Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

спеціальність *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Аналіз способів забезпечення анонімності при криптовалютних транзакціях***

Виконавець: студент ***2*** **курсу, групи** ***125м-16-1***

(підпис) ***Шевченко Денис Ігорович*** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.ф.-м.н., проф. Гусєв О.Ю.		
розділів:			
спеціальний	ст. викл. Саксонов Г.М.		
економічний	к.е.н., доц. Волотковська Ю.О.		

Рецензент			

Нормоконтроль	ас. Мєшков В.І.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *Кібербезпека*
(код і назва спеціальності)

студенту **125м-16-1** **Шевченко Денис Ігорович**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Аналіз способів забезпечення анонімності при криптовалютних транзакціях***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від 26.12.17 № 2127-л .

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***Способи забезпечення анонімності при криптовалютних транзакціях***

Предмет досліджень ***Процес забезпечення анонімності при криптовалютних транзакціях***

Мета НДР ***Розробити керівництво з анонімного здійснення криптовалютних транзакцій***

Вихідні дані для проведення роботи ***Матеріали науково-дослідної та переддипломної практики***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *Розробка керівництва по використанню сучасних способів забезпечення анонімності з урахуванням існуючих загроз деанонімізації*

Практична цінність *Підвищення рівня забезпечення анонімності*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Відповідність методичним рекомендація до підготовки та захисту дипломної роботи (проекту) для студентів галузі знань «Кібербезпека»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Аналіз стану забезпечення анонімності при криптовалютних транзакціях та способів її підвищення	1.07.2017 – 1.09.2017
Розробка керівництва по здійснення транзакцій з урахуванням доцільності використання існуючих способів забезпечення анонімності	1.09.2017 – 30.11.2017
Економічне обґрунтування доцільності розробки керівництва та його впровадження	1.12.2017 – 1.01.2018
Оформлення результатів роботи	1.01.2018 – 1.01.2018

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зменьшення збитків від цільових атак на криптовалютні активи*

Соціальний ефект *Можливість анонімного використання криптовалюти*

7 ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Саксонов Г.М.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Шевченко Д.І.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 10.09.2017
Термін подання дипломної роботи до ДЕК 24.01.2018

РЕФЕРАТ

Пояснювальна записка _ с., ___ рис., ___ табл., ___ додатка, ___ джерела.

Об’єкт дослідження: способи забезпечення анонімності криптовалютних транзакцій.

Мета роботи : розробити керівництво з анонімного здійснення криптовалютних транзакцій.

Методи дослідження: аналіз, синтез, індукція, дедукція, системний аналіз, структурний аналіз, методи порівняння та спостереження.

Виконуючи аналіз існуючих способів забезпечення анонімності при криптовалютних транзакціях, були виявлені основні переваги та недоліки функціювання цих способів в окремих випадках .

У спеціальній частині було разроблене керівництво, що поєднує у собі найкращі практики для забезпечення анонімності при здійсненні криптовалютних транзакцій .

В економічному розділі наведено економічне обґрунтування доцільності використання розробленого керівництва.

Практичне значення роботи полягає в створенні можливості анонімного використання криптовалют.

Наукова новизна роботи полягає у розробці керівництва по використанню сучасних способів забезпечення анонімності з урахуванням існуючих загроз деанонімізації.

КРИПТОВАЛЮТА, АНОНІМНІСТЬ, КРИПТОВАЛЮТНІ ТРАНЗАКЦІІ, СЕРВІСИ-МІКСЕРИ, ЦИБУЛЕВА МАРШРУТИЗАЦІЯ.

РЕФЕРАТ

Пояснительная записка ___ с., ___ рис., ___ табл., ___ прилож., ___ ист.

Объект исследования: способы обеспечения анонимности криптовалютных транзакций.

Цель работы: разработать руководство по анонимному совершению криптовалютных транзакций .

Методы исследования: анализ, синтез, индукция, дедукция, системный анализ, структурный анализ, методы сравнения и наблюдения.

Выполняя анализ существующих способов обеспечения анонимности при криптовалютных транзакциях, были выявлены основные преимущества и недостатки функционирования этих способов в отдельных случаях.

В специальной части было разработано руководство, объеденяющее в себе лучшие практики для обеспечения анонимности при совершении криптовалютных транзакций.

В экономическом разделе приведено экономическое обоснование целесообразности использования разработанного руководства.

Практическое значение работы состоит в создании возможности анонимного использованя криптовалют.

Научная новизна работы заключается в разработке руководства по использованию современных способов обеспечения анонимности с учётом существующих угроз деанонимизации.

КРИПТОВАЛЮТА, АНОНИМНОСТЬ, КРИПТОВАЛЮТНЫЕ ТРАНЗАКЦИИ, СЕРВИСЫ-МИКСЕРЫ, ЛУКОВАЯ МАРШРУТИЗАЦИЯ.

ABSTRACT

Explanatory note ___ p., ___ pic., ___ tables, ___ applications, ___ sources.

Object of research: ways to ensure the anonymity of crypto-currency transactions.

Objective: develop a guide to anonymous of crypto-transactions.

Research methods: analysis, synthesis, induction, deduction, system analysis, structural analysis, methods of comparison and observation.

Analyzing the existing methods of providing anonymity for crypto-currency transactions, the main advantages and disadvantages of the functioning of these methods were revealed in individual cases.

In a special part the guide has been developed, it unites the best practices to ensure anonymity of crypto-currency transactions.

The economic section provides an economic justification for the use of the developed guide.

The practical importance of the work is to create the possibility of anonymous use of crypto-currency.

The scientific novelty of this work is to develop guidance on the use of modern methods of ensuring anonymity in view of the existing threats of deannonization.

CRYPTO-CURRENCY, ANONYMITY, CRYPTO-CURRENCY TRANSACTION, MIXING SERVCES, ONION ROUTING.

ЗМІСТ

ВСТУП

Під анонімністю розуміють процес захисту ідентифікатора і даних про місцезнаходження користувача. Здатність забезпечувати анонімний доступ до послуг, при якому уникає відстеження персональної інформації про користувача і про його поведінку, такої як місце розташування користувача, частота користування послугою і т.д. Якість або стан анонімності, є умовою володіння ім'ям або ідентифікатором, які невідомі або замасковані. Іншими словами, під анонімністю в Інтернеті маються на увазі різні способи залишитися непоміченим у Всесвітній мережі. Причини для того, щоб приховувати свої дії на Інтернет-сайтах, різноманітні. Вони можуть бути пов'язані як з прагненням захиститися від можливих протиправних дій третіх осіб, так і з вчиненням протиправних дій самою особою, що прагне до анонімності.

Для досягнення анонімності застосовуються анонімні мережі, що працюють поверх глобальної сеті. Анонімние мережі - комп'ютерні мережі, створені для досягнення анонімності в Інтернеті і працюють поверх глобальної мережі. Специфіка таких мереж полягає в тому, що розробники змушені йти на компроміс між ступенем захисту і легкістю використання системи, її «прозорістю» для кінцевого користувача. Також важливий аспект збереження анонімності і конфіденційності за умови впливу методів соціальної інженерії або будь-якого тиску на оператора сервера. Багаторівневе шифрування і розподілене характер анонімних мереж, усувають єдину точку відмови і єдиний вектор атак, дозволяють зробити перехоплення трафіку або навіть злом частини вузлів мережі не фатальною подією. За анонімність користувач розплачується збільшенням часу відгуку, зниженням швидкості, а також великими обсягами мережевого трафіка. Для того, щоб досягти більш високого рівня анонімності в Інтернеті, використовуються анонімайзери. Вони являють собою технічні засоби для приховування інформації про Інтернет-користувача і його діях в мережі. До них відносяться проксі-сервери, до яких вдаються при необхідності

приховати джерело Інтернет-запиту або відобразити неправдиву інформацію про користувача.

Анонімні комерційні транзакції можуть захистити конфіденційність споживачів. Деякі споживачі вважають за краще використовувати готівку при купівлі товарів повсякденного попиту (наприклад, продукти харчування та інструменти), щоб не допустити того, щоб продавці збирали інформацію і користувалися нею. Кредитні картки пов'язані з ім'ям людини і можуть використовуватися для пошуку інших даних, таких як поштовий адрес, номер телефону і т.д. Існують анонімні системи електронних грошей, непідконтрольні державі і іншим фінансовим організаціям на кшталт WebMoney, Qiwi, PayPal і ін. На цих сервісах відкриваються рахунки (електронні гаманці) і користувачі можуть переводити гроші в різних валютах один одному і організаціям-партнерам даних систем. Однак такі організації працюють в суворій відповідності з національним законодавством, як правило, мають представництва в країнах, де здійснюють діяльність по залученню клієнтів, і розкривають всю інформацію про емітентів за запитом компетентних органів (в тому числі за міжнародними запитам). На даний момент є більш анонімні і альтернативні види грошей, ліквідність і затребуваність яких визначають не скільки споживчі кошики і біржові котирування (хоча такі валюти успішно торгуються на спеціалізованих біржах), і не законодавче закріплення їхнього статусу, скільки інтерес самих користувачів і довіру ширшого кола компаній , які приймають її в якості оплати. Йдеться про криптовалюти, їх емісія виробляється за допомогою обчислювальних потужностей користувачів (для емісії потрібно затратити енергію і обчислювальні ресурси) і зазвичай алгоритмічно обмежена. Дозволяють анонімно і безпечно володіти, емітувати і передавати грошові кошти.

РОЗДІЛ 1
КРИПТОВАЛЮТИ І МЕХАНІЗМИ ЇХ РОБОТИ

Криптовалюта - електронний механізм обміну, цифровий актив, емісія та облік якого часто децентралізовані. Функціонування системи відбувається в рамках розподіленої комп'ютерної мережі. При цьому зазвичай вся інформація про транзакції не шифрується і завжди доступна у відкритому вигляді. Криптографія використовується не для обмеження доступу до даних про транзакції, а для гарантування незмінності ланцюжка блоків, бази транзакцій. Термін закріпився внаслідок статті о Bitcoin «Crypto currency» (Криптографічна валюта), опублікованій в 2011 році в журналі Forbes. Сам же автор Bitcoin, як і багато інших, використовував термін «електронна готівка»[1].

1.1 Криптовалюти на основі блокчейна

У криптовалюті на основі блокчейна спеціальні вузли, звані майнери, збирають транзакції, що транслюються по мережі, і використовують свою обчислювальну потужність щоб згенерувати коректний блок транзакцій. Генерація здійснюється шляхом послідовного виклику хеш-функцій на даних, які майнер вирішив включити в свій блок, разом з попереднім коректним блоком і його власною адресою в мережі криптовалюти. Таким чином, функціонування мережі, що містить послідовності таких блоків, які спільно генерують майнери, відбувається наступним чином:

• Коли майнер успішно згенерував блок (що означає, що хеш цього блоку менше заданого рівня складності, "difficulty threshhold"), він відправляє цей блок в мережу.

• У випадку якщо інші майнери бачать, що блок є коректним, і що це найдовший ланцюг блоків, вони переключаються на нього і намагаються збільшити цей ланцюг.

• Наявність отриманого блоку в ланцюзі підтверджує, що нові згенеровані кошти, а так само комісії від транзакцій перечислені на певну адресу в мережі.

Тільки власник цієї адреси, що має приватний ключ від неї, може розпоряджатися цими коштами.

Синхронізація між майнерами і генерація нових засобів відрізняються в різних системах, в загальному випадку (на основі Bitcoin):

• Рівень складності адаптується до сумарною обчислювальною потужності майнерів. Це здійснюється шляхом поновлення порогового значення кожні 2016 блоків, що відбувається приблизно раз на два тижні (кожен новий блок генерується в середньому раз в 10 хвилин).

• Нагорода за створення блоку на початку функціонування мережі становила 50 одиниць (Bitcoin) в січні 2009 року, і зменшується вдвічі за кожні 210 тис. Згенерованих блоків, тобто приблизно кожні 4 роки.

Блокчейн, або ланцюжок блоків транзакцій - вибудуваний за певними правилами з формованих блоків транзакцій. Блок транзакцій - спеціальна структура для запису групи транзакцій в системі Bitcoin і аналогічних їй[2].

Щоб транзакція вважалася достовірною («підтвердженої»), її формат і підписи повинні перевірити і потім групу транзакцій записати в спеціальну структуру - блок. Інформацію в блоках можна швидко перевірити ще раз. Кожен блок завжди містить інформацію про попередній блок. Всі блоки можна вибудувати в один ланцюжок, який містить інформацію про всі скоєні коли-небудь операції в цій базі. Найперший блок в ланцюжку - первинний блок - розглядається як окремий випадок, так як у нього відсутній батьківський блок.

Блок складається з заголовка і списку транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеші транзакцій і додаткову службову інформацію. В системі Bitcoin першої транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок.

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоці використовується деревоподібна хешування. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію з попереднім станом даних (в

системі Bitcoin дається посилання на ту транзакцію, по якій були отримані біткойни, що витрачаються). Комісійні транзакції можуть містити в атрибуті будь-яку інформацію (для них це поле зветься Coinbase parameter), оскільки у них немає батьківських транзакцій[3].

Створений блок буде прийнятий іншими користувачами, якщо числове значення хеша заголовка нижче певного числа, величина якого періодично коригується. Так як результат хешування (функції SHA-256) є незворотним, немає алгоритму отримання бажаного результату, крім випадкового перебору. Якщо хеш не задовольняє умові, то в заголовку змінюється параметр nonce і хеш перераховується. Зазвичай потрібна велика кількість перерахунків. Коли варіант знайдений, вузол розсилає отриманий блок іншим підключеним вузлів, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш. Схема прийняття блоку позначена на рисунку 1.1.

