взаємодії між різними блокчейн-технологіями, такими як Ethereum, Polkadot, Cosmos та інші. Це дає можливість взаємодії між різними додатками та сервісами, незалежно від використовуваної платформи.

4) Розумні контракти та Decentralized Application (dApps): Web3 сприяє створенню розумних контрактів та децентралізованих додатків, які можуть працювати на блокчейні та автоматично виконувати дії на основі заданих умов. Розумні контракти є надійними та прозорими, оскільки вони працюють на основі коду, який може бути перевіреним, і їх результати зберігаються в блокчейні. dApps, зі своєї сторони, забезпечують ефективність, автономність та безпеку, оскільки вони не залежать від централізованого сервера або посередника.

5) Ідентифікація користувачів та управління цифровими активами: Web3 прагне створити нові методи ідентифікації користувачів, які забезпечують безпеку

та приватність. Один з таких методів – це використання децентралізованих ідентифікаторів, які дозволяють користувачам контролювати свою ідентичність та ділитися своїми даними на свій розсуд. Також Web3 сприяє створенню та управлінню цифровими активами, такими як криптовалюта, токени або NFT, через різні платформи та додатки.

6) Інтероперабельність та масштабованість: Web3 прагне до забезпечення інтероперабельності між різними блокчейн-мережами та іншими технологіями, такими як InterPlanetary File System або децентралізовані протоколи зберігання. Це дозволяє створювати великі масштабовані додатки та сервіси, які можуть працювати на різних платформах та взаємодіяти один з одним.

У цілому, Web3 має потенціал зробити революцію у способі, яким людство взаємодіє з Інтернетом та викоритовує його можливості. Він може привести до створення нових економічних моделей, глобального доступу до фінансових послуг, децентралізації влади та більшої приватності для користувачів. Однак, як і з будь-якою новою технологією, є виклики та проблеми, які потрібно вирішити, такі як масштабованість, енергоефективність та регулятивне середовище.

Можливі напрямки розвитку та досліджень у контексті Web3.

1) Удосконалення консенсусних алгоритмів: для забезпечення безпеки та масштабованості блокчейнів у майбутньому, дослідники можуть продовжувати розробляти нові консенсусні алгоритми та покращувати існуючі, такі як Proof of Work та Proof of Stake.

2) Енергоефективність: енергетична стійкість та ефективність є одними з ключових питань для розвитку Web3. Нові технології та алгоритми можуть допомогти зменшити відбиток блокчейну на навколишнє середовище та зробити його більш сталим.

3) Регулятивне середовище: у майбутньому потрібно врахувати регулятивні аспекти Web3. Влада та законодавчі органи можуть працювати над адаптацією існуючих законів або створенням нових, щоб контролювати децентралізовані технології та захищати інтереси користувачів.

4) Освіта та відповідальність користувачів: оскільки Web3 надає користувачам більше контролю над своїми даними та активами, зростає і відповідальність користувачів. Освіта та просвітництво є важливими аспектами для забезпечення того, що користувачі розуміють нові технології, ризики та можливості, які вони пропонують. Це може включати розробку навчальних матеріалів, курсів та ініціатив, що підвищують обізнаність користувачів.

5) Забезпечення приватності та безпеки: хоча Web3 прагне забезпечити більшу приватність та безпеку, це не означає, що він автоматично захищений від зловмисників та атак. Розробники та дослідники повинні продовжувати зосереджуватись на створенні надійних, безпечних та приватних протоколів та додатків.

6) Взаємодія між традиційними та децентралізованими сервісами: на початкових стадіях розвитку Web3, важливо забезпечити плавний перехід між традиційними сервісами та новими децентралізованими сервісами. Це може передбачати розробку шлюзів, мостів та інших рішень, що дозволяють обмінювати дані та активи між різними платформами та екосистемами.

7) Відкриті стандарти та протоколи: щоб сприяти інтероперабельності та співпраці між різними платформами та розробниками, важливо працювати над створенням відкритих стандартів та протоколів для Web3. Це може включати розробку спільних мов, архітектур та інтерфейсів для спілкування та взаємодії між різними технологіями та додатками.

Використання Web3 може призвести до нових можливостей для співпраці, інновацій, глобальної фінансової інклюзії та соціального змін. Якщо ці можливості будуть використані ефективно, Web3 може відкрити нові горизонти для взаємодії в інтернеті та допомогти втілити більш відкрите, прозоре та децентралізоване майбутнє для всіх.

2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У БЛОКЧЕЙН-ТЕХНОЛОГІЯХ

2.1 Криптографічні алгоритми та хешування

Хешування є важливим елементом блокчейну. Воно забезпечує збереження інформації в безпечному та стислому вигляді. Хеш-функції перетворюють вхідні дані на фіксовану довжину бітів, забезпечуючи унікальність та відповідність кожному набору даних. Найпопулярніші хеш-функції включають SHA-256 та Scrypt.

Хеш-функції використовуються в блокчейні через свої основні властивості, які забезпечують безпеку і надійність системи.

1) Відповідність: дві різні вхідні послідовності не можуть мати однаковий хеш. Це означає, що навіть незначна зміна вхідних даних призведе до повністю відрізняємого хешу, що сприяє безпеці та автентичності даних.

2) Швидкість обчислень: хеш-функції відносно швидко обчислюються, що забезпечує ефективність системи.

3) Неповоротність: відновлення вихідних даних з хешу є майже неможливим, що забезпечує конфіденційність даних.

Відбитки повідомлень є стислими відображеннями вихідних даних, що генеруються за допомогою хеш-функцій. Вони використовуються для перевірки цілісності та автентичності даних без необхідності зберігати відкриті тексти. Відбитки повідомлень забезпечують додатковий рівень безпеки, оскільки вони допомагають забезпечити, що навіть якщо хеш було змінено, вихідні дані все ще можна перевірити на автентичність.

Крім хеш-функцій та шифрування, в блокчейні використовуються різні криптографічні протоколи, такі як протоколи непересічних рівнів довіри (Zero-Knowledge Proofs) та Мультипартійні обчислення. Ці протоколи дозволяють виконувати операції з даними без необхідності розкривати конфіденційну інформацію або розкривати ключі.

Криптографічні підписи є іншим важливим елементом блокчейну, що забезпечує безпеку та автентичність даних. Вони використовуються для підтвердження того, що відправник повідомлення або транзакції дійсно є тим, хто він стверджує, що він є. Це досягається шляхом створення унікального підпису за допомогою приватного ключа відправника, який може бути перевірений за

допомогою відповідного відкритого ключа. Еліптична крива криптографія та цифрові підписи Едвардса-Куртона-Голдассера є популярними алгоритмами для створення криптографічних підписів в блокчейн-технологіях.

Мерклеві дерева є структурою даних, яка використовується в блокчейні для ефективного зберігання та перевірки даних. Вони дозволяють учасникам мережі перевіряти наявність та автентичність транзакцій без потреби зберігати повний блокчейн. Мерклеві дерева будуються шляхом об'єднання хешів транзакцій у пари, а потім хешування цих пар разом, поки не буде створено єдиний корінь – кореневий хеш (Merkle root). Кореневий хеш зберігається в заголовку блоку та служить відображенням всіх транзакцій у блоку.

2.2 Асиметричне шифрування

Асиметричне шифрування широко використовується в різних сферах, таких як електронна пошта, безпечні комунікації та фінансові транзакції. Цей метод шифрування забезпечує конфіденційність, автентифікацію та цілісність даних, що передаються через небезпечні канали комунікації, такі як Інтернет.

Одним з ключових застосувань асиметричного шифрування є цифровий підпис. Цифровий підпис дозволяє переконатися, що повідомлення або документ був створений відомою стороною (автентифікація) та не був змінений після підпису (цілісність). Для створення цифрового підпису, автор повідомлення або документа використовує свій приватний ключ для шифрування хешу повідомлення. Отриманий підпис можна перевірити, використовуючи публічний ключ автора, що гарантує автентичність підпису.

Асиметричне шифрування відіграє важливу роль в блокчейн технологіях, особливо в криптовалютних транзакціях. Учасники мережі використовують свої приватні та публічні ключі для створення цифрових підписів та перевірки транзакцій. Це забезпечує безпеку, приватність та надійність криптовалютних транзакцій.

Хоча асиметричне шифрування має переваги у вигляді безпеки та приватності, воно також має деякі виклики та обмеження. Одним з них є швидкість обчислень: асиметричні алгоритми шифрування зазвичай потребують більше часу для обробки, порівняно з симетричними алгоритмами. Це може стати проблемою, коли необхідно обробляти великі обсяги даних або високу кількість транзакцій.

Розвиток квантових комп'ютерів може створити виклики для сучасних

методів асиметричного шифрування, оскільки квантові комп'ютери можуть здійснювати обчислення значно швидше, ніж класичні комп'ютери. Це ставить під загрозу безпеку багатьох алгоритмів, таких як RSA, Digital Signature Algorithm (DSA) та Elliptic Curve Cryptography (ECC), оскільки квантові комп'ютери можуть потенційно розкрити приватні ключі.

Відповіддю на загрозу, яку представляють квантові комп'ютери, є постквантове шифрування. Це нові методи шифрування, які розробляються з метою захисту інформації від атак з використанням квантових комп'ютерів. Постквантові алгоритми базуються на складних математичних проблемах, для розв'язання яких навіть квантові комп'ютери потребують значних ресурсів та часу. Деякі приклади постквантових алгоритмів включають коди з відновленням помилок, решіткове шифрування та мультиваріатне квадратичне шифрування.

У майбутньому асиметричне шифрування ймовірно продовжить розвиватися, щоб протистояти новим загрозам та викликам. Нові алгоритми та методи захисту даних будуть відповідати на зростаючі потреби в безпеці, приватності та швидкодії в різних сферах, включаючи криптовалюти, блокчейн, електронну комерцію та комунікації.

Для успішного застосування асиметричного шифрування на глобальному рівні важливо мати стандартні протоколи та регуляції. Організації, такі як Національний інститут стандартів та технологій працює над розробкою та узгодженням стандартів для асиметричних алгоритмів шифрування. Ці стандарти дозволяють забезпечити сумісність, надійність та безпеку різних систем, які використовують асиметричне шифрування.

Оскільки асиметричне шифрування стає все більш поширеним та важливим інструментом в сучасному світі, зростає потреба в освіті та підвищенні свідомості щодо цієї технології. Важливо, щоб користувачі розуміли, як працює асиметричне шифрування, які переваги воно надає, а також які ризики пов'язані з його використанням. Інформування користувачів про асиметричне шифрування може допомогти підвищити загальний рівень кібербезпеки та приватності в Інтернеті.

2.3 Симетричне шифрування

Симетричне шифрування базується на використанні одного ключа для шифрування та розшифрування інформації. Цей підхід має певні переваги порівняно з асиметричним шифруванням, зокрема він є швидшим та зазвичай

вимагає менше обчислювальних ресурсів. Однак основним недоліком симетричного шифрування є те, що обидві сторони повинні мати доступ до одного й того ж ключа, що може створювати проблеми з безпекою та конфіденційністю.

У контексті блокчейн-технологій симетричне шифрування може використовуватися для захисту даних, які зберігаються на вузлах мережі. В деяких випадках, особливо в приватних блокчейнах, симетричне шифрування може використовуватися для обмеження доступу до інформації лише для певних учасників мережі, які мають відповідний ключ. З іншого боку, публічні блокчейни, такі як Bitcoin та Ethereum, в основному використовують асиметричне шифрування для забезпечення безпеки та приватності.

Однак, симетричне шифрування може використовуватися у комбінації з асиметричним шифруванням у гібридних схемах, що дозволяють забезпечити високу безпеку та швидкість обробки даних. Наприклад, у протоколах забезпечення конфіденційності транзакцій, таких як Monero та Zcash, симетричне шифрування може бути використане для шифрування даних транзакцій, тоді як асиметричне шифрування може бути використане для безпечного обміну ключів між учасниками транзакцій.

Окремо від блокчейну, симетричне шифрування також може використовуватися у різних криптографічних протоколах, які забезпечують конфіденційність, цілісність та автентичність даних. Деякі з найбільш популярних симетричних алгоритмів включають.

1) Advanced Encryption Standard (AES) – це широко використовуваний алгоритм симетричного шифрування, який підтримує ключі довжиною 128, 192 та 256 біт. AES надійний та ефективний, і використовується у багатьох застосунках, включаючи захист даних у мережах та файлових системах.

2) Data Encryption Standard (DES) – це один з найраніших алгоритмів симетричного шифрування, який використовує ключ довжиною 56 біт. Хоча DES зараз вважається застарілим і вразливим до атак на основі перебору ключів, він зіграв важливу роль у розвитку сучасних криптографічних систем.

3) Blowfish – це ще один алгоритм симетричного шифрування, який підтримує різні довжини ключів (від 32 до 448 біт). Blowfish відомий своєю швидкістю та гнучкістю, і часто використовується у різних застосунках для забезпечення безпеки даних.

