УДК 004.891

к.т.н., доц., **Джулій В.М. (Хм. НУ)**
Філюк Є.В. (Хм. НУ)

DOI: http://doi.org/10.17721/2519-481X/2024/83-07

МЕТОД БАГАТОСТОРОННІХ ОБЧИСЛЕНЬ КЕРУВАННЯ КРИПТОАКТИВАМИ НА ОСНОВІ ТЕХНОЛОГІЇ MULTI-PARTY COMPUTATION

Розглянута задача побудови ефективного та безпечного криптовалютного гаманця на основі технології багатосторонніх обчислень, який може забезпечити надійне та захищене використання в різних галузях, що працюють з криптовалютами.

Сучасні алгоритми багатосторонніх обчислень, такі як Дженнаро та Голдфедера, Лінделли, Доернера, пропонують значні переваги у захисті даних, але вони мають певні обмеження. Основними з них є недостатня ефективність у кількості раундів підпису та відсутність підтримки холодного зберігання. Це підкреслює необхідність подальших досліджень і розробок у сфері технології Multi-Party Computation для досягнення більш високого рівня операційної ефективності та гнучкості.

Метод забезпечення конфіденційності та безпеки криптоактивів на сонові технології багатосторонніх обчислень для Ethereum мережі полягає в: забезпеченні високого рівня безпеки для збереження приватних ключів та процесу підписання транзакції, використовуючи передові методи криптографічного захисту; гарантуванні конфіденційності та приватності користувачів, захищаючи їх особисту інформацію від несанкціонованого доступу або витоку даних; використанні передових технологій, включаючи технологію Multi-Party Computation, для підвищення рівня безпеки та приватності зберігання активів.

На основі проведеного дослідження та аналізу характеристик стандартів протоколів багатосторонніх обчислень запропонований протокол, який враховує наявні покращення та недоліки попередніх протоколів. Для покращення безпеки, у протоколі впроваджено принцип інтервального оновлення спільного секрету.

Система керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації. Система надає можливість надійного зберігання криптоактивів, зокрема приватних ключів до гаманців Ethereum мережі, з використанням технології Multi-Party Computation, яка може бути використана у різних криптопроектах для безпечного переказу криптоактивів.

Архітектура системи передбачає взаємодію основних компонентів для забезпечення надійної та безпечної роботи. Запропоновано схему встановлення безпечного з'єднання вузлів та описано модель локального сховища, яке забезпечує безпечне зберігання часток ключів, підписів та системних логів.

Ключові слова: криптоактиви, конфіденційна інформація, безпека криптоактивів, технологія multi-party computation, безпечне з'єднання, інформаційна безпека, криптовалюта, цифрові активи, криптовалютний гаманець.

Вступ. З кожним роком популярність використання криптовалюти зростає, так само як і попит на безпечні криптовалютні гаманці. Люди використовують криптовалюту з різних причин: як засіб обміну та збереження вартості, інструмент інвестування та спосіб здійснення міжнародних переказів. Криптовалюти є цифровими активами, які використовують криптографічні протоколи для забезпечення безпеки транзакцій та контролю за створенням нових одиниць цифрової валюти. Вони працюють на базі технології блокчейн, яка дозволяє записувати транзакції у розподіленій базі даних, забезпечуючи безпеку та непідробність операцій [1,2].

Основною перевагою криптовалют є їх децентралізація: вони не контролюються центральними органами управління, такими як уряди чи банки, і можуть бути використані у будь-якій частині світу без обмежень. Додатковими перевагами є анонімність, що дозволяє

користувачам зберігати конфіденційність своїх фінансових операцій, та зручність, що забезпечує швидкі та прості перекази без посередників. Найвідомішою криптовалютою є біткоїн, також існує безліч інших криптовалют, як Ethereum, Ripple, Tether та інші [4,8].

Криптовалютні гаманці є ключовими інструментами для зберігання, відправлення та отримання криптовалюти. Вони можуть бути онлайн-сервісами, програмами для смартфонів або настільними програмами, дозволяючи користувачам відстежувати свої баланси та історію транзакцій. У зв'язку з цим створення ефективного та безпечного криптовалютного гаманця є актуальним завданням для багатьох галузей, які працюють з криптовалютами, таких як фінансові послуги, торгівля, інтернет-магазини, туризм та благодійність [11,13].

Сучасні криптовалютні гаманці розробляють на основі технології Multi-Party Computation (MPC). Використання MPC дозволяє значно підвищити безпеку криптовалютних транзакцій. Дана технологія забезпечує захист даних навіть у випадку компрометації частини учасників системи, оскільки вона розподіляє обробку і зберігання інформації між декількома учасниками, уникаючи центральної точки вразливості. MPC використовує криптографічні методи для розподіленої обробки даних, що дозволяє кільком сторонам виконувати обчислення над даними, не розкриваючи їх один одному. Це гарантує, що жодна сторона не має повного доступу до всієї інформації, що значно знижує ризик витоку даних або зловживань, якщо один або декілька учасників системи будуть зламані або скомпрометовані, конфіденційність та цілісність транзакцій залишаться під захистом [14,18].

Предметом дослідження роботи є створення ефективного та безпечного криптовалютного гаманця на основі технології MPC, який може забезпечити надійне та захищене використання в різних галузях, що працюють з криптовалютами.

Аналіз останніх досліджень та постановка задачі. Блокчейн –децентралізована та розподілена база даних, яка використовується для безпечного, незмінного та прозорого зберігання записів. Ця технологія функціонує на основі принципу послідовного об'єднання блоків даних у ланцюг. Кожен блок містить список транзакцій і пов'язаний з попереднім блоком за допомогою криптографічного хешу, що утворює ланцюг блоків, або блокчейн.

Децентралізація у блокчейні – контроль і повноваження щодо прийняття рішень у мережі розподіляються між її користувачами, а не контролюються однією особою. Це може бути корисним у ситуаціях, коли учасникам необхідно координувати свої дії з незнайомцями або коли вони хочуть подбати про безпеку й цілісність своїх даних [1,2]. У децентралізованій блокчейн-мережі немає центрального органу, який контролює потік даних чи транзакцій. Натомість транзакції перевіряються й записуються розподіленою мережею комп'ютерів, які працюють для підтримки цілісності мережі. Безпека досягається за допомогою криптографічних методів, які захищають дані від несанкціонованого доступу.

У цьому контексті фундаментальне значення мають так звані криптографічні хеш-функції. Хешування – це процес, при якому алгоритм отримує вхідні дані будь-якого розміру і повертає результат, що містить передбачуваний та фіксований розмір. Дана властивість хеш-функцій широко використовується в інформаційній безпеці, зокрема для захисту паролів. Хеші в блокчейнах використовуються як унікальні ідентифікатори для блоків даних і створюють ланцюжок зв'язаних блоків (рис. 1) [2,8].

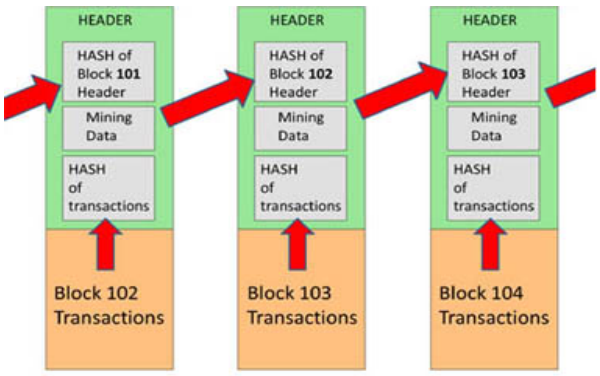

Рисунок 1 – Схематична структура блокчейну

Для обробки транзакцій у блоці використовується метод, відомий як алгоритм дерева Меркла (рис. 2), і в цьому процесі застосовується хешування [4,5].