Блоки одночасно формуються безліччю майнерів. Блоки, що задовольняють критеріям, відправляються в мережу, включаючись в розподілену базу блоків. Регулярно виникають ситуації, коли кілька нових блоків в різних частинах розподіленої мережі називають попереднім один і той же блок, тобто ланцюжок блоків може гілкуватися.

Приклад такого гілкування наведено на рисунку 1.2.

Спеціально чи випадково можна обмежити ретрансляцію інформації про нові блоках (наприклад, одна з ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливо паралельне нарощування різних гілок. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один з них. Коли ретрансляція блоків відновлюється, майнери починають вважати головною ланцюжок з урахуванням рівня складності хеша і довжини ланцюжка. У разі рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Транзакції, що увійшли тільки в відхилену гілку (в тому числі по виплаті винагороди), втрачають статус підтверджених. Якщо це

транзакція з передачі біткойнів, то вона буде поставлена в чергу і потім включена в черговий блок. Транзакції отримання винагороди за створення відсічених блоків не дублюються в іншій гілці, тобто «зайві» біткойни, виплачені за формування відсічених блоків, не отримують подальших підтверджень і втрачаються. Таким чином, ланцюжок блоків містить історію володіння, з якою можна ознайомитися, наприклад, на спеціалізованих web-ресурсах[4].

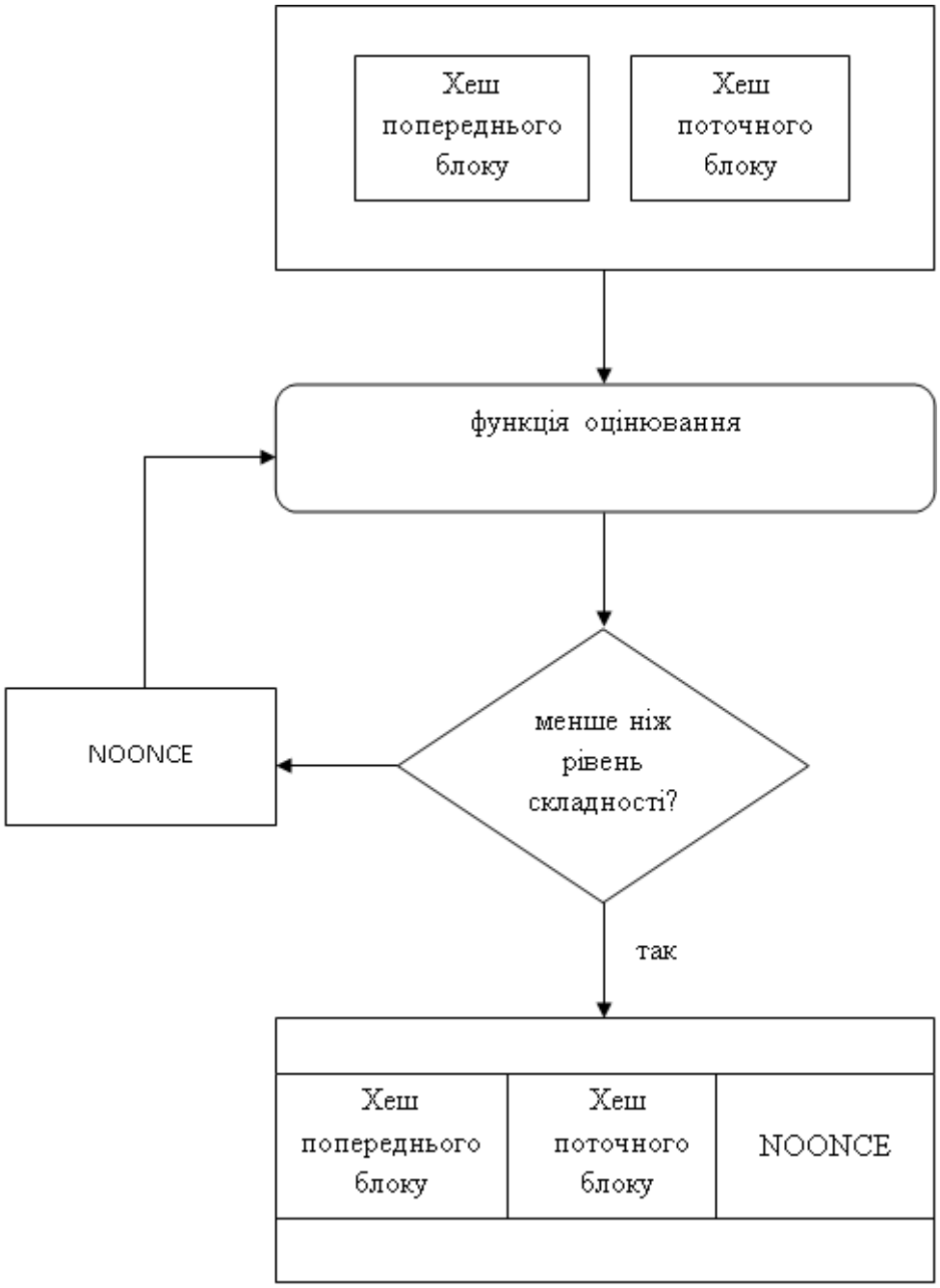

Рисунок 1.1 - Схема прийняття блоку

Спеціально чи випадково можна обмежити ретрансляцію інформації про нові блоках (наприклад, одна з ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливо паралельне нарощування різних гілок. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один з них. Коли ретрансляція блоків відновлюється, Майнер починають вважати головною ланцюжок з урахуванням рівня складності хеша і довжини ланцюжка. У разі рівного розподілу складності і довжини перевага віддається тій ланцюжку, кінцевий блок якої з'явився раніше. Транзакції, що увійшли тільки в відхилену гілку (в тому числі по виплаті винагороди), втрачають статус підтверджених. Якщо це транзакція з передачі біткойнов, то вона буде поставлена в чергу і потім включена в черговий блок. Транзакції отримання винагороди за створення відсічених блоків не дублюються в іншій гілці, тобто «зайві» біткойни, виплачені за формування відсічених блоків, не отримують подальших підтверджень і втрачаються. Таким чином, ланцюжок блоків містить історію володіння, з якою можна ознайомитися, наприклад, на спеціалізованих web-ресурсах.

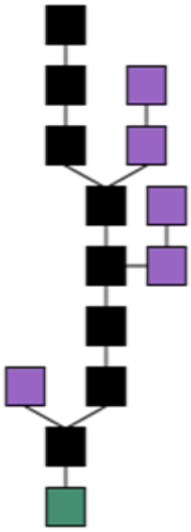

Рисунок 1.2 – Приклад гілкування

1.2 Механізм транзакцій

У своїй суті, криптовалюта на основі блокчейн являє собою ланцюжок цифрових підписів, що відображають шлях грошових коштів в системі. Ключовим поняттям в даному контексті є транзакція. Фактично, транзакція - це

мінімальний елемент блоку, що адресується, який в свою чергу є елементом ланцюжка блоків, що адресується.

Існує два види транзакцій:

• "Стандартні" транзакції, які кодують передачу коштів від одних користувачів системи,

• "Генеруючі" транзакції, в яких знову згенеровані кошти передаються "Майнер" в якості нагороди за генерацію блокчейна.

Всі кошти, які є результатом угоди, що розглядається як єдина сума, яка може бути розділена тільки за допомогою іншої транзакції. Фактично, стандартна транзакція не реєструє жодного переказу коштів від одного клієнта іншому, а скоріше являє собою суму коштів, яка повинна бути збалансована: кількість переданих коштів (можливо, зібраних від різних відправників) має збігатися з кількістю коштів, призначених для одержувачів (одного або декількох). Як приклад можна привести "мито" для майнерів (яка в загальному випадку не є обов'язковою, але реалізована в багатьох засобах за замовчуванням). Передача "мита" не може бути здійснена заздалегідь, так як одержувач коштів стане відомий тільки після отримання найкращого ланцюжка блоків. Тому "мита" включаються в суму транзакції, але не беруть безпосередньої участі в цій транзакції[5].

Специфікація транзакцій вимагає системи адресації, що включає в себе відправника, одержувача і майнера (тобто, в кінцевому рахунку, кожен можливий вузол системи). Більш того, транзакції повинні бути унікально пов'язані з відправником P таким чином, щоб ніяка сторона, відмінна від P, не могла ідентифікувати себе в транзакції як P (справжність), і щоб сам P не міг відмовитися від вже здійсненої угоди (неспростовності).

Кінцева мета механізму транзакцій полягає в тому, щоб будь-який вузол системи міг дізнатися подробиці здійсненої угоди, відображені в транзакції. Це досягається шляхом здійснення підпису і перевірки деяких елементів транзакції з використанням схем електронного підпису. Таким чином, учасники системи

можуть легко відстежувати шляхи переміщення коштів в системі, а також контролювати цілісність сервісу.

Ці механізми, вперше застосовані в Bitcoin, згодом були застосовані і в інших системах криптовалюта. Більш того, цей підхід справедливий для взагалі будь-яких систем на основі блокчейн.

1.2.1 Адреси

Оскільки перевірка транзакції здійснюється з використанням механізмів цифрового підпису, а вузли мережі реалізовані з використанням спеціального програмного забезпечення, званого гаманець (англ. Wallet), повинно мати місце однозначна відповідність між гаманцями і набором ключів для підпису і перевірки підписів транзакцій.

Ключі як правило пов'язані з ідентифікаторами, дійсними тільки в контексті системи, званими адреса, а не на реальних персональних даних, як це відбувається в інфраструктурі відкритих ключів. Таким чином, відсутня необхідність в довіреної третьої сторони, а користувачі можуть розраховувати на анонімність. Анонімність користувачів часто головна мета, на яку спрямована система криптовалюта, що є однією з причин можливості зв'язати кілька ідентифікаторів користувачів з одним і тим же гаманцем.

Насправді, ключі перевірки самі по собі можуть використовуватися як адреси до системи, так як зберігаються у відкритому доступі. Однак, такий підхід непридатний в разі необхідності тривалого існування адреси, оскільки механізми управління ключами включають в себе такі процедури, як оновлення і відгук ключа. Ці міркування, однак, не були взяті до уваги розробниками систем криптовалюти на основі блокчейна, і адреси представляються хеш-дайджестами ключів перевірки. Так, Bitcoin-адреси являють собою закодовану за допомогою base58 рядок, що містить номер версії адреси, який закодований за допомогою алгоритму RIPEMD-160 перевірочного ключа, і контрольну суму.

1.2.2 Входи і виходи транзакцій

Мета транзакцій - відстежувати шляхи переміщення коштів усередині системи. Для досягнення цього, в транзакцію включається інформація про переданих засобах, звана вхід і вихід транзакції.

Вхід транзакції містить відправника транзакції P, а так само підтвердження, яке гарантуватиме кожному вузлу в системі, що P дійсно збирається зробити операцію.

Вихід транзакції містить одержувача транзакції, призначену йому суму, а так само підтвердження, яке гарантуватиме кожному вузлу в системі, що кошти дійсно призначені саме цьому одержувачу.

У найпростішому випадку кожен вхід транзакції повинен бути пов'язаний зі виходом будь-якої попередньої транзакції, що знаходиться в блоці підтвердженої ланцюга. Відповідність між поточним входом транзакції I і попереднім входом транзакції O доводить, що всі кошти, передані в O, доступні для I, тому кожному входу I може відповідати тільки один вихід O.

Інакше йдуть справи з транзакціями, де кілька (0 і більш) входів можу бути асоційовані з декількома входами (1 і більше). Транзакції без входів використовуються в "генеруючих" транзакціях для передачі знову отриманих коштів одному або декільком одержувачам.

Транзакції з множинними входами і виходами використовуються для передачі коштів від усіх відправників всім одержувачам транзакції. Основне правило для цих транзакцій: сумарна кількість відправлених коштів Im має збігатися з сумарною кількістю коштів, що отримуються Om. Im і Om обчислюються "на льоту" і не містяться в транзакції в явному вигляді. Таким чином, кілька входів можуть об'єднуватися в один вихід, і навпаки, один вхід може розгалужуватися на кілька виходів.

Так, в Bitcoin кожна транзакція є передачу певної суми, а кожен вхід має посилатися на один з виходів раніше схвалених транзакцій. Вхід і вихід визначаються наступним чином:

I: = (sha256 (Tp), i, SgnCode),

O: = (v, VrfCode),

де:

- sha256 (Tp) це SHA-256 хеш попередньої транзакції Tp, який використовується для ідентифікації Tp як транзакцію, що породила I.
- Індекс входу і це невід'ємне число, яке вказує, який саме вихід попередньої транзакції Tp використовується як вхід в поточної транзакції T.
- Код підписи SgnCode це набір інструкцій і дані, що підтверджують справжність транзакції, як правило, це просто підписані відправником входи і виходи транзакції на увазі SHA-256 хеша.
- Сума коштів v, асоційована з O.
- Код перевірки VrfCode це набір інструкцій і дані, що визначають одержувачів коштів, що передаються в O.

Приклад ланцюжка транзакцій в системі Bitcoin представлений на рисунку 1.3.