Використання симетричного шифрування у блокчейн-технологіях вимагає ретельного підходу до управління ключами та протоколів безпеки. Хоча

симетричне шифрування може не завжди бути основним методом захисту даних у публічних блокчейнах, воно може стати важливим інструментом у комб інації з іншими криптографічними методами для підвищення рівня безпеки та приватності в різних сценаріях використання блокчейн-технологій.

Наприклад, симетричне шифрування може бути використане у приватних блокчейнах для захисту конфіденційної інформації, такої як фінансові документи, особисті дані або корпоративна інформація. У таких ситуаціях, ключі шифрування можуть бути розподілені серед довірених учасників мережі, що дозволяє контролювати доступ до зашифрованої інформації.

Крім того, симетричне шифрування може бути корисним у децентралізованих додатках, які використовують блокчейн для передачі та зберігання даних. Це може забезпечити додатковий рівень безпеки, коли передаються чутливі дані, такі як паролі або персональна інформація.

Також варто зазначити, що симетричне шифрування може бути використане у різних криптографічних протоколах, таких як протоколи забезпечення цілісності даних та протоколи аутентифікації. В цих ситуаціях, симетричне шифрування може допомогти забезпечити, що дані не були змінені або підроблені під час передачі чи зберігання.

2.4 Криптографічні підписи

Криптографічні підписи є важливим елементом блокчейн-технологій, оскільки вони забезпечують аутентичність, цілісність та невідкидність транзакцій та інших даних. Вони використовуються для підтвердження того, що відправник повідомлення або транзакції дійсно є тим, хто він стверджує, що він є. Криптографічні підписи засновані

на асиметричній криптографії, яка використовує пару ключів – приватний та відкритий.

Ось деякі основні види криптографічних підписів, які використовуються в блокчейні.

1) Еліптична крива криптографія є формою асиметричної криптографії, заснованої на математичних властивостях еліптичних кривих. Вона дозволяє створювати менші ключі при збереженні того ж рівня безпеки, що й інші алгоритми, такі як RSA. Bitcoin та інші криптовалюти використовують ECC для створення криптографічних підписів.

2) Цифрові підписи Едвардса-Куртона-Голдассера – це схема цифрових підписів, заснована на еліптичних кривих, яка пропонує високу безпеку та швидкість. Вона використовується в деяких блокчейн-системах, таких як Monero та Libra.

3) RSA-підписи – це загальновживаний алгоритм асиметричного шифрування та цифрових підписів. Хоча RSA не є стандартом у сучасних блокчейн-технологіях через більш високі вимоги до розміру ключів та повільнішу швидкість роботи порівняно з ECC та EdDSA. Проте, RSA все ще може використовуватися в деяких випадках, зокрема в корпоративних блокчейн-рішеннях або системах, що вимагають сумісності з наявними інфраструктурами.

Процес створення криптографічного підпису складається з трьох наступних кроків.

1) Генерація ключів: користувач генерує пару ключів – приватний та відкритий. Приватний ключ зберігається в таємниці, а відкритий ключ може бути розголошений.

2) Підписання: для створення підпису відправник транзакції використовує свій приватний ключ, щоб підписати хеш транзакції або повідомлення. Цей підпис додається до транзакції.

3) Верифікація: отримувач транзакції або повідомлення може перевірити підпис, використовуючи відкритий ключ відправника. Якщо підпис вірний, це означає, що транзакція або повідомлення не були змінені під час передачі, і відправник дійсно є тим, хто він стверджує, що він є.

Криптографічні підписи допомагають забезпечити довіру та безпеку в блокчейн-мережах. Вони дозволяють учасникам мережі відправляти та отримувати транзакції без необхідності довіри до інших сторін, що знижує ризик шахрайства та атак.

2.5 Мерклеві дерева

Мерклеві дерева – це структура даних, використовувана в блокчейн-технологіях для ефективного зберігання та перевірки даних. Мерклеві дерева є бінарними деревами, де листями є хеші окремих транзакцій або інших даних. Вершинами дерева є хеші від попередніх двох вершин на нижчому рівні. Побудова дерева продовжується, поки не буде створено єдиний корінь – кореневий хеш. Кореневий хеш зберігається в заголовку блоку та слугує відображенням всіх

транзакцій у блоку.

Схематичне зображеня Мерклевого дерева можна побачити на рисунку 2.1.

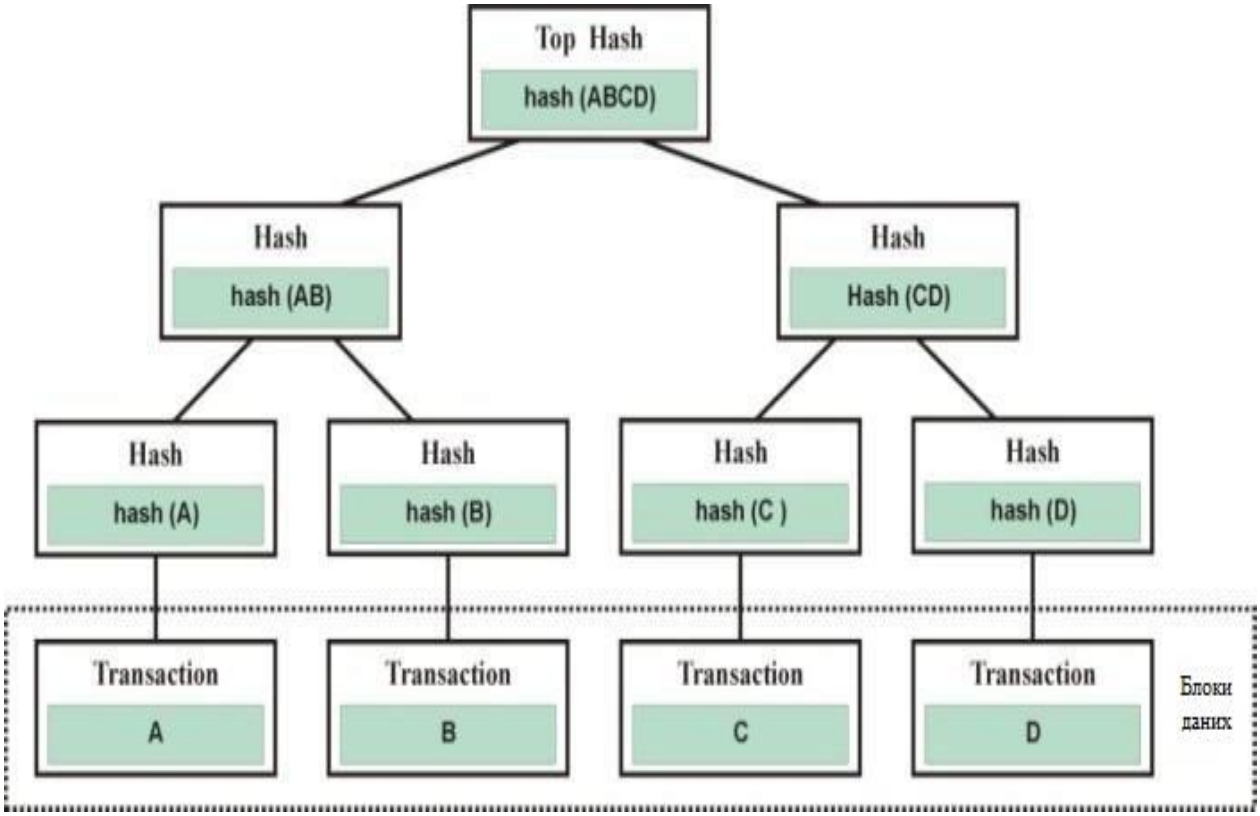

Рисунок 2.1 – Мерклеве дерево

Основні переваги використання Мерклевих дерев в блокчейні.

1) Ефективність: завдяки Мерклевим деревам учасники мережі можуть перевіряти наявність та автентичність транзакцій за допомогою невеликого набору хешів, а не переглядаючи всі транзакції у блоку.

2) Економія простору: Мерклеві дерева дозволяють зберігати транзакції в стислому вигляді, що зменшує обсяг даних, необхідних для зберігання та обробки.

3) Безпека: кореневий хеш у заголовку блоку гарантує, що всі транзакції в блоку залишаються незмінними. Якщо хтось спробує змінити транзакцію, це змінить хеш листка дерева, що призведе до зміни хешів на верхніх рівнях дерев і, в кінці кінців, зміни кореневого хешу. Оскільки кореневий хеш зберігається в заголовку блоку і пов'язаний з наступним блоком через хеш-посилання, будь-яка спроба змінити транзакцію легко виявиться.

4) Легкі клієнти: Мерклеві дерева спрощують створення легких клієнтів, які можуть перевіряти транзакції без зберігання повного блокчейну. Легкі клієнти можуть запитати вузол мережі надати доказ наявності транзакції в блокчейні

шляхом надання шляху Мерклевого дерева від листка до кореневого хешу. Це дозволяє легким клієнтам перевіряти транзакції, використовуючи менше ресурсів.

5) Фрагментація даних: Мерклеві дерева дозволяють виконувати віддалені процедури виклику для доступу до окремих частин даних, не вимагаючи доступу до всього блоку або всього блокчейну. Це може бути корисним для додатків, які потребують доступу лише до певних частин даних в блокчейні.

Загалом, Мерклеві дерева є важливим компонентом блокчейн-технологій, які допомагають забезпечити безпеку, ефективність та масштабованість системи. Вони дозволяють учасникам мережі перевіряти наявність та автентичність транзакцій без потреби зберігати повний блокчейн, полегшують створення легких клієнтів та дозволяють доступ до окремих частин даних.

2.6 Мультипартійні обчислення

Мультипартійні обчислення – це технологія, яка дозволяє декільком сторонам спільно обчислювати функції на їхніх приватних даних без необхідності розкривати ці дані один одному. Це дозволяє створювати безпечні та приватні розподілені системи, які можуть бути застосовані в різних галузях, включаючи фінанси, медицину, телекомунікації та інші.

Звісно що ця технологія використовується і у блокчейн-технологіях. У блокчейні важливими є валідація транзакцій та консенсус, але це може створити проблеми з приватністю. Наприклад, у традиційному блокчейні транзакції зберігаються відкрито, тому можливо встановити зв'язок між конкретним користувачем та його транзакціями.

Використання їх у блокчейн-технологіях може допомогти вирішити проблему приватності. За допомогою них можна створити протоколи, які дозволяють зберігати дані приватними та безпечними способом. Наприклад, використовуючи їх, можна створити протоколи конфіденційних транзакцій, які дозволяють учасникам блокчейн-мережі обмінюватися транзакціями, не розкриваючи конкретні дані.

Крім того, вони можуть бути використаний для створення децентралізованих ринків та обмінів, де учасники можуть взаємодіяти між собою та здійснювати транзакції, не розкриваючи своїх особистих даних. Це може бути особливо корисним у фінансовій сфері, де приватність та безпека є критичними чинниками.

Однак, використання їх також має свої обмеження та виклики. Наприклад,

процес обчислень може бути досить складним та ресурсомістким, що може впливати на швидкість транзакцій та загальну ефективність системи. Крім того, забезпечення безпеки та правильного функціонування системи вимагає належної налагодженості та розробки відповідних захисних механізмів.

У цілому, використання їх у блокчейн-технологіях може бути корисним та ефективним рішенням для забезпечення приватності та безпеки транзакцій. Однак, для успішного використання їх в блокчейні необхідно продовжувати досліджувати та розвивати цю технологію, вирішувати виклики та обмеження, а також створювати ефективні механізми для забезпечення безпеки та приватності системи.

3 МЕТОДИ ЗБЕРЕЖЕННЯ БЕЗПЕКИ КЛЮЧІВ У БЛОКЧЕЙНІ

3.1 Апаратні гаманці

Апаратні гаманці – це фізичні пристрої, які використовуються для зберігання приватних ключів користувачів в безпечному середовищі, ізольованому від інтернету. Ці гаманці надають високий рівень безпеки для криптовалют і активів користувачів, оскільки їх значно складніше атакувати або компрометувати порівняно з онлайн-гаманцями. Це стосується і вірусів, і хакерських атак.

Переваги апаратних гаманців.

1) Безпека: апаратні гаманці забезпечують надійне зберігання приватних ключів, оскільки вони ізольовані від інтернет-з'єднань і потенційних хакерських атак. Вони також мають додаткові рівні захисту, такі як пін-коди та двофакторна аутентифікація.

2) Зручність: апаратні гаманці дозволяють швидко і легко проводити транзакції, зазвичай через додаток на смартфоні або комп'ютері. Вони також можуть підтримувати багато різних криптовалют, що робить їх зручним варіантом для користувачів, які володіють декількома типами монет.

3) Зберігання офлайн: апаратні гаманці забезпечують так зване «холодне зберігання», коли ваші активи зберігаються офлайн, що зменшує ризик втрати коштів через онлайн-атаки.

4) Контроль: апаратні гаманці дають користувачам повний контроль над своїми приватними ключами, що забезпечує найвищий рівень безпеки для їх криптовалютних активів.

