

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут інформатики та радіoeлектроніки
Факультет радіoeлектроніки та телекомунікацій
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра
(ступінь вищої освіти (освітній ступінь))

на тему "Моделювання та аналіз процесу формування біткоїн-адреси"

Виконав: студент 6 курсу, групи РТ-813м
спеціальності (напряму підготовки)

125 – Кібербезпека
(код і назва напряму підготовки, спеціальності)

Трухачов А.В.
(прізвище та ініціали)

Керівник Козіна Г.Л.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

м.Запоріжжя
2018 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет
 (повне найменування вищого навчального закладу)

Інститут, факультет ІРЕ, ФРЕТ
 Кафедра захисту інформації
 Ступінь вищої освіти (освітній ступінь) магістр
 Спеціальність 125 Кібербезпека
(код і назва)
 Напрямок підготовки Безпека інформаційних і комунікаційних систем
(код і назва)

ЗАТВЕРДЖУЮ
 Завідувач кафедри захисту інформації,
проф., д.т.н., Карпуков Л.М.
 “ ” 2018 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Трухачову Андрію Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) моделювання та аналіз процесу формування біткоін-адреси

керівник проекту (роботи) Козіна Галина Леонідівна, канд. фіз.-мат. наук, доцент кафедри захисту інформації

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “_7_” листопада 2018 року №328

2. Строк подання студентом проекту (роботи) 3 грудня 2018 року

3. Вихідні дані до проекту (роботи) Література по системі Біткоін, пакети прикладних програм для математичних обчислень.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) формування секретного ключа, генерація відкритого ключа, процедура подвійного хешування, генерація Біткоін-адреси, побудова моделі формування Біткоін-адреси, аналіз процесу формування Біткоін-адреси

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) схема перетворення секретного ключа у Біткоін-адресу, схема процедури подвійного хешування, схема кодування у формат Base58Check

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основний	Козіна Г.Л., доцент кафедри захисту інформації		
Охорона праці	Коробко О.В., старший викладач кафедри ОПНС		
Економічна частина	Левченко Н.М., завідувач кафедри обліку і оподаткування		
Нормо-контроль	Нікуліщев Г.І., старший викладач кафедри захисту інформації		

7. Дата видачі завдання _____ 3 жовтня _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з літературою	03.10-05.10	
2	Дослідження алгоритму вибору секретних ключів	06.10-14.10	
3	Ознайомлення з алгоритмом генерації відкритих ключів	15.10-20.10	
4	Дослідження процедури подвійного хешування	21.10-28.10	
5	Ознайомлення з процесом кодування у формат Base58Check	29.10-04.11	
6	Створення моделі формування Біткоїн-адреси	05.11-10.11	
7	Аналіз колізій секретних ключів	11.11-15.11	
8	Аналіз колізій хеш-функцій	16.11-21.11	
9	Охорона праці та безпека у надзвичайних ситуаціях	22.11-23.11	
10	Діагностика економічного ризику використання системи біткоїн	24.11-26.11	
11	Оформлення пояснювальної записки	27.11-30.11	

Студент

(підпис)

(прізвище та ініціали)

Керівник проекту (роботи)

(підпис)

(прізвище та ініціали)

РЕФЕРАТ

ПЗ: 83с., 16 рисунків, 8 таблиць, 16 джерел.

Об'єкт дослідження - процес формування Біткоін-адреси.

Мета роботи - дослідження процесу формування Біткоін-адреси і проблеми виникнення колізій при генерації Біткоін-адрес.

Метод дослідження - моделювання процесу формування Біткоін-адреси.

У роботі досліджується метод ідентифікації користувачів у системі Біткоін, виділяються основні вимоги, що висуваються до Біткоін-адрес. Описується механізм вибору секретних і генерації відкритих ключів, розглядаються методи зберігання цифрових ключів у Біткоін-гаманцях. Досліджується схема перетворення відкритого ключа у Біткоін-адресу і проводиться повне поетапне моделювання формування Біткоін-адреси. Проводиться аналіз процесу формування Біткоін-адреси і дослідження проблеми виникнення колізій.

СИСТЕМА БІТКОІН, СЕКРЕТНІ КЛЮЧІ, ВІДКРИТІ КЛЮЧІ, БІТКОІН-ГАМАНЦІ, БІТКОІН-АДРЕСИ, КОДУВАННЯ BASE58CHECK, ЕЛІПТИЧНА КРИВА, ХЕШУВАННЯ.

ЗМІСТ

Список скорочень.....	7
Вступ.....	8
1. Система Біткоїн	9
1.1.Ідентифікація клієнта у системі Біткоїн	9
1.2.Вимоги, що висуваються до Біткоїн-адрес.....	10
1.3.Біткоїн-гаманці	11
2. Формування Біткоїн-адреси	15
2.1.Загальна схема перетворення секретного ключа у Біткоїн-адресу.....	15
2.2.Перетворення секретного ключа у відкритий ключ	16
2.3.Перетворення відкритого ключа у Біткоїн-адресу	19
3. Реалізація процесу формування Біткоїн-адреси	21
3.1.Секретні ключі.....	21
3.2.Формати секретних ключів	21
3.3.Відкриті ключі	25
3.4.Формати відкритих ключів.....	26
3.5.Біткоїн-адреси.....	28
3.6.Формати Біткоїн-адрес	34
3.7.Модель формування Біткоїн-адреси	37
4. Аналіз процесу формування Біткоїн-адреси	38
4.1.Аналіз колізій секретних ключів	39
4.2.Аналіз колізій хеш-функцій	42
4.3.Ризики клієнта у випадку колізій	50
5. Охорона праці та безпека у надзвичайних ситуаціях.....	51
5.1.Аналіз потенційних небезпек.....	51
5.2.Заходи забезпечення безпеки.....	52
5.3.Заходи щодо виробничої санітарії та гігієни праці	53
5.4.Заходи з пожежної безпеки	60
5.5.Заходи забезпечення безпеки у надзвичайних ситуаціях	62
6. Діагностика економічного ризику використання системи Біткоїн.....	69

6.1.Види ризиків	69
6.2.Ризик використання системи Біткоїн у економічній діяльності підприємства	73
6.3.Оцінка ризику використання системи Біткоїн	75
Висновки	79
Список літератури	80
Додаток А.....	82

СПИСОК СКОРОЧЕНЬ

BIP - Bitcoin Improvement Proposal

WIF - Wallet import format

P2SH - pay-to-script hash

P2PKH pay-to-public-key-hash

ПЗ - програмне забезпечення

ПК - персональний комп'ютер

ВСТУП

Останнє десятиріччя характеризується стрімким розвитком цифрових платіжних систем. Однією з найвідоміших і найбільш розповсюджених систем віртуальних цифрових грошей є Біткоїн.

Система Біткоїн була створена у січні 2009 року людиною або групою людей під псевдонімом Сатоші Накамото. Біткоїн - це пірингова платіжна система, яка використовує однойменну одиницю для обліку операцій і однойменний протокол передачі даних. Для забезпечення функціонування і захисту системи використовуються криптографічні методи. Біткоїн - це система з повністю децентралізованим дизайном, без центрального пункту управління, який міг би бути атакований або пошкоджений [1].

Користувачі мають можливість переміщувати біткоїни по мережі так само, як це відбувається зі звичайними валютами: купувати і продавати товари, посилати гроші людям або організаціям. Біткоїни можуть бути куплені, продані або обмінені на інші валюти на спеціалізованих біржах.

Біткоїни існують тільки у вигляді записів в розподіленій базі даних (блокчейн), в якій в загальнодоступному відкритому вигляді зберігаються всі транзакції, із зазначенням біткоїн-адрес відправників і одержувачів, але без інформації про реального власника цих адрес. У базі немає окремих записів про поточну кількість біткоїнів у певного власника. Лише на підставі ланцюгів транзакцій стає відома поточна кількість біткоїнів, пов'язаних з певною біткоїн-адресою.

Володіння біткоїнами встановлюється через секретні і відкриті ключі та Біткоїн-адреси. Секретні ключі використовуються при генерації відкритих ключів, а також для створення цифрового підпису, необхідного для підтвердження факту володіння біткоїнами. Відкриті ключі використовуються у процесі формування Біткоїн-адреси, а також для перевірки достовірності цифрового підпису. Біткоїн-адреси використовуються для ідентифікації відправника і одержувача коштів в системі Біткоїн.

1 СИСТЕМА БІТКОІН

У 2008 році людина або група людей під псевдонімом Сатоші Накамото опублікувала статтю у якій містився опис протоколу і принцип роботи мережі Біткоін. У 2009 році був опублікований код програми-клієнта. 3 Січня 2009 року відбувся запуск системи Біткоін і був згенерований перший блок.

Біткоін - пірингова платіжна система, яка використовує однойменну одиницю для обліку операцій і однойменний протокол передачі даних. Для забезпечення функціонування і захисту системи використовуються криптографічні методи. Біткоін - це система з повністю децентралізованим дизайном, без центрального пункту управління, який міг би бути атакований або пошкоджений.

Користувачі мають можливість переміщувати біткоіни по мережі так само, як це відбувається зі звичайними валютами: купувати і продавати товари, посилати гроші людям або організаціям. Біткоіни можуть бути куплені, продані або обмінені на інші валюти на спеціалізованих біржах.

Біткоіни існують тільки у вигляді записів в розподіленій базі даних (блокчейн), в якій в загальнодоступному відкритому вигляді зберігаються всі транзакції, із зазначенням біткоін-адрес відправників і одержувачів, але без інформації про реального власника цих адрес. У базі немає окремих записів про поточну кількість біткоінів у будь-якого власника. Лише на підставі ланцюгів транзакцій стає відома поточна кількість біткоінів, пов'язаних з певною біткоін-адресою.

1.1 Ідентифікація клієнта у системі Біткоін

Володіння біткоінами встановлюється через секретні і відкриті ключі та Біткоін-адреси. Секретні ключі використовуються при генерації відкритих ключів, а також для створення цифрового підпису, необхідного для підтвердження факту володіння біткоінами. Відкриті ключі використовуються у

процесі формування Біткоїн-адреси, а також для перевірки достовірності цифрового підпису. Біткоїн-адреси використовуються для ідентифікації користувача в системі Біткоїн [1].

Цифрові ключі не зберігається в мережі, а створюються і зберігається користувачами в файлі, або простій базі даних, яку називають гаманцем. Цифрові ключі в гаманці користувача повністю незалежні від протоколу Біткоїн. Вони створюються і управляється за допомогою програмного забезпечення гаманця користувача без посилання на блокчейн або доступу до мережі Інтернет. Кожна транзакція в Біткоїн вимагає включення в блокчейн дійсного підпису, який може бути згенерований тільки за допомогою дійсних цифрових ключів; тому, будь-який власник копії ключів має повний контроль над засобами облікового запису. Цифрові ключі зберігаються в зашифрованому файлі і управляються програмним забезпеченням гаманця [2].

1.2 Вимоги, що висуваються до Біткоїн-адрес

Біткоїн-адреси покликані облегшити процес взаємодії користувача і системи Біткоїн. Процес оптимізації цієї взаємодії зумовив створення низки вимог, які висуваються до Біткоїн-адрес.

До Біткоїн-адрес висуваються наступні вимоги:

1. Унікальність. Кожному секретному ключу повинна відповідати унікальна біткоїн-адреса. На практиці це досягається шляхом використання функцій хешування, які мають високу чутливість до змін вхідної послідовності. Різні вхідні послідовності повинні давати різний результат. Широкий діапазон можливих секретних ключів дозволяє згенерувати приблизно 10^{77} різних біткоїн-адрес.

2. Одноразове використання. Для кожної транзакції рекомендується використовувати нову біткоїн-адресу. Повторне використання адрес завдає шкоди конфіденційності не тільки конкретного користувача, але і іншим. Багаторазове використання біткоїн-адреси дозволяє зловмисникам набагато

легше і надійніше визначати його власника. Кожен раз, коли секретний ключ повторно використовуваної адреси підписує нову транзакцію, будь-хто, хто її отримує, може використовувати історію цієї адреси, щоб заволодіти інформацією про власника адреси.

3. Прийнятний розмір. Попередня вимога створює необхідність зменшення розміру Біткоїн-адреси. Базовими методами, що дозволяють скоротити довжину Біткоїн-адреси є хешування та кодування у форматі Base58.

4. Уніфікований формат. Біткоїн-адреси повинні мати стандартизовану структуру, зручну для сприйняття користувачем. Однозначність в написанні і читанні є необхідною умовою, що дозволяє користувачеві уникнути помилок в адресі.

5. Захист від помилок. Біткоїн-адреса повинна мати базові засоби для перевірки коректності написання. На практиці використовується формат кодування з контрольною сумою Base58Check.

1.3 Біткоїн-гаманці

Біткоїн-гаманці - це контейнери для секретних і відкритих ключів, а також Біткоїн-адрес, які, як правило, реалізуються у вигляді структурованих файлів або простих баз даних. Програмне забезпечення Біткоїн-гаманця може також підтримувати можливість проведення розрахункових операцій, резервного копіювання тощо [2].

У перших біткоїн-клієнтах, гаманцями були просто колекції випадково згенерованих секретних ключів. Цей тип гаманця називається не детермінованим гаманцем Тип-0. Наприклад, клієнт Bitcoin Core генерує 100 випадкових секретних ключів при першому запуску, і генерує нові за необхідністю.

Основним недоліком випадкових ключів є ускладнений процес резервного копіювання. Виникає необхідність проводити резервне копіювання кожного разу при генерації нових ключів. Інакше, у разі безповоротної втрати

ключа, кошти будуть назавжди втрачені. Подібна незручність тягне за собою повторне використання біткоїн-адрес, що зменшує конфіденційність, дозволяючи будувати асоціації між різними адресами і транзакціями.

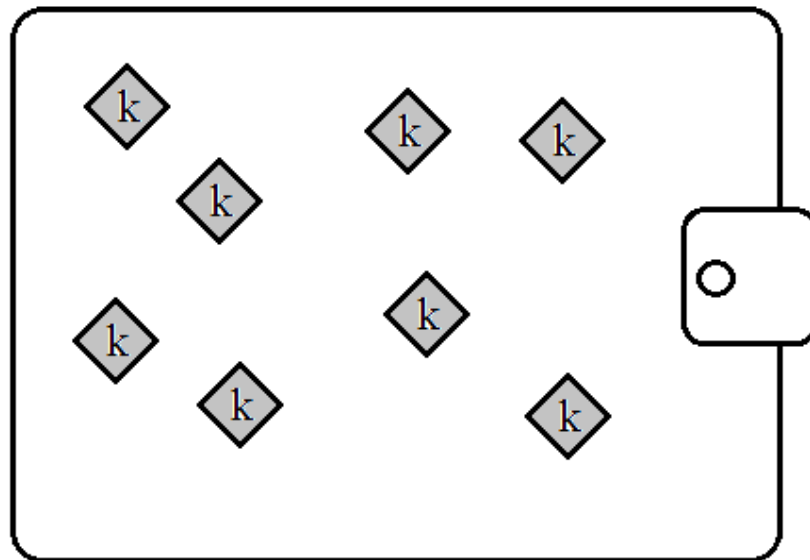


Рисунок 1.1 - Недетермінований гаманець Тип-0: колекція випадково згенерованих ключів

Недетермінований тип гаманців був незручний для резервного копіювання, імпорту, експорту, і йому на заміну приходять детерміновані гаманці.

Детерміновані, або гаманці з зерном - це гаманці, в яких секретні ключі походять від спільного зерна шляхом використання односторонньої хеш-функції. Зерно - це випадкове число, що в поєднанні з іншими даними (номер індексу, код ланцюга) дозволяє отримати секретні ключі.

У детермінованому гаманці для відновлення всіх ключів досить знати зерно, а отже, достатньо провести резервне копіювання один раз під час його створення. Інформації, що зберігається у зерні, також достатньо для експорту або імпорту гаманця. Це дозволяє легко переносити всі ключі користувача між різними реалізаціями гаманця [3].

Мнемонічні коди - це послідовності англійських слів, які кодують випадкове число, що використовується в якості зерна для детермінованого гаманця. Мнемонічний код дозволяє відновити зерно, і з нього відтворити гаманець і всі похідні ключі. Додаток гаманця, що реалізує детерміновані гаманці з мнемонічним кодом показує користувачеві послідовність з від 12 до 24 слів при створенні гаманця. Ця послідовність слів є резервною копією гаманця і може бути використана для відновлення і повторного створення всіх ключі в тому ж або будь-якому іншому сумісному додатку гаманця. Мнемонічні кодові слова читаються і транскрибуються легше в порівнянні з випадковою послідовністю чисел [3].

Детерміновані гаманці були розроблені, щоб можна було легко отримати багато ключів з одного «зерна». Найбільш просунутою формою детермінованих гаманців є ієрархічний детермінований гаманець або HD-гаманець, описаний в стандарті BIP0032 [4]. Ієрархічні детерміновані гаманці містять ключі у вигляді дерева, що дозволяє вивести послідовність похідних ключі з батьківського, від кожного з яких, в свою чергу, також виходить послідовність похідних ключів і так далі без обмеження глибини вкладеності.

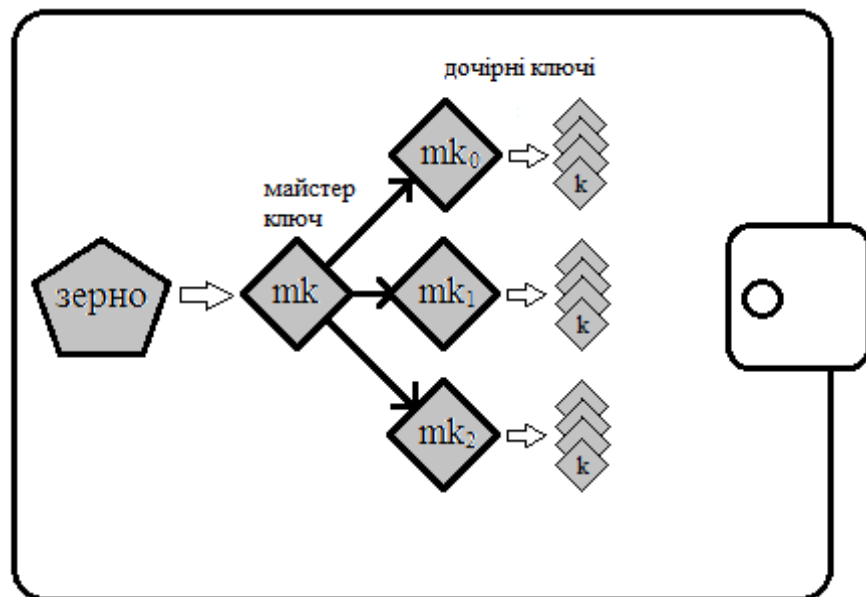


Рисунок 1.2 - Ієрархічно детермінований гаманець Тип-2

HD-гаманці пропонують дві основні переваги в порівнянні з недетермінованими. По-перше, структура дерева може бути використана для додаткової організації, наприклад, коли конкретна гілка ключів використовується для отримання вхідних платежів, а інша гілка - для вихідних платежів. Розгалуження ключів також можуть бути використані в корпоративному середовищі для різних відділів, філій, конкретних функцій, або категорій бухгалтерського обліку [2].