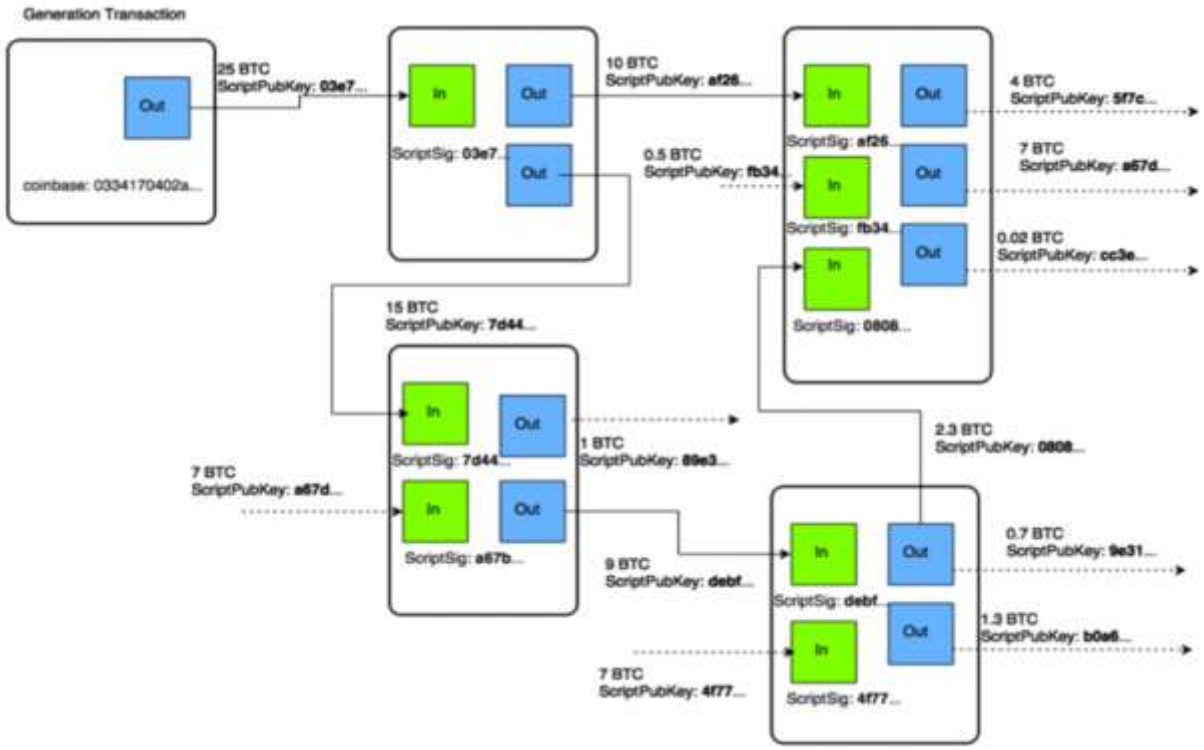

Рисунок 1.3 – Приклад ланцюжка транзакцій в системі Bitcoin

1.3 Проблема анонімності

Анонімність не завжди визнається в суспільстві. У політичних, урядових і деяких приватних організаціях анонімність не має місце. Наприклад, у багатьох країнах тільки під справжнім ім'ям особистість має право голосувати. В аеропортах більшості країн пасажирам не пропускають на борт літака без пред'явлення посвідчення особи. З іншого боку, деякі політичні процеси вимагають анонімності.

Під анонімністю розуміють процес захисту ідентифікатора і даних про місцезнаходження користувача. Здатність забезпечувати анонімний доступ до послуг, при якій уникає відстеження персональної інформації про користувача і про поведінку користувача, такий як місце розташування користувача, частота користування послугою і т.д. Якість або стан анонімності, яке є умовою володіння ім'ям або ідентифікатора, які невідомі або замасковані.

Іншими словами, під анонімністю в Інтернеті маються на увазі різні способи залишитися непоміченим у Всесвітній мережі. Причини для того, щоб приховувати свої дії на Інтернет-сайтах, різноманітні. Вони можуть бути пов'язані як з прагненням захиститися від можливих протиправних дій третіх осіб, так і з вчиненням протиправних дій самою особою, що прагнуть до анонімності.

Для досягнення анонімності застосовуються анонімні мережі, що працюють поверх глобальної сеті. Анонімние мережі - комп'ютерні мережі, створені для досягнення анонімності в Інтернеті і працюють поверх глобальної мережі. Специфіка таких мереж полягає в тому, що розробники змушені йти на компроміс між ступенем захисту і легкістю використання системи, її «прозорістю» для кінцевого користувача. Також важливий аспект збереження анонімності і конфіденційності за умови впливу методів соціальної інженерії або будь-якого тиску на оператора сервера. Багаторівневе шифрування і розподілене характер анонімних мереж, усуваючи єдину точку відмови і єдиний вектор атак, дозволяють зробити перехоплення трафіку або навіть злом частини вузлів мережі не фатальним подією.

За анонімність користувач розплачується збільшенням часу відгуку, зниженням швидкості, а також великими обсягами мережевого трафіка.Первой щодо успішної анонімної мережею був комерційний сервіс Freedom, який функціонував з 1998 до 2001 року. Компанією ZKS були встановлені виділені сервери, з якими клієнти з'єднувалися за допомогою криптографічного протоколу. Вузол, на який приходили пакети від користувача Freedom, не міг ідентіфіціроватьнастоящего відправника. Сама мережа функціонувала на рівні протоколу IP. В цей же час почали активно розвиватися інші проекти.

Для того, щоб досягти більш високого рівня анонімності в Інтернеті, використовуються анонімайзери. Вони являють собою технічні засоби для приховування інформації про Інтернет-користувача і його діях в Мережі. До них відносяться проксі-сервери, до яких вдаються при необхідності приховати джерело Інтернет-запиту або відобразити неправдиву інформацію про користувача.

Також можна звернутися до VPN-сервісу, який дозволяє користувачеві приховати реальний IP-адресу і самостійно вибрати віртуальне місце розташування.

Одним з найбільш надійних способів вважається Tor, який сприяє анонімізації трафіку за рахунок цибулевої маршрутизації.

Зазвичай секретність досягається за допомогою обмеження доступу до інформації. Про операцію знають тільки дві беруть участь сторони і банк. В системі Bitcoin все коли-небудь зроблені транзакції публічні і зберігаються відкрито. Конфіденційність забезпечується відсутністю зв'язку ідентифікаційних даних власника і адреси гаманця. Так як можливо створювати яке завгодно кількість адрес, для досягнення найбільшої конфіденційності слід використовувати для кожної транзакції нову адресу. Цим ускладнюється встановлення відповідностей між адресами і власником. Якби адреси зв'язувалися з конкретною особистістю, то анонімності транзакцій б не було. Проте система Bitcoin не є абсолютно анонімною. Було продемонстровано, що на основі відкритої інформації можна встановити відповідності між багатьма

відкритими ключами один з одним та іншою інформацією. Спираючись на e-mail, IP-адреси, номери кредитних карт, що зберігаються в базах даних магазинів та сховищах гаманців, можливо ідентифікувати значну частину операцій.

Для досягнення максимальної анонімності рекомендується використовувати допоміжні інструменти, такі як Tor, що дозволяє приховати реальний IP-адресу, для маніпулювання біткойнов.

Також може бути використаний перемешиватель Bitcoin-транзакцій. Біткойни з декількох адрес служать входом. Далі вони відправляються на кілька адрес; зв'язок вхідних і вихідних адрес втрачається і ззовні ставати незрозуміло, який вхідний адресу відправляв біткойни на який вихідний адресу.

Біткойни існують тільки у вигляді записів в розподіленої базі, в якій в загальнодоступному відкритому (нешифрованому) вигляді зберігаються всі транзакції, із зазначенням біткойн-адрес відправників / одержувачів, але без інформації про реального власника цих адрес. У базі немає окремих записів про поточну кількість біткойнов у будь-якого власника. Лише на підставі ланцюжків транзакцій стає зрозумілим поточну кількість біткойнов, пов'язаних з тим чи іншим біткойн-адресою. Тобто можна побачити, що на адресу надійшов 1 біткойн, а по інший транзакції на цю ж адресу надійшло 2 біткойнов, третя транзакція відправила з цієї адреси 1 біткойн. Але в базі не зберігається окремого запису, скільки всього зараз біткойнов за даними адресою - просто надається можливість будь-якої миті це легко підрахувати. Такі підрахунки автоматично роблять клієнтські програми, користувач може і не помічати роздробленості інформації.

1.4 Правовий статус криптовалюта в Україні та світі

Популярність біткоіни змусила заговорити про нього на міжнародному рівні, а уряди окремих країн - зважати на нього. Деякі країни навіть визнали біткоіни валютою. У Німеччині - це приватні гроші і ними, наприклад, навіть можуть розраховуватися між собою підприємства. Японія визнає криптовалюта законним платіжним засобом. Міністерство фінансів США розглядає біткоіни

як бізнес, який надає розрахунково-касові послуги населенню, але не як валюту. А Податкове управління США вважає їх цінним активом, як, наприклад, золото. У Китаї операції з криптовалюта дозволені для фізосіб і заборонені для банків, вона вважається віртуальним товаром. У Швейцарії конкретно біткоіни має статус іноземної валюти. Однак більшість все ж схиляється до визнання біткоіни майновим активом, операції з яким повинні обкладатися податком.

Головною проблемою, що встала перед міжнародними фінансовими організаціями і керівництвом окремих країн, є питання контролю за обігом криптовалюта, адже безконтрольна - вона створює великий простір для розвитку тіньової економіки.

Крім того, неврегульована сфера криптовалюта відкриває великі можливості для шахраїв, дії яких неможливо буде класифікувати, а потім і покарати зловмисників, при відсутності відповідного законодавства в країні. Наприклад, якщо ви купили за біткоіни товар, який вам не надали, і ви прийшли з цим в правоохоронні органи, то ні поліція, ні суд не знатимуть, що з цим робити.

На сьогодні серед регуляторів провідних країн світу, в тому числі країн Євросоюзу, немає єдиного підходу до визначення правового статусу кріптовалюа і регулювання операцій з ними.

Сьогодні налічується більше тисячі видів криптовалюта, серед яких найбільшу капіталізацію мають Bitcoin, Ethereum, Bitcoin Cash, Ripple, IOTA, DASH, Litecoin і інші. Загальна капіталізація криптовалюта постійно зростає. Так, згідно з даними сайту Coinmarketcap на 4 грудня вона перевищила $ 340 млрд.

Зростання їх популярності в світі відбувається на тлі відсутності єдиного поняття «криптовалюта» - воно варіюється від ототожнення з поняттями «товар», «платіжний засіб», «розрахункова одиниця» до понять «нематеріальний цифровий актив», «інвестиційний актив», «фінансовий актив »,« окремий вид цінних паперів »та інші.

Також їх ще називають «віртуальною валютою» і «цифровий валютою», однак ці терміни не можна вважати абсолютними синонімами криптовалюта, оскільки вони ширше цього поняття і є одним з видів «децентралізованих віртуальних валют» (доповідь FATF «Віртуальні валюти», 2014 рік).

Помилкове і застосування до криптовалюта правового режиму валюти виключно через загальноприйнята назва, на думку НБУ, породжує ряд правових колізій.

Варто взяти до уваги, що більшість регуляторів інших країн світу, в тому числі Європейський Центробанк, обережно підходять до законодавчих ініціатив і паралельно з власними дослідженнями уважно стежать за подальшим розвитком нових технологій і явищ для розробки найбільш ефективного підходу щодо регулювання операцій з криптовалюта.

З огляду на діючі норми законодавства України (Цивільний кодекс України, Закон України «Про НБУ», Декрет КМУ «Про систему валютного регулювання і валютного контролю», Закон України «Про платіжні системи та переказ коштів в Україні», Закон України «Про інформацію» та інші) поняття «криптовалюта» і регулювання операцій з нею не підпадають під режим регулювання:

- Звернення грошових коштів. Оскільки криптовалюта не існує в формі банкнот, монет, записів на рахунках в банках, вона не може бути визнана грошима (грошовими коштами, коштами, грошовими знаками) в трактуванні українського законодавства.
- Валютного законодавства. Оскільки криптовалюта не має прив'язки до грошової одиниці однієї з держави, вона не може бути визнана валютою або законним платіжним засобом іноземної держави, і не є валютною цінністю в трактуванні валютного законодавства.
- Звернення електронних грошей і використання платіжних засобів. Оскільки криптовалюта не випускається банком і не є грошовим зобов'язанням певної особи, вона не може бути визнана електронними грошима.

- Цивільних правовідносин щодо регулювання діяльності з цінними паперами. У криптовалюта відсутні ознаки документа і емітента, а саме: невстановленої форми документа з відповідними реквізитами, що посвідчує грошове або інше майнове право, не має визначення взаємовідносин емітента цінних паперів (особи, яка видала цінний папір) і особи, яка має права на цінний папір, і не передбачає виконання зобов'язань по такого цінного паперу. А значить, криптовалюта не може бути цінним папером.

- У криптовалюта відсутні ознаки документа у вигляді грошових знаків, відсутня емітент, а також відсутня мета виготовлення. Таким чином, криптовалюта не може бути визнана грошовим сурогатом (згідно з його визначенням в Законі України «Про Національний банк України»).

Зараз у Верховній Раді зареєстровано два законопроекти, які претендують на регуляцію ринку криптовалюта, - про звернення криптовалюта в Україні (№7138) та про стимулювання ринку криптовалюта і їх похідних (№7183-1).

1.4 Висновки до першого розділу

Описані у цьому розділі механізми реалізфції криптовалютних транзакцій мають певні недоліки с точки зору забезпечення анонімності. Виникає необхідність в використані допоміжних заходів, щоб уникнути деанонімізації. Спершу розглянемо окремі рішення. В разі недостатнього зменьшеня ризику, запропонуємо комплексний підхід.