Недоліки апаратних гаманців.

1) Вартість: апаратні гаманці можуть бути дорожчими, ніж інші типи гаманців, такі як онлайн-гаманці або мобільні гаманці. Від цього можуть відмовитись користувачі з обмеженим бюджетом або ті, хто не володіє великою кількістю криптовалют.

2) Зручність у використанні: апаратні гаманці можуть бути менш зручними для деяких користувачів, оскільки вони вимагають фізичної взаємодії з пристроєм для проведення транзакцій. Онлайн-гаманці або мобільні гаманці можуть надавати більше зручності в певних ситуаціях.

3) Втрата пристрою: якщо апаратний гаманець втрачений або

пошкоджений, користувач може втратити доступ до своїх криптовалютних активів. Хоча більшість апаратних гаманців мають рішення для відновлення аккаунту, такі як резервні фрази, втрата пристрою все одно може стати стресом для користувача.

4) Обмежений доступ до підтримуваних криптовалют: деякі апаратні гаманці можуть підтримувати обмежену кількість криптовалют. Це може стати проблемою для користувачів, які володіють різними типами активів, що не підтримуються апаратним гаманцем [8].

Приклад зовнішнього вигляду апаратного гаманця SafePal S1 можна побачити на рисунку 3.1.

Рисунок 3.1 – Апаратний гаманець SafePal S1

3.2 Гарячі та холодні програмні гаманці

Гарячі та холодні програмні гаманці представляють два різних типи гаманців для зберігання криптовалют. Вони відрізняються за своїми рівнями безпеки та зручності використання.

Приклад інтерфейсу гарячого гаманця Metamask можна побачити на рисунку 3.2.

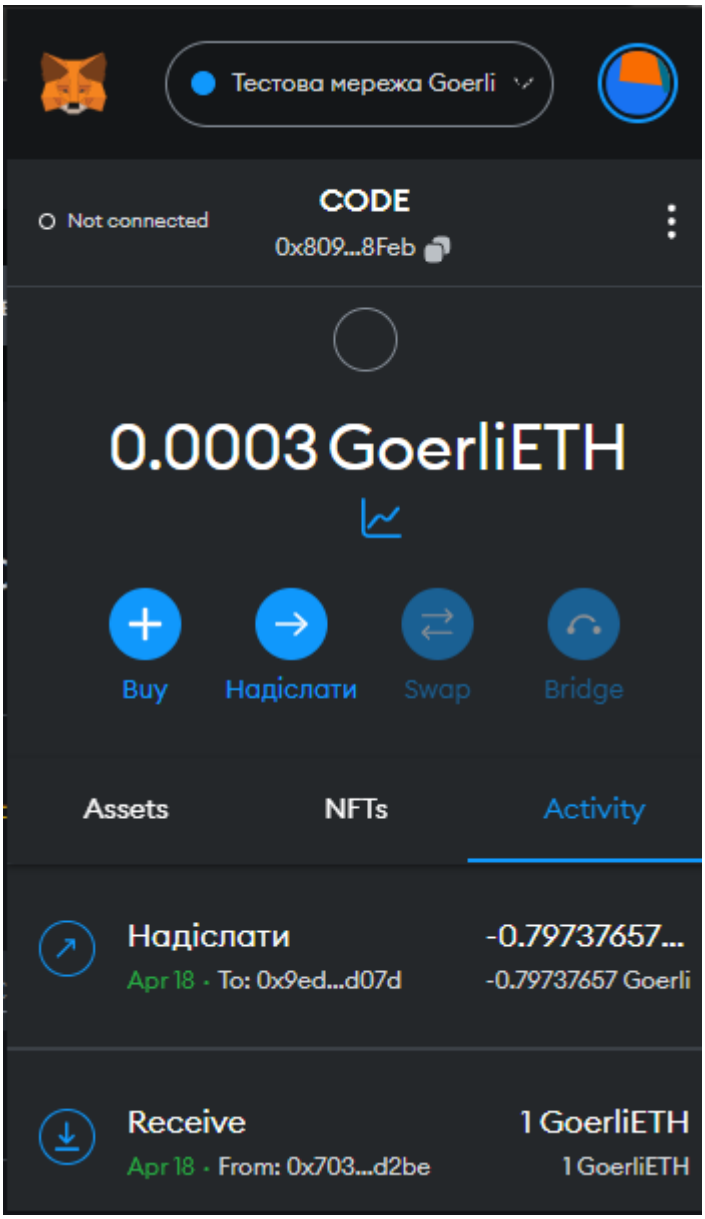

Рисунок 3.2 – Інтерфейс гарячого гаманця Metamask

Переваги гарячих гаманців.

1) Швидкий та простий доступ: гарячі гаманці забезпечують швидкий доступ до коштів через інтернет, що забезпечує зручність управління та проведення

транзакцій.

2) Безкоштовні або недорогі: більшість гарячих гаманців доступна безкоштовно або за невисоку плату, що робить їх доступними для широкої аудиторії.

3) Інтеграція зі сторонніми сервісами: гарячі гаманці часто інтегруються з криптовалютними обмінниками, децентралізованими біржами та іншими сервісами, що спрощує використання криптовалют.

До недоліків гарячих гаманців можна віднести меншу безпеку. Оскільки гарячи гаманці знаходяться онлайн, вони більш вразливі до хакерських атак та інших видів крадіжок.

Приклад зовнішнього вигляду холодного гаманця Ledger Nano S можна побачити на рисунку 3.3.

Рисунок 3.3 – Холодний гаманець Ledger Nano S

Переваги холодних гаманців.

1) Вища безпека: холодні гаманці зберігають приватні ключі офлайн, що робить їх менш вразливими до хакерських атак і вірусів. Це забезпечує вищий рівень безпеки для коштів користувача.

2) Зберігання резервної копії: холодні гаманці дозволяють створювати резервні копії приватних ключів, що забезпечує можливість відновлення коштів у разі втрати або пошкодження пристрою.

3) Контроль над приватними ключами: у холодних гаманцях користувач повністю контролює свої приватні ключі, що забезпечує більшу конфіденційність і безпеку.

Недоліки холодних гаманців.

1) Менша зручність: холодні гаманці можуть бути менш зручними для швидкого доступу та проведення транзакцій, оскільки потребують додаткових кроків для підключення до мережі та перевірки транзакцій.

2) Витрати на налаштування та зберігання: холодні гаманці можуть вимагати від користувача витрат на налаштування та зберігання, такі як закупівля апаратного гаманця або встановлення додаткового програмного забезпечення.

3) Потенційна складність використання: для деяких користувачів, особливо новачків у криптовалютному світі, холодні гаманці можуть бути складнішими у використанні, ніж гарячі гаманці, оскільки вони вимагають більше технічних знань та обережності.

3.3 Мультипідпис

Мультипідпис – це технологія, яка вимагає підписів кількох сторін для авторизації транзакції в блокчейні. Мультипідпис використовується для забезпечення підвищеної безпеки ключів та активів користувачів, оскільки він розподіляє контроль над активами між кількома сторонами, замість того, щоб централізувати його в одного власника ключа [9].

Переваги використання мультипідпису.

1) Збільшення безпеки: мультипідпис забезпечує додатковий рівень безпеки, оскільки зловмисники повинні скомпрометувати кілька приватних ключів, щоб отримати доступ до активів. Це зменшує ризик втрати активів через крадіжку або злом.

2) Розподіл відповідальності: мультипідпис дозволяє розподілити

відповідальність за активи між кількома сторонами, що може бути корисним для компаній або груп осіб, які спільно володіють активами.

3) Запобігання шахрайству: мультипідпис зменшує ризик шахрайства оскільки потрібує більше ніж одного підпису для здійснення транзакцій.

4) Регулювання доступу: мультипідпис може бути використаний для встановлення рівнів доступу та контролю над активами, наприклад, в компанії, де різні співробітники мають різний рівень дозволів на проведення транзакцій.

5) Резервне копіювання та відновлення: у разі втрати або пошкодження одного з приватних ключів, мультипідпис дозволяє вам продовжити використовувати активи, оскільки вам не потрібні всі підписи для проведення транзакцій.

Недоліки використання мультипідпису.

1) Складність: мультипідпис може бути складнішим у налаштуванні та управлінні, порівняно з традиційними гаманцями з одним підписом. Користувачам потрібно координувати свої дії для підписання транзакцій, що може ускладнити процес.

2) Відповідальність: хоча мультипідпис розподіляє відповідальність між учасниками, він також може створювати проблеми у випадку невиконання обов'язків одним з учасників. Це може призвести до блокування активів або затримок у проведенні транзакцій.

3) Затримки у проведенні транзакцій: мультипідпис може збільшити час проведення транзакцій, оскільки кожна сторона повинна підписати транзакцію перед її виконанням. У випадку відсутності або затримки одного з учасників, транзакція може затриматися на невизначений час.

Схематичне зображення роботи технології мультипідпису можна побачити на рисунку 3.4.

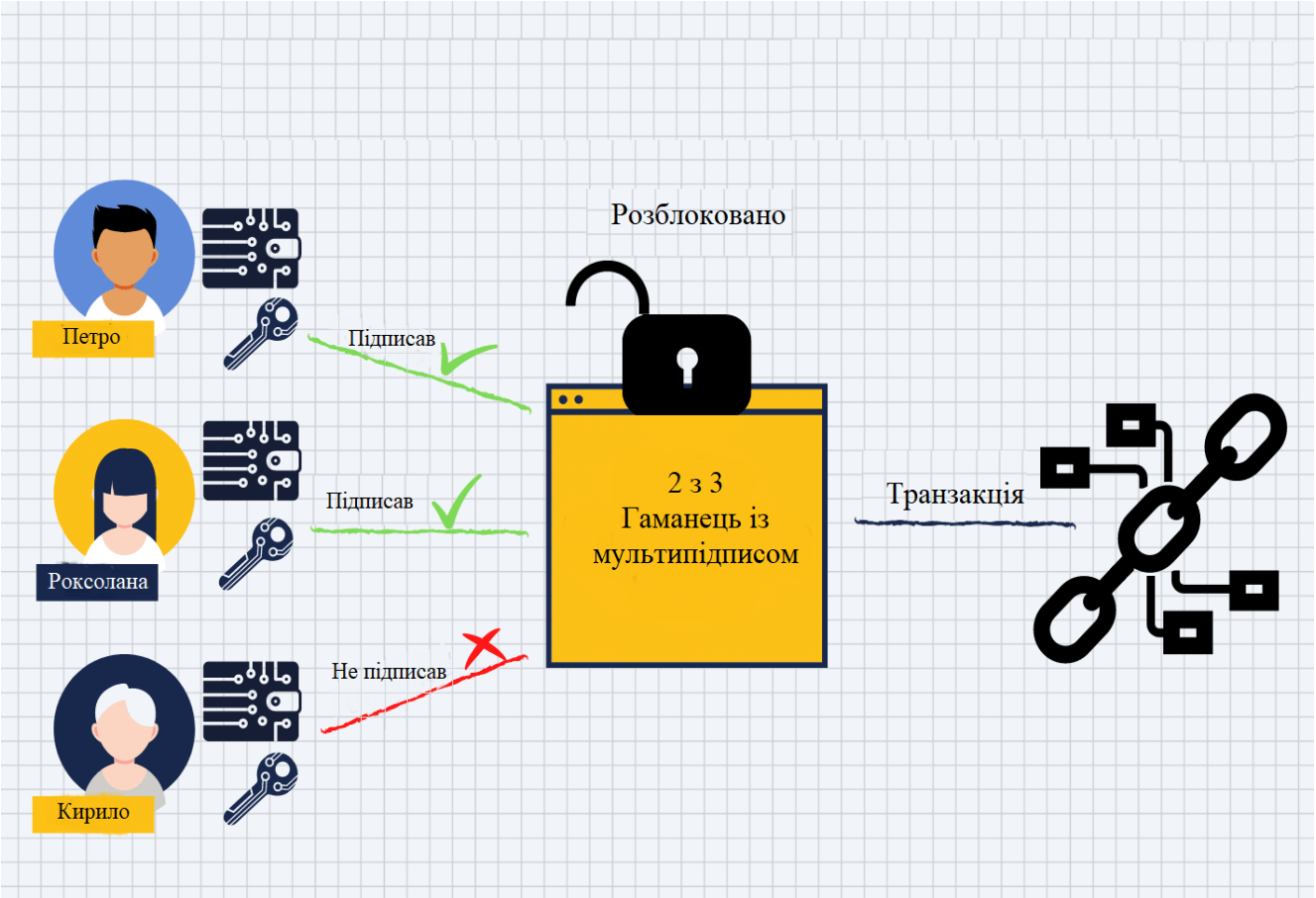

Рисунок 3.4 – Схема роботи мультипідпису

На відміну від однопідписних гаманців, мультипідпис використовує кілька приватних ключів для забезпечення безпеки активів користувачів. Це робить його популярним варіантом для компаній, співробітників та груп осіб, які мають спільні активи або потребують розподіленого контролю над активами. Однак, з урахуванням недоліків мультипідпису, користувачам слід вибирати цей варіант з обережністю та враховувати свої індивідуальні потреби та обставини.