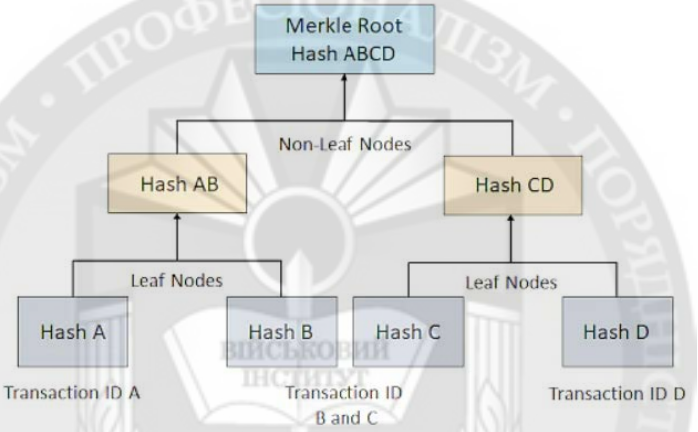

Рисунок 2 – Дерево Меркла

Кожна транзакція в блоці спочатку хешується індивідуально. Потім хеші кожної транзакції об'єднуються і хешуються разом. Якщо кількість транзакцій непарна, останній хеш дублюється і хешується сам із собою, щоб створити парну кількість хешів. Цей процес повторюється поки залишиться лише один кореневий хеш, чи корінь Меркла. Кожен хеш блоку генерується на основі даних в ньому та хешу попереднього блоку (рис. 3) [10].

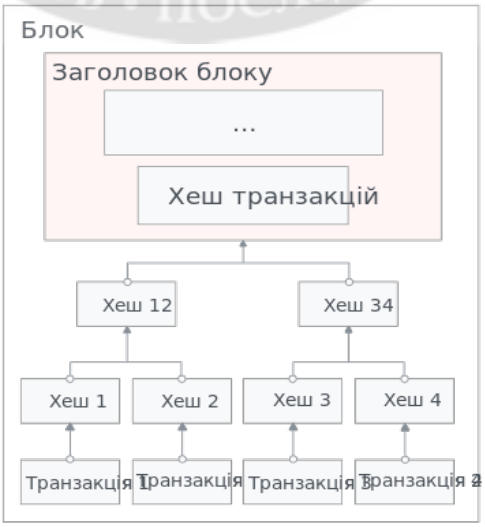

Рисунок 3 – Схематична структура блоку

Дана взаємозалежність гарантує безпеку та незмінність блокчейну. Хешування також використовується в алгоритмах консенсусу, які в свою чергу використовуються для перевірки транзакцій [2,8].

У блокчейні Bitcoin використовується алгоритм Proof of Work (PoW), процес виконання консенсусу Proof of Work (PoW) полягає у тому, щоб мережа визначала, який блок буде доданий до ланцюжка блоків (blockchain). У спрощеному вигляді, учасники мережі, такі як майнери, змагаються за право знайти блок і додати його до ланцюжка. Для цього вони повинні вирішити складну математичну задачу, яка вимагає великої обчислювальної потужності. PoW, зазвичай базуються на хеш-функції SHA-256. Валідатори мережі повинні знайти створений хеш для нового блоку, який задовольняє певні умови (рис. 4) [10,17].

Саме завдяки консенсусу мережа захищена від атак, таких як подвійне витрачання та модифікація історії транзакцій. Він робить такі атаки вкрай важкими, оскільки будь-яка спроба зміни історії потребує повторного обчислення хешів для всіх попередніх блоків у ланцюжку, а також виграшу у конкуренції з іншими валідаторами для створення нових блоків. Чим більша обчислювальна потужність у мережі, тим важче здійснити подібні атаки, що робить мережу більш стійкою до зловживань.

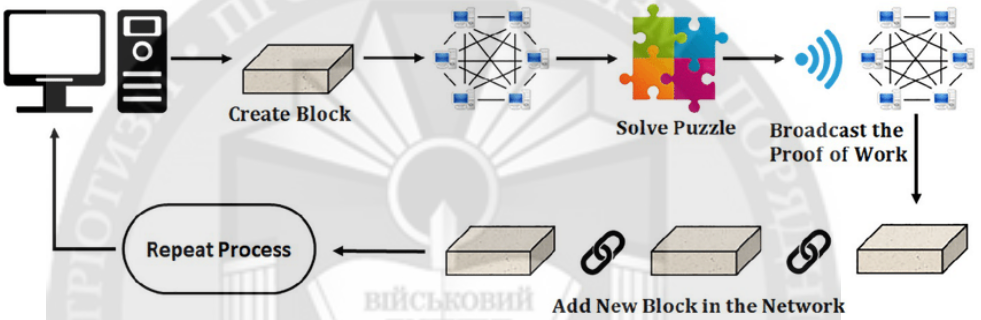

Рисунок 4 – Схематичне зображення Proof of Work (PoW)

Для здійснення будь яких операцій у мережі, звичайні користувачі, повинні ініціювати криптотранзакції. Для того, щоб відправити криптовалюту, кожному учаснику необхідно мати свій рахунок. Акаунт управляється парою ключів, де відкритий ключ це адреса, яку користувач вказує для отримання цифрових активів, а закритий контролює дії всередині облікового запису, тобто підписує транзакції [18-25]. Кожен рахунок має один закритий ключ [17].

Для підписання транзакції у блокчейн мережі використовується алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) (рис. 5) [17, 26]. Для підписання алгоритм використовує приватний ключ, що є випадковим числом, а публічний ключ генерується за допомогою множення приватного ключа на генераторну точку еліптичної кривої [26]. Перевірка включає використання публічного ключа для перевірки автентичності підпису. Процес полягає в обчисленні двох точок на еліптичній кривій і перевірці, чи збігаються ці точки з підписом та хешем повідомлення. Ефективність та безпека ECDSA забезпечується властивостями еліптичних кривих, які дозволяють досягнути високого рівня стійкості до криптографічних атак при відносно невеликих обчислювальних витратах [11, 26].

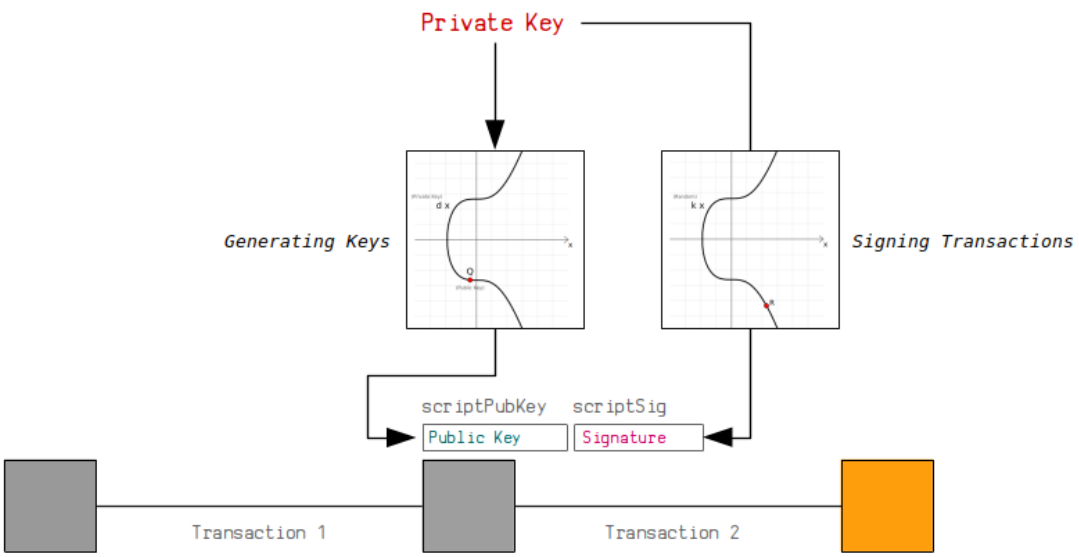

Рисунок 5 – Схематичне зображення роботи алгоритму ECDSA

Весь процес обробки криптовалютних транзакцій (рис. 6) можна поділити на три окремі етапи: створення, підписання, трансляцію та підтвердження (автентифікація та авторизація) [4,6,12].