РОЗДІЛ 2
СПОСОБИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ КРИПТОВАЛЮТНИХ ТРАНЗАКЦІЙ

2.1 Причини відсутності анонімності

Кожна транзакція повинна бути публічно зареєстрована. Всі користувачі можуть бачити грошовий потік криптовалюта, що переходить від адреси до адреси. З одного боку, користувачі не можуть ідентифікувати цю інформацію, оскільки номери транзакцій - це випадкові цифри. З іншого боку, якщо хоча б одна транзакція може бути ідентифікована і обчислений власник, то існує ймовірність, що власники інших транзакцій будуть обчислені також. Дані про власників можна отримати з аналізу мережі, за допомогою стеження або за допомогою пошукових систем, які допоможуть знайти адреси. Захистом від ідентифікації та ускладненням для атак хакерів є те, що кожної нової транзакції присвоюється новий номер.

Транзакції через обмінники можуть стати причиною обчислення рахунку біткоіни. Наприклад, якщо якийсь Іванов вирішить скористатися послугами обмінників, після чого зайде за покупками на сайт-пастку, то існує ймовірність, що людина, яка хоче вистежити адресу Іванова, побачивши дві транзакції, зможе довести, що здійснював їх один і той же чоловік з однієї адреси.

Історія всіх транзакцій системи біткоіни повинна бути публічною в цілях безпеки. Проте є способи мінімізації витоку особистої інформації в мережу. Наприклад, Майнінг або використання адреси, в захисті якого користувач впевнений.

Користувачі повинні розуміти, що таке відсутність анонімності в системі, є основою мінімізації «брудних» транзакцій, дій шахраїв і падіння системи біткоіни. Якщо рахунок містить анонімні і неанонімні фінансові надходження, користувач повинен зробити його «чистим».

2.1.1 Кластеризація

Зв'язок біткоіни-адрес називається кластеризацией, і розглянемо особливості цієї процедури детальніше.

Найпростішим способом кластеризації є аналіз транзакційних мереж. У загальному випадку під цим мається на увазі визначення декількох входів, які об'єднані в одну транзакцію. У той час як ці входи могли виходити від інших адрес, факт їх з'єднання в одну транзакцію, вказує на те, що ці входи, а отже і всі адреси, пов'язані з ними, контролюються одним користувачем.

Для визначення «адрес для здачі» існує безліч способів, а за цими даними легко вони зв'язуються з відправником кріптомонет. Найпростіший спосіб визначити це при отриманні цифрової валюти: вихід, який не має до вас відносини, часто (але не завжди) є «адресою для здачі», підконтрольним відправнику. Також існують спеціальні програми, за допомогою яких уважним користувачам вдається відшукувати «адреси для здачі». Наприклад, такі програми здатні завжди ставити подібні адреси в транзакції останніми виходами.

Другим методом кластеризації є так званий «аналіз поширення». Він відрізняється прямолінійністю і доступний з використанням декількох доступних блоків. «Аналіз поширення» супроводжується розрахунком відсотка кріптомонет на конкретну адресу, які прийшли з іншого біткоіни-адреси, і визначає зв'язок цих адрес одній прямій транзакцією або ланцюжком транзакцій.

Також існує часовий аналіз і кількісний аналіз. При кількісному аналізі, як можна зрозуміти з його назви, вивчаються не конкретні операції, а суми монет, прохідних між входами і виходами. Часовий аналіз відстежує певні часові відрізки. Якщо, наприклад, один вхід становить 2,6539924 біткойнов, а в наступному блоці вихід, не пов'язаний з ним, дорівнює 2,6539924 біткойнов без комісії Майнер, можна припустити, що обидві адреси контролює один користувач, який використовує міксер.

2.1.2 Атака Сивіли

Атака Сивіли - вид атаки в тимчасової мережі, в результаті якої жертва підключається тільки до вузлів, контрольованих зловмисником. Термін запропонований в 2002 співробітником Microsoft Research Брайаном ЗІЛом. Назва обрана на честь псевдоніма головної героїні книги-бестселера 1973 року "Сивіла 'про лікування диссоциативного розлади особистості. Незважаючи на те, що в російській перекладі книги - першоджерела назви - використовується варіант 'Сивіла', також зустрічається використання транслітерації 'Сибілла'. До 2002 року атаки того ж класу були відомі під терміном псевдоспуфінг, який ввів Л. Детвейлер в списку розсилки шіфропанков.

У однорангових мережах, де жоден вузол не є довіреною, кожен запит дублюється декільком одержувачам з тим, щоб не виявилося єдиного вузла, відповіді якого було б необхідно повністю довіряти. У той же час, користувачі мережі можуть мати кілька ідентифікаторів, фізично що відносяться до різних вузлів. Сумлінно ці ідентифікатори можна використовувати, щоб розділяти загальні ресурси або мати кілька їх копій. Останнє створить надмірність, яка дозволить перевіряти цілісність даних, прийнятих з мережі незалежно. Зворотною стороною такого підходу є те, що в якийсь момент всі доступні вузли, які повинні представляти різних одержувачів деякого запиту, можуть контролюватися одним і тим же користувачем. Таким чином, якщо цей користувач виявиться зловмисником, у нього в даному сеансі будуть всі можливості посередника, невиправдано отримав повне довіру ініціатора сеансу. Чим більше ідентифікаторів належить зловмиснику, тим більше шансів, що наступний сеанс деякого користувача з p2p-мережею виявиться замкнутий на цих вузлах-псевдонімах. При цьому зловмиснику важливо, щоб новий ідентифікатор було досить легко створити.

В силу відсутності довіреної центру, в тимчасової мережі є 2 способи визнати новий ідентифікатор: або отримати гарантії його сумлінності від інших вузлів, або самостійно його перевірити будь-яким чином.

При прямій перевірці: навіть якщо ресурси обмежені, зловмисник все одно може контролювати якесь число ідентифікаторів; зловмисник може створювати ідентифікатори-псевдоніми знову і знову, якщо він не зобов'язаний підтверджуючого володіння усіма ними одночасно.

При непрямої перевірці: досить велика кількість підконтрольних ідентифікаторів дозволяє підробляти необмежену кількість нових; зловмисник завжди зможе контролювати велике число ідентифікаторів, якщо він не зобов'язаний безперервно їх підтверджувати.

З ростом децентралізованої мережі зростає і кількість ідентифікаторів-псевдонімів. Стає недоцільно вимагати кожного користувача підтверджувати володіння своїми ідентифікаторами одночасно і безперервно, оскільки це суттєво заважає масштабованості мережі. У 2012 році було показано, що широкомасштабні атаки можна проводити дешево і ефективно в існуючих системах, таких як BitTorrent Mainline DHT. Активне увагу атаці Сивіли приділяється в рамках розробки автомобільних мереж vehicle-to-vehicle (v2v).

Вважається, що єдиний прямий спосіб переконати учасника в тому, що два вузли відносяться до різних користувачам - це вирішення завдання, яку один користувач не може вирішити самостійно. При цьому враховується, що ресурси вузлів обмежені.

Якщо врахувати обмеженість швидкості з'єднання, то учасник може відправити циркулярний запит і приймати відповіді тільки протягом обмеженого інтервалу часу.

Якщо враховувати обмеженість ресурсів зберігання, учасник може зажадати від ідентифікаторів зберігати велику кількість унікальної інформації. Разом з тим, маючи при собі невелику вижимки з цих даних, учасник зможе упевнитися в тому, що з високою ймовірністю ці дані все ще зберігаються в цих вузлах.

Якщо використовувати обмеженість обчислювальних ресурсів, то учасник може зажадати від кожного ідентифікатора вирішувати унікальну, обчислювально складну задачу.

Можна заощадити власні ресурси, якщо делегувати завдання валідації вузлів іншим учасникам. Крім того, при такому підході додатковим аргументом на користь успішного проходження валідації стане число перевірок, успішно пройдених вузлом до цього. Чаян Банерджі запропонував схему непрямої перевірки вузла, що складається з двох стадій. На першій стадії результат перевірки - ступінь довіри перевіряється вузла - повідомляють найближчі вузли, що дозволяє не відправляти дані далеко. Отримані значення порівнюються з результатами аналогічної перевірки декількома іншими, випадково вибраними віддаленими вузлами. У переважній більшості випадків це дозволяє виявити вузли-псевдоніми, які брали участь в перевірці на першому етапі.

2.2. Сервіси-міксери

Суть подібних сервісів полягає в тому, щоб змішувати біткоіни всіх користувачів мережі, в результаті чого відбувається анонімізація платежів. Зазвичай для того, щоб почати користуватися Bitcoin-міксером, досить пройти просту процедуру реєстрації на сайті одного з популярних сервісів, а після можна відправляти біткоіни на вказаний в кабінеті адресу. Через деякий час ви зможете отримати свої кошти за вирахуванням комісії системи.

Ідея проста: об'єднати кошти одного користувача з біткойнов інших людей, тим самим опускаючи шлях назад до вихідного джерела коштів. У традиційних фінансових системах це еквівалентно передачі коштів через ряд банківських рахунків. Коли ви змішуєте біткойни, ви відправляєте свої гроші (і довіряєте) за допомогою послуги мікшування, яка відправляє вам біткойни іншої людини за допомогою серії транзакцій. Тому, якщо хтось намагається відстежувати вашу активність через Blockchain, вони повинні сортувати тисячі або навіть мільйони транзакцій. Кожна транзакція призводить до збільшення кількості рахунків в біткойнов, які виступають в якості ретранслятора для послуги мікшування, передаючи через них кошти по шляху до остаточного призначеного адресою. Найголовніше, кошти, які в кінцевому підсумку

залишаються незайнятими і не мають посилання на вихідний адресу, з якого вони прийшли.

Крок 1: біткойнов-адреса зловмисника (відзначений рожевим кольором називати його L0) отримав початковий платіж від жертви і перемістив його на перший біткойн-адреса(L1) в ланцюжку(Рисунок 2.1).

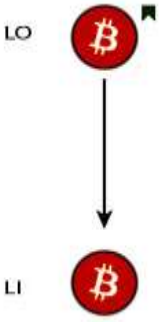

Рисунок 2.1 – Крок 1

Крок 2: Після проходження біткойн-атаки зловмисника бачимо, що L1 в контакті з 25 різними адресами біткойнов, що ускладнювало відстеження сліду(Рисунок 2.2).

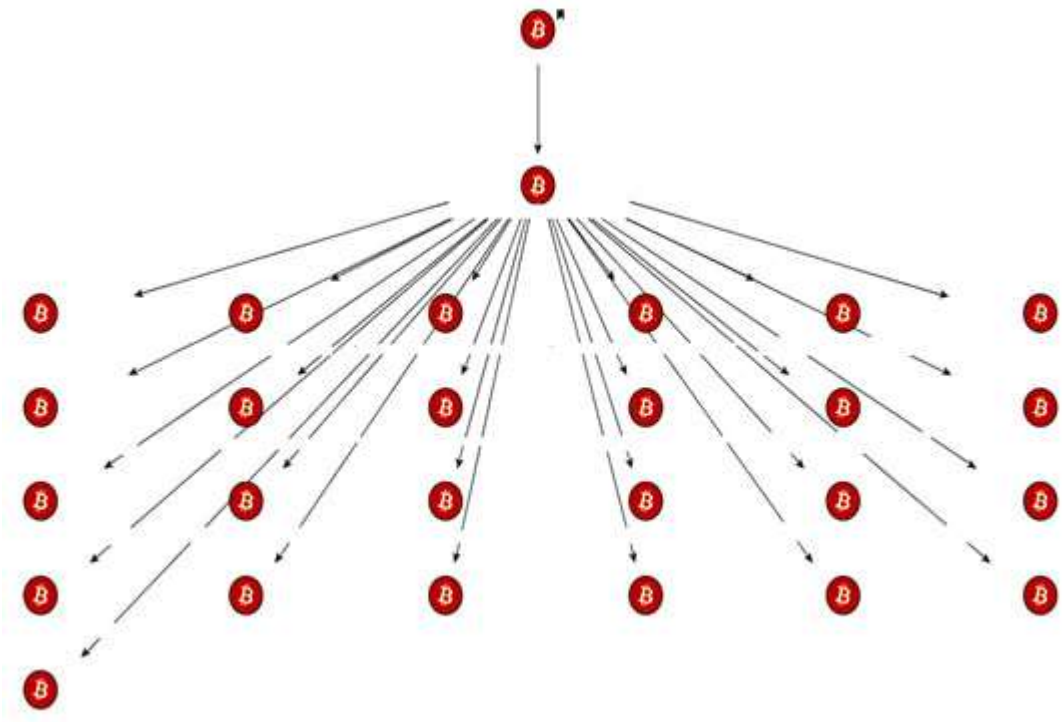

Рисунок 2.1 – Крок 2

Крок 3: Після проходження треку по кожній адресі біткойнов, з яким зіткнулися, отримоємо величезну схему перехоплення, в якій кожен біткойн-адреса знаходиться в випадковому числі інших адрес біткойнов(Рисунок 2.3).