Враховуючи всі ці чинники, можна зробити висновок, що мультипідпис є ефективним інструментом для забезпечення безпеки ключів у блокчейні за умови правильної інфраструктури та управління. Вибір найбільш вдалого методу збереження ключів в блокчейні залежить від індивідуальних потреб, ресурсів та рівня довіри між учасниками.

3.4 Розподілене зберігання ключів

Розподілене зберігання ключів – це криптографічний метод розділення приватного ключа на декілька часток, які потім зберігаються окремо. Це забезпечує

високий рівень безпеки та надійності збереження приватних ключів.

Метод Shamir's Secret Sharing пропонує алгоритм, який дозволяє розділити приватний ключ на певну кількість шматків, при цьому задається необхідна кількість шматків, що мають бути зібрані разом для відновлення ключа. Наприклад, ключ може бути розділений на 5 шматків, з яких необхідно зібрати щонайменше 3 для відновлення повного ключа.

Переваги розподіленного зберігання ключів.

1) Безпека: розділення ключа на шматки зменшує ризик втрати або крадіжки ключа, оскільки зловмисники мають отримати достатню кількість шматків для відновлення ключа.

2) Надійність: якщо один або декілька шматків приватного ключа загубляться або знищаться, ключ може бути відновлений за допомогою інших шматків.

3) Децентралізація: розподілене зберігання ключів дозволяє децентралізувати зберігання приватних ключів та захистити їх від можливих атак.

Недоліки розподіленого зберігання ключів.

1) Складність: розподілене зберігання ключів може бути менш простим у використанні та реалізації порівняно з традиційними методами зберігання ключів.

2) Координація: зберігання та відновлення шматків ключів вимагає координації між учасниками або установами, які мають ці шматки. Це може бути досить трудомістким процесом, особливо в разі екстрених ситуацій або непередбачуваних обставин.

3) Зберігання шматків: зберігання шматків ключів вимагає додаткової уваги до безпеки, оскільки кожен шматок містить часткову інформацію про приватний ключ. Залежно від кількості шматків та їх розташування, може знадобитися забезпечити додаткові ресурси та заходи безпеки.

4) Потенційний ризик злому: якщо зловмисники зможуть отримати доступ до необхідної кількості шматків ключа, вони зможуть відновити приватний ключ. Це може бути менш ймовірним, ніж зламати традиційний гаманець, проте такий ризик все ж існує.

Незважаючи на недоліки, розподілене зберігання ключів може бути дуже ефективним методом забезпечення безпеки та надійності приватних ключів у блокчейні. Важливо знайти оптимальний баланс між зручністю використання, складністю реалізації та рівнем безпеки, щоб гарантувати максимальну захищеність ключів та активів користувачів.

3.5 Додаткові методи зберігання

Додаткові методи зберігання ключів можуть забезпечити додатковий рівень безпеки та захисту цифрових активів. Найпопулярнішими з таких методів є наступні.

1) Зберігання приватних ключів на фізичних носіях, таких як флеш-накопичувачі, карти пам’яті. Зберігання ключів на фізичних носіях може забезпечити відмінну ізоляцію від онлайн-загроз, але важливо захистити такі носії від фізичного пошкодження та забезпечити їх конфіденційність.

2) Бумажні гаманці є фізичними копіями приватного ключа або фрази відновлення, які роздруковані на папері. Вони зазвичай містять коди для швидкого сканування та імпорту ключів. Бумажні гаманці повинні зберігатися в безпечних місцях, віддалених від вологи та вогню, оскільки вони можуть легко пошкодитися.

3) Металеві гаманці є більш стійкими до пошкоджень в порівнянні з бумажними гаманцями. Вони створені з металу, який витримує високі температури та корозію. Металеві гаманці можуть містити ключі або фрази відновлення, вигравірувані на поверхні. Це забезпечує більш тривалий та безпечний спосіб зберігання ключів, але також потребує додаткового забезпечення щодо конфіденційності.

4) Використання так званого «камуфляжу». Наприклад, записати ключ або фразу відновлення на сторінці книги. Важливо обрати місце, що не буде очевидним для інших людей.

5) Для зберігання ключів у найбільш безпечних умовах можна використовувати сейфи або навіть банківські сховища. Це забезпечує найвищий рівень захисту від фізичного пошкодження та крадіжок. Однак такий метод може бути дорогим та не завжди зручним для швидкого доступу до ключів.

3.6 Мнемонічні фрази

Мнемонічна фраза відновлення – це набір випадково відібраних слів, які використовуються для генерації приватних ключів у криптовалютних гаманцях. Ці фрази дозволяють відновити доступ до гаманця і криптовалютних активів у випадку втрати або пошкодження пристрою чи програмного гаманця.

Мнемонічні фрази відновлення зазвичай складаються з 12, 18 або 24 слів, залежно від рівня безпеки, який бажано забезпечити. Слова вибираються з певного

словника, який містить велику кількість слів, і вони повинні записуватися та зберігатися в безпечному місці. Важливо зберігати мнемонічну фразу відокремлено від криптогаманця, оскільки зловмисники можуть отримати доступ до гаманця, якщо вони знайдуть мнемонічну фразу.

Ось деякі правила безпеки, яких слід дотримуватися при зберіганні мнемонічної фрази відновлення.

1) Не зберігати мнемонічну фразу в електронному вигляді на комп'ютері або пристрої з доступом до інтернету. Це може збільшити ризик крадіжки фрази зловмисниками.

2) Запис мнемонічної фрази на папері або іншому носії, що стійкий до вологи, вогню та інших зовнішніх впливів.

3) Зберігати мнемонічну фразу у безпечному місці, як-то сейф або банківське сховище, де вона буде відокремлена від гаманця.

4) Створення декількох копій мнемонічної фрази та зберігання їх у різних безпечних місцях. Це зменшить ризик втрати всіх копій через стихійни лиха, крадіжки або інші непередбачувані обставини.

5) Уникнення розголошення мнемонічної фрази та факту наявності криптогаманця. Це зменшить ризик стати ціллю зловмисників.

Мнемонічні фрази відновлення є суттєвим елементом криптовалютної безпеки, і дотримання вищезазначених порад допоможе забезпечити надійне зберігання та відновленн криптовалютних активів [10].

3.7 Безпека відкритих ключів

Відкриті ключі відіграють важливу роль у криптографічних системах на основі асиметричного шифрування, таких як блокчейн. Вони дозволяють ідентифікувати користувачів та підтверджувати справжність транзакцій, не розкриваючи приватні ключі. Враховуючи це, безпека відкритих ключів є важливим аспектом зберігання ключів в блокчейні. На відміну від приватних ключів, відкриті ключі можуть бути доступними публічно. Однак, важливо використовувати надійні способи зберігання та передачі відкритих ключів, щоб уникнути зміни або підробки ключів зловмисниками.

Для забезпечення безпеки транзакцій у блокчейні важливо переконатися, що відкриті ключі належать дійсному власнику приватного ключа. Одним із способів перевірки автентичності відкритого ключа є використання криптографічного

підпису, який генерується за допомогою приватного ключа та може бути перевірений за допомогою відкритого ключа.

Сертифікати безпеки та цифрові підписи можуть використовуватися для підтвердження автентичності відкритих ключів та забезпечення безпеки комунікацій. Наприклад, відкриті ключі можуть бути підписані центром сертифікації, який діє як довірена сторона та гарантує автентичність ключів.

Щоб спростити процес використання відкритих ключів та підвищити безпеку, відкриті ключі можуть бути представлені у вигляді адрес блокчейн. Адреса блокчейн є хешем відкритого ключа і має деякі переваги.

1) Коротший розмір: адреси блокчейн мають менший розмір, що спрощує обробку та передачу.

2) Підвищення безпеки: хешування відкритого ключа забезпечує додатковий рівень безпеки, оскільки атакувальнику потрібно буде відновити відкритий ключ з адреси блокчейн перед тим, як він зможе зробити будь-які спроби атаки.

3) Зручність: використання адрес забезпечує зручність та простоту управління активами та виконання транзакцій.

Щоб забезпечити більшу безпеку та конфіденційність, ротація ключів може бути застосована для зміни відкритих ключів. Це означає створення нового пари ключів та перенесення активів на нову адресу. Це може допомогти уникнути витоку інформації про транзакції або зменшити ризик компрометації ключів. У разі втрати або компрометації відкритого ключа, плани аварійного відновлення можуть допомогти швидко відновити доступ до активів. Це може включати в себе резервні копії ключів, відновлення ключів за допомогою мнемонічних фраз або використання служб відновлення ключів.

Один з ключових аспектів забезпечення безпеки ключів в блокчейні полягає в освіті користувачів. Користувачам слід розуміти основи криптографії, процеси генерації та зберігання ключів, а також ризики, пов'язані з неправильним використанням ключів. Регулярні сесії навчання та інформаційні матеріали можуть допомогти користувачам забезпечити максимальний рівень безпеки своїх ключів.

Використання стандартів безпеки, таких як NIST або ISO може допомогти забезпечити, що процеси та технології, пов'язані зі зберіганням ключів, відповідають високим стандартам безпеки. Використання таких стандартів може також полегшити аудит та моніторинг систем зберігання ключів. Підготовка до

кризових ситуацій та відповідне планування можуть бути важливою частиною загальної стратегії зберігання ключів в блокчейні. Це може включати розробку планів відновлення ключів у випадку їх втрати, компрометації або крадіжки, а також забезпечення регулярних вправ з відновлення ключів, щоб користувачі мали уявлення про процеси, які повинні відбуватися у випадку таких подій.

3.8 Тайм-локові скрипти

Тайм-локові скрипти – це спеціальні скрипти, які встановлюють умови для розблокування або доступу до приватних ключів на основі часу або інших параметрів. Вони дозволяють створити додатковий рівень захисту для ключів, оскільки ключі стають доступними тільки після виконання певних умов.

Деякі приклади використання тайм-локових скриптів.

1) Часові умови: використання тайм-локових скриптів для забезпечення доступу до приватних ключів тільки після минулого певного часового проміжку. Це може бути корисним, наприклад, для створення ескроу-угод або відкладеного розблокування коштів.

2) Умови на основі подій: тайм-локові скрипти можуть також встановлювати умови доступу до ключів на основі певних подій або дій, наприклад, досягнення певного рівня ціни криптовалюти або виконання інших контрактів.

3) Мультипідпис з умовами: умови зберігання ключів можуть бути використані разом з мультипідписом для створення ще більш безпечних схем зберігання. Наприклад, можна створити схему, де ключі зберігаються в розподіленому вигляді, а доступ до них здійснюється тільки при задоволенні певних умов, таких як підтвердження ідентичності або виконання інших контрактів [11].

4) Умови на основі оракулів: використання оракулів для створення умов зберігання ключів, що залежать від даних зовнішнього середовища. Наприклад, умова може передбачати розблокування ключів тільки після отримання певного підтвердження від оракула, як-то підтвердження оплати або інших дій користувача.

Використання тайм-локових скриптів та інших умов зберігання ключів дозволяє підвищити рівень безпеки ключів у блокчейні, роблячи їх доступними лише за певних умов. Завдяки цьому користувачі можуть мати більше контролю над своїми ключами та активами, а також зменшити ризики втрати або компрометації ключів.

4 ВПРОВАДЖЕННЯ ВЛАСНОГО РІШЕННЯ ДЛЯ ЗБЕРЕЖЕННЯ БЕЗПЕКИ КЛЮЧІВ

4.1 Актуальність проблеми

Актуальність проблеми зберігання приватних ключів у блокчейн-технологіях постійно зростає з розвитком криптовалют та інших децентралізованих додатків. Приватні ключі є основним компонентом безпеки користувачів, оскільки вони дають контроль над активами та ідентичністю в децентралізованих мережах. Тому забезпечення надійного зберігання приватних ключів є важливим аспектом для забезпечення безпеки користувачів та збереження їх цифрових активів.

Основні причини актуальності проблеми зберігання приватних ключів.

1) Збільшення кількості криптовалютних інвесторів: з ростом популярності криптовалют, все більше людей вкладають свої кошти у цифрові активи, збільшуючи потребу в надійних методах зберігання приватних ключів.

2) Розвиток децентралізованих фінансових сервісів: DeFi-додатки надають користувачам можливість отримувати кредити, здійснювати ставки на стейкінг, обмінювати активи та інші фінансові операції без посередників, що збільшує відповідальність користувачів за зберігання своїх приватних ключів.

3) Широкий спектр загроз безпеці: від фішингу і вірусів до фізичних крадіжок та втрат, приватні ключі піддаються численним загрозам, які можуть призвести до втрати активів.

4) Людський фактор: користувачі часто забувають свої приватні ключі, втрачають записи або некоректно використовують резервні копії, що також створює ризик втрати контролю над своїми цифровими активами. Освіта користувачів та розвиток простих та надійних інструментів для зберігання приватних ключів можуть допомогти зменшити цей ризик.