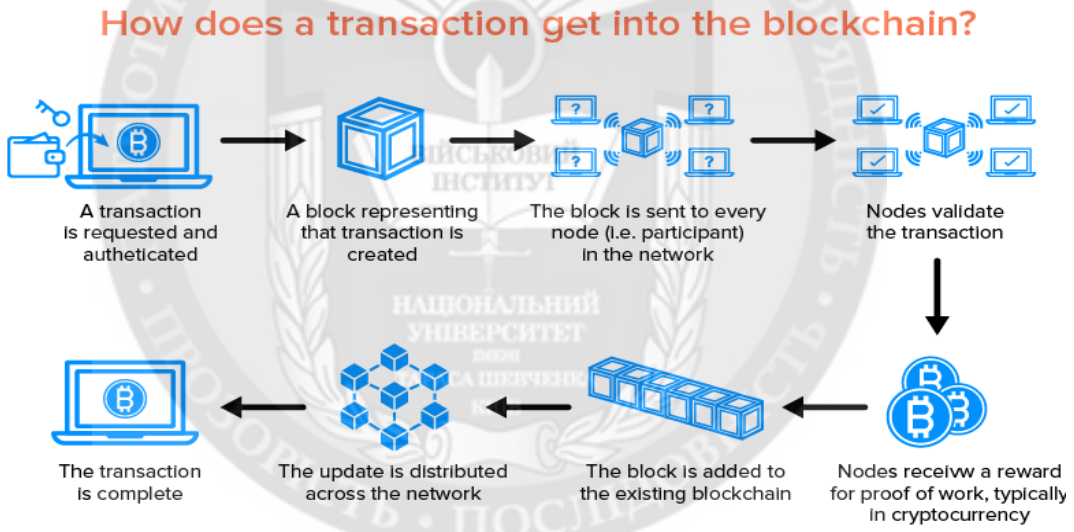

Рисунок 6 – Схематичне зображення взаємодії блокчейна та криптотранзакції

Багатосторонні обчислення MPC (Multi-Party Computation) - набір методів, за допомогою яких декілька учасників можуть спільно вирішувати обчислювальні задачі, не розкриваючи свої вхідні дані один одному. У контексті MPC, кожен учасник має свої власні приватні дані, і мета полягає в тому, щоб вони могли обчислити якийсь результат або функцію, використовуючи ці дані разом, при цьому не розкриваючи їх один одному. Такий тип обчислень стає альтернативою кастодіальним криптогаманцям з мультипідписом, так як дає можливість розділити відповідальність зберігання приватних ключів між декількома сторонами [14,17].

Технологія MPC застосовується для низки варіантів, таких як захист цифрових активів у MPC-гаманцях або збереження певної інформації в таємниці під час цифрових аукціонів.

Основні протоколи MPC, які застосовуються для реалізації кастодіальних криптогаманців:

1. Алгоритм Дженнаро та Голдфедера наразі є одним із найкращих доступних алгоритмів MPC, і багато установ, які захищають свої приватні дані за допомогою MPC, використовують саме цей алгоритм. Однак, незважаючи на його переваги, затримка зв'язку між спільними ресурсами MPC (пристроями, які зберігають ключові спільні ресурси) не досягає найвищого рівня ефективності. Це обумовлено тим, що користувачі повинні чекати до 9 раундів підпису для завершення транзакцій. Крім того, алгоритм Дженнаро та Голдфедера не пропонує жодної гнучкості для установ, яким потрібно використовувати холодне зберігання. Це суттєво обмежує його застосування у сценаріях, де необхідно забезпечити високий рівень безпеки при зберіганні даних офлайн.

2. Алгоритм багатосторонніх обчислень, запропонований Лінделлом та ін., забезпечує незначне зменшення кількості транзакцій, які повинні бути підписані, у порівнянні з алгоритмом Дженнаро та Голдфедера – до 8 раундів. Однак цей алгоритм не досягає рівня операційної ефективності, необхідного для сучасних ринків. Як і алгоритм Дженнаро та Голдфедера, рішення Лінделла також не підтримує холодне зберігання, що обмежує його використання в певних сферах [17,20,21].

3. Алгоритм MPC Доернера та ін. демонструє значний прогрес, досягаючи порогу лише за 6 підписів. Проте, навіть цей рівень ефективності не відповідає потенціалу сучасних технологій. Більше того, подібно до попередніх двох алгоритмів, рішення Доернера також не надає можливості використання холодного зберігання разом із MPC [14].

Таким чином, хоча сучасні алгоритми багатосторонніх обчислень, пропонують значні переваги у захисті даних, вони мають певні обмеження. Основними з них є недостатня ефективність у кількості раундів підпису та відсутність підтримки холодного зберігання. Це підкреслює необхідність подальших досліджень і розробок у сфері MPC для досягнення більш високого рівня операційної ефективності та гнучкості.

Розглянемо алгоритми, які застосовуються для розробки протоколів у MPC гаманцях:

1. Схема розподілу секрету Шаміра (Shamir's Secret Sharing) - дозволяє розділити інформацію на багато часток, при цьому для відновлення оригінального секрету потрібно лише частину з цих часток (рис. 7) [8,11].

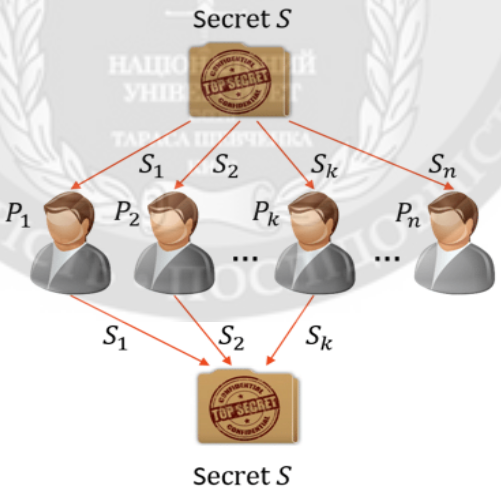

Рисунок 7 – Схематичне зображення роботи схеми розподілу секрету

Для відновлення оригінального секрету, схема Шаміра вимагає мінімальну кількість часток — ця мінімальна кількість називається порогом. Для відновлення секрету необхідно досягти порогу. Якщо кількість часток менша за порогову, секрет не може бути відновлений, що робить схему розподілу секрету Шаміра захищеною від зловмисників з необмеженою обчислювальною потужністю.

2. Порогова схема підпису (Threshold Signature Scheme, TSS) є криптографічним примітивом для розподіленого генерації ключів та підписання (рис 8). Використання TSS у

клієнтах блокчейн, системах зберігання ключів є новою парадигмою, яка може надати численні переваги, особливо в аспекті безпеки. TSS може вплинути на дизайн систем управління ключами (таких як криптогаманці) та прокласти шлях для підтримки нативних випадків використання в DeFi. Втім, варто зазначити, що TSS все ще є новою технологією, тому ризики та обмеження також слід враховувати. Порогові підписи вимагають підмножину сторін, уповноважених створювати підписи від імені групи. Повідомлення вважається підписаним лише в тому випадку, якщо поріг (*t* із *n*, де *t* —поріг підписувачів, а *n* — кількість усіх підписувачів) підписувачів підписують повідомлення [14].