Друга перевага HD-гаманців в тому, що їх користувачі можуть створювати послідовності відкритих ключів, не маючи доступу до відповідних секретних ключів. Це дозволяє використовувати HD-гаманці на небезпечних серверах або тільки в режимі прийому коштів з видачею нового відкритого ключа для кожної нової транзакції. Відкриті ключі не повинні бути попередньо завантажені або отримані заздалегідь і сервер не містить секретні ключі, які можуть використовуватися для витрачання коштів.

HD-гаманці створюються з єдиного кореневого зерна, яке представляє собою 128, 256, або 512-бітове випадкове число. Все інше в HD-гаманці є похідним від цього кореневого зерна, що робить можливим відтворити весь HD-гаманець з зерна в будь-якому сумісному ПЗ [4].

2 ФОРМУВАННЯ БІТКОІН-АДРЕСИ

2.1 Загальна схема перетворення секретного ключа у Біткоїн-адресу

Біткоїн-гаманець містить колекцію з пар ключів, кожна з яких складається з секретного і відкритого ключа. Секретний ключ k являє собою число, як правило, взате навмання. Використовуючи секретний ключ, за допомогою односторонньої функції множення на еліптичних кривих, формується відкритий ключ Q . З відкритого ключа Q , використовуючи функцію криптографічного хеша, формується відбиток або хеш відкритого ключа. Результатом кодування хешу відкритого ключа у формат Base58Check є Біткоїн-адреса A [1]. Відносини між секретним ключем, відкритим ключем і Біткоїн-адресою показано на рисунку 2.1.

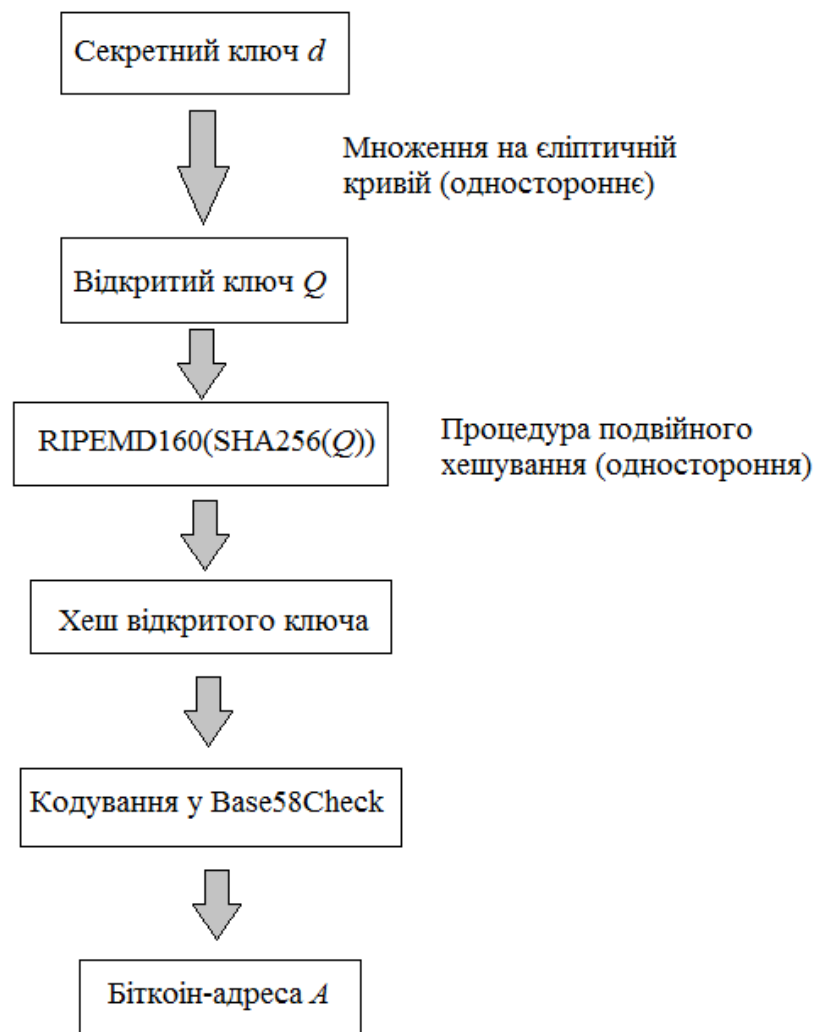


Рисунок 2.1 - Схема перетворення секретного ключа у Біткоїн-адресу

Модель формування Біткоїн-адреси реалізована таким чином, що критичні з точки зору безпеки перетворення здійсненні тільки в один бік. Знаючи Біткоїн-адресу можливо декодувати її у хеш відкритого ключа, але відновлення відкритого ключа з хешу не є можливим. Так само неможливо за прийнятний час знайти секретний ключ, знаючи відкритий ключ і значення загальносистемних параметрів.

2.2 Перетворення секретного ключа у відкритий ключ

Секретний ключ - це випадково взяте число з певного діапазону. Володіння секретним ключем необхідно для контролю користувача над коштами, пов'язаними з відповідною Біткоїн-адресою. Секретний ключ також використовується для створення підпису, який необхідний як доказ володіння коштами в транзакції. Приклад випадковим чином обраного секретного ключа наведено нижче:

*d = BDBEAE888B6593C55F0EAC4C0D324FFD778882B313114F135996FF0
F48C9A11D*

Відкритий ключ обчислюється з секретного ключа за допомогою незворотного множення на еліптичних кривих [2]:

$$Q = d * G, \quad (2.1)$$

де *d* — це секретний ключ, *G* — базова точка, а *Q* — результуючий відкритий ключ. Приклад відкритого ключа наведено нижче:

*Q = 0462540717DADFBFC736D926FEC1D7F9656A8ED6A1D1E635A81E6D
02E7E6589F000455C18D638E2251FC725E66389C4007D69F8C21692E2ED*

72E606D4641D4B598

У Біткоїн використовується певна еліптична крива і набір математичних констант зі стандарту під назвою `secp256k1`, встановленого Національним Інститутом Стандартів і Технологій (NIST) [5]. Параметри домену еліптичної кривої над F_p , пов'язані з кривою Кобліца `secp256k1`, задані значенням $T = (p, a, b, G, n, h)$, де кінцеве поле F_p визначене:

$p = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFC2F}$

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

Еліптична крива $E: y^2 = x^3 + ax + b$ над полем F_p визначена:

$a = \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000}$

$b = \text{00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007}$

Базова точка G у стиснутому вигляді:

$G = \text{02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798}$

та у не стиснутому вигляді:

$G = \text{04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8}$

Порядок базової точки n і кофактор h визначені:

$n = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B}$
 BFD25E8C D0364141

$h = 01$

На рисунку 2.2 зображено приклад еліптичної кривої secp256k1 над полем дійсних чисел.

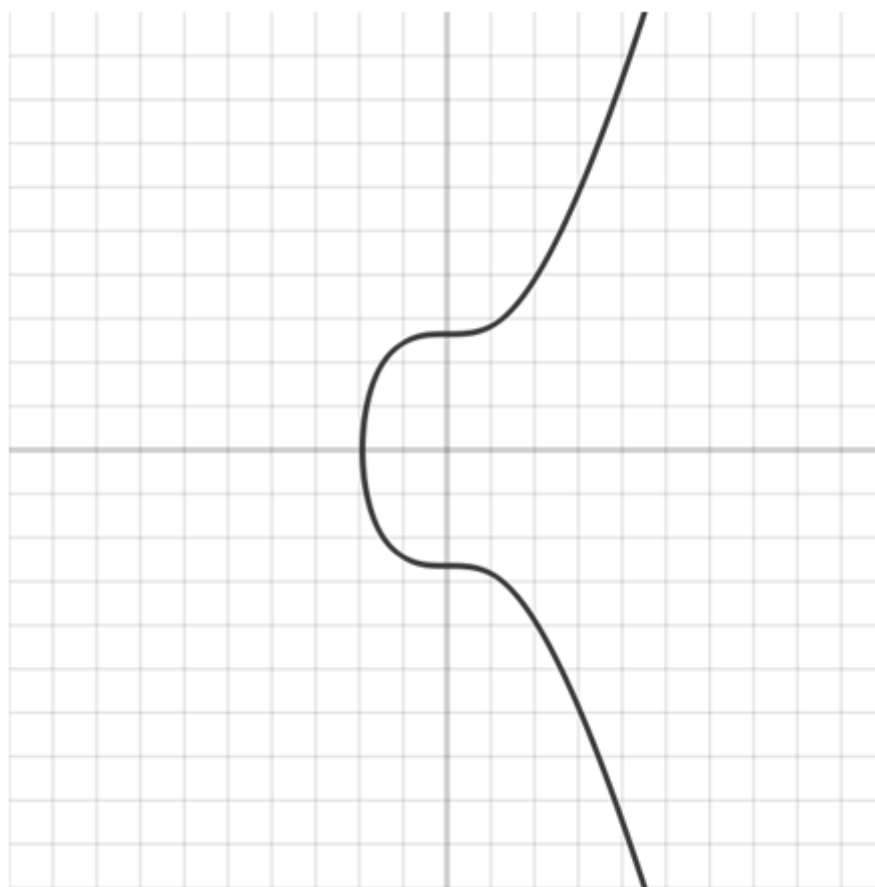


Рисунок 2.2 - Еліптична крива secp256k1

Так як ця крива визначена над кінцевим полем простого порядку, а не дійсних чисел, вона виглядає як набір точок, розсіяних в двох вимірах. Як приклад, на рисунку 2.3 зображена та ж еліптична крива над кінцевим полем набагато меншого простого порядку 17.

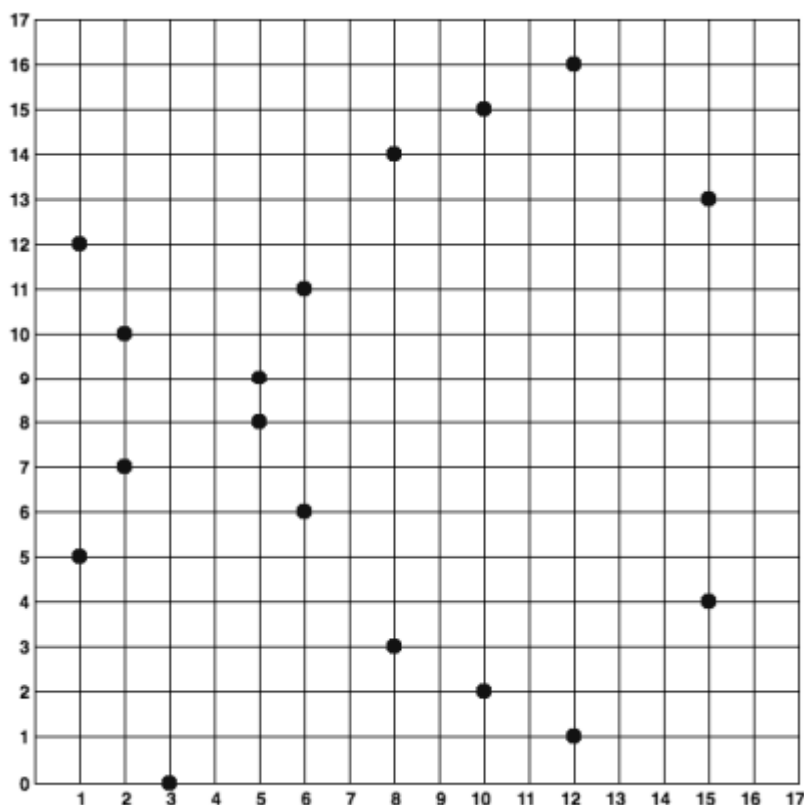


Рисунок 2.3 - Візуалізація еліптичної кривої над кінцевим полем простого порядку

Еліптична крива біткоїн `secp256k1` може розглядатися як набагато більш складна картина точок на незмірно великій координатній сітці[2].

Вибір секретного ключа і генерація відкритого ключа будуть розглянуті більш детально у наступному розділі.

2.3 Перетворення відкритого ключа у Біткоїн-адресу

Біткоїн-адреса генерується з відкритого ключа шляхом використання односторонньої криптографічної операції хешування. Алгоритм хешування - це одностороння функція, яка створює відбиток або хеш довільної кількості даних на вході. Криптографічні хеш-функції широко використовуються в Біткоїн: в біткоїн-адресах, в адресах сценаріїв, і в алгоритмі доказу роботи в майнінгу [2].

Адреса з відкритого ключа отримується в результаті застосування алгоритму Secure Hash Algorithm (SHA) і RACE Integrity Primitives Evaluation Message Digest (RIPEMD), конкретно SHA256 і RIPEMD160.

Відкритий ключ Q хешується алгоритмом SHA256. Отриманий результат хешується повторно алгоритмом RIPEMD160. Результатом даного перетворення є 160-ти бітний хеш відкритого ключа. Останнім кроком формування Біткоїн-адреси у стандартному вигляді є кодування хешу відкритого ключа у формат Base58Check.

Біткоїн-адреси майже завжди представлені користувачам в кодуванні Base58Check, в якому використовується 58 символів (формат Base58) і контрольна сума для підвищення читаності, уникнення двозначностей в написанні, і захисту від помилок. Base58Check використовується і в багатьох інших випадках, коли важливо коректне прочитання або транскрибування числа, біткоїн-адреси, секретного ключа, зашифрованого ключа, або хешу сценарію [2].

Приклад Біткоїн-адреси у стандартному вигляді наведено нижче:

$$A = 1PRQujzribtj542PJfKX7QRfBXKVncRSNE$$

Більш детально процес формування Біткоїн-адреси з відкритого ключа буде розглянуто у наступному розділі.

3 РЕАЛІЗАЦІЯ ПРОЦЕСУ ФОРМУВАННЯ БІТКОІН-АДРЕСИ

3.1 Секретні ключі

Секретний ключ обирається випадково з діапазону чисел від 1 до $n - 1$, де n константа ($n = 1.158 \times 10^{77}$) визначається як порядок базової точки, що використовується в біткоін. Це досягається шляхом подання великого рядка випадкових бітів, взятих з криптографічно стійкого джерела випадковості, на вхід хеш-алгоритму SHA256, який видає 256-бітове число. Якщо результат менше, ніж $n - 1$, секретний ключ вважається придатним. В іншому випадку, процедура повторюється ще раз з іншим випадковим числом [2].

Нижче наведено випадковим чином згенерований секретний ключ $d1$ в шістнадцятковому форматі:

$d1 = F6E7AB9474A24C186C21879FD1669F437BD1E3ACAF386D3496D11B$
 $ACB681974E$

Програмне забезпечення Біткоін використовує генератори випадкових чисел операційної системи. Як правило, генератор випадкових чисел ОС ініціалізується джерелом випадковості користувача [2]. Онлайн Біткоін-гаманці зазвичай використовують вбудовані генератори випадкових чисел, абстраговані від операційної системи користувача.

3.2 Формати секретних ключів

Секретний ключ може бути представлений в різних форматах, кожен з яких відповідає одному 256-бітному числу.

У таблиці 3.1 показані три поширених формати, які використовуються для подання секретних ключів [2].

Шістнадцятковий формат є стандартним видом подання секретного ключа.

Таблиця 3.1 - Формати секретних ключів

Тип	Префікс	Секретний ключ
Шістнадцятковий	Немає	1e99423a4ed27608a15a2616a2b0e9e52ce d330ac53 0edcc32c8ffc6a526aedd
WIF	5	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5 tfcvU2Jpbnk eyhfsYB1Jcn
Стиснутий WIF	K або L	KxFC1jmwWCoACiCAWZ3eXa96mBM6 tb3TYzGmf 6YwgdGWZgawvrtJ

Wallet import format (WIF) - це формат представлення секретних ключів, базовою функцією якого є спрощення процедури копіювання і обробки. Використання контрольної суми при кодуванні дозволяє уникнути помилок.

Стиснутий WIF - це підвид Wallet import format, який використовується, коли секретному ключу відповідає стиснутий відкритий ключ. Цей формат дозволяє програмному забезпеченню гарантувати коректно імпортувати і здійснювати пошук ключів у блокчейні.

Схема перетворення секретного ключа у формат WIF представлена на рисунку 3.1.

На першому етапі до секретного ключа додається префікс, званий байтом версії, який визначає до якої мережі належить кодований секретний ключ. Для основної мережі (Mainnet) використовується префікс 0x80, а для тестової (Testnet) - 0xEF. На цьому ж етапі за необхідності додається суфікс, званий байтом компресії 0x01, який є індикатором того, що секретний ключ відповідає стиснутому відкритому ключу.

Наступним етапом є обчислення контрольної суми. Секретний ключ, префікс і суфікс хешуються алгоритмом SHA256. Отриманий байтовий рядок хешується знову цим самим алгоритмом. З отриманого значення виділяються перші 4 байти, які використовуються як контрольна сума. Контрольна сума додається до кінця кодованого рядка.

Останнім етапом є кодування у Base58. Результатом є секретний ключ у форматі WIF.