5) Розвиток технологій та стандартів безпеки: технології безпеки та криптографічні стандарти продовжують розвиватися, що вимагає постійної адаптації та оновлення методів зберігання приватних ключів. Останні відкриття в квантових комп'ютерах та потенційні загрози, які вони створюють для криптографії, можуть змусити розробників шукати нові підходи до зберігання ключів у майбутньому.

6) Законодавчі та регуляторні вимоги: у деяких країнах законодавство зобов'язує криптовалютні компанії та сервіси до суворого забезпечення зберігання ключів своїх користувачів. Це може сприяти розвитку та впровадженню нових рішень для зберігання приватних ключів.

Враховуючи ці фактори, проблема зберігання приватних ключів у блокчейн-технологіях залишається актуальною та вимагає постійної уваги від розробників, користувачів та регуляторів. Дослідження та розробка нових методів збереження ключів, що забезпечують кращу безпеку та зручність для користувачів, можуть допомогти вирішити цю проблему та забезпечити стабільне та безпечне функціонування децентралізованих мереж.

Саме тому було прийнято рішення розробити свою програму для зв’язку із блокчейном, тобто крипто-гаманець. Даний гаманець має наступний функціонал.

1) Створення нового гаманця, а саме пари з приватного ключа та мнемонічної фрази.

2) Можливість роздрукувати приватний ключ та мнемонічну фразу.

3) Імпорт існуючого гаманця за домогою приватного ключа або мнемонічної фрази.

4) Відображення балансу гаманця.

5) Створення транзакції та відправлення токенів на іншу адресу.

Основною причиною для створення цього програмного забезпечення та головною його перевагою є те, що приватний ключ та мнемонічна фраза ніде не зберігаються та після закінчення роботи з програмою видаляються. На відміну від інших криптогаманців, де приватний ключ зберігається на постійній основі, а аутентифікація проходить за допомогою пароля, біометрії тощо.

Але одночасно це є і великим недоліком. Для багатьох користувачів може бути дуже складно та набридливо кожного разу заново вводити свій приватний ключ або мнемонічну фразу, але це програмне забезпечення має за ціль не повсякденне використання для взаємодії із додатками та смарт-контрактами, а безпосередньо зберігання коштів із можливістю лише відправляти їх за такої потреби.

На даний момент у програмі реалізовано функціонал трекінгу балансу та виконання транзакцій лише для токену ETH, але у майбутньому за потреби цей функціонал може бути розширений шляхом додання нових токенів.

Використання програмного забезпечення може бути здійснено для майже будь-якої EVM-мережі, що не вносили особливих змін до функціоналу

відображення балансів, контрактів токенів або ж функцій відправлення активів. Список актуальних мереж, що можуть бути використані у програмному забезпеченні: Ethereum, Binance Smart Chain, Polygon, Arbitrum, zkSync, Fantom, Avalanche, Scroll, а також тестові мережі, такі як Goerli та Sepolia.

4.2 Програна реалізація

Функціонал програми та приклад її роботи розглянуто для мережі Goerli, що являється тестовим аналогом мережі Ethereum. Програмний код написано на мові програмування Python. Для розробки використовується середовище PyCharm.

Головним інструментов для взаємодії між Python та блокчейном є бібліотека Web3.py, що дозволяє спілкуватися з Ethereum-мережою, керувати гаманцями та інтерактивно взаємодіяти зі смарт-контрактами. Вона реалізує специфікацію JSON-RPC, який є загальноприйнятим методом взаємодії з Ethereum-нодами [12].

Спочатку необхідно імпортувати усі бібліотеки, що знадобляться для роботи. Їх можна побачити на рисунку 4.1.

```
1  import os
   from tkinter import Tk, Label, Button, Entry, END, Text, messagebox, Toplevel
3  import pyperclip
4  from eth_account import Account
5  from mnemonic import Mnemonic
6  import tempfile
7  from web3 import Web3
8
   # Connect to Goerli Testnet
```

Рисунок 4.1 – Імпорт необхідних бібліотек

Для програмного забезпечення використовуються наступні бібліотеки.

1) OS – модуль стандартнох бібліотеки Python, який забезпечує можливість взаємодії з операційною системою.

2) Tkinter – модуль стандартної бібліотеки Python, який дозволяє створювати графічні інтерфейси користувача.

3) Pyperclip – модуль, що дозволяє копіювати та вставляти текст з буферу обміну між різними програмами та процесами.

4) Eth_account – бібліотека для створення та роботи з Ethereum-акаунтами.

5) Mnemonic – бібліотека для генерації мнемонічних фраз.

6) Tempfile – стандартна бібліотека, що дозволяє створювати тимчасові файли та каталоги.

7) Web3 – основна бібліотека для взаємодії з EVM-блокчейнами.

Далі виконується підключення до ноди, у даному випадку до власної ноди Goerli, що можна побачити на рисунку 4.2.

```
8
9   # Connect to Goerli Testnet
10  w3 = Web3(Web3.HTTPProvider("https://goerli.infura.io/v3/5f235b6d6ac9446c867ab7067a751421"))
11
    1 usage
```

Рисунок 4.2 – Налаштування підключення до вузла блокчейну

Функція генерації гаманця генерує приватний ключ та мнемонічну фразу англійскою мовою, що має довжину у 24 слова.Все це можна побачити на рисунку 4.3.

```
    1 usage
12  def generate_wallet():
13      # Generate a new private key
14      private_key = Account.create().key
15
16      # Generate a 24-word BIP39 mnemonic (seed phrase)
17      mnemonic = Mnemonic("english")
18      seed_phrase = mnemonic.generate(strength=256)
19
20      return private_key, seed_phrase
21
```

Рисунок 4.3 – Функція генерації гаманця

Далі виконуються налаштування для першого вікна програми, що містить у собі налаштування розміру вікна, фону, кнопок та їх функціоналу, текстових полів. При натисканні на кнопку з генерацією буде викликатися функція генерації, при цьому у текстових полях з’являться згенеровані приватний ключ та мнемонічна фраза. При натисканні на кнопки для копіювання будуть виконані функції копіювання. При натисканні на кнопку друку буде виконана функція друку. Все це можна побачити на рисунку 4.4.

```python
class WalletGeneratorGUI:
    def __init__(self, master):
        self.master = master
        master.title("Marked Man wallet")

        # Set fixed window size, background color, and disable resizing
        master.geometry("1120x630")
        master.configure(bg="black")
        master.resizable(0, 0)

        self.private_key_label = Label(master, text="Private Key:", bg="black", fg="white")
        self.private_key_label.place(relx=0.5, rely=0.2, anchor="center")

        self.seed_phrase_label = Label(master, text="Seed Phrase:", bg="black", fg="white")
        self.seed_phrase_label.place(relx=0.5, rely=0.35, anchor="center")

        self.private_key_entry = Entry(master, width=80)
        self.private_key_entry.place(relx=0.5, rely=0.25, anchor="center")

        self.seed_phrase_entry = Text(master, width=80, height=3)
        self.seed_phrase_entry.place(relx=0.5, rely=0.45, anchor="center")

        self.generate_button = Button(master, text="Generate Wallet", command=self.generate_wallet_gui)
        self.generate_button.place(relx=0.4, rely=0.6, anchor="center")

        self.print_button = Button(master, text="Print", command=self.print_wallet, state="disabled")
        self.print_button.place(relx=0.5, rely=0.6, anchor="center")

        self.use_existing_wallet_button = Button(master, text="Use an existing wallet", command=self.use_existing_wallet)
        self.use_existing_wallet_button.place(relx=0.6, rely=0.6, anchor="center")

        self.copy_private_key_button = Button(master, text="Copy", command=self.copy_private_key)
        self.copy_private_key_button.place(relx=0.9, rely=0.25, anchor="center")

        self.copy_seed_phrase_button = Button(master, text="Copy", command=self.copy_seed_phrase)
        self.copy_seed_phrase_button.place(relx=0.9, rely=0.45, anchor="center")
```

Рисунок 4.4 – Налаштування графічного відображення першого вікна

На випадок, якщо користувач бажає створити декілька гаманців поспіль, створена наступна функція, що видаляє попередні значення текстових полі, заново викликає функцію генерації приватного ключа та мнемонічної фрази і додає їх до текстових полів. Це можна переглянути на рисунку 4.5.

```
1 usage
def generate_wallet_gui(self):
    private_key, seed_phrase = generate_wallet()
    self.private_key_entry.delete(0, END)
    self.private_key_entry.insert(0, private_key.hex())
    self.seed_phrase_entry.delete(1.0, END)
    self.seed_phrase_entry.insert(1.0, seed_phrase)
    self.print_button.config(state="normal")
```

Рисунок 4.5 – Функція заміни приватного ключа та мнемонічної фрази при повторному натисканні на кнопку генерації

Перша функція зчитує значення текстового поля з приватним ключем, зберігає його та передає його до буфера обміну. Друга функція робить все те ж саме, але тільки із мнемонічною фразою. Це все можна побачити на рисунку 4.6.

```
1 usage
def copy_private_key(self):
    private_key = self.private_key_entry.get()
    pyperclip.copy(private_key)

1 usage
def copy_seed_phrase(self):
    seed_phrase = self.seed_phrase_entry.get(1.0, END).strip()
    pyperclip.copy(seed_phrase)
```

Рисунок 4.6 – Функції копіювання до буферу обміну

Функція друку спочатку зчитує значення приватного ключа та мнемонічної фрази із текстових полів. Після чого створюється тимчасовий файл, що відправляється на друк. Це можна побачити на рисунку 4.7.

```
1 usage
def print_wallet(self):
    private_key = self.private_key_entry.get()
    seed_phrase = self.seed_phrase_entry.get(1.0, END).strip()

    content = f"Private Key: {private_key}\n\nSeed Phrase:\n{seed_phrase}"

    with tempfile.NamedTemporaryFile(mode="w", delete=False, suffix=".txt") as temp:
        temp.write(content)
        temp.flush()
        os.startfile(temp.name, "print")
        messagebox.showinfo("Print Wallet", "Sending wallet details to the printer.")
```

Рисунок 4.7 – Функція друку приватного ключа та мнемонічної фрази

Наступна функція відповідає за створення другого вікна, що з’являється при переході до використання вже існуючого гаманця. Функція містить у собі налаштування розміру вікна, фону, кнопок та їх функціоналу, текстових полів. У даному вікні лише одна активна кнопка, що зчитує приватний ключ або мнемонічну фразу із текстового поля, після чого закриває це вікно та відкриває третє. Все це можна побачити на рисунку 4.8.

```
1 usage
def use_existing_wallet(self):
    self.master.withdraw()
    self.import_window = Toplevel(self.master)
    self.import_window.title("Import Existing Wallet")
    self.import_window.geometry("1120x630")
    self.import_window.configure(bg="black")
    self.import_window.resizable(0, 0)

    self.import_private_key_label = Label(self.import_window, text="Private Key:", bg="black", fg="white")
    self.import_private_key_label.place(relx=0.5, rely=0.25, anchor="center")

    self.import_seed_phrase_label = Label(self.import_window, text="Seed Phrase:", bg="black", fg="white")
    self.import_seed_phrase_label.place(relx=0.5, rely=0.45, anchor="center")

    self.import_private_key_entry = Entry(self.import_window, width=80)
    self.import_private_key_entry.place(relx=0.5, rely=0.3, anchor="center")

    self.import_seed_phrase_entry = Text(self.import_window, width=80, height=3)
    self.import_seed_phrase_entry.place(relx=0.5, rely=0.55, anchor="center")

    self.import_button = Button(self.import_window, text="Import", command=self.import_wallet)
    self.import_button.place(relx=0.5, rely=0.7, anchor="center")
```

Рисунок 4.8 – Налаштування графічного відображення другого вікна

Після введення користувачем приватного ключа або мнемонічної фрази та натискання кнопки для імпорту програма переходить до функції, що розпізнає введені дані та викликає наступне вікно. Якщо користувачем було введено приватний ключ, то він одразу імпортується та дає можливість зчитувати баланс та ініціювати транзакції. Якщо ж користувачем була введена мнемонічна фраза, то спочатку вона перетворюється на приватний ключ, а вже потім імпортується. У кінці викликається функція для відкриття наступного вікна та відображення балансу. Це можна побачити на рисунку 4.9.

```
1 usage
def import_wallet(self):
    global private_key
    priv_key = self.import_private_key_entry.get()
    seed_phrase = self.import_seed_phrase_entry.get(1.0, END).strip()

    # Perform necessary actions to import the wallet using the private key or seed phrase
    # This part will depend on how you want to handle the imported wallet

    # Assuming the private key is used for the import
    if priv_key:
        private_key = Account.from_key(priv_key)

    elif seed_phrase:
        # Assuming the seed phrase is used for the import
        mnemonic = Mnemonic("english")
        derived_private_key = mnemonic.to_seed(seed_phrase)
        imported_account = Account.from_key(derived_private_key)


    self.show_balance()
```