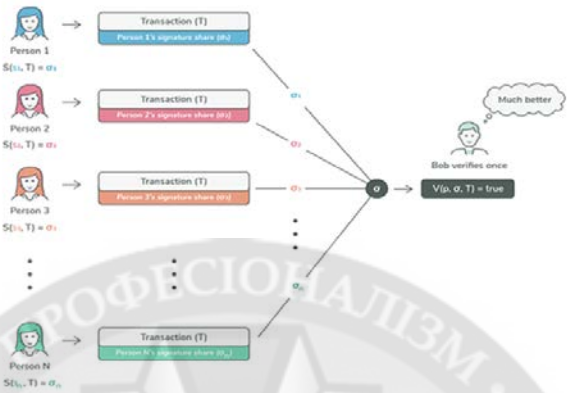

Рисунок 8 – Схематичне зображення роботи протоколу схеми порогового підпису

3. Розподілена генерація ключів (Distributed Key Generation, DKG) - криптографічний протокол, який дозволяє спільно генерувати криптографічні ключі багатьма учасниками, кожен з яких має частину секретного ключа) (рис. 9). Розподіляючи процес генерації ключів між групою учасників, DKG гарантує, що жоден суб'єкт не матиме повного контролю, таким чином суттєво сприяючи безпеці та відмовостійкості розподілених систем. За своєю суттю DKG включає групу учасників, які об'єднуються для створення колективного закритого ключа. Процес організований таким чином, що кожен учасник вносить частину ключа, не розкриваючи свій конкретний внесок іншим. Ця криптографічна магія полягає в її здатності поєднувати окремі внески для створення спільного ключа без розкриття точних внесків [15].

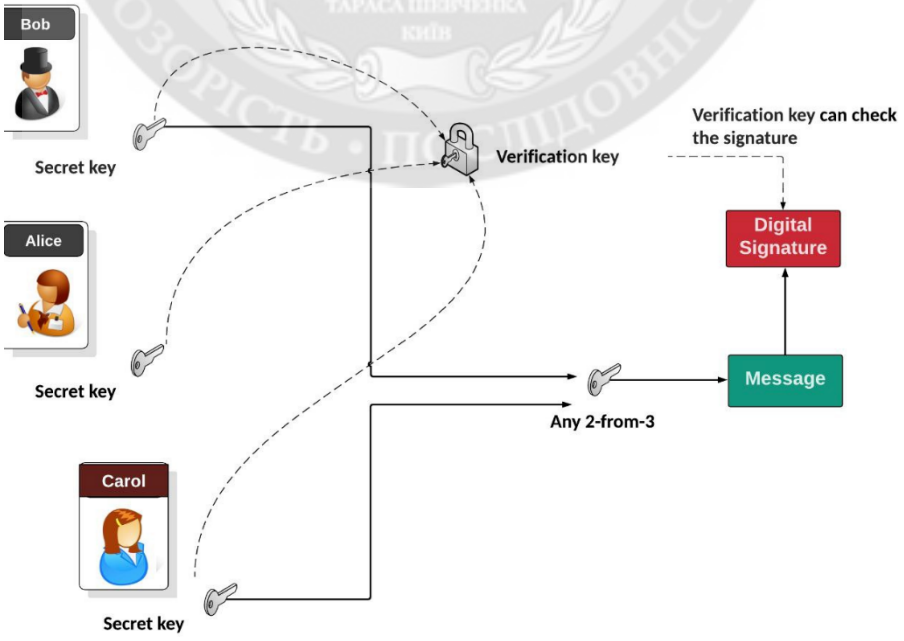

Рисунок 9 – Схематичне зображення розподіленої генерації ключа (DKG)

Порівнюючи розглянуті алгоритми можна виділити те що, SSS (Схема розподілу секрету Шаміра) забезпечує можливість зберігання приватного ключа (PK) у розподіленому вигляді, що підвищує безпеку. Проте, SSS має недоліки, такі як необхідність "дилера" для генерації частин секрету та вимога для всіх сторін відновити повний PK для підпису [17,21].

Протокол порогового підпису (TSS) пропонує певні переваги. TSS ґрунтується на чистій криптографії, що робить його незалежним від конкретних реалізацій блокчейн клієнтів. TSS усуває потребу в центральному "дилері", оскільки його роль розподілена, і повний PK ніколи не зберігається в одному місці. TSS дозволяє розподілене підписання без відновлення частин секрету, покращуючи як безпеку, так і ефективність.

За результатами проведеного дослідження наявних технологій та проблем, пов'язаних з ними, а також з урахуванням зростаючої популярності криптовалют, постає задача розробки та створення системи конфіденційності та безпеки криптоактивів на основі технології багатосторонніх обчислень.

Визначена необхідність розробки системи для надійного зберігання активів, а саме у вигляді приватних ключів до створених користувачем гаманців Ethereum мережі. Це є важливою задачею, що передбачає створення рішення для забезпечення безпеки, приватності та зручності для користувачів.

Метод забезпечення конфіденційності та безпеки криптоактивів на сонові технології багатосторонніх обчислень для Ethereum мережі полягає в:

- забезпеченні високого рівня безпеки для збереження приватних ключів та процесу підписання транзакції, використовуючи передові методи криптографічного захисту;
- гарантуванні конфіденційності та приватності користувачів, захищаючи їх особисту інформацію від несанкціонованого доступу або витоку даних.
- використанні передових технологій, включаючи технологію Multi-Party Computation (MPC), для підвищення рівня безпеки та приватності зберігання активів.

Метод багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Протокол багатосторонніх обчислень для системи конфіденційності та безпеки криптоактивів є основою на якій будується принцип контролю приватних ключів користувачів та здійснення усіх необхідних операцій, таких як підписання транзакції та її валідація. При проєктуванні таких протоколів необхідно запобігти усіх наявних мінусів попередніх протоколів.

Проблемою алгоритму секретного поділу Шаміра є одна точка відмови, а саме центральний сервер який виконує розподіл і збирання секретного ключа, і цей фактор потрібно врахувати при проектуванні протоколу для системи. Проте перевагою є можливість розділити приватний ключ на частинки з порогом відновлення.

Хоча доведено, що протокол порогового підпису є безпечним, його реалізація також може вимагати деяких додаткових заходів для захисту секретних даних. Тому використовуючи запропоновані варіанти про пороговий протокол ECDSA [26], розширимо протокол додатковими механізмами для досягнення активної безпеки:

1. Механізм оновлення секретного ключ. У пороговій криптографії секрет розподіляється між n сторонами, і щоб використовувати секретний ключ, t+1 сторони повинні об’єднати свої частки. З точки зору суперництва, зловмисник повинен порушити t+1 сторін, щоб атакувати таку схему. Якщо припустити, що зловмисник порушує сторони одну за одною, механізм оновлення ключа пом’якшує таку атаку, під час оновлення ключа секретні спільні ресурси оновлюються через певний період. Таким чином, якщо зловмиснику вдається порушити деякий відсоток сторін протягом певного періоду та порушувати решту в наступному періоді, вони не можуть розкрити таємницю, оскільки акції поновлюються в кінці першого періоду. Єдиний спосіб для зловмисника досягти успіху - атакувати t + 1 сторін одночасно, що набагато складніше.