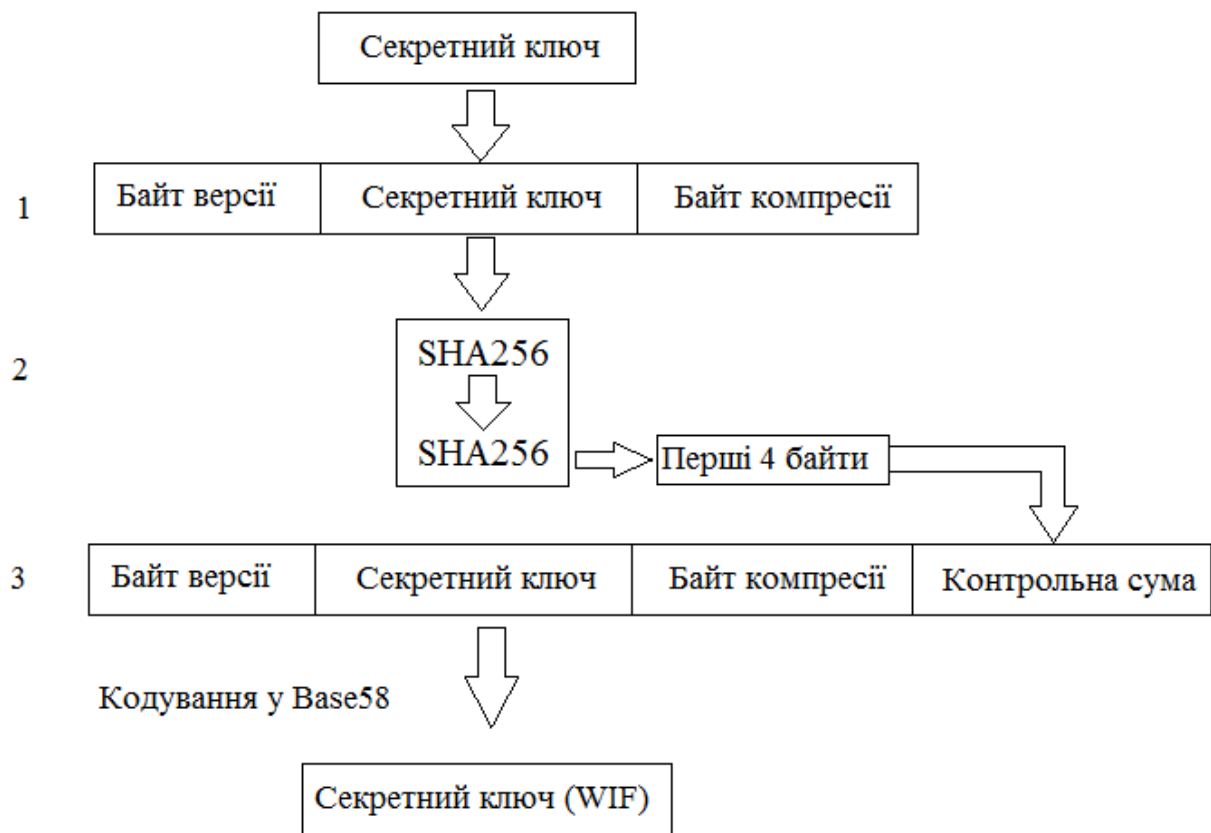


Рисунок 3.1 - Схема перетворення секретного ключа у формат WIF

Ще одним з видів є шифровані секретні ключі. Для підвищення захищеності і забезпечення зручності резервного копіювання був створений стандарт шифрування закритих ключів Bitcoin Improvement Proposal 38 або BIP0038 [6].

BIP0038 пропонує загальний стандарт для шифрування секретних ключів за допомогою кодової фрази і кодування за допомогою Base58Check так, що ключі можуть надійно зберігатися на резервних носіях, передаватися між гаманцями, або перебувати в будь-яких інших умовах, при яких ключ може бути виявлений. Стандартом для шифрування був обраний AES [6], прийнятий в National Institute of Standards and Technology (NIST).

Схема шифрування VIP0038 приймає на вході секретний ключ, який зазвичай кодується в Wallet Import Format (WIF), у вигляді рядка Base58Check з приставкою «5». Додатково, алгоритм шифрування VIP0038 приймає ключову фразу - пароль, який складається з декількох слів або складної послідовності алфавітно-цифрових символів.

На виході VIP0038 створюється зашифрований секретний ключ в кодуванні Base58Check, який починається з префікса 6P. Багато додатків-гаманців у даний час підтримують VIP0038 і запропонують користувачеві ввести секретну фразу для імпортування ключа. Для розшифровки ключів VIP0038 можуть бути використані спеціалізовані додатки.

У таблиці 3.2 наведено приклад секретного ключа, пароля і результуючого зашифрованого секретного ключа [2].

Таблиця 3.2 - Приклад зашифрованого секретного ключа VIP0038

Приватний ключ (WIF)	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2Jpbnk eyhfsYB1Jcn
Пароль	MyTestPassphrase
Зашифрований ключ (VIP0038)	6PRTL6mWa48xSopbU1cKrVjpKbBZxcLRRCdctL J3z5yxE87MobKoXdTsJ

Найпоширеніший випадок використання VIP0038 - це шифрування ключів для паперових гаманців, які можуть бути використані для резервного копіювання закритих ключів на аркуші паперу. На рисунку 3.2 наведено приклад паперового гаманця.



Рисунок 3.2 - Зашифрований паперовий гаманець

Якщо користувач вибирає надійну секретну фразу, паперовий гаманець з VIP0038-зашифрованими секретними ключами стає досить безпечним способом для зберігання офлайн.

3.3 Відкриті ключі

Як вже зазначалося раніше, відкритий ключ являє собою 512-бітне число і обчислюється з секретного ключа за допомогою незворотного множення на еліптичних кривих. Зв'язок між секретним ключем d і відкритим ключем Q визначений формулою (2.1). Зворотна операція, відома як "знаходження дискретного логарифму", обчислення d при відомому Q нездійсненна за прийнятний проміжок часу.

Так як базова точка завжди однакова для всіх користувачів біткоїн, секретний ключ d при множенні на G завжди дасть один і той же відкритий ключ Q . Відношення між d і Q зафіксовано, але може бути практично обчислено тільки в одному напрямку, від d до Q . Ця властивість дозволяє ділитися біткоїн-адресою з ким завгодно без ризику розкриття секретного ключа d .

Нижче наведено відкритий ключ $Q1$ в шістнадцятковому форматі, який був згенерований з обраного раніше секретного ключа $d1$ і займає 65 байт:

$Q1 = 043E003CE77CA09B836CA6A8ADF46A23810B04BFD58CF0C98EB97$
 $4CB7773793120AB1FEAAC0AE274CF2131FD7F3717240E93F10226052193$
 $B8099056F641A39144$

Відкритий ключ являє собою точку еліптичної кривої $Q(x, y)$, де перший байт 04 відповідає шістнадцятковому кодуванню, а наступні 64 байти відповідають координатам x та y , по 32 байти кожна.

3.4 Формати відкритих ключів

Відкриті ключі також можуть бути представлені по-різному, а саме, в стиснутому або не стиснутому вигляді.

Стиснуті відкриті ключі були введені для того, щоб зменшити розмір транзакцій і заощадити місце в блокчейні. Більшість транзакцій включає відкритий ключ, необхідний для перевірки облікових даних власника при проведенні платежу.

Відкритий ключ - це точка (x, y) на еліптичній кривій. Оскільки крива виражає математичну функцію, точка на кривій є рішенням рівняння, а значить, знаючи x координату, можна обчислити y координату, вирішивши рівняння $y^2 = x^3 + 7 \bmod p$ [2].

Це дозволяє зберігати тільки x координату відкритого ключа, опускаючи y координату і зменшити розмір ключа і простір, необхідний для його зберігання, на 256 біт.

Не стиснуті відкриті ключі мають префікс 04, стислі починаються або з 02, або з 03. Так як в лівій частині рівняння знаходиться y^2 , це означає, що координата y може бути парною і не парною. Тип y -координати необхідно

зберегти, бо кожен з цих варіантів відповідає різним точкам і різним відкритим ключам [7].

Таким чином, для розрізнення цих двох можливих значень y , стиснутий відкритий ключ зберігається з префіксом 02, якщо y парне, і, 03, якщо непарне, дозволяючи програмному забезпеченню правильно виводити координату y з x і розпаковувати відкритий ключ Q до повних координат точки [7].

Схема стиснення відкритого ключа зображена на рисунку 3.3.

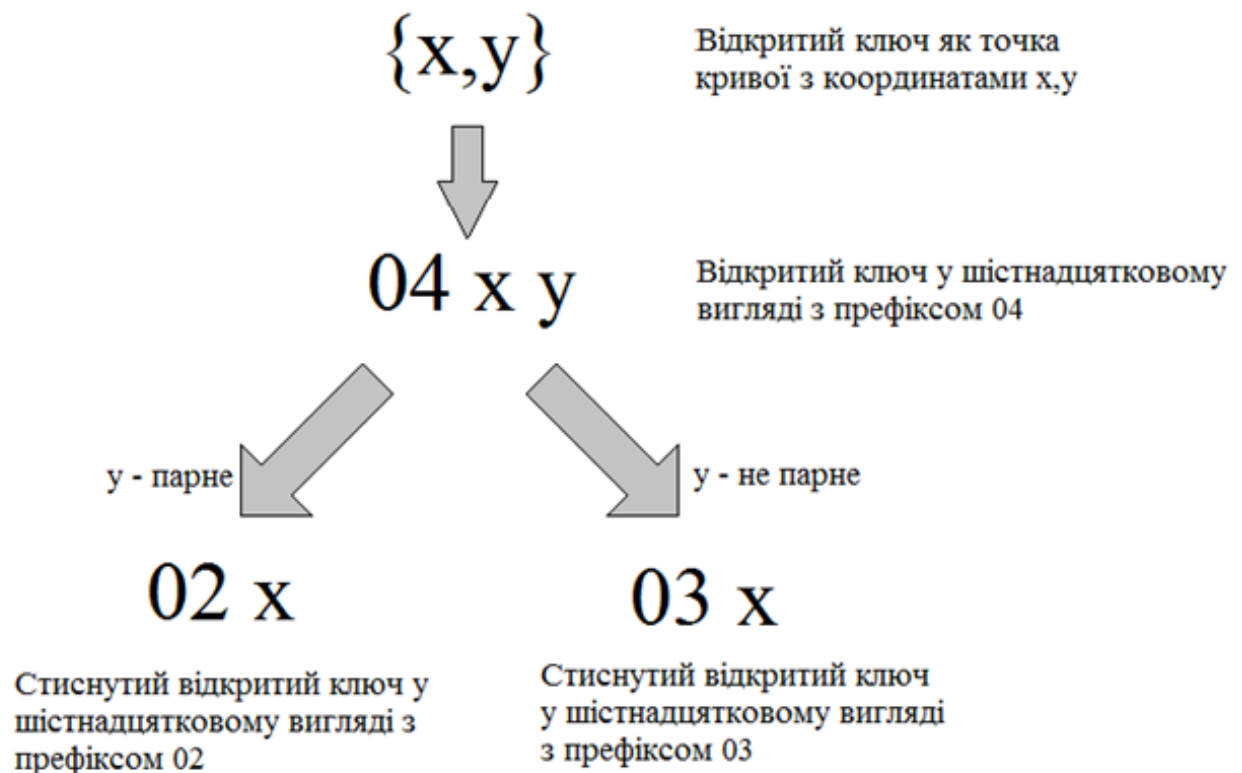


Рисунок 3.3 - Схема стиснення відкритого ключа

Нижче наведений згенерований раніше відкритий ключ, який у стиснутому вигляді має довжину 264 біт (66 шістнадцяткових цифр) і префікс 02 для зазначення надлишкової y координати:

$Q = 023E003CE77CA09B836CA6A8ADF46A23810B04BFD58CF0C98EB974CB7773793120$

Не стиснуті відкриті ключі поступово витісняються в клієнтському ПО, а стиснуті використовуються за замовчуванням, що значно впливає на зменшення розміру транзакцій і, отже, блокчейна.

Проте, ще не всі клієнти підтримують стиснуті відкриті ключі. Нові клієнти, що підтримують стиснуті відкриті ключі повинні також підтримувати транзакції, створені більш старими клієнтами, які не підтримують стиснуті формати відкритих ключів. Це особливо важливо, коли додаток гаманця імпортує секретні ключі з іншої програми, тому що новий гаманець повинен просканувати блокчейн і знайти транзакції, які відповідають цим імпортованим ключам. Біткоїн-адреси, отримані від не стиснутих або стиснутих відкритих ключів є валідними, але вони різні.

Щоб вирішити цю проблему, коли секретні ключі експортуються з гаманця, Wallet Import Format, який використовується для їх подання реалізується по-іншому в нових Біткоїн-гаманцях, щоб вказати, що ці секретні ключі були використані для отримання стислих відкритих ключів і, отже, стислих біткоїн-адрес. Це дозволяє гаманцю, що імпортує, відрізнити секретні ключі, що походять від старих або нових гаманців і знайти в блокчейні транзакції з адресами від не стиснутих або стиснутих відкритих ключів відповідно [2].

3.5 Біткоїн-адреси

Біткоїн-адреса являє собою рядок з цифр і символів латинського алфавіту, довжиною від 26 до 34 знаків.

Як вже зазначалося раніше, Біткоїн-адреса з відкритого ключа отримується в результаті застосування алгоритмів SHA256 і RIPEMD160.

Схема процедури подвійного хешування зображена на рисунку 3.4.

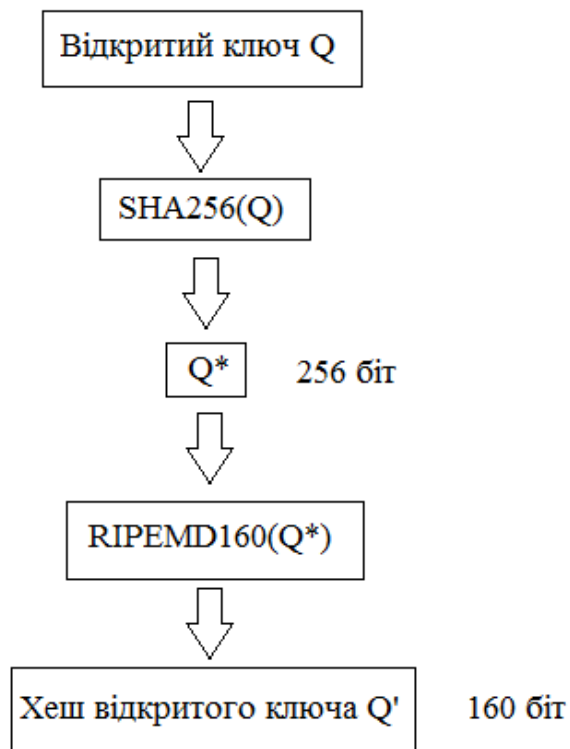


Рисунок 3.4 - Схема процедури подвійного хешування

На першому етапі відкритий ключ $Q1$ хешується алгоритмом SHA256. Результатом даного перетворення є 256-бітний хеш $Q1^*$:

$$Q1^* = SHA256(Q1) \quad (3.1)$$

$Q1^* = 3CC19F8FE98EEF9DFF1007B493F101D0B5A20ADE09BE22F6BD0CF$
 $CE4D7BCE13B$

Отриманий результат хешується повторно алгоритмом RIPEMD160. Результатом даного перетворення є 160-ти бітний хеш $Q1'$:

$$Q1' = RIPEMD160(Q1^*) \quad (3.2)$$

$Q1' = 77BA2708231A0F418B7B5F23C038ACB547F9305C$

Основною метою хешування є зменшення розміру результуючої Біткоїн-адреси. Подвійне хешування використовується як засіб підвищення захищеності, а саме унеможливлення проведення "атак подовженням повідомлення".

На останньому етапі хеш відкритого ключа кодується у форматі Base58Check. Результатом є Біткоїн адреса *A1* у стандартному вигляді:

$$A1 = 1Bv4QvpvqhpuhchEa6EX1Trr5zwS8nihGZ$$

Як вже зазначалося раніше, формат Base58Check використовується для зменшення розміру Біткоїн-адреси, спрощення сприйняття інформації людиною і захисту від помилок.

Base58 - це підмножина Base64, що використовує прописні і заголовні букви і цифри, але без символів, які часто помилково приймають один за одного і які можуть відображатися ідентично деякими шрифтами. Зокрема, Base58 - це Base64 без числа 0 (нуль), O (заголовна буква O), l (маленька L), I (велика i), і символів "+" і "/" [8]. Алфавіт формату Base58 наведено нижче:

123456789ABCDEFGHIJKLMNPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Для перетворення десяткового числа в Base58 використовується операція ділення з залишком. Процедура повторюється необхідну кількість разів. Залишки від ділення потім перетворюються в відповідні символи алфавіту Base58 [8]. Нижче наведено приклад перетворення десяткового числа у формат Base58.

```
base10 = 123456789
```

```
123456789 % 58 = 19
```

```
2128565 % 58 = 23
```

```
36699 % 58 = 43
```

```
632 % 58 = 52
```

```
10 % 58 = 10
```

```
base58 = [19][23][43][52][10]
```

```
base58 = BukQL
```

Рисунок 3.5 - Приклад переведення десяткового числа в Base58

У таблиці 3.3 наведено символну схему формату кодування Base58. Кожному десятковому значенню від 0 до 57 поставлений у відповідність символ алфавіту Base58.

Таблиця 3.3- Символьна схема формату кодування Base58

Значення	Символ	Значення	Символ	Значення	Символ	Значення	Символ
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c

Продовження таблиці 3.3 - Символьна схема формату кодування Base58

Значення	Символ	Значення	Символ	Значення	Символ	Значення	Символ
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

Для додаткового захисту від помилок використовується формат кодування Base58Check - це Base58 з вбудованим кодом перевірки помилок. Чотири байта контрольної суми додаються в кінець кодованих даних. Контрольна сума генерується шляхом хешування кодованих даних і, отже, може бути використана для виявлення і запобігання помилок транскрипції і друкарських помилок. Програмне забезпечення обчислює контрольну суму даних при декодуванні і порівнює його з контрольною сумою з коду. Розбіжність означатиме внесену помилку, а дані Base58Check недійсними. Наприклад, подібна перевірка запобігає можливість відправити кошти на неіснуючу біткоїн-адресою і таким чином втратити кошти.

Для конвертації даних в формат Base58Check, до даних спочатку потрібно додати префікс, званий "байтом версії", який служить для визначення типу кодованих даних. Наприклад, в разі біткоїн-адреси префікс 0 (0x00 в шістнадцятковій системі), а префікс для приватного ключа 128 (0x80 в шістнадцятковій системі) [2].