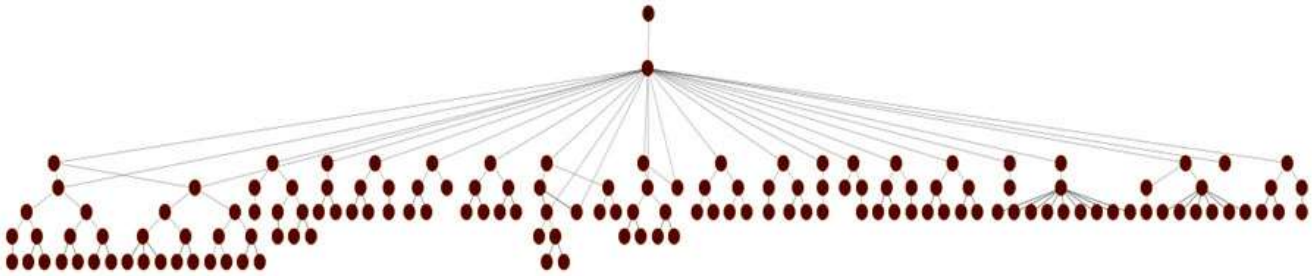

Рисунок 2.3 – Крок 3

Всі сервіси змішування працюють практично однаково, причому кожна послуга має певні варіації. Як тільки кошти переміщуються від замовника до першої облікового запису мікшування (званої шлюзом служби мікшування), вони відскакують навколо декількох облікових записів і в якийсь момент проходять через один або кілька масивних вузлів (званих пулами).

На рисунку 2.4 ми спостерігаємо техніку підстрибування в дії.

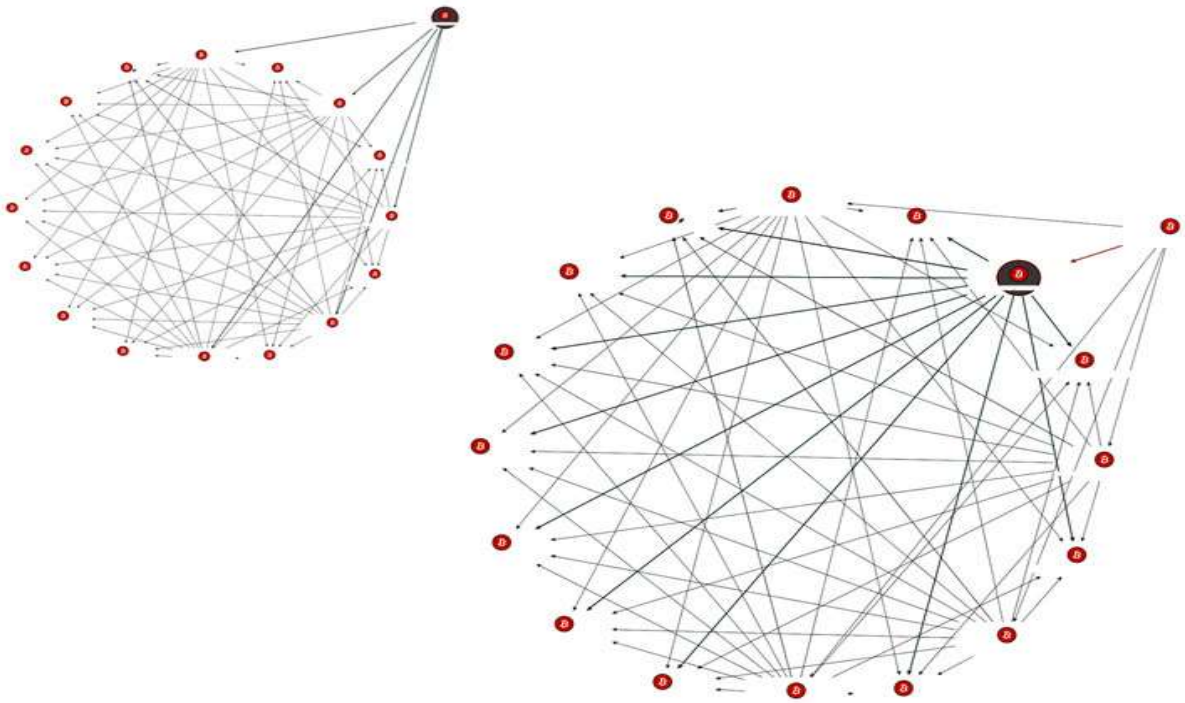

Рисунок 2.4 – Техніка підстрибування

Крок 1: Керуючий вузол переносить засоби на п'ять інших вузлів (жирні посилання).

Крок 2: Кожен з цих вузлів розподіляє свої кошти між додатковими вузлами, які, в свою чергу, підтримують це колесо.

Ми можемо зробити деякі висновки з даних:

- «Підстрибування» використовується для покриття треків і плутає будь-якого, хто намагається стежити за грошовим тропом. Виробляються тисячі транзакцій з тисячами «свіжих» рахунків Bitcoin.

- Пули збільшують взаємозамінність (тобто кожен елемент може бути замінений іншим), і вони усувають будь-який зв'язок між першою обліковим записом замовника і його останнім. Фонди міняються місцями між безліччю різних користувачів, що будь-які спроби пов'язати акаунти марні.

Подібно тому, як наливається чай у чашки, змішувальна служба "легко заливає" (розподіляє) біткіни. На рисунку 2.5 показують іншу техніку, яка використовується змішувальними службами, "крапає" невелику кількість біткойнів у масивний вузол, а потім віддаляє решту в новий вузол, який у свою чергу робить точно так само. Щоб продовжити аналогію з чашкою, кожна чашка капає невелику частину свого чаю у дуже велику чашку та наливає решту чаю в відповідну нащадкову чашку під нею.

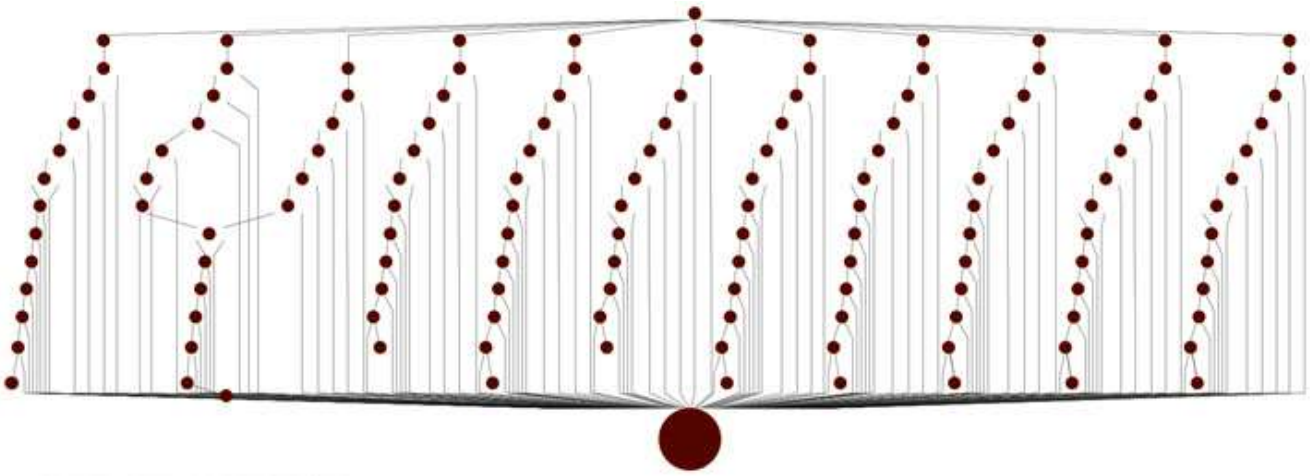

Рисунок 2.5 – Техніка «крапель»

Використовуючи графовий аналіз на Blockchain, виявляється досить швидко, що краще шукати кругові відносини. На відміну від форми «дерева»,

де вузли розміщуються в різних порядках, багато адреси біткойнов знаходяться в прямій залежності (отримані або відправлені кошти) з різними адресами з усіх рівнів дерева. Наприклад, віддалений вузол міг отримати платіж від масивного вузла на три рівні вище нього.

При розгляді графіка в круговому вигляді з'являються цікаві утворення(рисунок 2.6).

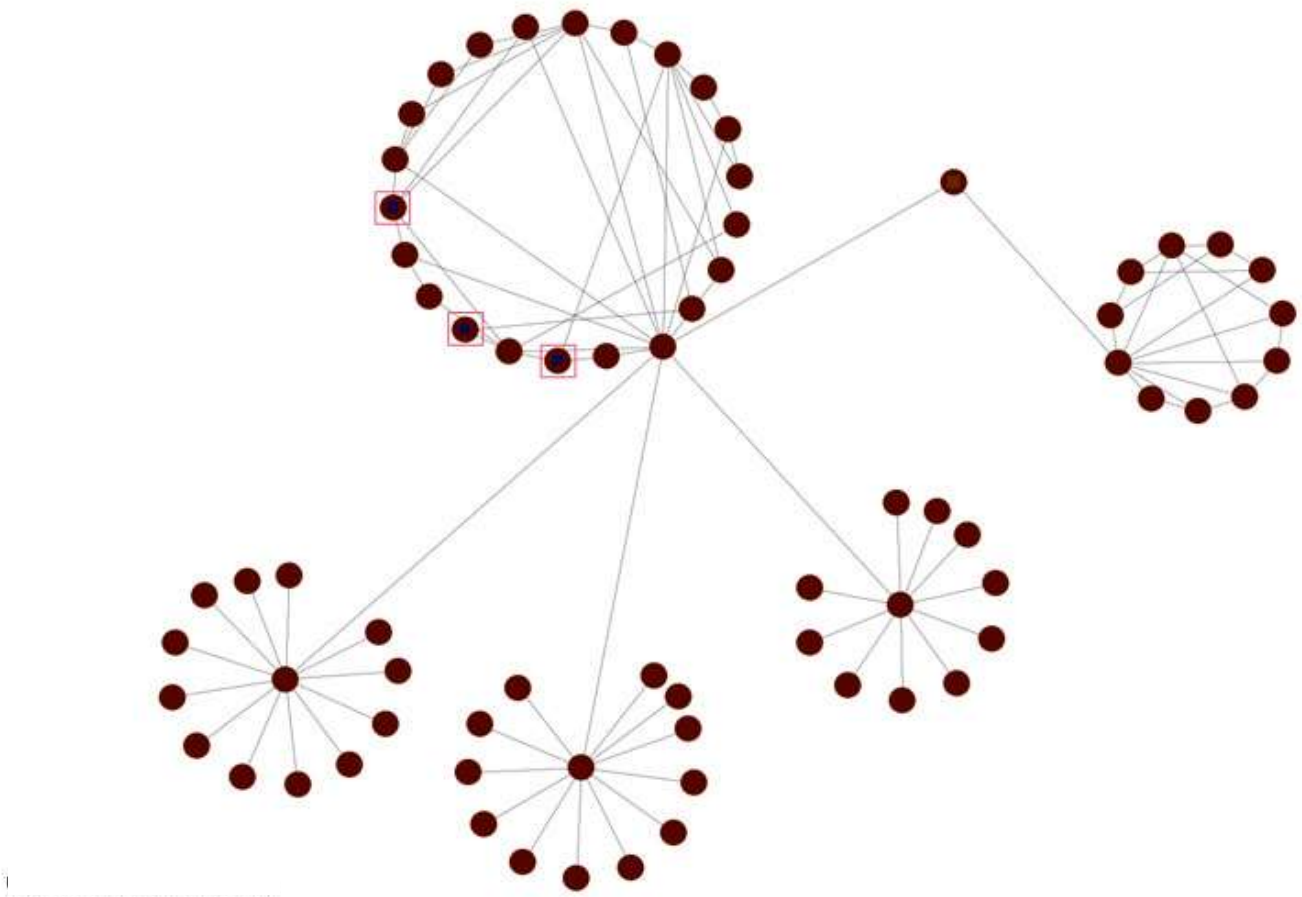

Рисунок 2.6 – Кругові утворення

Три вузла в верхньому лівому колі, відмічені рожевими квадратами швидше за все, «Exit nodes», де кошти закінчуються і чекають свого власника.

Можливі ризики

При використанні Bitcoin-міксерів потрібно тверезо оцінювати ризики. Завжди є ймовірність, що сервіс, що надає послуги міксера, є шахрайським.

Використовуючи міксер, ви відправляєте кошти невідомій особі, яка може і не повернути їх, а «відмотати» назад транзакцію вже буде неможливо. А з огляду на те, що система Bitcoin є децентралізованою, то вам просто не буде кому поскаржитися, оскільки служби підтримки просто не існує.

Також користувач повинен враховувати ризики передачі своїх особистих даних третім особам. В теорії сервіси-міксери можуть надавати логи співробітникам спецслужб за умови, якщо на них буде чинитися тиск. В першу чергу ці ризики стосуються власників великих сум, тому інвестори, у яких на гаманці лежить пара монет, не варто панікувати.

Потрібно усвідомлювати, що жоден сервіс-міксер не дасть стовідсоткової гарантії якісного перемішування біткоіни. Якщо алгоритм перемішування занадто простий, то його можна легко обчислити, а, отже, дізнатися, хто заводив гроші в систему і куди виводив. До того ж, якщо з міксера до вас надійдуть біткоіни, зароблені нечесним способом, це також може викликати підозру. Ваші кошти, чесно зароблені на «хайп», здадуться Вам нешкідливою забавою в порівнянні з грошима, зробленими на торгівлі наркотиками або зброєю.

2.3 VPN та цибулева маршрутизація

Tor (The Onion Router) — вільне і відкрите програмне забезпечення для реалізації другого покоління так званої цибулевої маршрутизації. Це система проксі-серверів, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослуховування. Розглядається як анонімна мережа віртуальних тунелів, що надає передачу даних в зашифрованому вигляді. Написана переважно на мовах програмування C, C ++ і Python.

За допомогою Tor користувачі можуть зберігати анонімність в Інтернеті при відвідуванні сайтів, веденні блогів, відправлення миттєвих і поштових повідомлень, а також при роботі з іншими додатками, що використовують протокол TCP. Анонімізація трафіку забезпечується за рахунок використання розподіленої мережі серверів - вузлів. Технологія Tor також забезпечує захист від механізмів аналізу трафіку, які ставлять під загрозу не тільки приватність в

Інтернеті, але також конфіденційність комерційних таємниць, ділових контактів і таємницю зв'язку в цілому.