2. Докази з нульовим знанням. У такому випадку протокол використовує «оптимістичний» підхід і повинен використовувати мінімальну кількість доказів з нульовим знанням у протоколі для отримання кращих результатів продуктивності. Одним із типів доказів нульового знання, є докази діапазону в протоколі MtA (Multiplicative to Additive), які використовуються для підтвердження того, що секретні частки менші за певне число, але через ці перевірки протокол стає відносно дорогим у продуктивності, та впливає на швидкодію програми.

Видалення даних механізмів із протоколу може призвести до витоку інформації про секретний ключ, який обмежений і не впливає на безпеку протоколу. Таким чином, дані механізми можуть бути включені в реалізацію або виключені з неї щодо компромісу між безпекою та продуктивністю.

Для знаходження компромісу між ефективністю та безпекою в системі, для покращення безпеки, використано принцип з інтервальним оновленням спільних поділених частин та не використанню механізму доказів нульової довіри для покращення продуктивності.

Протокол повинен відповідати властивостям багатосторонніх обчислень, а саме конфіденційності, де кожна сторона гарантує, що жодна зі сторін не знає загального секрету, але може гарантувати правильне розподілене обчислення над даними. Це можна досягти за допомогою розподіленої генерації ключа для ECDSA в контексті Ethereum. Такий підхід забезпечує, що приватний ключ ніколи не розкривається жодній стороні, а підписання транзакцій виконується спільно, що підвищує безпеку та конфіденційність. Даний алгоритм необхідно розширити інтервальним оновленням частин секрету, без втрати оригінального секрету, що є важливим аспектом забезпечення довготривалої безпеки в розподілених системах.

Процес розподіленої генерації ключа складається з наступних етапів: ініціалізація; генерація поліному; обрахунок частин ключа; надсилання частин ключа сторонам; обчислення власної частини стороною секрету. Ініціалізація розпочинається з ініціалізації однієї зі сторін протоколу генерації, і тоді кожен учасник генерує свою частину секретного ключа s_i випадковим чином, але так щоб згенероване значення відповідало вимозі, що число додатнє та менше за встановлений порядок поля q, де q це кінцева точка обраної еліптичної кривої для системи. У нашому випадку використовується крива secp256k1, що задається рівнянням (1)

$$y^2 = x^3 + ax + b \tag{1}$$

де a, b – параметри, задаються для кривої secp256k1 дорівнюють 0 та 7 відповідно.

Далі відбувається генерація поліному кожною стороною з $f(x)$ ступеня t з випадковими коефіцієнтами a_i, поліном задається наступним виразом (2):

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_t x^t \tag{2}$$

де t – поріг відновлення; a_0 – коефіцієнт який дорівнює s_i (згенерований секрет).

Після того як поліном згенеровано, сторона обчислює частки ключа для кожної іншої сторони передаючи до поліному $f(x)$ порядковий номер вузла у якості параметру x. Згенерований перелік частин власного секретного ключа, сторона розсилає до відповідного учасника через безпечний канал зв'язку. Після того як усі частинки надіслані та отримані сторонами, кожна зі сторін може безпечно обрахувати спільний секретний ключ сумуючи отримані частинки за модулем порядку поля q, цього вистачить для отримання публічного ключа, яким потім можна буде перевірити на валідність транзакцію. Алгоритм розподіленої генерації спільного секретного ключа наведений на рис.10.

Тепер необхідно розробити механізм інтервального оновлення часток секретного ключа, опираючись на математичні операції які застосовувались для їх генерації. Опираючись на

поділ секрету Шаміра [17] можна виділити наступні кроки оновлення часток спільного секретного ключа: ініціалізація; генерація та розподіл; обчислення нових часток.

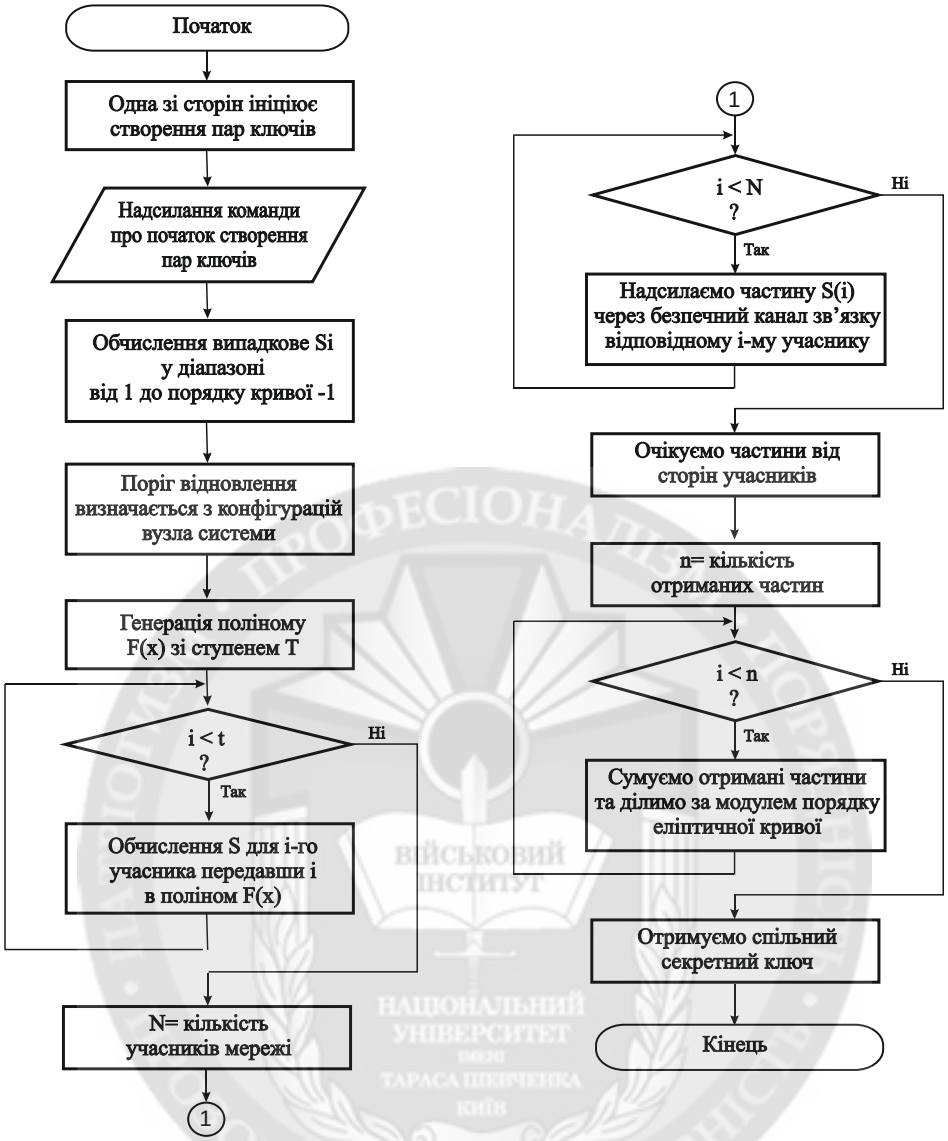

Рисунок 10 – Алгоритм розподіленої генерації спільного секретного ключа

Оновлення ключа розпочинається з того, що один із учасників повідомляє інших про початок раунду оновлення часток. Тоді кожен учасник повинен згенерувати випадкове число n_i, відповідно до того яке він генерував для власного секретного ключа. Це випадкове число буде використано для зміни його частки секретного ключа. Згенеровані частки обмінюються між учасниками через безпечний канал зв'язку. Після обміну новими частками ключа, учасники повинні обрахувати свій новий спільний ключ (3):

$$s_i^{'} = s_i + \sum_{j=i} n_i - n_i \qquad (3)$$

де s_i — це поточна частка учасника j; $s_i^{'}$ — оновлена частка ключа.