Наступним етапом є обчислення контрольної суми. Для обчислення контрольної суми префікс і дані хешуються алгоритмом SHA256. Потім отриманий результат хешується повторно цим же алгоритмом. Подвійне хешування SHA256 або SHA256d зазвичай використовується для захисту від

"атак подовженням повідомлення". При обчисленні контрольної суми подвійне хешування не є необхідним, але може використовуватися як запобіжна міра.

$$checksum = SHA256(SHA256(prefix + data)) \quad (3.3)$$

З отриманого тридцяти двох байтного хеша виділяються перші чотири байти. Ці чотири байти служать в якості коду перевірки помилковості, або контрольної суми. Контрольна сума потім додається до кінця рядка.

Результат складається з трьох елементів: префікса, даних і контрольної суми. Останнім етапом є перетворення результату з використанням кодування Base58.

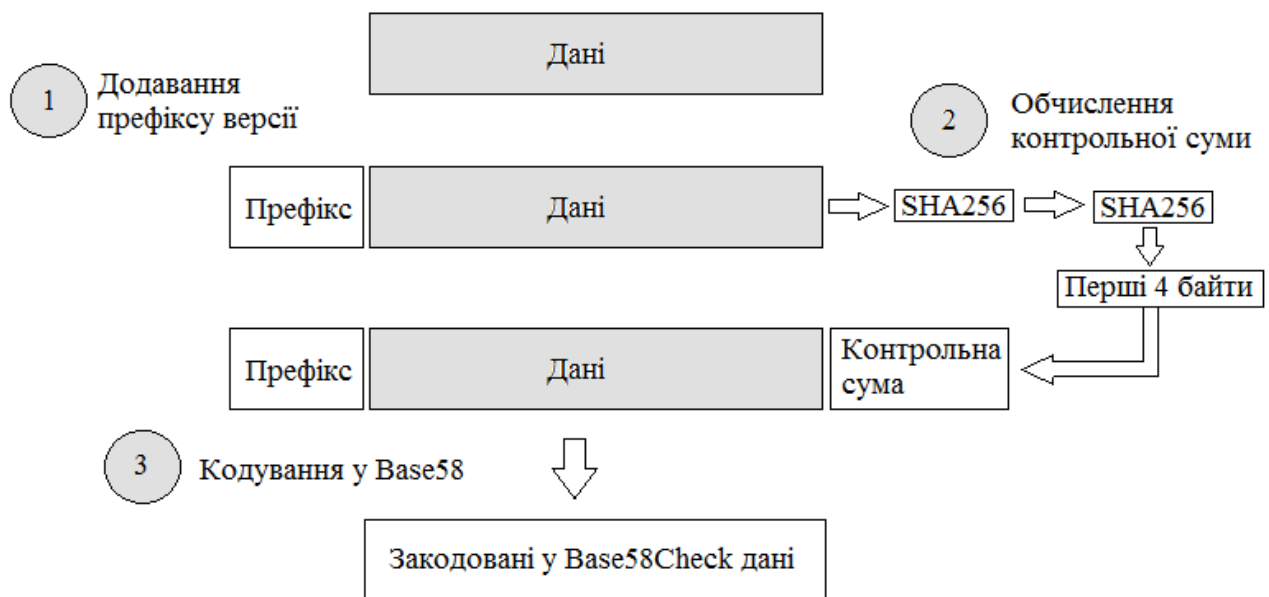


Рисунок 3.6 - Схема кодування в Base58Check

Префікс версії в кодуванні Base58Check використовується для створення різних форматів, які легко відрізнити за певними символами на початку рядків. Ці символи дозволяють людям легко визначати закодований тип даних.

Наприклад, біткоін-адреса в кодуванні Base58Check починається з 1, а приватний ключ формату WIF в кодуванні Base58Check починається з 5.

Приклади префіксів і результуючих символів алфавіту Base58 наведено в таблиці 3.4.

Таблиця 3.4 - Префікс версії в Base58Check і приклади закодованого результату

Тип даних	Префікс	Результат
Біткоін-адреса	0x00	1
Pay-to-Script-Hash адреса	0x05	3
Testnet-адреса	0x6F	m або n
Секретний ключ WIF	0x80	5, K або L
ВІР38 зашифрований секретний ключ	0x0142	6P
ВІР32 розширений відкритий ключ	0x0488B21E	xpub

У Біткоін, більшість даних представлені користувачам в кодуванні Base58Check, тому що це уявлення компактне, зручне для читання, і допомагає легко виявити помилки.

3.6 Формати Біткоін-адрес

Стандартні біткоін-адреси починаються з цифри "1" і виводяться з відкритого ключа, який, в свою чергу, є похідним від секретного ключа. Будь-хто може відправити біткоїни на такі адреси, але кошти можуть бути витрачені тільки тим, хто представить відповідний підпис секретним ключем і хеш відкритого ключа.

Біткоін-адреси, що починаються з цифри "3" - це pay-to-script hash (P2SH) адреси. Вони оголошують бенефіціаром транзакції хеш сценарію, а не власника відкритого ключа. Функція була введена в січні 2012 року з ВІР0016 [9], і в даний час широко застосовується, оскільки вона забезпечує можливість додавати функціональні можливості до самої адреси. На відміну від транзакцій

на стандартні адреси, відомі як pay-to-public-key-hash (P2PKH), кошти, відправлені на P2SH-адреси вимагають більше, ніж надати хеш одного відкритого ключа і підпис одним секретним ключем як доказ права власності. Вимоги визначаються в момент створення адреси, в сценарії, і всі входи на цю адресу будуть обмежені тими ж вимогами.

Адреса хешу pay-to-script отримується зі сценарію транзакції, який визначає, хто може розпоряджатися виходами транзакції. Для кодування адреси хешу pay-to-script використовується та ж функція подвійного хешування, яка використовується при створенні біткоін-адреси, тільки застосовується вона до сценарію, а не до відкритого ключу [9]:

$$script\ hash = RIPEMD160(SHA256(script)) \quad (3.4)$$

В даний час найбільш поширеною реалізацією функції P2SH є сценарій мультипідписної адреси. Основний сценарій вимагає більше одного підпису для підтвердження права власності і можливості використання коштів. Мультипідпис М-з-Н в Біткоін - це такий сценарій, коли потрібно М підписів (це число також називають "порогом") від загального числа N ключів.

Наприклад, мультипідписна адреса виду 2-з-3 гарантує, що ніякі кошти не можуть бути витрачені, якщо принаймні двоє з його власників не підпишуть транзакцію.

3.7 Модель формування Біткоін-адреси

Для моделювання формування Біткоін-адреси була використана утиліта командного рядка Bitcoin Explorer.

Першим етапом формування Біткоін-адреси є вибір випадкового зерна (seed), необхідного для генерації секретного ключа. Для генерації зерна використовується команда `bx seed`. Результатом роботи команди є зерно у шістнадцятковому вигляді.

```
$ bx seed
```

```
10a96779cea3f4643df196919b260d18b6b1fcb28b0af3a6
```

На наступному етапі генерується секретний ключ. Для генерації секретного ключа використовується команда `bx es-new`, яка приймає зерно як аргумент. Результатом роботи команди є секретний ключ у шістнадцятковому вигляді.

```
$ bx es-new 10a96779cea3f4643df196919b260d18b6b1fcb28b0af3a6
```

```
990dc233271a0abfefb6fddb0c5dc1037bf2c4817204dbcb389a727853a2e2e
```

Наступним етапом є формування відкритого ключа. Для генерації відкритого ключа використовується команда `bx es-to-public`, яка приймає секретний ключ як аргумент. Результатом роботи команди є стиснутий відкритий ключ у шістнадцятковому вигляді.

```
$ bx es-to-public 990dc233271a0abfefb6fddb0c5dc1037bf2c4817204dbcb389a727853a2e2e
```

```
389a727853a2e2e
```

```
03116116106f4fc0c7bc9e3b8650d2c52fe1f07c01a453485cdbd447bc499b
```

```
5a00
```

На наступному етапі відкритий ключ хешується алгоритмом SHA256. Для хешування використовується команда `bx sha256`, яка приймає шістнадцяткове число як аргумент. Результатом роботи команди є 256 бітний хеш у шістнадцятковому вигляді.

```
$ bx sha256 03116116106f4fc0c7bc9e3b8650d2c52fe1f07c01a453485cdbd4
```

```
47bc499b5a00
```

```
1d4304f840271e213c7751e2c6282e4a5c12d4917f35e17a083cf44ab9f0a8ff
```

На наступному етапі відкритий ключ хешується алгоритмом RIPEMD160. Для хешування використовується команда `bx ripemd160`, яка приймає шістнадцяткове число як аргумент. Результатом роботи команди є 160 бітний хеш у шістнадцятковому вигляді.

```
$ bx ripemd160 1d4304f840271e213c7751e2c6282e4a5c12d4917f35e17a0
```

```
83cf44ab9f0a8ff
```

```
65355aa83ffa0eb19f08f871294b6964f71ccfb5
```

Останнім етапом є кодування хешу відкритого ключа у формат Base58Check. Для кодування використовується команда `bx base58check-encode`, яка приймає байт версії і хеш відкритого ключа у шістнадцятковому вигляді як аргументи. Результатом є Біткоїн-адреса у стандартному вигляді.

```
$ bx base58check-encode -v 0 65355aa83ffa0eb19f08f871294b6964f71ccfb5  
1AE9AV7sLNWpJYPx36K3TKkoABwGV6ZzoN
```

4 АНАЛІЗ ПРОЦЕСУ ФОРМУВАННЯ БІТКОІН-АДРЕСИ

Модель формування Біткоін-адреси має низку недоліків, які можуть призвести до матеріальних або моральних збитків користувачів системи. Одним з таких недоліків є можливість виникнення колізій Біткоін-адрес.

Колізія Біткоін-адреси відбувається, коли два або більше користувачів отримали доступ до коштів однієї Біткоін-адреси.

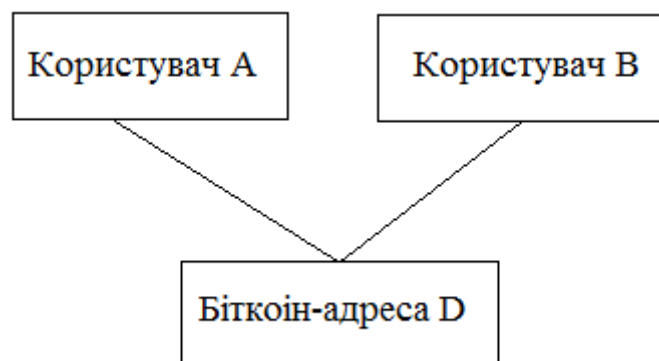


Рисунок 4.1- Колізія Біткоін-адреси

Якщо відбулася колізія Біткоін-адрес, то всі користувачі, що мають доступ до Біткоін-адреси, можуть витратити кошти, пов'язані з нею. Право витратити кошти з певних виходів отримує користувач, який першим сформував відповідну Біткоін-транзакцію. Після підтвердження транзакції і включення її до блокчейна, кошти з цих виходів вважаються витраченими [10].

На даний момент система Біткоін ніяк не реєструє і не реагує на виникнення колізій Біткоін-адрес. Базові засоби системи дозволяють проводити лише умовну перевірку коректності Біткоін-адреси [2]. Це підвищує загрозу втрати коштів для власників Біткоїнів, а також спонукає зловмисників до пошуку ефективних методів створення колізій Біткоін-адрес.

Програмне забезпечення Біткоін-гаманців може мати власний аналізатор колізій Біткоін-адрес і запобігати створенню однакових Біткоін-адрес [11]. Проте це не є обов'язковою вимогою і не всі розробники ПЗ витрачають

ресурси для створення власних аналізаторів колізій. До того ж утворення колізій може проводитися навмисно без використання програмного забезпечення сторонніх клієнтів Біткоїн-гаманців.

Колізії Біткоїн-адрес можуть виникати на етапі вибору секретних ключів. Незважаючи на те, що секретні ключі обираються з великого діапазону значень, цей діапазон є скінченним, а отже є шанс обрати однакові секретні ключі.

Колізії Біткоїн-адрес також можуть виникнути на етапі хешування. Використовувані в Біткоїн хеш-функції приймають на вхід значення довільної довжина, а повертають значення фіксованої довжини. У такій ситуації колізії обов'язково будуть існувати.

Виникнення колізій не є можливим на етапі генерації відкритого ключа, тому що множина можливих значень секретного ключа обмежена. Значення обмеження відповідає порядку базової точки, тому результат множення секретного ключа на базову точку буде завжди різний.

При кодуванні у формат Base58Check також неможливе виникнення колізій. Кодування є однозначним і результат кодування різний для кожного хешу відкритого ключа.

4.1 Аналіз колізій секретних ключів

Однією з причин виникнення колізій Біткоїн-адрес є вибір однакових секретних ключів.

Така колізія виникає, коли два або більше користувачів обрали однакові секретні ключі, згенерували однакові відкриті ключі і отримали однакові хеші, а відповідно і Біткоїн-адреси.

Виникнення колізій секретних ключів викликане абстрагованістю механізму генерації секретних ключів від системи Біткоїн. Створення пари ключів Біткоїн-гаманцем може бути реалізовано як Онлайн, так і Офлайн, але повністю незалежно від системи Біткоїн [2]. Аналіз збігу отриманої з пари

ключів Біткоїн-адреси з уже існуючими не є обов'язковим і може бути виконаний тільки шляхом підключення до системи Біткоїн.

На рисунку 4.2 зображена схема виникнення колізії Біткоїн-адрес, викликана вибором однакових секретних ключів.

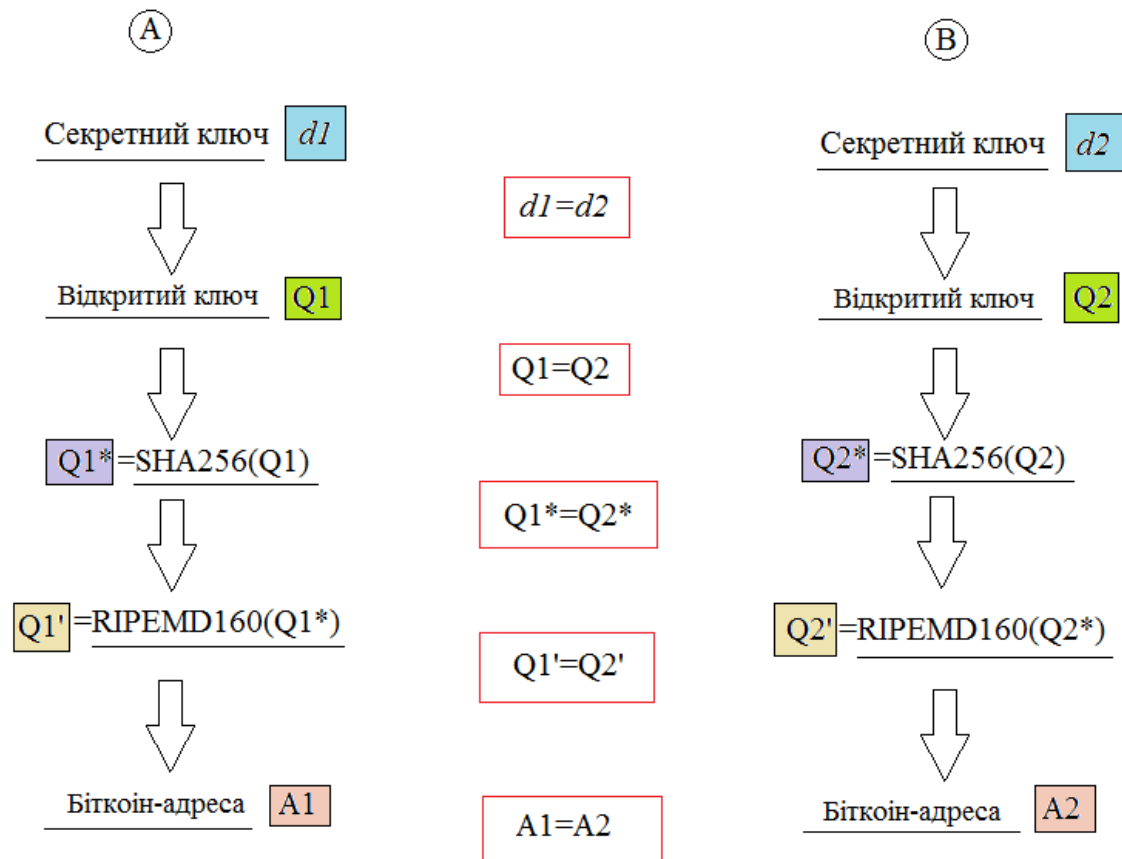


Рисунок 4.2 - Схема виникнення колізії Біткоїн-адреси, викликана вибором однакових секретних ключів

Критичним елементом при створенні секретних ключів виступає вибір генератора випадкових чисел. Офлайн Біткоїн-гаманці можуть використовувати як стандартні генератори випадкових чисел операційної системи [2], які не завжди є надійними, так і сторонні генератори випадкових чисел, надійність яких теж має бути перевірена. Реалізація програмного забезпечення онлайн гаманців або мобільних додатків зазвичай є закритою. Тому доволі важко або навіть неможливо дізнатися які генератори випадкових чисел

використовуються у такому ПЗ, а отже і оцінити ступінь їх криптографічної надійності.

Іншим джерелом виникнення колізій є алгоритм вибору секретних ключів. Розмір секретного ключа дорівнює 256 біт, тому доцільно використовувати алгоритми хешування розрядністю у 256 біт для генерації секретних ключів. На практиці це зазвичай реалізовано поданням великого числа, створеного генератором випадкових чисел на вхід хеш-алгоритму, наприклад, SHA256. Якщо отримане значення потрапляє у необхідний діапазон, то воно використовується як секретний ключ. В іншому випадку процедура генерації випадкового числа і хешування повторюється знову [2]. Використання хеш-алгоритмів при генерації секретного ключа є додатковим джерелом виникнення колізій.

Секретний ключ обирається з діапазону від 1 до $n-1$, де n відповідає порядку базової точки G . Нижче наведені значення параметру n у шістнадцятковому та десятковому вигляді.

$n_{16} = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF EBAEDCE6 AF48A03B}$
 BFD25E8C D0364141

$n_{10} = 11579208923731619542357098500868790785283756427907490438$
 2605163141518161494337

Секретний ключ може приймати $n-1$ різних значень.