Tor оперує мережевими рівнями onion-маршрутизаторів, дозволяючи забезпечувати анонімні вихідні з'єднання і анонімні приховані служби.

Користувачі мережі Tor запускають «цибульний» проксі-сервер на своїй машині, який підключається до серверів Tor, періодично створюючи ланцюжок крізь мережу Tor, яка використовує багаторівневе шифрування. Кожен пакет даних, що потрапляє в систему, проходить через три різних проксі-сервера - вузла, які вибираються випадковим чином. Перед відправленням пакет послідовно шифрується трьома ключами: спочатку для третього вузла, потім для другого і в кінці, для першого. Коли перший вузол отримує пакет, він розшифровує «верхній» шар шифру (аналогія з тим, як чистять цибулину) і дізнається, куди відправити пакет далі. Другий і третій сервер надходять аналогічним чином. У той же час, програмне забезпечення «цибульного» проксі-сервера надає SOCKS-інтерфейс. Програми, що працюють по SOCKS-інтерфейсу, можуть бути налаштовані на роботу через мережу Tor, який, мультіплексіруя трафік, направляє його через віртуальну ланцюжок Tor і забезпечує анонімний веб-серфінг в мережі.

На рисунку 2.7 зображен принцип роботи Tor.

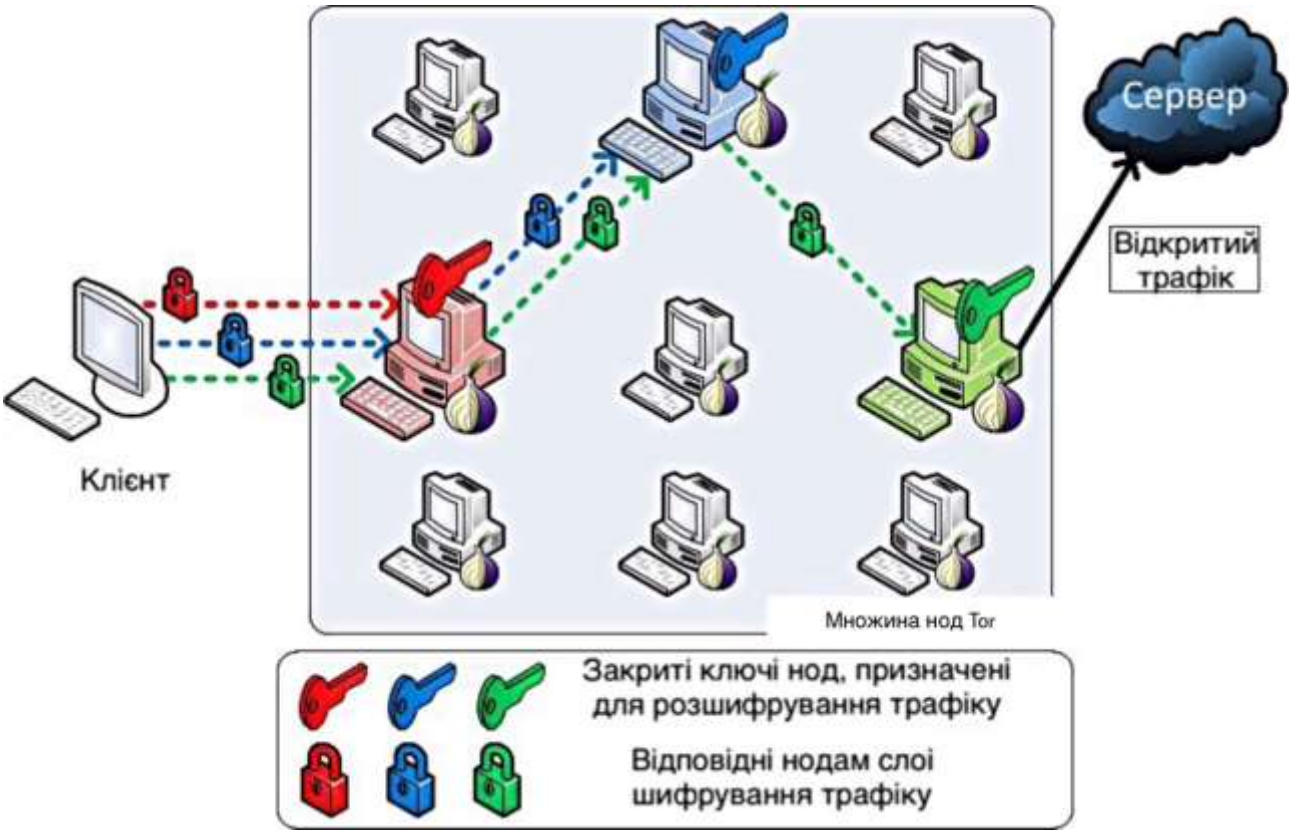

Рисунок 2.7 – Принцип роботи Tor

2.3.1 Види вузлів Tor

Вхідні вузли (entry node)

Вхідні вузли служать для прийняття ініційованих клієнтами мережі Tor з'єднань, їх шифрування і подальшого перенаправлення до наступного вузла. Слід зазначити, що зміна інформації, що передається на шляху від клієнта мережі до вхідного вузла не представляється можливим, тому що відповідно до технічної специфікації протоколу Tor, кожен пересилається блок даних захищений імітовставки. Також неможливий перехоплення з'єднання на шляху до вхідного вузла, оскільки застосовується гібридне шифрування сеансовим ключем TLS, що не допускає витоків інформації про тип або змісті пакетів.

Посередницькі вузли (middleman node)

Посередницький вузол, також іноді званий невихідний (non-exit node), передає зашифрований зв'язок тільки між іншими вузлами мережі Tor, що не дозволяє його користувачам безпосередньо підключатися до сайтів, що знаходяться поза зоною .onion. Обслуговування посередницького вузла

набагато менш ризиковано, оскільки він не стає причиною скарг, властивих для вихідного. Крім того, IP-адреси посередницьких вузлів не з'являються в логах.

Вихідні вузли (exit node)

Останні в ланцюжку сервери Tor називаються вихідними вузлами. Вони виконують роль передавальної ланки між клієнтом мережі Tor і публічним Інтернетом. Це робить їх найбільш вразливою частиною всієї системи. Тому кожен ретранслятор Tor має гнучкі налаштування правил виведення трафіку, які дозволяють регулювати використання тих чи інших портів, протоколів і лімітів швидкості для запущеного користувачем вузла мережі. Ці правила представлені в директорії Tor, отже, клієнт автоматично буде уникати підключення до закритих ресурсів. У будь-якому випадку, користувачеві, який вирішив запустити у себе вихідний вузол, слід бути готовим до виникнення різних нештатних ситуацій.

Сторожові вузли (guard node)

Мережа Tor вразлива до атак, при яких атакуючий контролює обидва кінці каналу передачі (тобто, вхідний і вихідний вузли ланцюжка). Кожен раз при побудові ланцюжка вузлів Tor існує небезпека, що вона буде скомпрометована таким чином.

Тому, в версії Tor 0.1.1.2-alpha були вперше впроваджені так звані сторожові вузли. Починаючи з версії Tor 0.1.1.11-alpha вони використовуються за замовчуванням. Філософська передумова цієї технології полягає в тому, що для більшості користувачів Tor поодинокі скомпрометовані з'єднання практично так само погані, як і постійні.

При використанні повністю випадкових вхідних і вихідних вузлів в кожній ланцюжку, ймовірність компрометації ланцюжка постійна і становить приблизно $(C / N)^2$ де C - кількість вузлів, контрольованих атакуючим, а N - загальна кількість вузлів мережі. З цього випливає, що якщо атакуючий досить довго контролює навіть незначне число вузлів, кожен постійний користувач Tor рано чи пізно використовує скомпрометований ланцюжок.

Щоб уникнути цього, клієнт Tor вибирає невелике число вузлів в якості сторожових і використовує один з них в якості вхідного вузла для кожної створюваної ланцюжка, поки ці вузли в робочому стані. Якщо жоден з сторожових вузлів користувача не контролюється атакуючим, все ланцюжка даного користувача будуть надійними. Але і в тому випадку, якщо один або навіть всі сторожові вузли користувача потрапили під контроль атакуючого, ймовірність компрометації кожної його ланцюжка складає не 100%, а менше, ніж C / N

Таким чином, в умовах контролю атакуючим невеликої частини вузлів мережі, технологія сторожових вузлів зменшує ймовірність бути скомпрометованим хоча б один раз, не впливаючи на математичне очікування кількості скомпрометованих з'єднань для довільно обраного користувача. Простіше кажучи, вона забезпечує надійність з'єднань для більшості користувачів за рахунок «концентрації» скомпрометованих з'єднань у меншої частини користувачів. З урахуванням вищезгаданої філософії, це є виграшним рішенням для більшості користувачів мережі Tor.

Мостові вузли (bridge relay)

Ретранслятори, звані бриджами (Tor Bridges) є вузлами мережі Tor, адреси яких не публікуються в сервері каталогів і використовуються в якості точок входу як для завантаження директорій, так і для побудови ланцюжків. Оскільки відкритого списку мостів не існує, навіть блокування будь-яких громадських адрес Tor не вплине на доступність цих прихованих ретрансляторів. Кореневі сервери мостових вузлів збирають IP-адреси бриджів і передають їх користувачам по електронній пошті, через веб-сервери або шляхом запитів, що значно підвищує їх цензурозащіщённость. Додавання функції мостів в Tor стало відповіддю на спроби блокування адрес мережі деякими цензорами. Але навіть цього може бути недостатньо, оскільки ряд програм фільтрації може відстежити незашифровані запити до теки Tor. Тому програмне забезпечення мережі починаючи з версії 0.2.0.23-rc за замовчуванням використовують шифрування запитів і періодичну зміну TLS

для імітації роботи веб-браузерів. Однак, даний спосіб маскування є важкореалізовуваної завданням там, де відбувається блокування TLS, як, наприклад, в Ірані.

2.3.2 Організаційні вказівки по запобіганню витоку деанонімізуючих данних при використанні Tor

1 Відвідувати власний сайт в анонімному режимі

Краще уникати відвідування персональних сайтів, до яких прикріплені реальні імена або псевдоніми, особливо якщо до них коли-небудь пристрою без використання Tor / с реальним IP-адресою. Ймовірно, далеко не всі люди відвідують ваш особистий сайт через Tor. Це означає, що користувач може бути єдиним унікальним клієнтом Tor, який зробить це.

Така поведінка веде до витоку анонімності, оскільки після відвідин веб-сайту вся схема Tor стає «брудної». Якщо сайт малопопулярен і не отримує багато трафіку, то вихідні вузли Tor можуть бути майже впевнені, що відвідувач цього сайту - власник сайту. З цього моменту розумно припустити, що наступні з'єднання з цього вихідного вузла Tor теж йдуть з комп'ютера користувача.

2 Заходити в акаунти соціальних мереж і думати, що ви анонімні

Не заходьте в особистий аккаунт Facebook або іншої соціальної мережі через Tor. Навіть якщо замість реального імені використовується псевдонім, аккаунт ймовірно пов'язаний з друзями, які знають вас. В результаті, соціальна мережа може висунути розумне припущення, ким насправді є користувач.

Жодна система анонімності не ідеальна. Софт для онлайнової анонімності може приховувати IP-адреси і місце розташування, але Facebook і таким же корпораціям не потрібна ця інформація. Соціальні мережі вже знають користувача, його друзів, вміст «приватних» повідомлень між ними і так далі. Ці дані зберігаються як мінімум на серверах соціальної мережі, і ніяке програмне забезпечення не здатне видалити їх. Їх можуть видалити тільки самі платформи соціальних мереж або хакерські групи.

Користувачі, які заходять в свої акаунти Facebook і інші акаунти, отримують тільки захист розташування, але не анонімність

З Ніколи не заходьте в акаунти, якими ви користувалися без Tor

Завжди припускайте, що при кожному візиті журнал сервера зберігає наступне:

- Клієнтські IP-адреса / розташування.
- Дату і час запиту.
- Конкретні адреси запитаних сторінок.
- Код HTTP.
- Кількість байт, переданих користувачеві.
- Агент браузера у користувача.
- Сайт, що посилається (реферрер).

Також припускайте, що інтернет-провайдер (ISP) запише як мінімум час в онлайні і IP-адреса / розташування клієнта. Провайдер може також записати IP-адреси / розташування відвіданих сайтів, скільки трафіку (даних) передано і що конкретно було передано і отримано. До тих пір, поки трафік не зашифрований, ISP зможе бачити, які конкретно дії здійснювалися, отриману і відправлену інформацію.

У таблиці 2.1 надане спрощене уявлення, як ці логи можуть виглядати для адміністраторів.

Таблиця 2.1 – Логи

Ім'я	Час	IP/місце	Трафік	Адреса	Контент
Ivanov Ivan	16:00-17:00	1.1.1.1	1МБ	Google.com	Пошуковий запит 1, запит 2
Ivanov Ivan	16:00-17:00	1.1.1.1	500МБ	Youtube.com	Проглянуто відео 1, відео 2
Ivanov Ivan	16:00-17:00	1.1.1.1	9МБ	Facebook.com	Зашифрований трафік

4 Не авторизуйтесь в онлайн-банкінгу або платіжних системах, якщо не усвідомлюєте ризики

Не рекомендується авторизація в онлайн-банку, PayPal, eBay і інших важливих фінансових акаунтах, зареєстрованих на ім'я користувача. У фінансових системах будь-яке використання Tor загрожує заморожуванням аккаунта через «підозрілої активності», яка реєструється системою запобігання фрода. Причина в тому, що хакери іноді використовують Tor для здійснення шахрайських дій.