Рисунок 4.9 – Функція зчитування даних при імпорті гаманцю

Наступна функція відповідає за створення третього вікна, що з’являється після іморту приватного ключа або мнемонічної фрази. Функція містить у собі налаштування розміру вікна, фону, кнопок та їх функціоналу, текстоввих полів. Функція зв’язується із блокчейном та робить запит на отримання актуального балансу гаманця, після чого фіксує цей баланс та починає відображати його. Користувачу необхідно ввести кількість токенів, що буде відправлена та адресу гаманця отримувача. При натисканні на кнопку для відправки викликається функція відправки токенів. Все це можна побачити на рисунку 4.10.

```
1 usage
def show_balance(self):
    self.import_window.withdraw()
    self.balance_window = Toplevel(self.master)
    self.balance_window.title("Wallet Balance")
    self.balance_window.geometry("1120x630")
    self.balance_window.configure(bg="black")
    self.balance_window.resizable(0, 0)

    balance = w3.eth.get_balance(private_key.address)
    eth_balance = w3.from_wei(balance, "ether")

    self.balance_label = Label(self.balance_window, text=f"ETH Balance: {eth_balance} ETH", bg="black", fg="white")
    self.balance_label.place(relx=0.5, rely=0.3, anchor="center")

    self.amount_label = Label(self.balance_window, text="Amount:", bg="black", fg="white")
    self.amount_label.place(relx=0.3, rely=0.5, anchor="center")

    self.amount_entry = Entry(self.balance_window, width=30)
    self.amount_entry.place(relx=0.5, rely=0.5, anchor="center")

    self.address_label = Label(self.balance_window, text="Wallet address:", bg="black", fg="white")
    self.address_label.place(relx=0.3, rely=0.6, anchor="center")

    self.address_entry = Entry(self.balance_window, width=80)
    self.address_entry.place(relx=0.5, rely=0.6, anchor="center")

    self.send_button = Button(self.balance_window, text="Send", command=self.send_eth)
    self.send_button.place(relx=0.5, rely=0.7, anchor="center")
```

Рисунок 4.10 – Налаштування графічного відображення третього вікна та відображення балансу

Наступна функція відповідає безпосередньо за відправлення токенів. Спочатку функція зчитує значення кількості токенів да адресу гамманця отримувача із текстових полів. Якщо хоча б один з цих двох параметрів відсутній, то програма видасть помилку та нагадає, що необхідно ввести два значення.

Для усіх операцій у EVM-блокчейнах використовується не цілочисельне значення токенів ETH, а кількість Wei, що являється найменшою підроздільною одиницею Ether. Тому для відображення балансу та відправки в ETH необхідно спочатку перевести з Wei до ETH та навпаки.

У цій функції використовується словник, що має у собі наступні параметри.

1) Nonce – кількість транзакцій гаманця.
2) To – адреса отримувача.
3) Value – кількість токенів для відправки.

4) From – адреса гаманця, з якого ініціюється транзакція.

5) Gas – значення газ-ліміту.

6) GasPrice – ціна газу у даний момент.

Все це можна побачити на рисунку 4.11.

```
1 usage
def send_eth(self):
    amount = self.amount_entry.get()
    address = self.address_entry.get()

    if not amount or not address:
        messagebox.showerror("Error", "Please enter both amount and address.")
        return

    # Convert the amount to wei
    amount_wei = w3.to_wei(amount, "ether")

    # Get the current account's nonce value
    current_account = private_key
    nonce = w3.eth.get_transaction_count(current_account.address)

    # Create the transaction object
    tx = {
        "nonce": nonce,
        "to": address,
        "value": amount_wei,
        'from': current_account.address,
        "gas": 21000,
        "gasPrice": w3.eth.gas_price
    }
    balance = w3.eth.get_balance(current_account.address)

    # Sign the transaction with the current account's private key
    signed_tx = current_account.signTransaction(tx)

    # Send the signed transaction
    tx_hash = w3.eth.send_raw_transaction(signed_tx.rawTransaction)
    print(tx_hash.hex())
    messagebox.showinfo("Transaction Sent", f"Transaction sent successfully!\nTransaction Hash: {tx_hash.hex()}")
```

Рисунок 4.11 – Функція відправлення токенів

4.3 Виконання программи

Під час запуску програмного забезпечення відкривається перше вікно, що відповідає за генерацію приватного ключа та мнемонічної фрази. Вікно має наступні елементи.

1) Два текстових поля, у яких відображаються згенерований приватний ключ та мнемонічна фраза.

2) Кнопка для початку алгоритму генерації.

3) Кнопки для копіювання приватного ключа та мнемонічної фрази до буфера обміну.

4) Кнопка відправки приватного ключа та мнемонічної фрази на друк, що є неактивною до того моменту, поки приватний ключ та мнемонічна фраза не були згенеровані.

5) Кнопка для переходу до іншого вікна, в якому використовується вже існуючий приватний ключ або мнемонічна фраза.

Зовнішний вигляд вікна відразу після запуску програмного забезпечення можна побачити на рисунку 4.12.

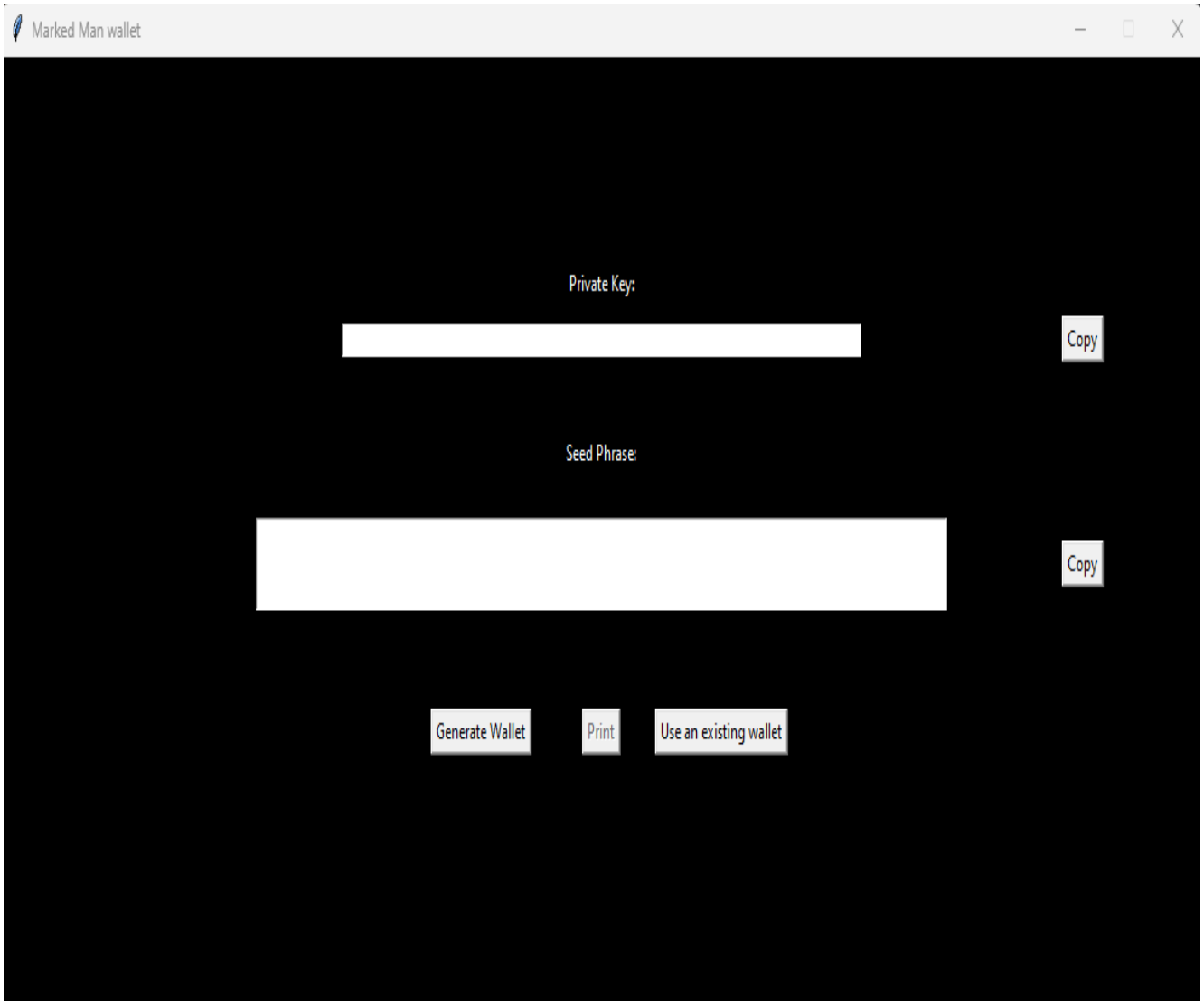

Рисунок 4.12 – Перше вікно після запуску програмного забезпечення

Після натискання на кнопку для генерації гаманця текстові поля приймають значення приватного ключа та мнемонічної фрази, що відповідають цьому

гаманцю. Також кнопка для відправки на друк стає активною. Це можна побачити на рисунку 4.13.

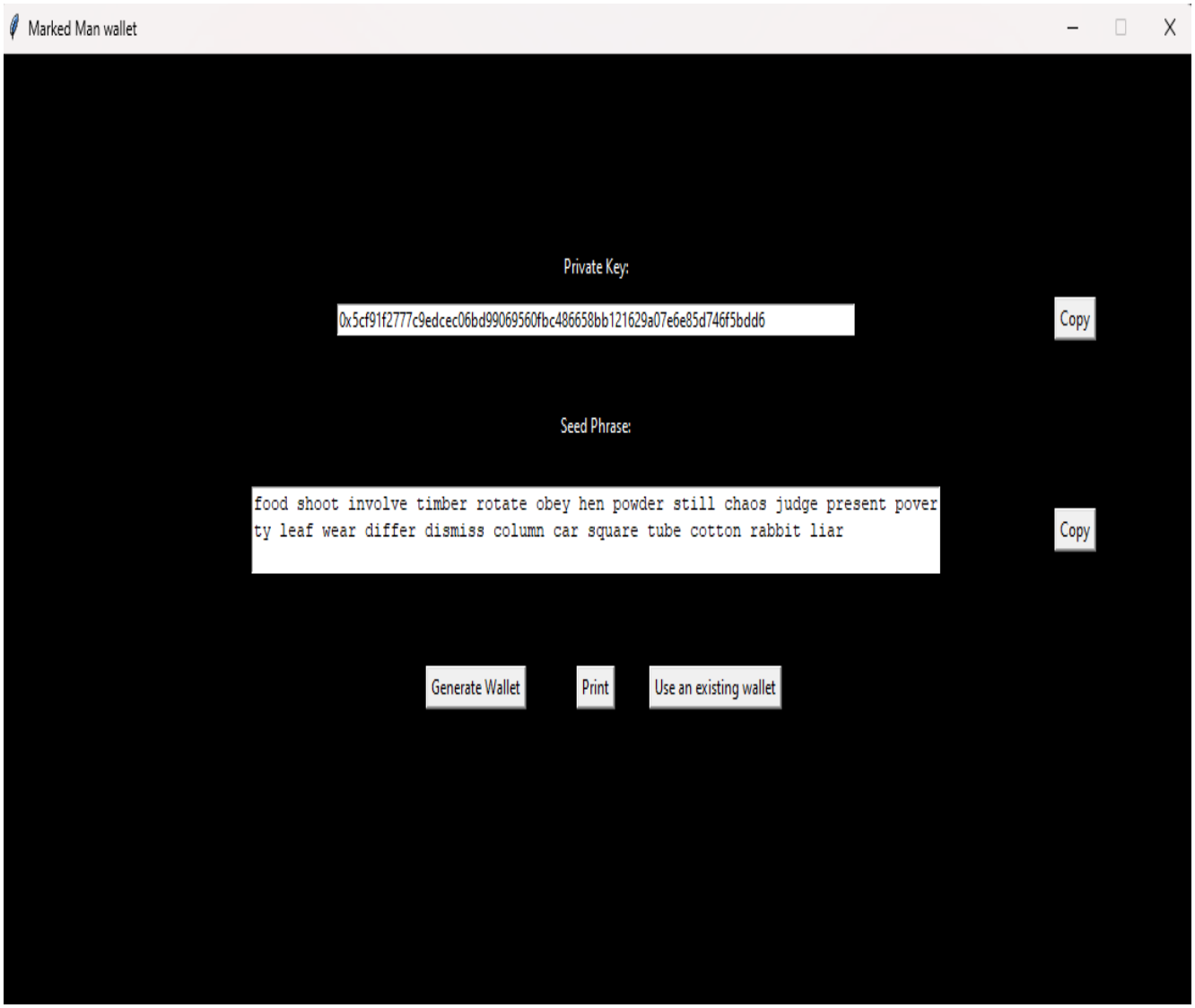

Рисунок 4.13 – Перше вікно після генерації гаманця

Після натискання на кнопку для використання вже існуючого гаманця перше вікно закривається та відкривається друге. У другому вікні є текстові поля для приватного ключа та мнемонічної фрази. Одне з цих полів повинно бути заповнене для вдалого імпорту гаманця. Зовнішній вигляд другого вікна одразу після його відкриття можна побачити на рисунку 4.14.