$n - 1 = 11579208923731619542357098500868790785283756427907490$
 $4382605163141518161494336$

Згідно до blockchair.com станом на 19.11.2018 у блокчейн внесено 358.069.203 транзакцій які мають 973.736.754 унікальних виходів, і, відповідно, стільки ж унікальних Біткоїн-адрес.

Кожній Біткоїн-адресі відповідає унікальний секретний ключ. Приймаємо, що кількість унікальних секретних ключів K у системі Біткоїн у даний момент дорівнює:

$$K = 973\,736\,754$$

Розрахунок імовірності виникнення випадкової колізії секретних ключів у системі Біткоїн зводиться до обчислення відношення кількості існуючих унікальних секретних ключів до загальної кількості можливих секретних ключів. Нехай $P(K)$ - імовірність виникнення випадкової колізії секретних ключів.

$$P(K) = \frac{K}{n - 1} \quad (4.1)$$

Таким чином $P(K) \approx 8.4 \times 10^{-67}$.

Незважаючи на те, що імовірність виникнення випадкової колізії секретних ключів досить низька, загроза вибору однакових секретних ключів все одно існує. Відсутність обов'язкових механізмів перевірки унікальності Біткоїн-адрес у сукупності з використанням нестійких генераторів випадкових чисел значно підвищують імовірність реалізації загрози вибору однакових секретних ключів.

Для зменшення вірогідності виникнення колізій секретних ключів рекомендовано використовувати криптографічно стійкий генератор випадкових чисел із зерном з джерела достатньої ентропії.

4.2 Аналіз колізій хеш-функцій

Ще однією причиною виникнення колізій Біткоїн-адрес є колізії алгоритмів хешування, що використовуються у системі Біткоїн при формуванні Біткоїн-адрес.

Такі колізії виникають коли двом або більше різним прообразами відповідає однакове значення хеш-функції [12]. У системі Біткоїн при формуванні Біткоїн-адрес використовуються два алгоритми хешування, а саме SHA256 та RIPEMD160.

Один із можливих варіантів виникнення колізії Біткоїн-адрес є колізія алгоритму хешування SHA256. Користувачі можуть обрати різні секретні ключі, згенерувати різні відкриті ключі, але в результаті колізії хеш-алгоритму SHA256 отримати однакові хеші відкритих ключів і, відповідно, однакові Біткоїн-адреси. На рисунку 4.3 зображена схема виникнення колізії Біткоїн-адрес, викликана колізією алгоритму хешування SHA256.

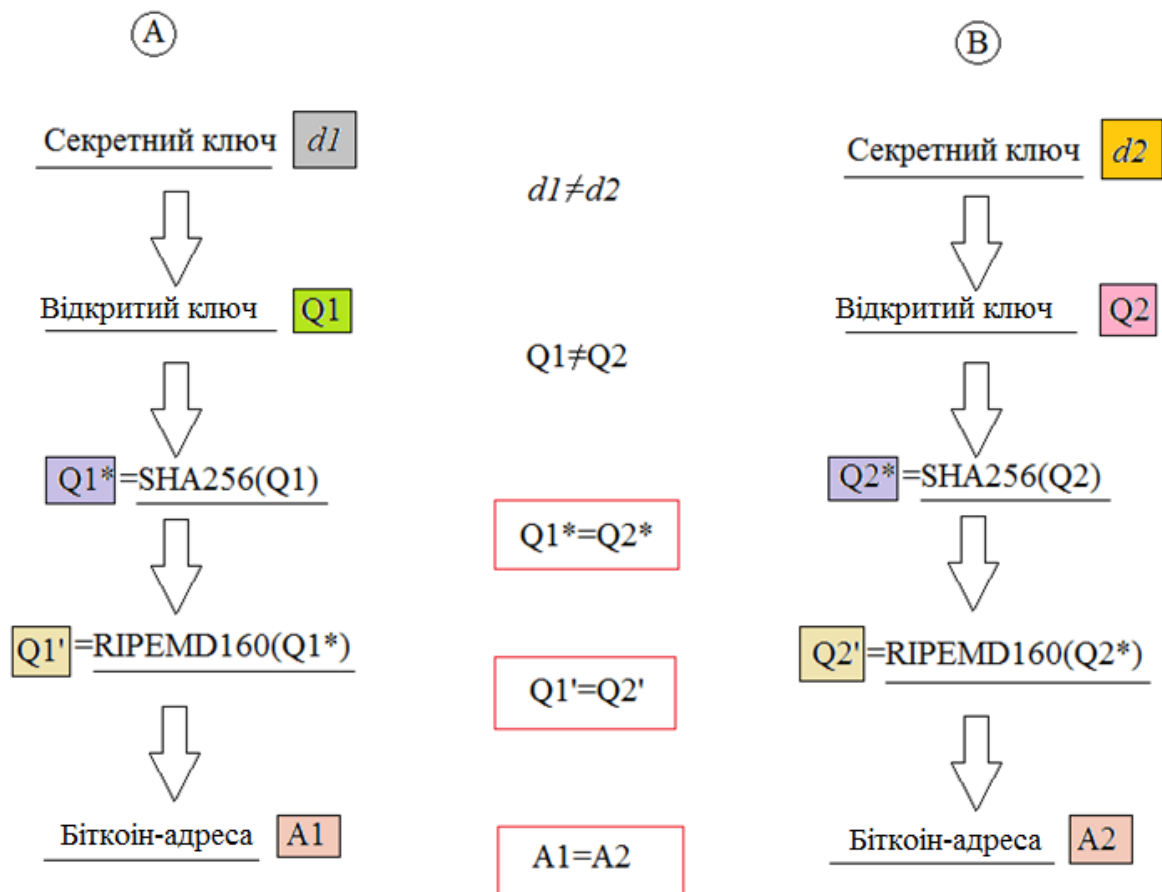


Рисунок 4.3 - Схема виникнення колізії Біткоїн-адреси, викликана колізією алгоритму хешування SHA256

Іншим можливим варіантом виникнення колізії Біткоїн-адрес є колізія алгоритму хешування RIPEMD160. Користувачі можуть обрати різні секретні

ключі, згенерувати різні відкриті ключі, отримати різні хеші SHA256, але в результаті колізії хеш-алгоритму RIPEMD160 отримати однакові хеші відкритих ключів і, відповідно, однакові Біткоїн-адреси. На рисунку 4.4 зображена схема виникнення колізії Біткоїн-адрес, викликана колізією алгоритму хешування RIPEMD160.

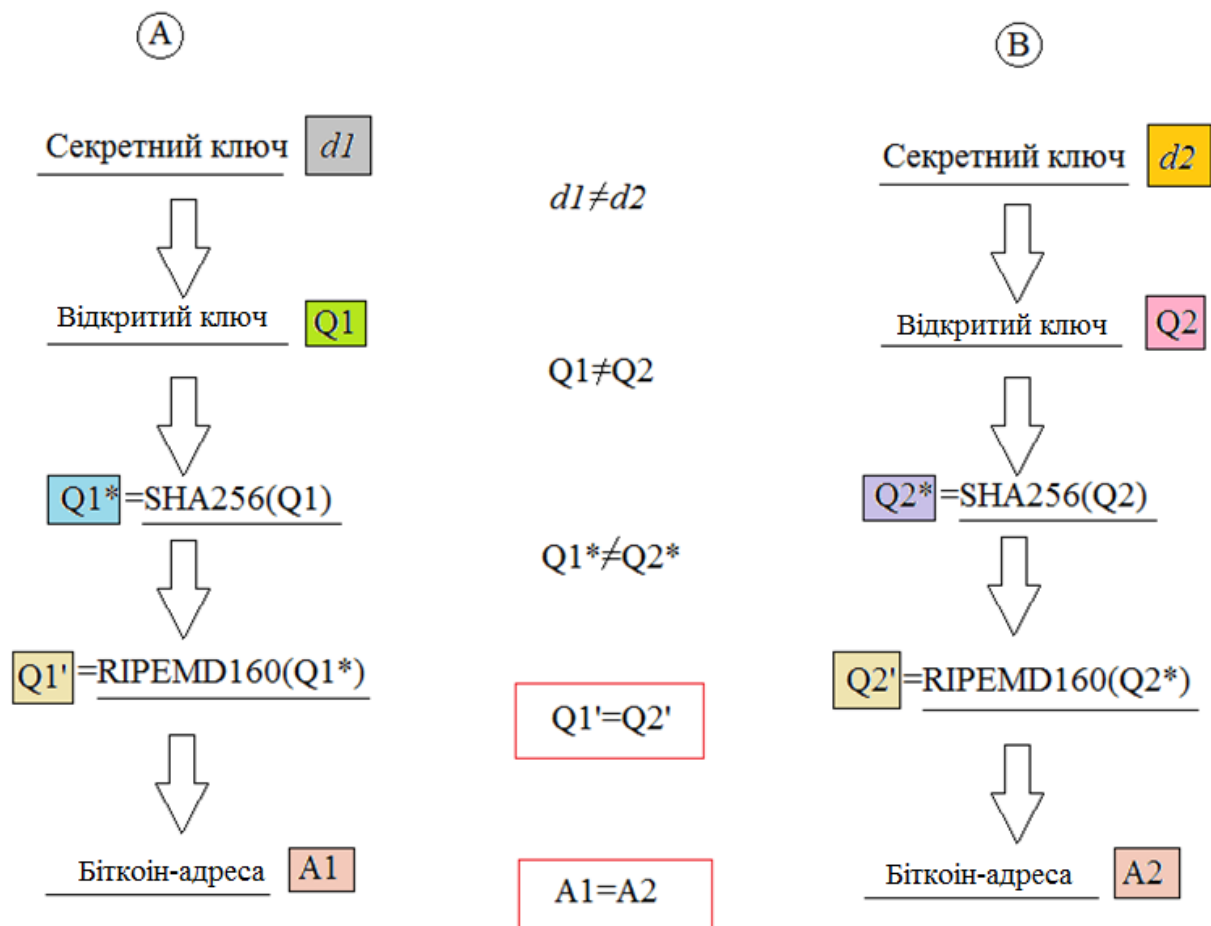


Рисунок 4.4 - Схема виникнення колізії Біткоїн-адреси, викликана колізією алгоритму хешування RIPEMD160

Виникнення колізій хеш-функцій обумовлене недосконалістю моделі алгоритмів хешування. Хеш-функції, які використовуються в системі Біткоїн, відносяться до типу алгоритмів хешування з довільним вхідним значенням і фіксованим вихідним значенням. Множина можливих вхідних значень на обох

етапах хешування значно більша ніж множина можливих вихідних значень. Тому виникнення колізій неминуче при використанні хеш-функцій такого типу.

Далі було проаналізована імовірність знаходження колізій хеш-функцій, які використовуються у системі Біткоїн.

Атака «днів народження» - один із методів пошуку колізій хеш-функцій на основі парадоксу днів народження. Суть методу полягає в значному зменшенні кількості переданих хеш-функції аргументів, необхідного для виявлення колізії, оскільки якщо хеш-функція генерує n -бітове значення, то число випадкових аргументів хеш-функції, для якого з великою ймовірністю буде виявлена хоча б одна колізія хеш-функції (тобто знайдеться хоча б одна пара рівних хешів, отриманих з різних аргументів), дорівнює не 2^n , а близько $2^{n/2}$.

Для заданої хеш-функції h метою атаки є пошук колізії другого роду. Для цього обчислюються значення h для випадково вибраних блоків вхідних даних до тих пір, поки не будуть знайдені два блоки, які мають один і той же хеш. Нехай h - хеш-функція.

Атака «днів народження» успішна, якщо знайдеться пара вхідних блоків $x_1 \neq x_2$ така, що $h(x_1) = h(x_2)$. Таким чином, якщо функція $h(x)$ дає будь-який з N різних виходів з однаковою ймовірністю і параметр N досить великий, то математичне сподівання кількості пар різних аргументів $x_1 \neq x_2$ для яких $h(x_1) = h(x_2)$, становить $1.25 \times \sqrt{N}$.

Нехай $P(n)$ - вірогідність того, що у групі з n вхідних значень ($n < N$) хоча б двом відповідає один і той самий хеш.

$$P(n) = 1 - 1 \times \left(1 - \frac{1}{N}\right) \times \left(1 - \frac{2}{N}\right) \times \dots \times \left(1 - \frac{n-1}{N}\right) = 1 - \prod_{i=0}^{n-1} \left(1 - \frac{i}{N}\right) \quad (4.2)$$

З перших двох членів розкладання в ряд Тейлора функції $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$, при $|x| \ll 1$ виконується $e^x \approx 1 + x$. Якщо замінити множники $(1 - \frac{i}{N})$ на $e^{-i/N}$, то отримуємо наступне рівняння:

$$P(n) \approx 1 - \prod_{i=0}^{n-1} e^{-i/N} \approx 1 - \exp \sum_{i=0}^{n-1} \left(-\frac{i}{N}\right) \approx 1 - e^{\frac{-n(n-1)}{2N}} \approx 1 - e^{-n^2/2N} \quad (4.3)$$

Задача зводиться до знаходження числа n , такого щоб вірогідність $P(n)$ була більше певного значення α .

$$P(n) \geq \alpha \quad (4.4)$$

Виходячи з формул (4.3) та (4.4), складається формула для обчислення значення n .

$$n = \sqrt{\ln\left(\frac{1}{1-\alpha}\right) \times 2 \times N} \quad (4.5)$$

Параметр n дозволяє оцінити імовірність виникнення колізії хеш-алгоритмів. Чисельне значення n відповідає кількості спроб генерації випадкових хешів, необхідних для знаходження випадкової колізії другого роду із заданою імовірністю α .

Далі було проведено розрахунок імовірності знаходження колізій другого роду хеш-функцій SHA256 та RIPEMD160 для різних значень параметру α . Дані розрахунків зведено у таблицю 4.1.

Таблиця 4.1 - Імовірність знаходження колізій другого роду хеш-функцій SHA256 та RIPEMD160:

Алгоритм	Кількість можливих значень хеш-функції N	Кількість спроб, необхідна для знаходження випадкової колізії другого роду із заданою імовірністю α			
		$\alpha=0,25$	$\alpha=0,5$	$\alpha=0,75$	$\alpha=1$
SHA256	$2^{256}=1,16*10^{77}$	$2,58*10^{38}$	$4,01*10^{38}$	$5,67*10^{38}$	$1,03*10^{39}$
RIPEMD160	$2^{160}=1,46*10^{48}$	$9,17*10^{23}$	$1,42*10^{24}$	$2,01*10^{24}$	$3,67*10^{24}$

Криптографічна стійкість хеш-функцій до знаходження колізій другого роду достатньо велика - приблизно 2^{128} та 2^{80} для алгоритмів SHA256 та RIPEMD160 відповідно. Незважаючи на це, імовірність виникнення колізій існує і її необхідно враховувати.

Для пошуку колізій хеш-функцій другого роду була використана еліптична крива $y^3 = x^3 + 7 \bmod 61$. Обрана базова точка $P(7,17)$ простого порядку $n = 61$.

Згідно з алгоритмом формування Біткоїн-адреси обрані секретні ключі d з діапазону значень від 1 до $n - 1$. Відкриті ключі Q сформовані шляхом множення відповідних секретних ключів на базову точку G , яка використовується у системі Біткоїн.

Відкриті ключі переведені у шістнадцятковий формат. На наступному етапі відкриті ключі були подані на вхід алгоритму хешування SHA256. Отриманий результат прохешовано алгоритмом хешування RIPEMD160. Для спрощення задачі пошуку колізій та більшої наочності були виділені лише останні 8 біт значення хеш-алгоритмів.

В результаті пошуку було виявлено чотири колізії алгоритму SHA256 і три колізії алгоритму RIPEMD160. Дані розрахунків зведені у таблицю 4.2.

Таблиця 4.2 - Результати пошуку колізій другого роду хеш-функцій SHA256 і RIPEMD160.

d	Q	Q hex	SHA256	RIPEMD160
1	7,17	711	d4	ed
2	42,38	2a26	37	aa
3	27,32	1b20	47	b2
4	39,20	2714	39	fa
5	19,20	1314	06	ac
6	16,57	1039	80	bc
7	57,59	393b	85	ee
8	2,36	224	b6	68
9	3,41	329	f8	99
10	26,36	1a24	94	02
11	29,22	1d16	28	c9
12	34,24	2218	b6	68
13	24,17	1811	d7	23
14	30,44	1e2c	ce	fb
15	15,24	f18	1b	58
16	35,50	2332	64	e7
17	20,57	1439	67	46
18	33,25	2119	b0	22
19	46,32	2e20	b0	22
20	28,50	1c32	d5	49
21	21,22	1516	f9	6e
22	49,29	311d	2e	e2
23	25,4	194	11	fc
24	9,59	93b	9c	54
25	59,50	3b32	d8	7e
26	22,38	1626	76	9b
27	12,37	c25	e2	bd
28	58,23	3a17	4b	0b
29	11,22	b16	f1	37
30	56,59	383b	99	e4
31	56,2	382	5c	28
32	11,39	b27	56	81
33	58,38	3a26	19	42
34	12,24	c18	ec	5e
35	22,23	1617	8f	0a
36	59,11	3bb	18	10
37	9,2	92	dd	81
38	25,57	1939	7c	8b
39	49,32	3120	05	b4

Продовження таблиці 4.2 - Результати пошуку колізій другого роду хеш-функцій SHA256 і RIPEMD160.

d	Q	Q hex	SHA256	RIPEMD160
40	21,39	1527	09	f6
41	28,11	1cb	83	da
42	46,29	2e1d	a9	ab
43	33,36	2124	3d	47
44	20,4	144	8d	ee
45	35,11	23b	7a	dd
46	15,37	f25	c1	e3
47	30,17	1e11	12	61
48	24,44	182c	2c	1a
49	34,37	2225	d3	1e
50	29,39	1d27	7e	9c
51	26,25	1a19	d0	3e
52	3,20	314	ce	fb
53	2,25	219	db	4f
54	57,2	392	43	e2
55	16,4	104	a3	09
56	19,41	1329	51	3d
57	39,41	2729	69	4a
58	27,29	1b1d	c5	87
59	42,23	2a17	3a	76
60	7,44	72c	a9	ab

В результаті пошуку було виявлено чотири колізії алгоритму хешування SHA256, яким відповідають пари секретних ключів 8 і 12, 14 і 52, 18 і 19, 42 і 60; та три колізії алгоритму хешування RIPEMD160, яким відповідають пари секретних ключів 7 і 44, 22 і 54, 32 і 37.