Використання Tor з онлайн-банкінгом і фінансовими акаунтами не є анонімним з причин, наведених вище. Це псевдонімного, яка забезпечує тільки приховування IP-адреси, або виверт для доступу до сайту, заблокованого провайдером. Різниця між анонімністю і псевдонімного описана у відповідній главі.

Якщо користувача заблокували, у багатьох випадках можна звернутися до служби підтримки, щоб розблокувати аккаунт. Деякі сервіси навіть допускають ослаблення правил визначення фрода для користувача аккаунтів.

5 Не чергуйте Tor і Open Wi-Fi

Деякі користувачі помилково думають, що відкритий Wi-Fi - більш швидка і безпечна «альтернатива Tor», оскільки IP-адреса не можна прив'язати до реального імені.

Нижче пояснимо причини, чому краще використовувати відкритий Wi-Fi і Tor, але не відкритий Wi-Fi або Tor.

Приблизне місцезнаходження будь-якого IP-адреси можна обчислити до міста, району або навіть вулиці. Навіть якщо користувач далеко від свого будинку, відкритий Wi-Fi все одно видає місто і зразкове місце розташування, оскільки більшість людей не подорожують по континентах.

Особу власника з відкритим Wi-Fi і налаштування маршрутизатора - теж невідомі змінні. Там може вестися журнал MAC-адрес користувачів з відповідною активністю цих користувачів в Інтернеті, яка відкрита для власника маршрутизатора.

Хоча журнал необов'язково порушує анонімність користувача, вона звужує коло підозрюваних з усього глобального населення Землі або континенту, або країни - до конкретного району. Цей ефект сильно погіршує анонімність. Користувачам слід завжди залишати у себе максимально можливу кількість інформації.

6 Не відправляйте конфіденційні дані без кінцевого шифрування

Як вже пояснювалося, вихідні вузли Tor можуть прослуховувати комунікації і здійснювати атаки посередника (MiTM), навіть при використанні HTTPS. Використання кінцевого шифрування – єдиний спосіб відправити конфіденційні дані одержувачу, уникнувши ризику перехоплення і розкриття ворожим третім особам.

7 Не розкривайте в онлайні ідентифікаційні дані

Деанонімізація можлива не тільки з сполуками і IP-адресами, але також соціальними способами. Ось деякі рекомендації захисту від деанонімізація:

- Не включайте в ники персональну інформацію або особисті інтереси.
- Не обговорюйте персональну інформацію, таку як місце проживання, вік, сімейний статус і т. Д. З часом дурні розмови на кшталт обговорення погоди можуть призвести до точного обчислення місця розташування користувача.
- Не згадуйте підлогу, татуювання, пірсинг, фізичні здібності або недоліки.
- Не згадуйте професію, хобі або участь в активістських групах.
- Не використовуйте спеціальні символи на клавіатурі, які існують тільки в вашій мові.
- Не публікуйте інформацію в звичайному Інтернеті (Clearnet), будучи анонімним.
- Не використовуйте Twitter, Facebook та інші соціальні мережі. Вас легко буде пов'язати з профілем.
- Не публікуйте посилання на зображення Facebook. В імені файлу міститься ваш персональний ID.

- Не заходьте на один сайт в один і той же час дня чи ночі. Намагайтеся варіювати час сеансів.

8 Не використовуйте чистий веб та Tor одночасно

Використовуючи водночас не-Tor браузер і Tor Browser, ви ризикуєте одного разу їх переплутати і деанонімізіровать себе.

При одночасному використанні чистого інтернету і Tor також виникають ризики одночасних з'єднань до сервера за анонімними і неанонімні каналах. Це не рекомендується з причин, викладених у наступному розділі. Користувач ніколи не може відчувати себе безпечно, відвідуючи одну і ту ж сторінку одночасно за анонімними і неанонімні каналам, тому що він бачить тільки URL, але не те, скільки ресурсів запитується в тлі. Багато різних сайтів розміщуються в одному хмарі. Сервіси на зразок Google Analytics представлені на більшості сайтів і тому бачать багато анонімних і неанонімних з'єднань.

9 Не підключайтеся до сервера анонімно і 44е анонімні одночасно

Сильно не рекомендується створювати з’єднання Tor і не-Tor також до одного віддаленого сервера. У разі розриву зв’язку з Інтернетом (а це з часом відбудеться) всі з’єднання урвуться одночасно. Після такої події противник легко визначить, який публічний IP-адреса / розташування належать якомусь IP-адресою / з’єднанню Tor, що потенційно безпосередньо ідентифікує користувача.

Такий сценарій також дає можливість провести інший вид атаки з боку веб-сервера. Швидкість Tor і не-Tor з’єднань може бути збільшена або зменшена, щоб перевірити наявність кореляції. Так, якщо обидва з’єднання прискорюються або сповільнюються в унісон, то можна встановити взаємозв’язок між сесіями Tor і не-Tor.

10 Не відкривайте випадкові файли і посилання

Якщо користувачеві прислали файл будь-якого типу або посилання на файл (або на випадковий URL / ресурс) по електронній пошті або іншим способом, потрібна обережність незалежно від формату файлу. [23] Відправник, поштовий ящик, аккаунт або ключ можуть бути скомпрометовані,

а файл або посилання могли бути спеціальним чином підготовлені для зараження системи користувача при відкритті в стандартному додатку.

Безпечніше не відкривати файл стандартним інструментом, який передбачається використовувати творцем файлу. Наприклад, PDF можна відкривати програмою перегляду PDF, або якщо файл доступний публічно, можна використовувати безкоштовний онлайновий сервіс перегляду PDF.

11 Не використовуйте верифікацію по (мобільному) телефону

Веб-сайти на кшталт Google, Facebook і інші попросять (мобільний) телефонний номер, як тільки ви спробуєте увійти через Tor. Якщо немає необхідності виключно розумний або має альтернативу, цю інформацію не можна надавати. Будь-які телефонні номери будуть внесені в журнал. SIM-карта швидше за все зареєстрована на ім'я користувача. Навіть якщо це не так, отримання SMS видає місце розташування. Користувачі можуть спробувати анонімно купити SIM-карту далеко від свого звичайного домашнього адреси, але все одно залишається ризик: сам телефон. Кожен раз при реєстрації в мережі провайдер зберігає серійний номер SIM-карти і серійний номер телефону. Якщо SIM-карта куплена анонімно, а телефон немає, то анонімності не буде, тому що два серійних номера зв'яжуть разом.

Користувачі можуть спробувати знайти онлайновий сервіс, який отримає персональне SMS від їх імені. Це спрацює і забезпечить анонімність. Проблема в тому, що в Google і Facebook такий метод навряд чи спрацює, тому що вони активно вносять в чорні списки такі номери верифікації. Інший варіант - знайти кого-небудь, хто отримає SMS замість вас, але це лише перенесе ризики на іншу людину.

Якщо користувач дійсно хоче пройти верифікацію за номером мобільного телефону, то рекомендується виїхати далеко від будинку, знайти свіжий телефон з новою SIM-картою. Після верифікації телефон слід вимкнути, і негайно після цього телефон і SIM-карту потрібно повністю знищити. Це робиться шляхом спалювання або іншими винахідливими (надійними) способами знищення.

2.3 Керівництво з анонімного застосування криптовалюти

З урахуванням описаних вище проблем і технологій підвищення анонімності пропонується наступний алгоритм, який передбачає затруднення деанонімізація користувача на всіх етапах транзакції:

Крок 1: Створити гаманець №1 у відкритому інтернеті.

Сьогодні існує чотири види біткоіни-гаманців:

Комп'ютерний (десктопний) дозволяє зберігати біткоіни на персональному комп'ютері. У цьому випадку буде потрібно завантажити спеціальний додаток для своєї операційної системи і встановити його на ПК, як будь-яку іншу програму.

Веб-гаманець надає для зберігання біткоіни спеціалізовані онлайн-сервіси, де необхідно всього лише зареєструватися.

Мобільний варіант гаманця допомагає проводити розрахунки на мобільному пристрої. Для його установки також буде потрібно вибрати програму для своєї мобільної операційної системи.

Апаратні гаманці - спеціальні знімні пристрої, на яких встановлено необхідне програмне забезпечення, що допомагає передавати або зберігати біткоіни.

Крок 2: Купити біткоіни і переслати їх в гаманець №1.

Перед тим, як купити біткоіни або іншу криптовалюта, клієнту потрібно зареєструватися і поповнити баланс в додатку. Внести гривні на свій рахунок в BTC Trade можна трьома способами: картою українського банку, через інтернет-банкінг Приват24 або в терміналі Приватбанку по попередньо згенеровані коду.

Крок 3: Створити гаманець №2 через мережу Tor.

Крок 4: Надіслати біткоіни з гаманця №1 в гаманець №2.

Крок 5: Створити гаманець №3 через Tor.

Крок 6: Вибрати міксер, який підтримує роботу з Tor, а потім створити набір адрес в гаманці №3 для отримання біткоіни з сервісу. Бажано

використовувати кілька адрес і виставляти час перемішування випадковим чином.

Крок 7: Надіслати засоби з гаманця №2 через Tor на адресу, створений міксером.

Крок 8: Використовуючи прихований адресу сервісу Blockchain.info в Tor, переконатися, що кошти повернулися з міксера.

Крок 9: Створити гаманець №4 через Tor та повторити кроки 6-8 з використанням іншого міксеру.

По закінченю цього кошти, які прийдуть на адресу, згенеровану міксером

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ КЕРІВНИЦТВА

При розробці керівництва з анонімного використання криптовалют одним з етапів є оцінка економічної ефективності його використання.

Так як проект являє собою послідовність дій, яка у чіткому порядку має бути виконана, при кожній транзакції з дотриманням багатьох умов, для контролю за виконанням цих дій слід мати певного співробітника організації.

Так як керівництво передбачає використання VPN-сервісу, то до розрахунку витрат необхідно включити щорічну плату за використання послугою, та плату за одноразове налаштування обладнання.

3.1 Розрахунок трудомісткості розробки керівництва

Спершу розрахуємо час, який буде витрачено на розробку керівництва:

$$t = t_{\text{тз}} + t_{\hat{a}} + t_{б} + t_{\text{пр}} + t_{\text{опр}} + t_{д}, \text{ годин,} \quad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку керівництва;

$t_{\hat{a}}$ – тривалість вивчення технічного завдання;

$t_{\ddot{a}}$ – тривалість вивчення ринку криптовалют;

$t_{б}$ – тривалість аналізу стану анонімності на ринку криптовалют;

$t_{\text{пр}}$ – тривалість аналізу існуючих засобів забезпечення анонімності;

$t_{\text{опр}}$ – тривалість опрацювання керівництва;

Таблиця 3.1 Трудомісткість процесів

Назва процесу	Трудомісткість, год.
Складання технічного завдання на розробку керівництва	24
Вивчення технічного завдання	8
Вивчення ринку криптовалют	40
Аналіз стану анонімності на ринку криптовалют	40
Аналіз існуючих засобів забезпечення анонімності	56
Опрацювання керівництва	56

t = 24 + 8 + 40 + 40 + 56 + 56=224 годин.

3.2 Розрахунок витрат на створення керівництва

$$К_{пз} = З_{зп} + З_{мч}. \text{ грн} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 224 \cdot 29.76 = 6666.24, \text{ грн}, \quad (3.3)$$

де t – загальна тривалість створення керівництва, годин;

$З_{пр}$ – средньогодинна заробітна плата фахівця з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_{м}}{168} = \frac{5000}{168} = 29.76, \text{ грн/годину}. \quad (3.4)$$

де $З_{м}$ – середня заробітна плата фахівця з інформаційної безпеки – 5000 грн.

Вартість машинного часу для впровадження керівництва визначається за формулою:

$$З_{\text{мч}} = t_{опр} C_{\text{мч}} + t_{д} \cdot C_{\text{мч}} = 0.98 \cdot 224 = 219.52, \text{ грн}. \quad (3.5)$$

де $t_{опр}$ – трудомісткість впровадження керівництва, годин;

$t_{д}$ – трудомісткість підготовки документації, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{\text{мч}} = P \cdot C_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}} = 0.5 \cdot 1.68 + \frac{2700 \cdot 0.1}{1920} = 0.98, \text{ грн/год}, \quad (3.6)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 1.68 грн/кВт·година;

$Ф_{перв}$– первісна вартість ПК на початок року, 2700 грн.;

H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920 год).

Отже, $K = 6666.24 + 219.52 = 6885.76$ грн (3.7)

3.3 Розрахунок річних експлуатаційних витрат

Витрати на річну експлуатацію становлять витрати на оплату VPN-сервісу.

Проаналізувавши список компаній, що надають послуги хостингу, в середньому на рік витрати будуть складати 1800 грн на рік.

Додаткові витрати на розробку та впровадження керівництва залежать від кількості криптовалюти гаманця, транзакції якого потребують анонімності

3.4 Економічне обґрунтування

У цьому розділі розраховується мінімальний розмір гаманця, для якого розмну використовувати керівництво

У-В-К ≥ 0 (3.8)

де У-вірогітний збиток від втрати коштів

В-додаткові, та річні експлуатаційні витрати

К-витрати на створення керівництва

Отже для ефективного використання керівництва вірогідні збитки за вичетом додаткових витрат мають перевищувати чи дорівнювати добуток витраи на створення і щорічних витрат.