Сума n, що надходить від інших учасників, додається, а своє власне n віднімається, щоб зберегти загальну суму секретного ключа незмінною. Алгоритм оновлення часток приватного ключа учасника протоколу наведено на рис.11.

Рисунок 11 – Алгоритм оновлення частинок приватного ключа учасника протоколу

Таким чином можемо досягти регулярного оновлення часток секретного ключа, зменшуючи ризики компрометації і підтримуючи високий рівень безпеки в розподілених системах. Шляхом розробки та впровадження протоколу багатосторонніх обчислень з ключами, розподіленими та періодично оновлюваними - ефективно покращуємо рівень безпеки, у порівнянні з традиційними методами зберігання ключів у єдиному місці, наш підхід забезпечує значно вищий ступінь захисту від потенційних атак. Замість того, щоб мати один централізований пункт доступу, який може стати мішенню для зловмисників, ми розподіляємо ключі між декількома довіреними елементами системи. Кожен ключ періодично оновлюється або змінюється, ускладнюючи можливість несанкціонованого доступу. Цей підхід не лише робить процес взлому системи значно складнішим завданням, але й активно захищає систему від потенційних атак, надаючи більшу впевненість у безпеці та надійності обчислень.

Система багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Система реалізована як однорангова (peer-to-peer, P2P) мережа для забезпечення децентралізації та підвищеної безпеки. Комп'ютерні мережі типу P2P засновані на принципі рівноправності учасників і характеризуються тим, що їх елементи

можуть зв'язуватися між собою, кожен вузол виконує роль учасника в процесі генерації та оновлення ключів, а також підписання транзакцій [4,16].

Для забезпечення комунікації між вузлами у системі використана технологія веб-сокетного з’єднання. Використання WebSocket дозволяє побудувати надійний та ефективний механізм обміну даними між вузлами. При використанні WebSocket можливо реалізувати різні типи повідомлень для обміну даними між центральним сервером і вузлами, такі як запити на підпис транзакцій, генерацію приватних ключів, а також статусні повідомлення для синхронізації даних між вузлами, дозволяє побудувати розширені механізми керування підключеннями, автентифікацію та авторизацію, що може бути корисним для забезпечення безпеки та надійності комунікації між центральним вузлами.

Важливим пунктом у організації такого з’єднання, є встановлення безпечного та конфіденційного каналу зв’язку між вузлами. Загальну схему встановлення безпечного каналу зв’язку між двома вузлами наведено на рис.12.

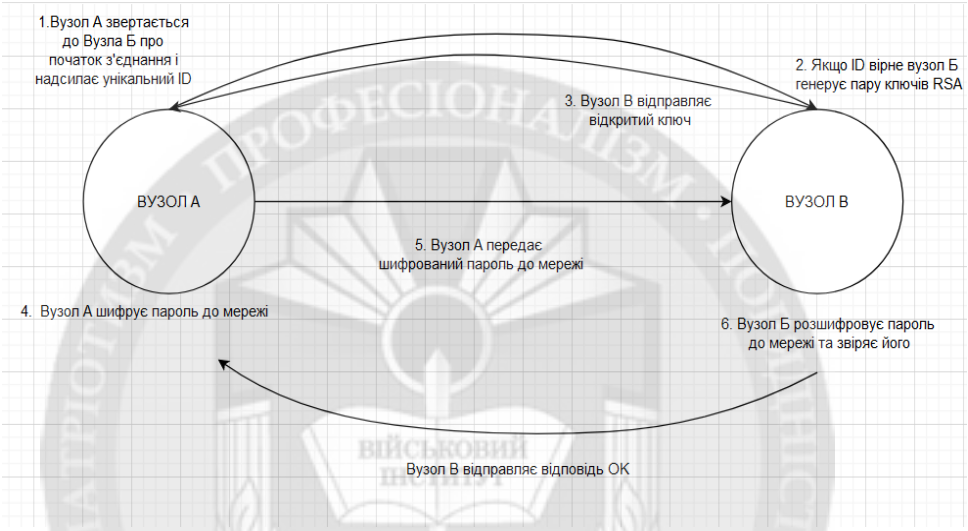

Рисунок 12 - Загальна схема встановлення безпечного зв’язку

Схема описує процес встановлення безпечного з'єднання між двома вузлами (*A* і *B*) у одноранговій мережі з вмкористанням асиметричної криптографії RSA, складається з наступних кроків: початок з’єднання; перевірка *ID*; передача відкритого ключа; шифрування пароля; передача шифрованого пароля; дешифрування та верифікація.

Процес встановлення безпечного зв’язку між вузлами (*A* і *B*) у одноранговій мережі:

1. Вузол *A* звертається до Вузла *B* з проханням про початок з’єднання. Вузол *A* надсилає унікальний ідентифікатор (*ID*), який використовується для автентифікації, його встановлює адміністратор системи при розгортанні.

2. Після отримання запиту, Вузол *B* перевіряє надісланий *ID*. Якщо *ID* вірний, Вузол *B* генерує пару ключів RSA, яка складається з відкритого і приватного ключів.

3. Вузол *B* відправляє свій відкритий ключ до Вузла *A*. Відкритий ключ буде використовуватись для шифрування повідомлень з паролем мережі від Вузла *A* до Вузла *B*.

4. Вузол А отримує відкритий ключ і використовує його для шифрування пароля.

5. Шифрований пароль передається через мережу до Вузла *B*.

6. Вузол *B* отримує шифрований пароль, дешифровує його за допомогою свого приватного ключа RSA. Після успішного дешифрування Вузол *B* перевіряє правильність отриманого пароля. Якщо пароль вірний, Вузол *B* надсилає відповідь "OK" до Вузла *A*, що підтверджує успішне встановлення безпечного з’єднання. Тоді обидва вузли можуть безпечно шифрувати та дешифрувати дані використовуючи пароль мережі, з використанням алгоритму симетричного шифрування AES.

Для кожної операції генерації адреси або підписання транзакції у системі вузла буде реалізована відповідна кінцева точка.

Загальну схему взаємодії компонентів системи наведено на рис.13. Мережевий компонент відповідає за зв'язок з іншими вузлами, забезпечуючи прийом і відправку повідомлень, таких як запити на підписання або частки ключів. Інтерфейс для ініціалізації з'єднань з вузлами дозволяє вузлу ефективно взаємодіяти в одноранговій мережі. Також цей компонент відповідає за API взаємодію з кінцевим клієнтом.