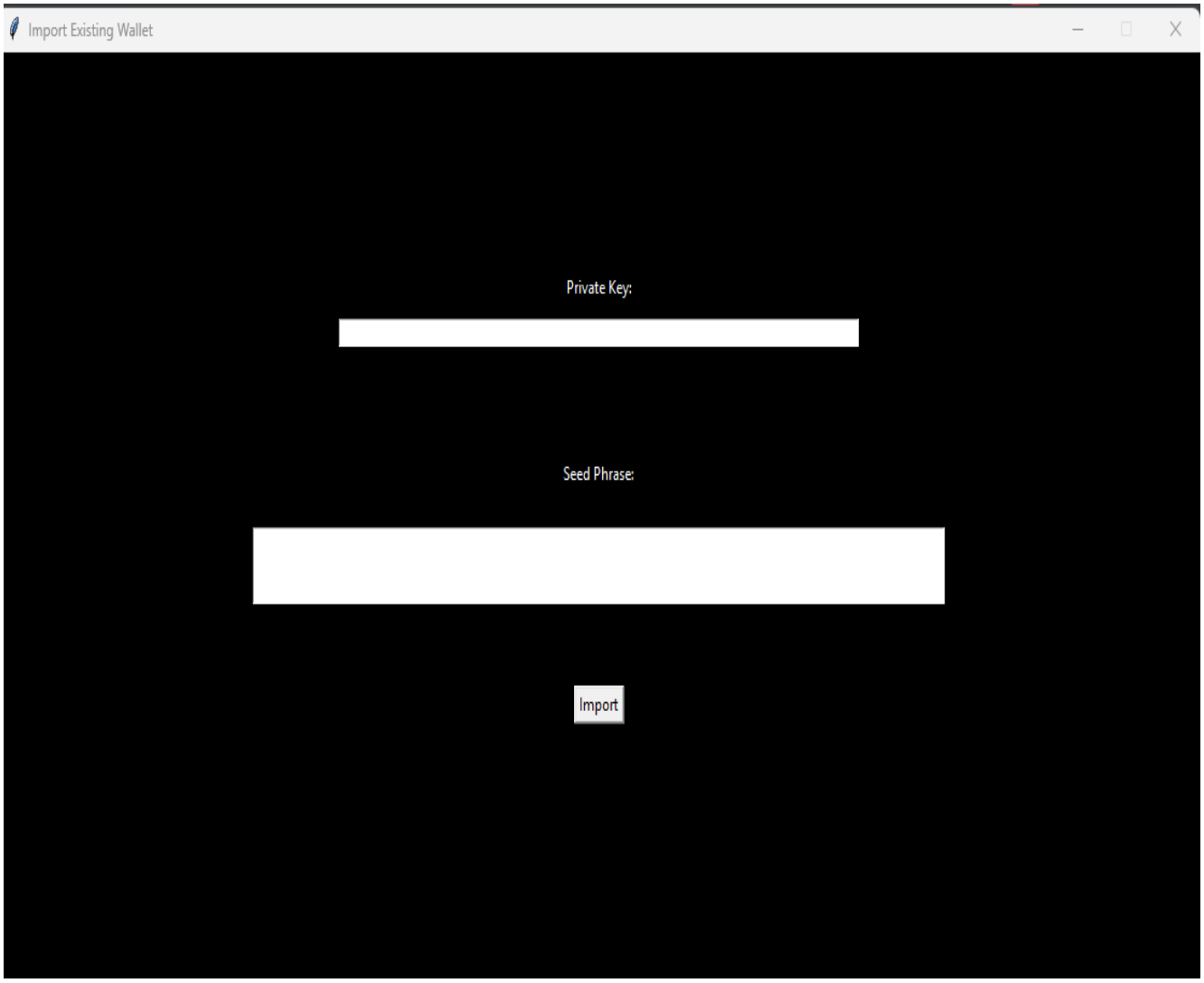

Рисунок 4.14 – Друге вікно після переходу до нього

Після введення приватного ключа або мнемонічної фрази до необхідного текстового поля необхідно натиснути кнопку для імпорту гаманця. Слід звернути увагу на те, що якщо довжина приватного ключа або ж кількість слів у мнемонічній фразі є правильними, то навіть за умови того, що вони були введені невірно, імпортується інший гаманець. Звісно що цей гаманець не матиме будь-якого балансу, але програма не буде видавати помилку. Вигляд другого вікна із введеним приватним ключем можна переглянути на рисунку 4.15.

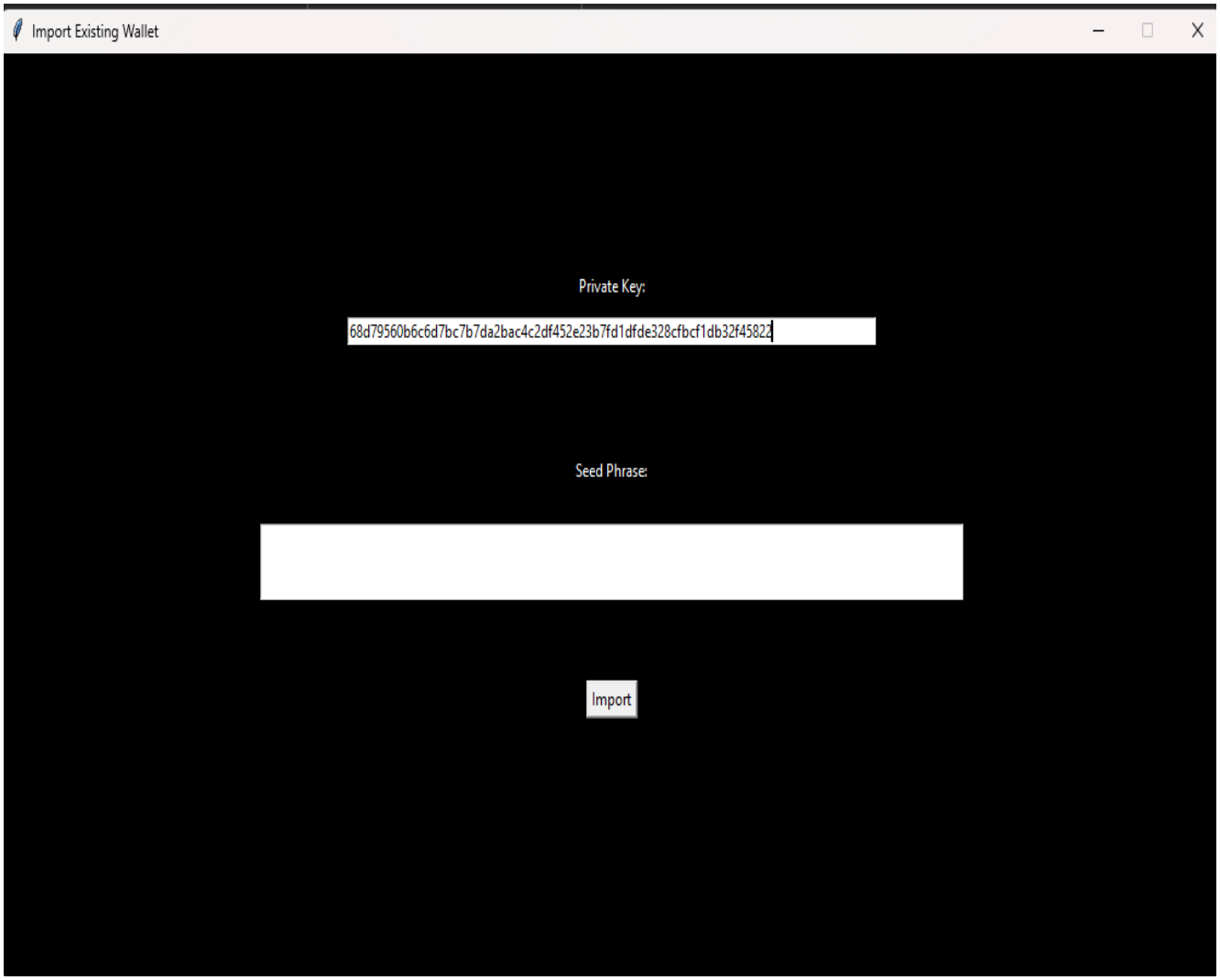

Рисунок 4.15 – Друге вікно після введення приватного ключа

Після введення приватного ключа або мнемонічної фрази та натискання на кнопку для імпорту гаманця друге вікно закривається, а відкривається третє вікно. У цьому вікні зпочатку відображаться актуальний баланс гаманця у токенах ETH. Також це вікно відповідає за функціонал ініціалізації відправлення транзакції на інший гаманець. Вікно містить два текстовіих поля, у перше необхідно ввести кількість токенів, що необхідно відправити, а у друге вікно необхідно ввести адресу гаманця, на який будуть відправлятися токени. Вигляд третього вікна з відображенням балансу для імпортованого гаманця можна переглянути на рисунку 4.16.

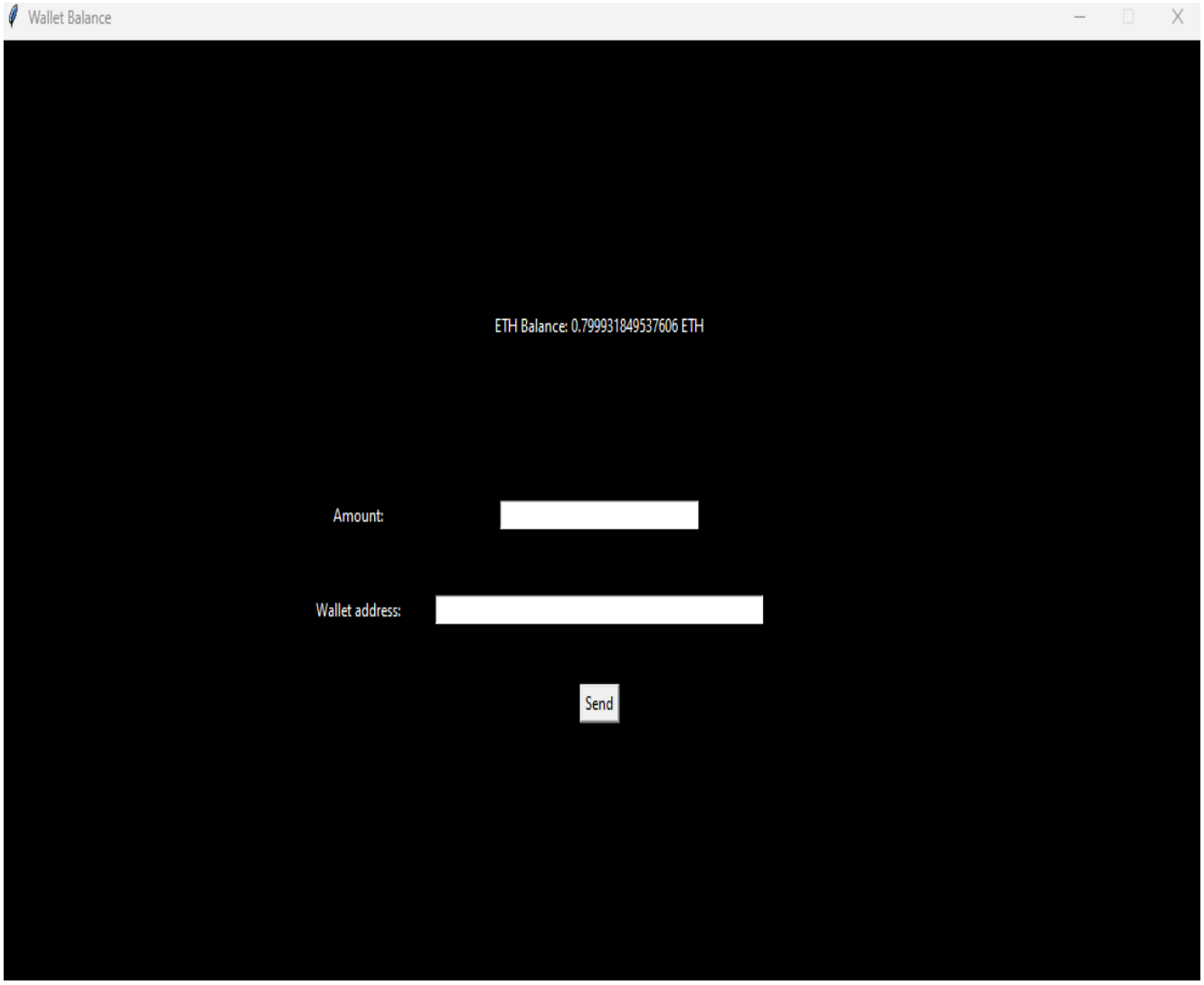

Рисунок 4.16 – Третє вікно з відображенням балансу імпортованого гаманця

Після введення необхідної кількості токенів та адреси гаманця, на який ці токени будуть відправлятися, необхідно натиснути на кнопку відправки. У випадку, якщо все добре, тобто відправник має достатню кількість токенів на рахунку для відправки та оплати газу, робочого стану обраного вузлу та інше, програмне забезпечення відкриє нове вікно, де буде повідомлення про те, що транзакція була вдало відправлена. Також у цьому вікні буде знаходитися хеш транзакції, що відразу робить більш легшим відстеження активності гаманцю та статусу транзакції. Вигляд третього вікна після вдалої ініціалізації транзакції відправлення токенів можна розглянути на рисунку 4.17.