У+додаткові витрати≥ 6885.76 +1800=8685,76 грн. (3.9)

Тобто мінімальний розмір гаманця дорівнює 8501.52, або приблизно 0.02924498BTC.

3.5 Висновок

Забезпечення анонімності при ведені фінансової діяльності має багато переваг, переважно це стосується приховання від конкурентів результатів бізнес-діяльності.

Також приховання інформації про стан своїх криптовалютних активів знижає ризик активних атак, направлених на викрадення ключів від електронного гаманця.

ВИСНОВКИ

У ході виконання дипломної роботи було проведено аналіз механізмів роботи криптовалют, проаналізован рівень забезпечення анонімності при здійснені криптовалютних транзакцій та існуючи загрози, які направлені на деанонімізацію користувачів, вивчені зовнішні методи підвищення рівня анонімності, проведено аналіз переваг та недоліків, ризиків що виникають при їх застосуванні.

Було розроблено пошагове керівництво по використанню способів підвищення анонімності, у ньому були запропоновані найсучасніші та най доцільніші методи та їх комбінації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Complex Web: Bitcoin Mixing Services. [Електронний ресурс]. – Режим доступу : https://blog.checkpoint.com/2016/11/23/complex-web-bitcoin-mixing-services/

2. Биткоин P2P деньги с открытым кодом [Електронний ресурс]. – Режим доступу : https://bitcoin.org/ru/

3. The price of anonymity: empirical evidence from a market for Bitcoin anonymization [Електронний ресурс]. – Режим доступу : https://academic.oup.com/cybersecurity/advancearticle/doi/10.1093/cybsec/tyx007/4057584?searchresult=1

4. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries [Електронний ресурс]. – Режим доступу: http://econinfosec.org/wp-signup.php?new=www.weis2013

5. Blockchain [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/

6. Deanonymisation of clients in Bitcoin P2P network [Електронний ресурс]. – Режим доступу : https://arxiv.org/pdf/1405.7418v1.pdf

7. Blockchain [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/

8. An Analysis of Anonymity in the Bitcoin System [Електронний ресурс]. – Режим доступу: http://anonymity-in-bitcoin.blogspot.com/2011/07/bitcoin-is-not-anonymous.html

9. Криптовалюта Bitcoin [Електронний ресурс]. – Режим доступу: http://cryptowiki.net/index.php?title=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82a_Bitcoin.

10. Транзакция(криптовалюта) [Електронний ресурс]. – Режим доступу:

http://cryptowiki.net/index.php?title=%D0%A2%D1%80%D0%B0%D0%BD%D0%B7%D0%B0%D0%BA%D1%86%D0%B8%D1%8F(%D0%BA%D1%80%D

0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0)

11. PTES - Penetration Testing Execution Standard - Technical Guidelines. [Електронний ресурс]. – Режим доступу: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

12. Кількість підприємств за їх розмірами за видами економічної діяльності. [Електронний ресурс]. – Режим доступу: http://www.vn.ukrstat.gov.ua/index.php/statistical-information/-2016-/4108-2010-11-23-13-49-51.html.

13. Кримінальний Кодекс України. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14.

14. НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. [Електронний ресурс]. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106343.

15. Market Share Statistics for Internet Technologies. [Електронний ресурс]. – Режим доступу : https://www.netmarketshare.com/.

16. Демілітаризована зона (комп'ютерні мережі). [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Демілітаризована_зона_(комп%27ютерні_мережі).

17. Kali Linux Metapackages. [Електронний ресурс]. – Режим доступу : https://www.kali.org/news/kali-linux-metapackages/.

18. National Vulnerability Database. [Електронний ресурс]. – Режим доступу : http://nvd.nist.gov/.

19. Common Vulnerabilities and Exposures. [Електронний ресурс]. – Режим доступу : https://cve.mitre.org/.

20. Offensive Security’s Exploit Database Archive. [Електронний ресурс]. – Режим доступу : http://www.exploit-db.com.

21. Security Focus Vulnerabilities. [Електронний ресурс]. – Режим доступу : http://www.securityfocus.com.

22. Packetstorm Communications. [Електронний ресурс]. – Режим доступу : http://www.packetstorm.com

23. CXsecurity – Free information about cyber security. [Електронний ресурс]. – Режим доступу : http://www.securityreason.com.

24. CWE/SANS TOP 25 Most Dangerous Software Errors. [Електронний ресурс]. – Режим доступу : https://www.sans.org/top25-software-errors/.

25. Книга по Nmap на русском. [Електронний ресурс]. – Режим доступу : https://codeby.net/bezopasnost/kniga-po-nmap-na-russkom/#2.

26. Ціни на інформаційний аудит. [Електронний ресурс]. – Режим доступу: https://www.masiev.com/tseny-na-uslugi-kompanii.

27. О.Г. Вагонова, Ю.О. Волотковська, Н.М. Романюк. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека) – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

28. Закон України «Про Державний бюджет України на 2017 рік». [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1801-19.

29. Кодекс законів про працю України. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/322-08/page3.

30. Закон України «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування». [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2464-17.

31. Податковий Кодекс України. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2755-17/page19.

32. ДТЕК Дніпрообленерго. Тарифи на електроенергію на 2017 рік. [Електронний ресурс]. – Режим доступу : http://doe.com.ua/tarif_prom/2017.

ДОДАТОК А
ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Дипломний проект Шевченко Д.І. 125м–16–1.docx – Пояснювальна записка.
2. Шевченко Д.І.pttx – Презентація.

ДОДАТОК Б

ЗАКОН УКРАЇНИ

Про обіг криптовалюти в Україні

Верховна Рада України,

з метою регулювання правовідносини щодо обігу, зберігання, володіння, використання та проведення операцій за допомогою криптовалюти в Україні, приймає цей закон.

Глава І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі наведені нижче терміни та поняття вживаються в такому значенні:

1) криптовалюта – це програмний код (набір символів, цифр та букв), що є об’єктом права власності, який може виступати засобом міни, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду);

2) криптовалютна біржа – це організація, яка забезпечує взаємозв’язок між суб’єктами криптовалютних операцій, забезпечує обмін криптовалюти на електронні гроші, валютні цінності, цінні папери;

3) криптовалютний кошик - спеціалізоване програмне забезпечення або платформа, що дозволяє користувачу системи блокчейн зберігати криптовалюту і здійснювати криптовалютні транзакції;

4) криптовалютні транзакції - операція по переміщенню криптовалюти, відомості про яку зберігаються в системі блокчейн;

5) система блокчейн - децентралізований публічний реєстр усіх проведених криптовалютних транзакцій, які були проведені суб'єктом криптовалютних операцій;

6) користувач системи блокчейн – будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка за допомогою власного та/або орендованого технічного обладнання підтримує працездатність системи блокчейн, здійснює проведення криптовалютних транзакцій та захисту системи блокчейн;

7) суб'єкт криптовалютних операцій – криптовалютна біржа, користувач системи блокчейн, власник криптовалюти, майнер;

8) власник криптовалюти - будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка на законних підставах зберігає та володіє крипто валютою;

9) майнер – будь-яка фізична особа, фізична особа-підприємець або юридична особа, яка за допомогою власного та/або орендованого спеціалізованого обладнання забезпечує працездатність та безпечність системи блокчейн, криптовалютних транзакцій, і, в залежності від правил системи блокчейн, отримує винагороду системи блокчейн та/або набуває права власності на крипто валюту;

10) майнінг – це обчислювальні операції, які здійснює майнер за допомогою власного та/або орендованого спеціалізованого обладнання, з метою забезпечення працездатності та безпеки системи блокчейн, та залежно від умов системи блокчейн отримує винагороду системи блокчейн;

11) винагорода системи блокчейн - винагорода у вигляді облікових одиниць поточної системи блокчейн (криптовалюти), яку отримує майнер у випадку

знаходження (підписання) блоку транзакцій, який було записано до поточної системи блокчейн;

12) блок транзакцій – спеціально структурована складова одиниця системи блокчейн, яка містить у собі набір інформації, відповідно до вимог поточної системи блокчейн;

13) спеціалізоване обладнання – програмно-керований пристрій для обробки інформації (електронно-обчислювальна машина або її частини);

14) відомості про криптовалютні транзакції – дані щодо суб'єкту криптовалютних операцій, призначення криптовалютної транзакції та будь-які інші дані, що мають відношення до криптовалютних транзакцій.

Стаття 2. Законодавство в сфері обігу криптовалюти

1. Загальні засади обігу криптовалюти регулюються Конституцією України, Цивільним кодексом України, Господарським кодексом України, Податковим кодексом України, Законом України «Про інформацію», цим Законом, нормативно-правовими актами Національного Банку України та іншими законами України.

Стаття 3. Державне регулювання

1. Державне управління в сфері обігу криптовалюти здійснюється Національним Банком України.

Стаття 4. Державні гарантії

1. Держава не несе зобов'язань, а також не відшкодовує вартість криптовалюти у випадку її знецінювання або втрати з будь-яких інших причин.

2. Держава не гарантує та не здійснює будь-яких заходів із забезпечення діяльності онлайн-сервісів з обміну криптовалюти.

Стаття 5. Майнінг криптовалюти

1. Криптовалюта отримується як винагорода системи блокчейн, в результаті її генерації у системі блокчейн майнером, який виконав необхідні умови для її отримання.

2. Отримана в порядку частини 1 цієї статті криптовалюта є власністю майнера, та є об’єктом оподаткування.

3. Майнер самостійно вживає усі необхідні дії для захисту і зберігання власної криптовалюти.

4. Майнер на свій власний розсуд обирає тип криптовалюти для майнінгу.

5. Майнінг криптовалюти здійснюється власними та/або орендованими засобами майнера за власним вибором та на свій власний ризик.

Стаття 6. Використання криптовалюти

1. Суб’єкт криптовалютних операцій має право вільно розпоряджатись криптовалютою, зокрема здійснювати операції з міни (обміну) криптовалюти будь-яких видів на іншу криптовалюту, обмінювати її на електроні гроші, валютні цінності, цінні папери, послуги, товари тощо.

2. До криптовалюти застосовуються загальні норми які розповсюджуються на право приватної власності.

3. Порядок оподаткування операцій з майнінгу, міни (обміну) криптовалюти регулюється чинним законодавством України.

4. Використання криптовалюти не може бути застосовано проти основ національної безпеки України, для закликів до повалення конституційного ладу, порушення територіальної цілісності України, вчинення терористичних актів, фінансування тероризму, легалізації (відмивання) доходів одержаних злочином шляхом, обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших протиправних діяннях.

5. Суб'єкт криптовалютних операцій самостійно дбає про захист криптовалюти та цілісність системи блокчейн.

Глава ІІ. ПОРЯДОК ПРОВЕДЕННЯ ОПЕРАЦІЙ З КРИПТОВАЛЮТАМИ

Стаття 7. Криптовалютні транзакції

1. До криптовалютних транзакції застосовуються загальні положення про договір міни, у відповідності до законодавства України.

2. Дані про криптовалютні транзакції зберігаються у системі блокчейн та є відкритими та загальнодоступними для всіх суб'єктів криптовалютних операцій.

3. Криптовалютні транзакції містять відомості про криптовалютний кошик, з якого виконано передачу, одержувача, об'єм переказу, тимчасові мітки, що визначають момент передачі.

4. Суб'єкт криптовалютних операцій самостійно гарантує проведення транзакцій криптовалюти.

5. Суб'єкт криптовалютних операцій зобов'язується зберігати данні щодо проведених транзакцій протягом 5 років.

Стаття 8. Діяльність криптовалютної біржі

1. Порядок створення та діяльності криптовалютної біржі здійснюється виключно в порядку встановленому Національним Банком України.

2. Криптовалютна біржа зобов'язана здійснювати моніторинг всіх транзакцій, ідентифікацію та персоніфікацію суб'єкта криптовалютних операцій в порядку встановленому Національним Банком України.

3. Обмін криптовалюти на електронні гроші, фінансові цінності, цінні папери здійснюється виключно криптовалютною біржою.

4. Дохід отриманий криптовалютною біржою від здійснення криптовалютних операцій підлягає оподаткуванню у відповідності до вимог чинного законодавства України.

5. Обмін (переміщення) криптовалюти може здійснюватися за допомогою онлайн-сервісів з обміну криптовалюти в мережі Інтернет.

6. Суб'єкт криптовалютних операцій здійснює міну (обмін) криптовалюти за допомогою онлайн-сервісів з обміну криптовалюти на свій власний ризик.

Глава III. ВІДПОВІДАЛЬНІСТЬ

Стаття 9. Порушення законодавства України про використання обіг криптовалюти

1. Порушення законодавства України про використання та обіг криптовалюти тягне за собою цивільно-правову, адміністративну або кримінальну відповідальність згідно із законодавством України.

Глава IV. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через три місяці з дня його опублікування.

2. Внести зміни до Закону України «Про Національний банк України» (Відомості Верховної Ради України (ВВР), 1999, № 29, ст.238):

1) статтю 7 доповнити пунктом 32 такого змісту:

«32) визначає порядок створення та діяльності криптовалютної біржі, моніторингу всіх криптовалютних транзакцій, порядок ідентифікації суб'єкту криптовалютних операцій.».

3. Кабінету Міністрів України протягом двох місяців з дня набрання чинності цим Законом:

привести власні нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

4. Національному Банку України протягом двох місяців з дня набрання чинності цим Законом:

розробити порядок створення та діяльності криптовалютних бірж, порядок моніторингу всіх транзакцій, ідентифікацію та персоніфікацію суб'єктів криптовалютних операцій;

привести у відповідність із цим Законом власні нормативно-правові акти.

Голова Верховної Ради

України

ДОДАТОК Г
ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)