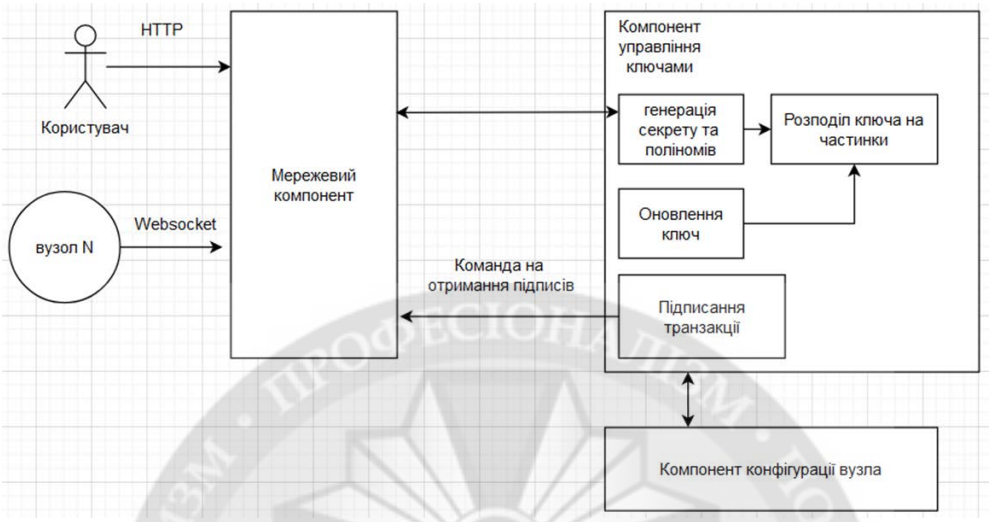

Рисунок 13 - Схема взаємодії компонентів архітектури вузла програмного забезпечення системи

Компонент управління ключами виконує генерацією поліномів та розподілом часток ключів. Компонент шифрує частки ключів перед їх передачею іншим вузлам та дешифровує отримані частки, забезпечує безпеку ключової інформації під час її обміну між вузлами мережі. Компонент також включає в себе оновлення ключа та своєчасне виконання протоколу багатосторонніх обчислень для оновлення часток секретного ключа.

Компонент підписання відповідає за генерацію часток підпису. Виконує верифікацію часток підпису, отриманих від інших вузлів, і комбінує їх для створення загального підпису. Це критично важливий процес, який забезпечує цілісність та авторитетність транзакцій у системі.

Компонент конфігурації налаштовує параметри безпеки, такі як шифрування та генерація ключів, а також параметри мережевого з'єднання, включаючи IP-адреси та порти. Параметри порогової криптографії, зокрема кількість учасників, інтервал оновлення частинок ключа та поріг, також налаштовуються через даний компонент. Це дозволяє вузлу функціонувати в рамках визначених безпекових політик та забезпечує гнучкість системи.

Розгортання системи керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв’язку та маршрутизації.

Система керування криптоактивами, використовує технології багатосторонніх обчислень, дозволяє генерувати ключі та підписувати транзакції, виконуючи операції між різними вузлами. Це дозволяє підвищити безпеку активів, адже приватний ключ перебуває у розподіленому стані.

Висновки. Проведено дослідження предметної області та запропонований метод багатосторонніх обчислень керування криптоактивами на основі технології multi-party computation. Шляхом розробки та впровадження протоколу багатосторонніх обчислень з ключами, розподіленими та періодично оновлюваними - ефективно покращуємо рівень безпеки. У порівнянні з традиційними методами зберігання ключів у єдиному місці, наш підхід

забезпечує значно вищий ступінь захисту від потенційних атак. Замість централізованого пункту доступу, який може стати мішенню для зловмисників, ми розподіляємо ключі між декількома довіреними елементами системи. Кожен ключ періодично оновлюється або змінюється, ускладнюючи можливість несанкціонованого доступу. Даний підхід не лише робить процес взлому системи значно складнішим завданням, але й активно захищає систему від потенційних атак, надаючи більшу впевненість у безпеці та надійності обчислень.

Системи керування криптоактивами на основі багатосторонніх обчислень включає кілька важливих етапів: вибір хмарних провайдерів, створення та налаштування інстансів, контейнеризація додатків, налаштування захищеного зв'язку та маршрутизації. Система надає можливість надійного зберігання криптоактивів, зокрема приватних ключів до гаманців Ethereum мережі, з використанням технології MPC, яка може бути використана у різних криптопроектах для безпечного переказу криптоактивів.

На основі проведеного дослідження та аналізу характеристик стандартів протоколів багатосторонніх обчислень запропонований протокол, який враховує наявні покращення та недоліки попередніх протоколів. Для покращення безпеки, у протоколі було впроваджено принцип інтервального оновлення спільного секрету.

Архітектура системи передбачає взаємодію основних компонентів для забезпечення надійної та безпечної роботи. Запропоновано схему встановлення безпечного з'єднання вузлів та описано модель локального сховища, яке забезпечує безпечне зберігання часток ключів, підписів та системних логів.

ЛІТЕРАТУРА:

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.

2.What Makes a Blockchain Secure? Академія Binance: веб-сайт. URL: https://academy.binance.com/en/articles/what-makes-a-blockchain-secure (дата звернення: 20.02.2024).

3. Бем, М. В. Стандарти захисту персональних даних в соціальній сфері. / М. В.Бем, І. М. Городиський -Львів:, 2018р. - 110 с.

4. Що таке транзакції у блокчейні? Incrypted : веб-сайт. URL: https://incrypted.com/tranzakcii-v-blokcheyn/ (дата звернення: 20.02.2024).

5. Голубєв, О.В. Програмно-технічні засоби захисту даних від комп'ютерних злочинів / О. В. Голубєв– Запоріжжя : «Павел», 2018. – 145 с.

6. Горбулін, В. П. Проблеми захисту інформаційного простору України / М.М. Биченок, В.П. Горбулін – К.: Інтертехнологія, 2019. – 138 с.

7. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.

8. What Is a Merkle Tree & What Is Its Role in Blockchain? Learn ByBit: веб-сайт. URL: https://learn.bybit.com/blockchain/what-is-merkle-tree/(дата звернення: 20.02.2024).

9. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

10.Proof of Work (PoW) Process flow. ResearchGate : веб-сайт. URL: https://www.researchgate.net/figure/Proof-of-Work-PoW-Process-flow-Latif-et-al-2021_fig2_374870812 (дата звернення: 20.02.2024).

11.Why is so Much Important to have Digital Signatures? Medium: веб-сайт. URL: https://saurabh57788.medium.com/why-is-so-much-important-to-have-digital-signatures-8583abec63d1 (дата звернення: 20.02.2024).

12. Ємельянов, С.Л. Основи інформаційної безпеки. / С.Л. Ємельянов– Одеса: Фенікс, 2019р.– 357 с.

13. Кастодіальні та некастодіальні гаманці: у чому різниця? Академія Binance : веб-сайт. URL: https://academy.binance.com/uk/articles/custodial-vs-non-custodial-wallets-what-s-the-difference (дата звернення: 20.02.2024).

14. An overview of Multi-Party Computation (MPC), Threshold Signatures (TSS) and MPC-TSS wallets. Medium : веб-сайт. URL: https://mmasmoudi.medium.com/an-overview-of-multi-party-computation-mpc-threshold-signatures-tss-and-mpc-tss-wallets-4253adacd1b2 (дата звернення: 20.02.2024).

15.Secure multi-party computation. Wikipedia : веб-сайт. URL: https://en.wikipedia.org/wiki/Secure_multi-party_computation (дата звернення: 20.02.2024).

16. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.

17. Building A New Digital World: Threshold Signing and Key Distribution Generation. Medium : веб-сайт. URL: https://medium.com/asecuritysite-when-bob-met-alice/building-a-new-digital-world-threshold-signing-and-key-distribution-generation-a1235390b6aa (дата звернення: 20.02.2024).

18. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

19. Рибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – с.57-62

20. Threshold Signatures Explained. Академія Binance : веб-сайт. URL: https://academy.binance.com/uk/articles/threshold-signatures-explained (дата звернення: 20.02.2024).

21. Multisig vs. (SSS vs. TSS). Typefully : веб-сайт. URL: https://typefully.com/tomkowalczyk/JAfJzji (дата звернення: 20.02.2024).

22. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.

23. WebSocket. Wikipedia : веб-сайт. URL: https://uk.wikipedia.org/wiki/WebSocket (дата звернення: 20.02.2024).

24. Хорошко, В.О. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський - Київ., 2019р. 164 с.