Очевидно, що чим більш вихідне значення хеш-функції, тим складніше знайти випадкову колізію другого роду.

На даному етапі пошук колізій хеш-функцій повного розміру є дуже складною задачею і потребує великий обсяг обчислювальних ресурсів. Проте, стрімкий розвиток обчислювальних технологій, нові методи обчислення, квантові комп'ютери тощо, стають реальною загрозою для надійності хеш-алгоритмів, які використовуються у системі Біткоїн.

4.3 Ризики клієнта у випадку колізій

Як вже зазначалося раніше, модель формування Біткоїн-адреси системи Біткоїн має низку недоліків, які породжують загрозу виникнення колізій Біткоїн-адрес. У даному випадку розглядається ситуація, коли через колізію компрометується вже існуючої Біткоїн-адреса клієнта. Колізії у такому випадку супроводжуються економічними збитками клієнта.

Ризик виникнення колізій Біткоїн-адрес на будь-якому етапі формування відноситься до чистих зовнішніх ризиків.

Процес формування секретних ключів породжує ризикову ситуацію виникнення колізій секретних ключів, і, як наслідок, колізій Біткоїн-адрес. Ризик виникнення колізій на етапі генерації секретних ключів може мати як навмисний або злочинний, так і випадковий характер. Слід також окремо виділити ризик виникнення колізій секретних ключів, спричинений використанням ненадійних програмних рішень, які використовуються у процесі генерації.

Процес формування хешу відкритого ключа породжує ризикову ситуацію виникнення колізій алгоритмів хешування, і, як наслідок, колізій Біткоїн-адрес. Зазвичай ризик колізії алгоритмів хешування має випадковий характер, але теоретично можливі і зловмисні атаки, націлені на утворення колізій хеш-функцій.

У розглянутій ситуації ризикова ситуація передбачає економічні збитки власника адреси, проте доступ до вже існуючої Біткоїн-адреси з іншого боку можна вважати джерелом доходів.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Аналіз потенційних небезпек

Робоче приміщення являє собою офіс, розташований на другому поверсі п'ятиповерхової офісної будівлі. Габарити приміщення складають 7м × 6м × 3м. Площа приміщення складає 42м². У приміщенні знаходиться п'ять робочих місць, обладнаних персональними комп'ютерами.

Основними потенційними небезпеками при роботі в офісі є [13]:

- небезпека ураження електричним струмом, внаслідок недотримання правил електробезпеки або виходу з ладу електроприладів;
- порушення роботи кістково-м'язового апарату внаслідок тривалих статичних навантажень при роботі з ПК.
- нервово-психічні перевантаження внаслідок постійного контакту з клієнтами, колегами по роботі, керівництвом при вирішенні робочих питань, які можуть носити конфліктний характер і призвести до емоційного дискомфорту, внутрішнього роздратування, емоційної нестабільності та захворювань нервової системи;
- незадовільні ергономічні характеристики робочого місця внаслідок нераціонального планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень кістково-м'язового апарату;
- негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;
- негативний вплив незадовільних параметрів повітряного середовища робочої зони на здоров'я працюючого, внаслідок неправильного проектування системи вентиляції або несправності її несправності;
- негативний вплив підвищеного рівня шуму на психоемоційний стан працюючого, який пов'язаний з використанням застарілої периферійної техніки, кондиціонерів, копіювальної техніки, освітлювальних приладів;
- небезпека загоряння у зв'язку із несправністю електричного

обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі;

- неправильні дії персоналу у надзвичайних ситуаціях.

Для створення безпечних і комфортних умов праці були використані нормативно-правові документи: Конституція України, Законодавства України про охорону здоров'я, Основи земельного законодавства України, Закон про трудові колективи, Закон України про охорону праці та ін. Єдиними правилами і нормами, що поширюються на всі галузі народного господарства, є вимоги державних стандартів ССБТ.

5.2 Заходи забезпечення безпеки

Приміщення офісу, в якому перебувають працівники, відносяться до приміщень без підвищеної небезпеки ураження електричним струмом.

Обладнання, що використовується в приміщенні є споживачем електроенергії, що живиться від змінного струму 220 В від мережі з заземленою нейтраллю, та відноситься до електроустановок до 1000В закритого виконання. За способом захисту людини від ураження електричним струмом відповідає згідно з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Вироби електротехнічні. Загальні вимоги безпеки» I (стаціонарні комп'ютери,) та II (освітлювальні прилади, кондиціонери, опалювальні пристрої, ноутбуки, сканери) класу захисту.

Основними причинами ураження персоналу електричним струмом є:

- дотик до струмопровідних частин, що знаходяться під напругою (оголені кабелі живлення, розетки 220В);
- дотик до металевих не струмопровідних частин після переходу на них напруги з струмоведучих частин.

Згідно «Правилам улаштування електроустановок» (ПУЕ) виконані такі групи заходів з електробезпеки:

Згідно з ГОСТ 12.1.009-76 (1999) «ССБТ. Електробезпека. Терміни та визначення» у приладах II класу захисту використовується подвійна ізоляція -

електрична ізоляція, що складається з робочої і додаткової ізоляції.

Так як згідно з НПАОП 40.1-1.32-01 «Правила улаштування електроустановок. Електрообладнання спеціальних установок» офісні приміщення у більшості своїй відносяться до класу пожежонебезпечної зони П-Па (приміщення, в яких містяться тверді горючі речовини), тому передбачений ступінь захисту ізоляції обладнання IP44.

Згідно з ГОСТ 12.1.030-81 (2001) «ССБТ. Електробезпека. Захисне заземлення, занулення» у приміщенні встановлене занулення, призначене для зменшення часу замикання, та захисне заземлення, яке, згідно з ПУЕ, забезпечує опір не більше 4 Ом.

Експлуатація електроустановок і електроустаткування проводиться відповідно до НПАОП 40.1-1.01-97 «Правила безпечної експлуатації електроустановок» (далі «ПБЕЕ») та НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів».

Розетки марковані попереджувальними мітками з зазначенням напруги (~220 В) згідно з ПБЕЕС 6.11.6.

Проведено навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;

5.3 Заходи щодо виробничої санітарії та гігієни праці

Показники мікроклімату в офісному приміщенні відповідають встановленим санітарно-гігієнічним вимогам ДСН 3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 (1991) «ССБТ. Загальні санітарно-гігієнічні вимоги до повітря робочої зони» і ГН 2152-80 «Санітарно-гігієнічні норми допустимих рівнів іонізації повітря виробничих та громадських приміщень».

Робота в приміщеннях, належать до категорії Іб - легка робота, тому

встановлені наступні оптимальні значення параметрів мікроклімату:

- у холодний період року: температура 21-23°; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с;
- у теплий період року: температура 22-24°; відносна вологість: 40-60%; швидкість переміщення повітря: 0,2 м/с;

Дотримання вимог цих документів досягається оснащенням приміщень пристроями кондиціонування і вентиляції, дезодорації повітря, опалювання згідно вимог ДБН В.2.5-67:2013 «Опалення, вентиляція та кондиціонування».

Згідно ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення» в офісних приміщеннях використовується природне та штучне освітлення. Природне освітлення здійснено через світлові прорізи, які забезпечують коефіцієнт природної освітленості (КПО) не нижче 1,5%. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски на поверхні екранів і клавіатури, використовуються сонцезахисні пристрої, на вікнах встановлені жалюзі.

Штучне освітлення в приміщенні здійснено у вигляді комбінованої системи освітлення з використанням люмінесцентних джерел світла у світильниках загального освітлення.

Величина освітленості при штучному освітленні люмінесцентними лампами відповідає в горизонтальній площині не нижче 300 лк - для системи загального освітлення і не нижче 750 лк - для систем комбінованого освітлення згідно з ДБН В.2.5-28-2006.

Проведено розрахунки для системи загального освітлення.

Як джерела загального освітлення використані люмінесцентні лампи типу ЛВП. Ступінь захисту світильників IP 54 (захист від пилу та бризок). Числове значення коефіцієнта світильника $[L/h] = 1.3$.

Розрахунок кількості рядів світильників у приміщенні N_p :

$$N_p = \frac{B}{(H - h_p) \times [L/h]} \quad (5.1)$$

де B – ширина приміщення, м; H – висота приміщення, м; h_p – висота робочої поверхні.

$$\text{Таким чином } N_p = \frac{6}{(3-0,725) \times 1,3} = 2,02 = 2(\text{шт}).$$

Визначення максимально припустимої відстані між рядами світильників L_{max} :

$$L_{max} = \frac{B}{N_p} \quad (5.2)$$

де B – ширина приміщення, м; N_p – кількість рядів світильників у приміщенні, шт.

$$\text{Виходячи з (5.2) } L_{max} = \frac{6}{3} = 2 \text{ (м)}.$$

Розрахунок висоти підвісу світильника над робочою поверхнею h :

$$h = \frac{L_{max}}{[L/h]} \quad (5.3)$$

де L_{max} – максимально припустима відстань між рядами світильників, м; $[L/h]$ – числове значення коефіцієнта світильника.

$$\text{Згідно з (5.3) } h = \frac{2}{1,3} = 1,54(\text{м}).$$

Знаходження висоти звисання світильника зі стелі h_3 :

$$h_3 = H - h_p - h \quad (5.4)$$

де H – висота приміщення, м; h_p – висота робочої поверхні, м; h – висота підвісу світильника над робочою поверхнею, м.

$$\text{Відповідно до (5.4) } h_3 = 0,73(\text{м}).$$

Визначення значення індексу приміщення i , що характеризує співвідношення розмірів освітлювального приміщення і висоти розміщення світильників:

$$i = \frac{A \times B}{h \times (A + B)} \quad (5.5)$$

де A – довжина приміщення, м; B – ширина приміщення, м; h – висота підвісу світильника над робочою поверхнею, м.

Таким чином $i = \frac{7 \times 6}{1,54 \times (7+6)} = 2,09$.

Коефіцієнт використання світлового потоку, створюваного світильниками вибраного типу $\eta=54\%$. Коефіцієнт відбиття стелі $\rho_c = 70\%$, стін $\rho_{ст} = 50\%$ та підлоги $\rho_{п} = 30\%$.

Визначення сумарного світлового потоку освітлювальної установки у даному приміщенні Φ_{Σ} . Для офісного приміщення коефіцієнт запасу приймається рівним $k_z = 1.5$. Коефіцієнт нерівномірності освітлення $z = 1.1$. У приміщенні розміром $6\text{м} \times 7\text{м} \times 3\text{м}$ потрібно створити освітленість $E_n = 300$ лк.

$$\Phi_{\Sigma} = \frac{E_n \times A \times B \times k_z \times z}{\eta} \quad (5.6)$$

де E_n – рівень нормованого загального освітлення, лк; A – довжина приміщення, м; B – ширина приміщення, м; k_z – коефіцієнт запасу; z – коефіцієнт нерівномірності (мінімальної) освітленості; η – коефіцієнт використання світлового потоку.

Відповідно до (5.6) $\Phi_{\Sigma} = \frac{300 \times 7 \times 6 \times 1.5 \times 1.1}{0.54} = 38500(\text{лм})$.

Визначення умовної загальної кількості світильників у приміщенні $N_{св}^*$:

$$N_{св}^* = \frac{A * B}{L_{max}^2} = \frac{7 \times 6}{4} \quad (5.7)$$

де A – довжина приміщення, м; B – ширина приміщення, м; L_{max} –

максимально припустима відстань між рядами світильників, м. Результат округлений до цілого значення, кратного кількості рядів N_p .

Таким чином $N_{cb}^* = 10,5 = 10$ (шт).

Розрахунок світлового потоку умовного джерела світла $\Phi_{л}^*$:

$$\Phi_{л}^* = \frac{\Phi_{\Sigma}}{N_{cb}^* \times n} \quad (5.8)$$

де Φ_{Σ} – сумарний світловий потік освітлювальної установки, лм; $n=2$ – кількість ламп у світильнику, шт; N_{cb}^* - умовна загальна кількість світильників у приміщенні.

$$\text{Згідно з (5.8)} \quad \Phi_{л}^* = \frac{38500}{10 \times 2} = 1925 \text{ (лм)}$$

Вибір типу стандартної лампи з найближчим значенням фактичного світлового потоку лампи $\Phi_{л}$, і знаходження коефіцієнту m (співвідношення між розрахунковим світловим потоком лампи $\Phi_{л}^*$ та фактичним світловим потоком вибраної стандартної лампи $\Phi_{л}$):

Тип лампи - ЛТБ потужністю 30Вт.

$$m = \frac{\Phi_{л}^*}{\Phi_{л}} \quad (5.9)$$

$$\text{Таким чином } m = \frac{1925}{1880} = 1,02.$$

Визначення оптимальної (фактичної) кількості світильників у приміщенні N_{cb} :

$$N_{cb} = N_{cb}^* \times m \quad (5.10)$$

де N_{cb}^* – умовна загальна кількість світильників у приміщенні, шт. m – співвідношення між розрахунковим світловим потоком лампи та фактичним світловим потоком вибраної стандартної лампи. Результат округлений до

цілого значення, кратного кількості рядів N_p .

Виходячи з (5.10) $N_{св} = 10 \times 1,02 = 10,2 = 10$ (шт)

Розрахунок загальної потужності освітлювальної установки P_{Σ} :

$$P_{\Sigma} = N_l \times P_l \quad (5.11)$$

де N_l – фактична кількість ламп у приміщенні, P_l - потужність однієї лампи.

Відповідно до (5.11) $P_{\Sigma} = 20 \times 30 = 600$ (Вт)

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях у приміщення не перевищують 45-50 дБ згідно ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» та ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

Вібрація (загальна) обладнання не перевищує гранично допустимих величин, встановлених Санітарними нормами вібрації робочих місць № 3044-84.

Для запобігання статистичного навантаження при користуванні ПК використовуються перерви в роботі 10 хв. через кожні дві години.

Загальні ергономічні вимоги встановлено ДСТУ ISO 9241-1:2003 «Ергономічні вимоги до роботи з відео терміналами в офісі. Частина 1. Загальні положення».

При організації робочих місць дотримані наступні вимоги:

- висота клавіатури від підлоги – 65-75 см;
- наявність ергономічних і зручних миші і клавіатури;
- можливість регулювання висоти і нахилу клавіатури (відстань від поверхні стола до середини клавіатури – не більше 30 мм, кут підйому клавіатури – від 2° до 15°);
- наявність у клавіатури підставки для рук;

- наявність килимка для миші з захистом від тунельного синдрому (спеціальний виступ забезпечує правильне положення кисті);
- наявність стільця або крісла з підлокітниками;
- наявність у стільця можливості регулювання висоти та куту нахилу спинки;
- ергономічна форма спинки для підтримки правильного положення спини при сидінні;

Для запобігання нервового напруження організоване правильне робоче місце, правильне робоче положення, ритм роботи, раціоналізовано трудовий процес, використовуються емоційні стимули, впроваджено раціональні режими праці і відпочинку тощо.

Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» є неприпустимим розташування приміщень, призначених для роботи з відео дисплейними терміналами (ВДТ) у підвалах та цокольних поверхах. Також забороняється розташування вибухонебезпечних приміщень категорії А і Б (НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною безпеки») та виробництв з мокрими технологічними процесами поряд з приміщенням, де розташовуються ЕОМ (ПЕОМ), а також над такими приміщеннями, або під ними. Окрім того, виробничі приміщення для роботи з ВДТ не повинні межувати з приміщеннями, у яких рівень шуму і вібрації перевищує допустимі значення.

Оскільки площа приміщення становить 42м², а площа, на якій розташовується одне робоче місце з ВДТ, відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» повинна становити не менше 6м², то в даному приміщенні можна розмістити щонайбільше 7 комп'ютеризованих робочих місць.

Відповідно до вимог ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-

обчислювальних машин» мінімальний об'єм приміщення на одне робоче місце з ВДТ становить 20м^3 . Об'єм приміщення становить 126м^3 , а об'єм, що припадає на одне комп'ютеризоване робоче місце - $25,2\text{м}^3$. Таким чином норматив щодо об'єму приміщення на одне робоче місце з ВДТ виконується.

Планування розміщення комп'ютеризованих робочих місць у приміщенні проведено із врахуванням наступних вимог:

- робочі місця з ВДТ розміщені на відстані не менше 1 м від стіни зі світловими прорізами;
- відстань між бічними поверхнями ВДТ складає не менше за 1,2 м;
- відстань між тильною поверхнею одного ВДТ та екраном іншого не менша за 2,5 м;
- прохід між рядами робочих місць не менший 1 м.

Відповідно до НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин» рекомендовані розміри столу для робочого місця з ВДТ становлять: висота – 725 мм, ширина – 600-1400 мм, глибина – 800-1000 мм. Встановлені робочі столи мають такі розміри: висота - 725 мм, ширина – 1200 мм, глибина – 800 мм.

Комп'ютеризовані робочі місця розміщено рядами вздовж стіни з вікнами. Це дає змогу унеможливити дзеркальне відбиття на екрані ВДТ джерел природного світла (вікон) та потрапляння останніх у поле зору операторів, що погіршує умови їх зорової роботи.

5.4 Заходи з пожежної безпеки

Закон України «Про пожежну безпеку» визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності.

Пожежна безпека – стан об'єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвиток пожежі і впливу

на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей [13].

Для забезпечення пожежної безпеки в приміщенні проведено пожежну профілактику, яка включає в себе комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження її поширення, а також на створення умов для успішного гасіння пожежі.

Для ліквідації пожежі у початковій стадії її розвитку силами персоналу об'єктів застосовуються первинні засоби пожежогасіння. До них відносяться: вогнегасники, пожежний інвентар (покривала з негорючого теплоізоляційного полотна, ящики з піском, пожежні відра, совкові лопати, лом, сокири тощо), системи автоматичного пожежогасіння.

Первинні засоби пожежогасіння, в залежності від категорії приміщень, можуть розташовуватись як окремо, так і в складі пожежних щитів

Залежно від агрегатного стану й особливостей горіння різних горючих речовин і матеріалів пожежі за ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва» поділяються на відповідні класи

В офісному приміщенні знаходиться дерев'яні меблі, електронна апаратура, паперові носії інформації.