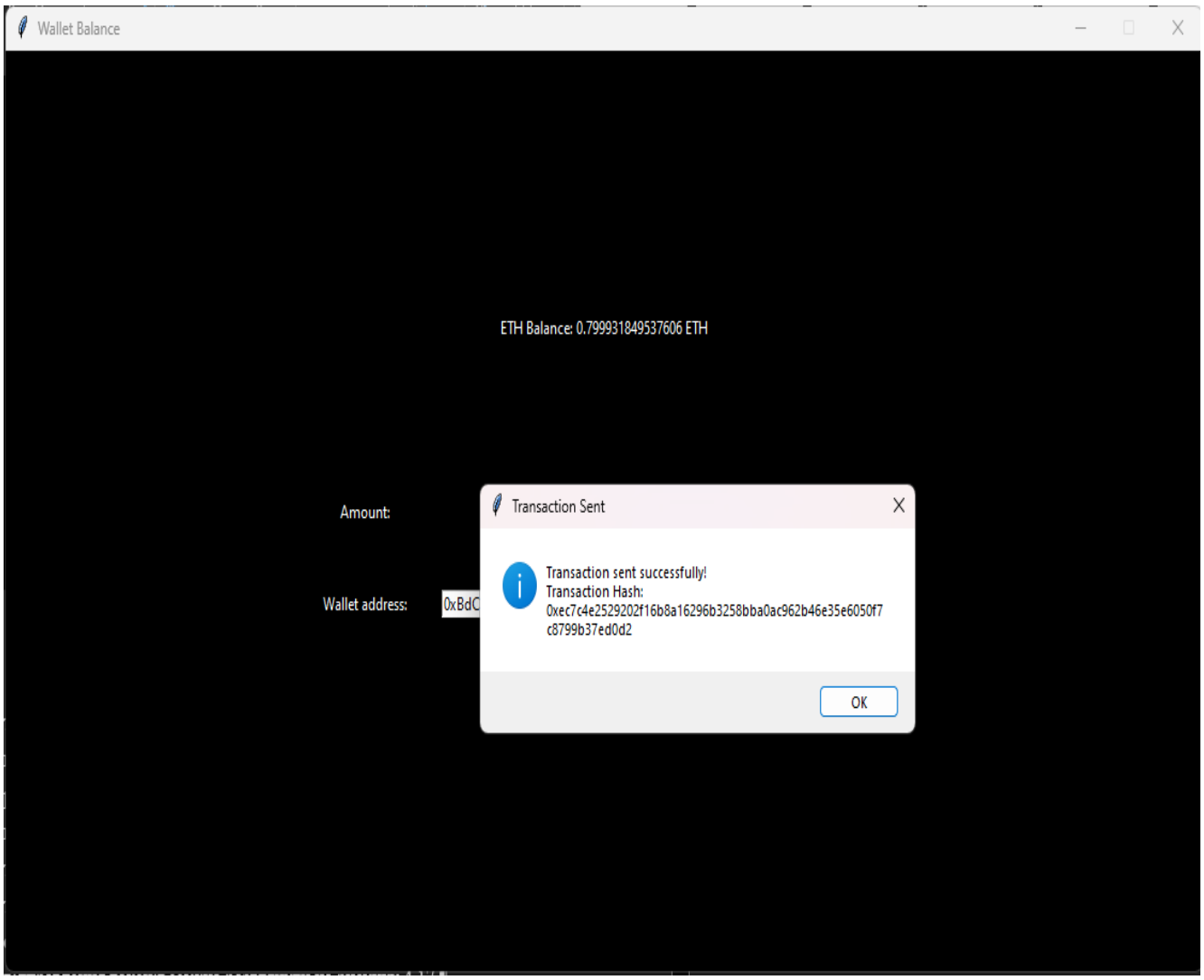

Рисунок 4.17 – Третє вікно після вдалої ініціалізації транзакції на відправлення токенів

За допомогою отриманого хешу транзакції можна розглянути транзакцію більш детально за допомогою есплореру блокчейну. Експлорер блокчейну – це пошукова програма, яка дозволяє користувачам переглядати інформацію про блоки, транзакції та адреси в певній блокчейн-мережі. Експлорери відіграють важливу роль у взаємодії з блокчейн-технологіями, так як вони надають зручний та прозорий спосіб відстеження і перевірки даних на блокчейні.

Експлорери блокчейнів можуть мати різні функції та особливості, але зазвичай вони надають наступні можливості.

1) Перегляд інформації про блоки: користувачі можуть переглядати деталі про окремі блоки, включаючи їх хеш, номер, час створення, кількість транзакцій та інше.

2) Перегляд інформації про транзакції: користувачі можуть переглядати деталі про транзакції, такі як хеш, статус, відправник, одержувач, суму та комісію.

3) Перегляд інформації про адреси: користувачі можуть переглядати баланс адреси, історію транзакцій та пов'язані контракти.

4) Пошук за хешем, номером блоку або адресою: користувачі можуть шукати конкретні елементи, вводячи відповідні ідентифікатори у поле пошуку.

Усі дані про транзакцію можна переглянути на рисунку 4.18.

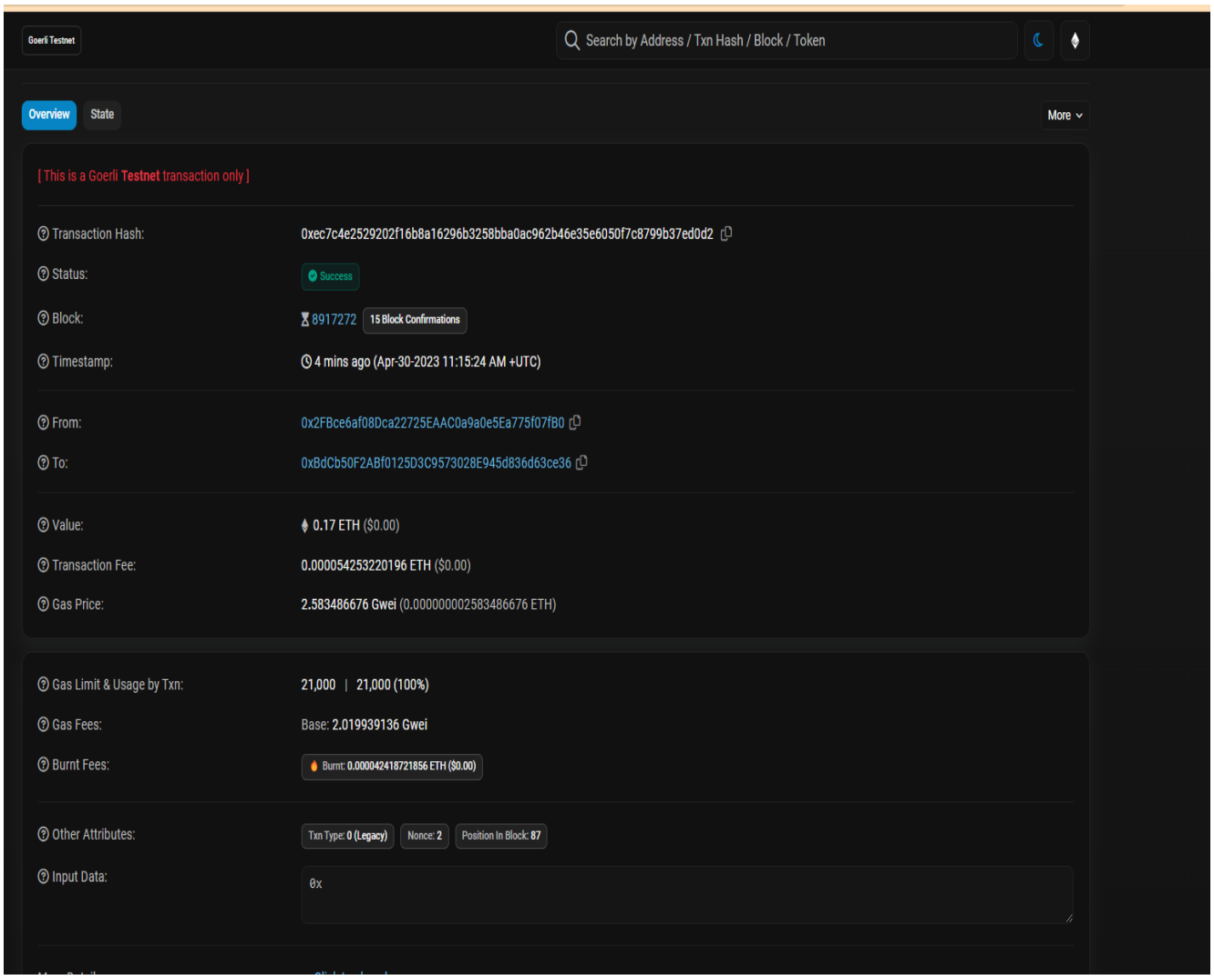

Рисунок 4.18 – Детальна інформаця про транзакцію

ВИСНОВКИ

В кваліфікаційній роботі було розглянути проблеми забезпечення безпеки зберігання ключів при використанні існуючих рішень для взаємодії із блокчейном.

Було проведено аналіз сучасних технологій роботи блокчейнів. Типи блокчейнів за моделями консенсусу, рівні блокчейнів, типи блокчейнів за видами доступу. Також було розглянуто трилему блокчейну, що являється однією з найголовніших проблем у блокчейн-технологіях. Розглянуто роботу смарт-контрактів, доказів із нульовим розголошенням, та оракули. Проаналізовано шляхи майбутнього розвитку Інтернету та блокчейн-технологій.

Також було досліджено використання хешування у блокчейн-технологіях. Розглянуто сучасні методи використання шифрування, криптографічних підписів, Мерклевих дерев та мультипартійних обчислень

Досліджені сучасні гаманці, що використовуються для взаємодії із блокчейнами. Проведено порівняння різних рішень для цих гаманців. Було проведено аналіз найбільш відомих методів захисту ключів від зловмисників. Було розглянуто способи протидії зловмисникам та оптимізації зберігання інформації.

Окремі результати роботи доповідалися на міжнародних наукових конференціях [4, 7, 9].

Досліджені питання можна практично використовувати у повсякденному житті. Доцільним буде використання комплексних методів захисту безпеки ключів.

В ході виконання роботи було досягнуто ціль – аналіз шляхів досягнення максимального ступіню збереження ключів та зниження потенційних рисків щодо їх компрометації, розробка власного програмного забезпечення для роботи із блокчейном зі зменшенням ризику компрометації ключів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Narayanan A. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction [Електронний ресурс] / A. Narayanan, J. Bonneau. – 2016. – Режим доступу до ресурсу: https://www.cs.princeton.edu/~arvindn/courses/685/bitcoinbook.pdf.

2. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger [Електронний ресурс] / Gavin Wood. – 2014. – Режим доступу до ресурсу: https://ethereum.github.io/yellowpaper/paper.pdf.

3. Casey M. The Truth Machine: The Blockchain and the Future of Everything [Електронний ресурс] / M. Casey, J. Vigna. – 2018. – Режим доступу до ресурсу: https://us.macmillan.com/books/9781250308013.

4. Зражевець К. П. Важливість блокчейн-технологій у сучасному світі / К. П. Зражевець // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 40-41.

5. Розробка смарт-контрактів на Ethereum [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://solidity.readthedocs.io/.

6. Smart Contract Auditing: What Is It And Why It Matters [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.consensys.net/blog/codefi/smart-contract-auditing-what-it-is-and-why-it-matters/.

7. Зражевець К. П. Розподілені технології обліку / К. П. Зражевець // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 43-44.

8. Cryptocurrency Wallet Guide: A Step-By-Step Tutorial [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

9. Зражевець К. П. Безпечність зберігання ключів у EVM-блокчейнах / К. П. Зражевець // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 46-47.

10. What is a Mnemonic, or Secret Code, Seed, or Recovery Phrase? [Електронний ресурс] // Vault12 Crypto Security. – 2023. – Режим доступу до ресурсу: https://vault12.com/securemycrypto/crypto-security-basics/mnemonic-seed-recovery-phrase/.

11. Warinschi B. How to build time-lock encryption [Електронний ресурс] / B. Warinschi, J. Liu, T. Jager. – 2017. – Режим доступу до ресурсу: https://eprint.iacr.org/2015/482.pdf.

12. Introduction to Web3.py [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://web3py.readthedocs.io/en/stable/.