25. Proactive Secret Share for Eigen Secret Recovery. EigenLab. 2021. URL: https://www.pdau.edu.ua/sites/default/files/node/4518/pravylaoformlennyaspyskuvykorystanyhdzherel.pdf (дата звернення: 20.02.2024).

26.Jens Groth and Victor Shoup. Design and analysis of a distributed ECDSA signing service. Cryptology ePrint Archive, Paper 2022/506. 2022. URL: https://eprint.iacr.org/2022/506(дата звернення: 20.02.2024).

REFERENCES:

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoi Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № №47/2017, 15s.

2.What Makes a Blockchain Secure? Akademiia Binance: veb-sait. URL: https://academy.binance.com/en/articles/what-makes-a-blockchain-secure (data zvernennia: 20.02.2024).

3. Bem, M. V. (2018) Standarty zakhystu personalnykh danykh v sotsialnii sferi. / M. V.Bem, I. M. Horodyskyi -Lviv - 110 s.

4. Shcho take tranzaktsii u blokcheini? Incrypted : veb-sait. URL: https://incrypted.com/tranzakcii-v-blokcheyn/ (data zvernennia: 20.02.2024).

5. Holubiev, O.V. (2018) Prohramno-tekhnichni zasoby zakhystu danykh vid kompiuternykh zlochyniv / O. V. Holubiev– Zaporizhzhia : «Pavel» – 145 s.

6. Horbulin, P.V. (2019) Problemy zakhystu informatsiinoho prostoru Ukrainy / M.M. Bychenok, P.V. Horbulin – K.: Intertekhnolohiia – 138 s.

7. Lenkov, S.V.(2023), Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv / S.V. Lienkov, V.M. Dzhulii, A.M. Bernaz, I.V. Muliar, I.V. Pampukha // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU -. №78. – C. 123-134.

8. What Is a Merkle Tree & What Is Its Role in Blockchain? Learn ByBit: веб-сайт. URL: https://learn.bybit.com/blockchain/what-is-merkle-tree/ (data zvernennia: 20.02.2024).

9. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.

10.Proof of Work (PoW) Process flow. ResearchGate : веб-сайт. URL: https://www.researchgate.net/figure/Proof-of-Work-PoW-Process-flow-Latif-et-al-2021_fig2_374870812 (data zvernennia: 20.02.2024).

11.Why is so Much Important to have Digital Signatures? Medium: веб-сайт. URL: https://saurabh57788.medium.com/why-is-so-much-important-to-have-digital-signatures-8583abec63d1 (data zvernennia: 20.02.2024).

12. Yemelianov, S.L. (2019) Osnovy informatsiinoi bezpeky./S.L.Yemelianov– Odesa: Feniks – 357s.

13. Kastodialni ta nekastodialni hamantsi: u chomu riznytsia? Akademiia Binance : veb-sait. URL: https://academy.binance.com/uk/articles/custodial-vs-non-custodial-wallets-what-s-the-difference (data zvernennia: 20.02.2024).

14. An overview of Multi-Party Computation (MPC), Threshold Signatures (TSS) and MPC-TSS wallets. Medium : veb-sait. URL: https://mmasmoudi.medium.com/an-overview-of-multi-party-computation-mpc-threshold-signatures-tss-and-mpc-tss-wallets-4253adacd1b2 (data zvernennia: 20.02.2024).

15.Secure multi-party computation. Wikipedia : veb-sait. URL: https://en.wikipedia.org/wiki/Secure_multi-party_computation (data zvernennia: 20.02.2024).

16. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.

17. Building A New Digital World: Threshold Signing and Key Distribution Generation. Medium : веб-сайт. URL: https://medium.com/asecuritysite-when-bob-met-alice/building-a-new-digital-world-threshold-signing-and-key-distribution-generation-a1235390b6aa (data zvernennia: 20.02.2024).

18. Buriachok, V. L. (2016) Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby : posibnyk / V. L. Buriachok, S. V. Toliupa, V. V. Semko – K. : DUT-KNU – 178 s.

19. Rybalchenko, L.V., Kosychenko, O.O. (2019) Problemy bezpeky personalnykh danykh v Ukraini / Rehionalna ekonomika / Zaporizhzhia – s.57-62

20.Threshold Signatures Explained. Академія Binance : веб-сайт. URL: https://academy.binance.com/uk/articles/threshold-signatures-explained (data zvernennia: 20.02.2024).

21.Multisig vs. (SSS vs. TSS). Typefully : веб-сайт. URL: https://typefully.com/tomkowalczyk/JAfJzji (data zvernennia: 20.02.2024).

22. Honchar, S. F. (2019) Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury : monohrafiia. / S. F. Honchar. – Kyiv – 175 s.

23. WebSocket. Wikipedia : veb-sait. URL: https://uk.wikipedia.org/wiki/WebSocket (data zvernennia: 20.02.2024)

24. Khoroshko, V.O. Zakhyst system elektronnykh komunikatsii: navch. posib. / V.O. Khoroshko, O.V. Kryvoruchko, M.M. Brailovskyi - Kyiv., 2019r. 164 s.

25. Proactive Secret Share for Eigen Secret Recovery. EigenLab. 2021. URL: https://www.pdau.edu.ua/sites/default/files/node/4518/pravylaoformlennyaspyskuvykorystanyhdzherel.pdf (data zvernennia: 20.02.2024).

26.Jens Groth and Victor Shoup. Design and analysis of a distributed ECDSA signing service. Cryptology ePrint Archive, Paper 2022/506. 2022. URL: https://eprint.iacr.org/2022/506 (data zvernennia: 20.02.2024).

Ph.D. Dzhuliy V.M., Filyuk E.V.

METHOD OF MULTI-PARTY COMPUTATION MANAGEMENT OF CRYPTOASSETS BASED ON MULTI-PARTY COMPUTATION TECHNOLOGY

The task of building an efficient and secure crypto-currency wallet based on multi-party computing technology, which can provide reliable and secure use in various industries working with cryptocurrencies, is considered.

Modern algorithms of multilateral calculations, such as those of Gennaro and Goldfeder, Lindella, Doerner, offer significant advantages in data protection, but they have certain limitations. The main ones are insufficient efficiency in the number of signature rounds and lack of cold storage support. This highlights the need for further research and development in the field of Multi-Party Computation technology to achieve higher levels of operational efficiency and flexibility.

The method of ensuring the confidentiality and security of cryptoassets on the dream technology of multilateral computing for the Ethereum network consists in: ensuring a high level of security for the storage of private keys and the process of signing the transaction, using advanced cryptographic protection methods; guaranteeing the confidentiality and privacy of users, protecting their personal information from unauthorized access or data leakage; using advanced technologies, including Multi-Party Computation technology, to increase the level of security and privacy of asset storage.

On the basis of the conducted research and analysis of the characteristics of multiparty computing protocol standards, a protocol is proposed that takes into account the existing improvements and shortcomings of previous protocols. To improve security, the protocol implements the principle of interval update of the shared secret.

A cryptoasset management system based on multilateral computing includes several important stages: choosing cloud providers, creating and configuring instances, containerizing applications, configuring secure communication and routing. The system provides the possibility of reliable storage of cryptoassets, in particular, private keys to wallets of the Ethereum network, using the Multi-Party Computation technology, which can be used in various cryptoprojects for the safe transfer of cryptoassets.

The architecture of the system involves the interaction of the main components to ensure reliable and safe operation. A scheme for establishing a secure connection of nodes is proposed and a local storage model is described, which provides secure storage of key shares, signatures, and system logs.

Keywords: cryptoassets, confidential information, cryptoasset security, multi-party computation technology, secure connection, information security, cryptocurrency, digital assets, cryptocurrency wallet.