Клас пожежі у офісному приміщенні (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») – пожежі твердих речовин, переважно органічного походження, горіння яких визначається як – супроводжується тлінням (деревина, пластмаси, папір) клас А та клас Е – займання електроустановок під напругою. Категорія приміщення (згідно із НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою») – визначається як категорії П-Па.

Визначення типу та розрахунок кількості первинних засобів пожежогасіння: (згідно із ДБН В.1.1.7-2002 «Захист від пожежі. Пожежна безпека об'єктів будівництва») – для офісного приміщення площею 42м²

категорій пожежонебезпеки А та Е застосовується 2 порошкових вогнегасника типу ВП-5, а також вуглецевий вогнегасник ВВ-5 (ВВК-5) (НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою», ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва»).

Згідно з ДБН В.2.5-56:2014 «Системи протипожежного захисту» у приміщенні встановлені чотири комбінованих оптично-теплових датчика СПД-3.5. У разі спрацювання сигнал тривоги подається на ППКП і передається на звукові і світлові сповіщувачі будівлі.

Згідно з ДБН В.1.1-7-2002. "Пожежна безпека об'єктів будівництва" на випадок пожежі передбачені шляхи евакуації працюючих - проходи, проїзди, евакуаційні виходи. Два евакуаційні виходи розташовані розсереджено. Коридори і проходи, призначені для евакуації, мають якомога меншу довжину і мінімальна кількість поворотів. На всьому протязі проходу немає порогів або проміжних ступенів.

Згідно з п. 13 "Рекомендацій по складанню планів евакуації людей на випадок пожежі" план евакуації розміром формату А4 розміщено на видному місці під склом (плівкою).

Згідно з НАПБ Б.02.005-2003 "Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України" працівники пройшли інструктаж з пожежної безпеки та ознайомлені з евакуаційними заходами при пожежі.

5.5 Заходи забезпечення безпеки у надзвичайних ситуаціях

Організація навчання працюючого та не працюючого населення діям у надзвичайних ситуаціях проводиться відповідно до статті 39 Цивільного кодексу України, а також відповідної постанови Кабінету Міністрів України від 26 червня 2013 р. № 444 [14].

1. Порядок здійснення навчання населення діям у надзвичайних ситуаціях визначає механізм організації навчання населення діям у надзвичайних ситуаціях (далі - навчання населення), його структуру, види та форми.

2. Навчання населення здійснюється:

- за місцем роботи - працюючого населення;
- за місцем навчання - дітей дошкільного віку, учнів та студентів;
- за місцем проживання - непрацюючого населення.

3. Організація навчання населення покладається:

- для працюючого та непрацюючого населення - на ДСНС, Раду міністрів Автономної Республіки Крим, місцеві державні адміністрації, органи місцевого самоврядування;
- дітей дошкільного віку, учнів та студентів - на МОН.

4. Навчально-методичне забезпечення навчання населення здійснюється ДСНС разом з МОН.

5. Навчання населення складається з:

- навчання безпосередньо на підприємствах, в установах та організаціях;
- навчання за межами підприємств, установ та організацій керівного складу і фахівців з питань цивільного захисту та пожежної безпеки;
- практичної підготовки під час проведення спеціальних об'єктових навчань і тренувань з питань цивільного захисту;
- навчання під час здобуття відповідного освітнього рівня у навчальних закладах системи освіти;
- самостійного вивчення інформації про дії в умовах надзвичайних ситуацій.

6. Навчання працюючого населення здійснюється безпосередньо на підприємстві, в установі та організації згідно з програмами підготовки працівників до дій у надзвичайних ситуаціях, а також під час проведення

спеціальних об'єктових навчань і тренувань з питань цивільного захисту.

7. Програми підготовки працівників до дій у надзвичайних ситуаціях розробляються і затверджуються підприємствами, установами, організаціями на підставі програм та організаційно-методичних вказівок з підготовки населення до дій у надзвичайних ситуаціях, що розробляються і затверджуються ДСНС, Радою міністрів Автономної Республіки Крим, місцевими державними адміністраціями, органами місцевого самоврядування.

Програми навчання з питань пожежної безпеки погоджуються із ДСНС.

8. Програми підготовки працівників до дій у надзвичайних ситуаціях поділяються на:

- загальної підготовки працівників підприємств, установ та організацій;
- спеціальної підготовки працівників, що входять до складу спеціалізованих служб і формувань цивільного захисту;
- додаткової підготовки з техногенної безпеки працівників об'єктів підвищеної небезпеки;
- пожежно-технічного мінімуму для працівників, зайнятих на роботах з підвищеною пожежною небезпекою;
- прискореної підготовки працівників до дій в особливий період.

9. Підготовка працівників до дій у надзвичайних ситуаціях передбачає вивчення та поглиблення знань:

- дії у надзвичайних ситуаціях;
- цивільний захист;
- техногенна безпека працівників об'єктів підвищеної небезпеки;
- пожежна безпека;
- способи захисту від наслідків надзвичайних ситуацій.

10. Навчання працівників на підприємстві, в установі та організації здійснюється шляхом курсового навчання, індивідуального навчання та

шляхом проведення інструктажів за програмою загальної підготовки працівників, які проводяться особами з питань цивільного захисту, призначеними в межах штатної чисельності суб'єкта господарювання.

12. З метою належної організації навчального процесу, забезпечення послідовності теоретичного і практичного навчання на підприємствах, в установах та організаціях розробляються і ведуться планувальні, облікові та звітні документи.

13. Для отримання працівниками відомостей про конкретні дії у надзвичайних ситуаціях на підприємстві, в установі та організації обладнується з урахуванням особливостей виробничої діяльності інформаційно-довідковий куточок з питань цивільного захисту.

14. Особи, що залучаються підприємствами, установами та організаціями (в тому числі на умовах договору) до проведення інструктажів, навчання і перевірки знань з питань цивільного захисту, пожежної та техногенної безпеки, зобов'язані пройти спеціальну підготовку на територіальних курсах, у навчально-методичних центрах цивільного захисту та безпеки життєдіяльності відповідно до вимог типового положення про них.

15. Навчання керівного складу підприємств, установ та організацій і фахівців, діяльність яких пов'язана з організацією і здійсненням заходів з питань цивільного захисту, здійснюється в установленому законодавством порядку.

16. Особи у разі прийняття на роботу та працівники щороку за місцем роботи проходять інструктаж з питань цивільного захисту, пожежної безпеки та дій у надзвичайних ситуаціях.

17. Спеціальні об'єктові навчання і тренування з питань цивільного захисту проводяться у порядку, затвердженому МВС.

18. Навчання працюючого населення здійснюється у робочий час за рахунок коштів підприємств, установ та організацій.

19. Організація навчання дітей дошкільного віку, учнів та студентів здійснюється МОН згідно із затвердженими ним і погодженими з ДСНС

навчальними програмами з вивчення заходів безпеки, способів захисту від впливу небезпечних факторів, викликаних надзвичайними ситуаціями, надання домедичної допомоги.

20. Підготовка студентів вищих навчальних закладів до дій у надзвичайних ситуаціях здійснюється за нормативними навчальними дисциплінами “Безпека життєдіяльності” та “Цивільний захист”.

21. Підготовка учнів загальноосвітніх та професійно-технічних навчальних закладів до дій у надзвичайних ситуаціях, що передбачає здобуття знань і вмінь з питань особистої безпеки в умовах загрози та виникнення надзвичайної ситуації, користування засобами захисту від її наслідків, вивчення правил пожежної безпеки та основ цивільного захисту, здійснюється в рамках вивчення предметів “Основи здоров’я” та “Захист Вітчизни”.

22. Навчально-виховна робота з дітьми дошкільного віку проводиться згідно з вимогами базового компонента дошкільної освіти і спрямовується на формування достатнього та необхідного рівня знань і умінь дитини для безпечного перебування в навколишньому середовищі, елементарних норм поведінки у надзвичайних ситуаціях і запобігання пожежам від дитячих пустощів з вогнем.

23. З метою координації науково-методичної діяльності, узагальнення і поширення ефективних форм і методів організації навчально-виховного процесу з питань безпеки життєдіяльності та цивільного захисту визначаються:

- МОН - базові за галуззю знань кафедри з безпеки життєдіяльності у вищих навчальних закладах;
- місцевими органами управління освіти - територіальні базові (опорні) загальноосвітні та дошкільні навчальні заклади.

24. Позашкільна освітня робота з питань формування культури безпеки життєдіяльності серед дітей та молоді, формування здорового способу життя, оволодіння ними навичками самозахисту і рятування проводиться у позашкільних закладах, а також шляхом організації шкільних, районних (міських), обласних та всеукраїнських змагань з безпеки життєдіяльності.

25. МОН здійснює контроль і бере участь у моніторингу якості підготовки у навчальних закладах дітей дошкільного віку, учнів та студентів з питань навчання діям у надзвичайних ситуаціях.

26. Навчання дітей дошкільного віку, учнів та студентів здійснюється під час навчально-виховного процесу за рахунок коштів, передбачених для фінансування навчальних закладів.

27. Навчання непрацюючого населення діям у надзвичайних ситуаціях здійснюється шляхом проведення інформаційно-просвітницької роботи за місцем проживання та самостійного вивчення загальної програми навчання населення діям у надзвичайних ситуаціях та інших інформаційно-довідкових матеріалів з питань цивільного захисту, правил пожежної безпеки у побуті та громадських місцях.

28. Інформаційно-просвітницька робота з питань поведінки в умовах надзвичайних ситуацій організовується місцевими органами виконавчої влади та органами місцевого самоврядування, в тому числі через утворені при них консультаційні пункти, та передбачає:

- інформування населення про методи реагування у разі виникнення надзвичайних ситуацій;
- створення в консультаційних пунктах умов для оволодіння громадянами навичками користування найбільш поширеними засобами захисту і надання першої само- та взаємодопомоги.

29. Для задоволення потреби у самостійному вивченні загальної програми навчання населення діям у надзвичайних ситуаціях місцеві органи виконавчої влади та органи місцевого самоврядування за методичного супроводження територіальних курсів, навчально-методичних центрів цивільного захисту та безпеки життєдіяльності видають навчальні, навчально-наочні посібники, брошури, розповсюджують інформаційні матеріали, буклети тощо.

Інформаційно-просвітницька робота з населенням щодо правил поведінки в умовах надзвичайних ситуацій проводиться шляхом запровадження

постійних рубрик у засобах масової інформації, зокрема друкованих, а також за допомогою інформаційно-комунікаційних технологій, аудіовізуальних та інтерактивних засобів та соціальної реклами.

Непрацююче населення має право отримувати від органів державної влади та органів місцевого самоврядування відомості про надзвичайні ситуації, у зоні яких або у зоні можливого ураження від яких може опинитися місце проживання непрацюючих громадян, а також про способи захисту від впливу небезпечних факторів, викликаних такими ситуаціями.

30. Пропаганда знань серед населення щодо власної та колективної безпеки у разі виникнення надзвичайної ситуації здійснюється за сприяння громадських організацій.

6 ДІАГНОСТИКА ЕКОНОМІЧНОГО РИЗИКУ ВИКОРИСТАННЯ СИСТЕМИ БІТКОІН

Використання системи Біткоін пов'язане з низкою ризиків, які можуть стати джерелом як економічних збитків, так і додаткових доходів. Незважаючи на відкритість і досить високу надійність, система Біткоін має певні недоліки і вразливості, які є загрозою і причиною виникнення економічних ризиків.

Економічний ризик — це об'єктивно-суб'єктивна категорія у діяльності суб'єктів господарювання, що пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору. Вона відображає міру (ступінь) відхилення від цілей, від бажаного (очікуваного) результату, міру невдачі (збитків) з урахуванням впливу керованих і некерованих чинників, прямих та зворотних зв'язків стосовно об'єкта керування [15].

У явищі «ризик» виділяють наступні основні елементи, взаємозв'язок яких і становить його сутність:

- можливість відхилення від передбачуваної мети, заради якої здійснювалася обрана альтернатива;
- ймовірність досягнення бажаного результату;
- відсутність впевненості в досягненні поставленої мети;
- можливість матеріальних, моральних та інших втрат, пов'язаних із здійсненням обраної в умовах невизначеності альтернативи.

6.1 Види ризиків

Найбільш важливими елементами, покладеними в основу класифікації ризиків, є:

- час виникнення;
- основні чинники виникнення;
- характер обліку;
- характер наслідків;

– сфера виникнення і ін.

За часом виникнення ризику розподіляються на ретроспективні, поточні та перспективні. Аналіз ретроспективних ризиків, їх характеру і способів зниження дає можливість більш точно прогнозувати поточні і перспективні ризики.

За чинниками виникнення ризику підрозділяються на політичні і економічні [15].

Політичні ризики - це ризики, зумовлені зміною політичної обстановки, що впливає на підприємницьку діяльність (закриття кордонів, заборона на вивезення товарів в інші країни, військові дії на території країни та ін.).

Політичні ризики поділяються на державний, валютний, податковий ризики та ризик форс-мажорних обставин.

Державні ризики безпосередньо пов'язані з інтернаціоналізацією підприємницької діяльності. Вони актуальні для всіх учасників зовнішньоекономічної діяльності і залежать від політико-економічної стабільності країн - імпортерів, експортерів. Причинами державного ризику можуть бути нестабільність державної влади, особливості державного устрою та законодавства, неефективна економічна політика, що проводиться урядом, етнічні та регіональні проблеми, різка поляризація інтересів різних соціальних груп і тощо. На результати підприємницької діяльності можуть впливати державне торгове і валютне регулювання, квотування, ліцензування, зміна митних зборів і багато іншого.

Валютний ризик полягає в можливості фінансових втрат суб'єктів валютного ринку в результаті довгострокових і короткострокових коливань валютних курсів, які залежать від попиту і пропозиції на валюту на національних і міжнародних валютних ринках.

Податковий ризик полягає в можливості фінансових втрат в результаті зміни податкової політики (поява нових податків, ліквідація або скорочення податкових пільг і т.п.), а також зміни величини податкових ставок.

Ризик форс-мажорних обставин - обставин непереборної сили, які неможливо ні запобігти, ні усунути будь-якими заходами. До таких обставин відносяться стихійні лиха (природні катастрофи), повені, землетруси, шторми та інші кліматичні катаклізми, війни, революції, путчі, страйки і т.п., які заважають підприємцю здійснювати свою діяльність.

Економічні ризики - це ризики, обумовлені несприятливими змінами в економіці підприємства або в економіці країни.

Економічні ризики поділяються на організаційні, ресурсні, портфельні, кредитні та інноваційні.

Організаційний ризик - ризик, обумовлений недоліками в організації роботи.

Ресурсний ризик полягає в можливості появи втрат в результаті відсутності запасу міцності по ресурсам в разі зміни ситуації, в якій здійснюється підприємницька діяльність (зміна оплати праці, зміни мит і податків, розкрадання, підвищений брак, псування товарів і матеріалів, зриви поставок, зміна вимог до ведення підприємницької діяльності та ін.).

Портфельний ризик. В процесі функціонування будь-якої фірми доводиться вирішувати важке завдання визначення розміру та сфери застосування інвестицій. Таке завдання виникає при наявності у фірми або окремого підприємця вільних коштів.

Кредитний ризик, або ризик неповернення боргу, - це ризик несплати позичальником основного боргу і відсотків по ньому у відповідності з термінами і умовами кредитного договору.

Інноваційний ризик пов'язаний з фінансуванням і застосуванням науково-технічних нововведень. Оскільки витрати і результати науково-технічного прогресу розтягнуті і віддалені в часі, вони можуть бути передбачені лише в деяких, зазвичай широких межах. Інноваційний ризик полягає в можливості втрат, що виникають при фінансуванні підприємцем (фірмою) розробки нової техніки і технологій, розробки нових товарів і послуг,

а також інших інновацій, які не знайдуть передбачуваного попиту на ринку і не принесуть очікуваного ефекту.

За характером обліку ризику діляться на зовнішні і внутрішні.

До зовнішніх відносяться ризики, безпосередньо не пов'язані з діяльністю підприємства або його контактної аудиторії. На рівень зовнішніх ризиків впливає дуже велика кількість факторів - політичні, економічні, демографічні, соціальні, географічні та ін.

До внутрішніх відносяться ризики, обумовлені діяльністю самого підприємства і його контактної аудиторії. На їх рівень впливає ділова активність керівництва підприємства, вибір оптимальної маркетингової стратегії, політики і тактики та інші фактори: виробничий потенціал, технічне оснащення, рівень спеціалізації, рівень продуктивності праці, техніки безпеки.

За характером наслідків ризику підрозділяються на чисті і спекулятивні.

Чисті ризики (прості, статичні) характеризуються тим, що вони практично завжди несуть в собі втрати для підприємницької діяльності.

Причинами чистих ризиків можуть бути стихійні лиха, війни, нещасні випадки, злочинні дії, недієздатність організації та багато іншого.

Спекулятивні ризики (динамічні, комерційні) характеризуються тим, що вони можуть нести в собі як втрати, так і додатковий прибуток для підприємця по відношенню до очікуваного результату.

Причинами спекулятивних ризиків можуть бути зміна кон'юнктури ринку, зміна курсів валют, зміна податкового законодавства та ін.

За сферою виникнення ризику поділяються на виробничі, комерційні, фінансові та страхові [16].

Виробничий ризик пов'язаний з невиконанням підприємством своїх планів і зобов'язань по виробництву продукції, товарів, послуг, інших видів виробничої діяльності в результаті несприятливого впливу зовнішнього середовища, а також неадекватного використання нової техніки і технологій, основних і оборотних фондів, сировини, робочого часу.

Серед найбільш важливих причин виникнення виробничого ризику - можливе зниження передбачуваних обсягів виробництва, зростання матеріальних і / або інших витрат, сплата підвищених відрахувань та податків, низька дисципліна поставок, загибель або пошкодження обладнання тощо.

Комерційний ризик - ризик, що виникає в процесі реалізації товарів і послуг, вироблених або закуплених підприємцем.

Причинами комерційного ризику є: зниження обсягу реалізації внаслідок зміни кон'юнктури чи інших обставин, підвищення закупівельної ціни товарів, втрати товару в процесі обігу, підвищення витрат обігу та ін.

Фінансовий ризик пов'язаний з можливістю невиконання фірмою своїх фінансових зобов'язань. Основними причинами фінансового ризику є: знецінення інвестиційно-фінансового портфеля внаслідок зміни валютних курсів, нездійснення платежів; війни, заворушення, катастрофи тощо

Страховий ризик - ризик настання передбаченого умовами страхування події, в результаті чого страховик зобов'язаний виплатити страхове відшкодування (страхову суму). результатом ризику є збитки, викликані неефективною страховою діяльністю як на етапі, що передуює укладенню договору страхування, так і на наступних етапах - перестраховування, формування страхових резервів і т.п. основними причинами страхового ризику є: неправильно певні страхові тарифи, азартна методологія страхувальника; війни, заворушення, катастрофи тощо

6.2 Ризик використання системи Біткоїн у економічній діяльності підприємства

Система Біткоїн є дуже гнучким інструментом, який має багато застосувань. Однією з базових функцій, які надає система, є проведення розрахунків. Проте, Біткоїн також може використовуватись як засіб зберігання грошових коштів підприємства, або навіть як джерело інвестицій.

Найбільш детальну картину у досліджуваній ситуації дає класифікація ризиків за чинниками виникнення.

Основними джерелами виникнення ризиків, пов'язаних з використанням системи Біткоїн є:

- суперечливий правовий статус системи Біткоїн (використання, ліцензування, оподаткування);
- втрата реквізитів гаманців або унеможливлення доступу до коштів Біткоїн-адрес;
- коливання курсу купівлі та продажу біткоїнів, коливання курсу національної валюти;
- компрометація біткоїн-адрес (випадкова або навмисна);

Найбільш вірогідну групу ризиків формує суперечливий правовий статус системи Біткоїн. До неї слід віднести державний ризик (правове регулювання щодо використання платіжних систем, ліцензування певних видів господарської діяльності) та податковий ризик (зміна правил оподаткування, нові види податкових внесків).

Наступну групу ризиків формує загроза втрати реквізитів Біткоїн-гаманців або унеможливлення доступу до коштів Біткоїн-адрес. До неї слід віднести організаційний ризик (реалізація загрози втрати реквізитів Біткоїн-гаманців внаслідок недостатнього рівня організації) ризик форс-мажорних ситуацій (втрата реквізитів для доступу до Біткоїн-гаманців внаслідок непередбачуваних природних катаклізмів), державний ризик (унеможливлення доступу до коштів Біткоїн-адрес внаслідок блокування на державному рівні).

Колівання курсу купівлі та продажу біткоїнів (загальне підвищення або зменшення цінності біткоїнів), а також коливання курсу національної валюти (підвищення або зменшення цінності біткоїнів відносно національної валюти) слід віднести до валютних ризиків. В разі використання системи Біткоїн як джерела інвестування також має місце портфельний ризик. Цю групу також слід класифікувати як спекулятивні ризики, тому що коливання курсів можуть призвести як до витрат, так і до прибутків.

Останню групу ризиків формує загроза компрометації Біткоїн-адрес. Цю групу слід віднести до чистих ризиків. Причиною компрометації Біткоїн адрес можуть стати як випадкові чинники (колізії Біткоїн-адрес), так і навмисні злочинні дії (викрадення реквізитів доступу до Біткоїн-гаманців).

6.3 Оцінка ризику використання системи Біткоїн

Розрахунок вірогідності для більшості з ризиків, пов'язаних з використанням системи Біткоїн, є доволі складною задачею, тому використання чисельних методів розрахунку не є раціональним у даному випадку.

Для оцінки ризику використання системи Біткоїн був обраний метод експертної оцінки.

На першому етапі була сформована група експертів. Для коректності оцінювання розмір експертної групи повинен бути оптимізованим таким чином, щоб думка кожного експерта мала достатню вагу. Виходячи з цієї вимоги, згідно з [16] розмір експертної групи був обраний рівним 5.

На наступному етапі була сформована шкала оцінювання, складені питання і створені анкети (Додаток А).

Таблиця 6.1 - Шкала оцінювання ступеня ризику

Бали	Ступінь ризику
1	мінімальний
2	малий
3	середній
4	високий
5	максимальний

На наступному етапі було проведено опитування експертів. Отримані результати зведено у таблицю.

Таблиця 6.2 - Визначення важливості ризиків

Експерти	Ризики									
	1	2	3	4	5	6	7	8	9	10
1	5	4	3	1	2	4	3	4	2	3
2	3	4	2	2	3	4	2	5	1	1
3	4	3	1	1	2	5	2	4	2	2
4	4	5	2	1	2	4	1	5	2	3
5	5	3	1	1	3	5	2	4	1	3
Сумарний ранг важливості	21	19	9	6	12	22	10	22	8	12

Для оцінки узгодженості дій експертів був використаний коефіцієнт конкординації. Він дозволяє оцінити ступінь узгодженості думок експертів, і, як наслідок, достовірність їх оцінок.

Величина коефіцієнта конкордації може змінюватися в межах від 0 до 1. При $W = 0$ узгодженості немає, тобто зв'язок між оцінками різних експертів відсутня. При $W = 1$ узгодженість думок експертів повна. Згідно з [15] достатнім вважається рівень $W > 0.5$.

Коефіцієнт конкординації розраховується за наступною формулою:

$$W = \frac{\sigma_{\Phi}^2}{\sigma_{\max}^2} \quad (6.1)$$

де σ_{Φ}^2 - фактична дисперсія сумарних (впорядкованих) оцінок, даних експертами; $\sigma_{\max}^2$ - дисперсія сумарних (впорядкованих) оцінок у випадку, коли думки експертів повністю збігаються.

При повністю узгодженому думці експертів кожен з них оцінив би: Ризик1 - 4 бали; Ризик2 - 4 бали; Ризик3 - 2 бали; Ризик4 - 1 бал; Ризик5 - 2 бали; Ризик6 - 4 бали; Ризик7 - 2 бали; Ризик8 - 4 бали; Ризик9 - 2 бали; Ризик10 - 2 бали;. В цьому випадку сумарний ранг важливості ризиків склав би відповідно 20, 20, 10, 5, 10, 20, 10, 20, 10, і 10 балів.

Відомо, що середнє значення сумарної оцінки для m об'єктів, що призначаються n експертами, складає $1/2 \cdot n (m + 1)$, і в даному випадку середнє значення становить 27.

$$\begin{aligned} \text{Тоді:} \quad \sigma_{\phi}^2 &= (21 - 27)^2 + (19 - 27)^2 + (9 - 27)^2 + (6 - 27)^2 + \\ &+ (12 - 27)^2 + (22 - 27)^2 + (10 - 27)^2 + (22 - 27)^2 + (8 - 27)^2 + (12 - \\ &27)^2 = 36 + 64 + 324 + 441 + 225 + 25 + 289 + 25 + 361 + 225 = 2015; \end{aligned}$$

$$\begin{aligned} \sigma_{max}^2 &= (20 - 27)^2 + (20 - 27)^2 + (10 - 27)^2 + (5 - 27)^2 + (10 - 27)^2 + \\ &+ (20 - 27)^2 + (10 - 27)^2 + (20 - 27)^2 + (10 - 27)^2 + (10 - 27)^2 = 49 + 49 + \\ &289 + 484 + 289 + 49 + 289 + 49 + 289 + 289 = 2125; \end{aligned}$$

$$W = \frac{2015}{2125} = 0,95;$$

Таким чином, думки експертів можна вважати достатньо узгодженими.

Спираючись на експертну оцінку робимо висновок, що найбільш важливими є державний, податковий, валютний та портфельний ризики. Усі інші ризики мають значно менший ранг важливості, однак їх також необхідно враховувати.

Вивчення вірогідності виникнення ризиків стало фундаментом побудови шкали оцінки ступеня ризику ординального (стратифікаційного) типу, на якій градацію здійснено за допомогою ординальних чисел.

Побудова шкали оцінки ступеня ризику ґрунтувалась на авторському розумінні поняття ризику, як діяльності, пов'язаної з подоланням невизначеності в ситуації неминучого вибору, в процесі якої є можливість кількісно і якісно оцінити ймовірність досягнення передбачуваного результату, невдачі і відхилення від мети.

Ординальним числом визнано ступінь ризику. За його рівнем та вірогідністю виникнення загроз здійснено стратифікацію рівнів ризику: безпечний рівень, рівень керованих загроз, небезпечний рівень, рівень некерованих та критичний рівень (рисунок 6.1).

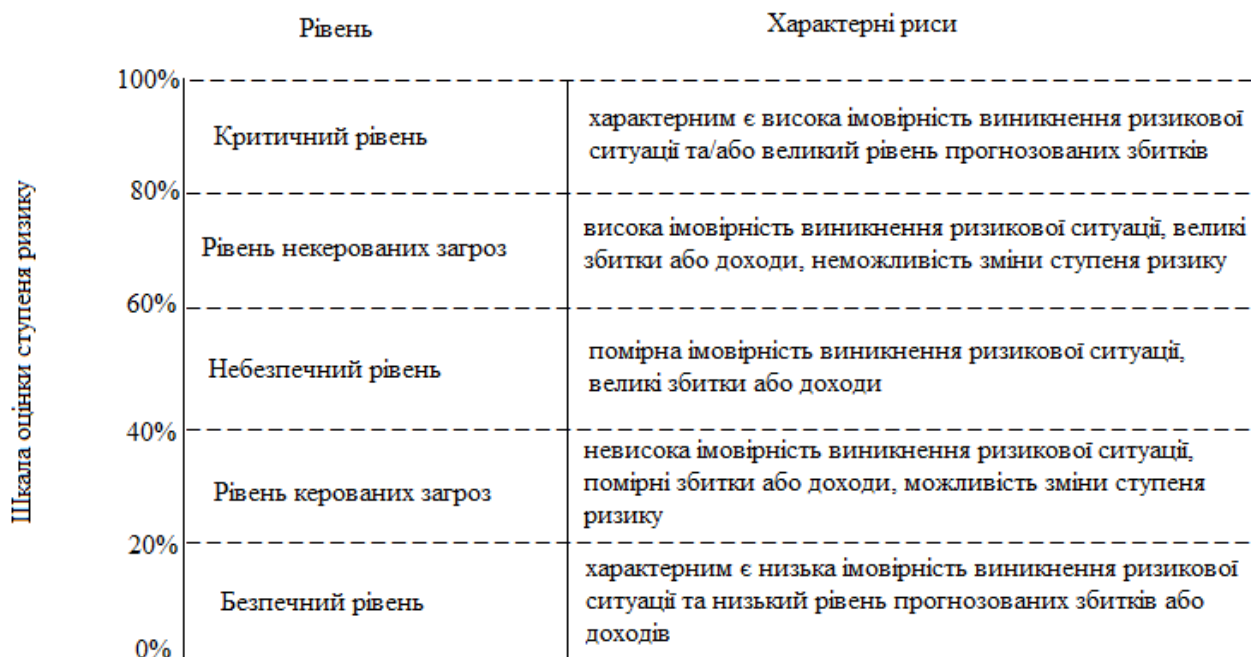


Рисунок 6.1 - Шкала оцінки ступеня ризику за рівнями

Спираючись на експертні оцінки і виходячи зі шкали оцінки ступеня ризику робимо висновок про високу ризикованість використання системи Біткоїн. Частина ризиків має низьку імовірність виникнення, невеликий рівень прогнозованих збитків та можливість зниження ступеню ризику. Проте більшість розглянутих ризиків мають досить високу імовірність виникнення, великий рівень прогнозованих збитків та є зовнішніми, тобто ефективно використання процедур по зниженню ступеня ризику найчастіше не є можливим.

ВИСНОВКИ

У роботі був досліджений метод ідентифікації користувачів у системі Біткоїн, виділені основні вимоги, що висуваються до Біткоїн-адрес. Проаналізований механізм вибору секретних і генерації відкритих ключів, основні формати їх подання. Розглянуті методи зберігання цифрових ключів у Біткоїн-гаманцях.

Досліджена схема перетворення відкритого ключа у Біткоїн-адресу і проведено повне поетапне моделювання формування Біткоїн-адреси. Проаналізовано процес формування Біткоїн-адреси і виділені основні недоліки моделі, що використовується.

Проведені розрахунки імовірності виникнення колізій секретних ключів і алгоритмів хешування, що використовуються у системі Біткоїн. Проведено пошук колізій хеш-функцій при малих значеннях параметрів.

СПИСОК ЛІТЕРАТУРИ

1. Arvind Narayanan Bitcoin and Cryptocurrency Technologies [Електронний ресурс] / Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. - Режим доступу: <http://www.uio.no/studier/emner/matnat/ifi/IN5420/v18/timeplan/resources/bitcoin-and-cryptocurrency-techniques.pdf>
2. Andreas M. Antonopoulos Mastering Bitcoin [Електронний ресурс] / Antonopoulos A. M. - Режим доступу: <https://github.com/bitcoinbook/bitcoinbook>
3. Marek Palatinus bip-0039 [Електронний ресурс] / Palatinus M., Rusnak P., Voisine A., Bowe S. - Режим доступу: <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki>
4. Pieter Wuille bip-0032 [Електронний ресурс] / Wuille P. - Режим доступу: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>
5. Certicom Research Standards for Efficient Cryptography 2 (SEC 2): Recommended Elliptic Curve Domain Parameters [Електронний ресурс] / Certicom Research - Режим доступу: <http://www.secg.org/sec2-v2.pdf>
6. Mike Caldwell bip-0038 [Електронний ресурс] / Caldwell M., Voisine A. - Режим доступу: <https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki>
7. Greg Walker Public Key [Електронний ресурс] / Walker G. - Режим доступу: <http://learnmeabitcoin.com/glossary/public-key>
8. Greg Walker Base58 [Електронний ресурс] / Walker G. - Режим доступу: <http://learnmeabitcoin.com/glossary/base58>
9. Gavin Andresen bip-0016 [Електронний ресурс] / Andersen G. - Режим доступу: <https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki>
10. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Nakamoto S. - Режим доступу: <https://bitcoin.org/bitcoin.pdf>
11. Justin Tormey Blockchain Wallet API [Електронний ресурс] / Walker G. - Режим доступу: <https://github.com/blockchain/service-my-wallet-v3>

12. Shafi Goldwasser Lecture Notes on Cryptography [Електронний ресурс] / Shafi G., Mihir B. - Режим доступу: <http://cseweb.ucsd.edu/~mihir/papers/gb.pdf>
13. Катренко Л.А., Кіт Ю.В., Пістун І. П. Охорона праці. Курс лекцій. Практикум: Навч. посіб. – Суми: Університетська книга, 2009. – 540 с.
14. Постанова Кабінету Міністрів України від 26 червня 2013 р. № 444 [Електронний ресурс] / - Режим доступу: <http://zakon.rada.gov.ua/laws/show/444-2013-п>
15. Гранатуров В. Экономический риск: сущность, методы измерения, пути снижения: Учебное пособие/ В.М. Гранатуров. - М.: Дело и Сервис, 2002. - 208с.
16. Тэпман Л. Риски в экономике: Учебное пособие для вузов/ Л.М. Тэпман - М.: Юнити, 2002. - 380с.

Додаток А

Анкета для оцінки ризику використання системи Біткоїн

Використання системи Біткоїн пов'язане з низкою ризиків, які можуть стати джерелом як економічних збитків, так і додаткових доходів. Незважаючи на відкритість і досить високу надійність, система Біткоїн має певні недоліки і вразливості, які є загрозою і причиною виникнення економічних ризиків.

При оцінці важливості ризиків використовується п'ятибальна шкала від одного до п'яти:

- 1-мінімальний ризик;
- 2-малий ризик;
- 3-середній ризик;
- 4-високий ризик;
- 5-максимальний ризик;

При оцінці ризиків слід враховувати як ступінь імовірності, так і ступінь тяжкості наслідків.

Шановний експерте, просимо вас відповісти на приведені нижче питання. Будь ласка, обведіть найбільш відповідну, на вашу думку, оцінку.

- 1) Оцініть ступінь важливості державного ризику (Ризик 1), пов'язаного з суперечливим правовим статусом системи Біткоїн (правове регулювання щодо використання платіжних систем, ліцензування певних видів господарської діяльності).

1 2 3 4 5

- 2) Оцініть ступінь важливості податкового ризику (Ризик 2), пов'язаного з суперечливим правовим статусом системи Біткоїн (зміна правил оподаткування, нові види податкових внесків)

1 2 3 4 5

3) Оцініть ступінь важливості організаційного ризику (Ризик 3), пов'язаного з можливістю втрати реквізитів Біткоїн-гаманців, (реалізація загрози втрати реквізитів Біткоїн-гаманців внаслідок недостатнього рівня організації роботи з системою Біткоїн).

1 2 3 4 5

4) Оцініть ступінь важливості ризику форс-мажорних ситуацій (Ризик 4), пов'язаного з можливістю втрати реквізитів Біткоїн-гаманців, (втрата реквізитів для доступу до Біткоїн-гаманців внаслідок непередбачуваних природних катаклізмів).

1 2 3 4 5

5) Оцініть ступінь важливості державного ризику (Ризик 5), пов'язаного з унеможливленням доступу до коштів Біткоїн-адрес, (унеможливлення доступу до коштів Біткоїн-адрес внаслідок блокування на державному рівні).

1 2 3 4 5

6) Оцініть ступінь важливості валютного ризику (Ризик 6), пов'язаного з коливанням курсу купівлі та продажу біткоїнів (загальне підвищення або зменшення цінності біткоїнів).

1 2 3 4 5

7) Оцініть ступінь важливості валютного ризику (Ризик 7), пов'язаного з коливанням курсу національної валюти (підвищення або зменшення цінності біткоїнів відносно національної валюти).

1 2 3 4 5

8) Оцініть ступінь важливості портфельного ризику (Ризик 8), пов'язаного з можливістю збитків або прибутків при використанні системи Біткоїн як джерела інвестицій.

1 2 3 4 5

9) Оцініть ступінь важливості чистого ризику (Ризик 9), пов'язаного з можливістю компрометації Біткоін-адрес (випадкові чинники; колізії Біткоін-адрес).

1 2 3 4 5

10) Оцініть ступінь важливості чистого ризику (Ризик 10), пов'язаного з можливістю компрометації Біткоін-адрес (навмисні злочинні дії; викрадення реквізитів доступу до Біткоін-гаманців).

1 2 3 4 5