**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені ІГОРЯ СІКОРСЬКОГО»**

**Радіотехнічний факультет**

**Кафедра приймання та оброблення сигналів**

|  |  |
| --- | --- |
| «На правах рукопису»  УДК \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | До захисту допущено:  Завідувач кафедри  \_\_\_\_\_\_\_\_  «\_\_\_». травня 2020 р. |

**Магістерська дисертація**

**на здобуття ступеня магістра**

**за освітньо-науковою програмою «Радіозвязок та оброблення сигналів»**

**зі спеціальності 172«Телекомунікація та радіотехніка »**

**на тему: «Децентралізований VoIP зв’язок з використанням методів блокчейн»**

Виконав:

студент VІ курсу, групи РА-81мн

Цимбаленко Іван Миколайович. \_\_\_\_\_\_\_\_\_\_

Консультант з охорони праці:

к.т.н., доцент Каштанов Сергій Федорович \_\_\_\_\_\_\_\_\_\_

Керівник:

Доцент каф. РОС, к.т.н., доцент,

Мосійчук Віталій Сергійович \_\_\_\_\_\_\_\_\_\_

Рецензент:

Доцент каф. РТПС, к.т.н., доцент

Могильний Сергій Борисович \_\_\_\_\_\_\_\_\_\_

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент (-ка) \_\_\_\_\_\_\_\_\_\_\_\_\_

Київ – 2020 року

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Радіотехнічний факультет**

**Кафедра радіоприймання та оброблення сигналів**

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 Телекомунікація та радіотехніка

Освітньо-наукова програма – Радіотехнічні інформаційні технології

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 р.

**ЗАВДАННЯ**

**на магістерську дисертацію студенту**

**Цимбаленко Іван Миколайович**

1. Тема дисертації «Децентралізований VoIP зв’язок з використанням методів блокчейн», науковий керівник дисертації Мосійчук Віталій Сергійович, кандидат наук, доцент, затверджені наказом по університету від «\_\_\_»\_\_\_\_\_\_\_\_\_ 20\_\_ р. №\_\_\_\_\_

2. Термін подання студентом дисертації

3. Об’єкт дослідження є процеси встановлення з'єднання та автентифікації абонентів IP телефонії.

4. Предмет дослідження є методи та алгоритми публічної автентифікації абонентів IP телефонії на основі ланцюжків блоків транзакцій (блокчейн).

5. Перелік завдань, які потрібно розробити

6. Орієнтовний перелік графічного (ілюстративного) матеріалу презентація PowerPoint у вигляді слайдів

7. Орієнтовний перелік публікацій

8. Консультанти розділів дисертації[[1]](#footnote-2)\*

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Підпис, дата | |
| завдання  видав | завдання прийняв |
| Охорона праці | Каштанов С.Ф., к.т.н., доцент |  |  |

9. Дата видачі завдання

Календарний план

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Назва етапів виконання  магістерської дисертації | Термін виконання етапів магістерської дисертації | Примітка |
|  | Аналіз централізованих VoIP мереж | 3.02 – 21.02 |  |
|  | Аналіз децентралізованих VoIP мереж | 21.02 – 04.03 |  |
|  | Аналіз P2P мереж на основі блокчейну | 04.03 – 18.03 |  |
|  | Розробка моделі VoIP клієнта | 18.03 – 01.04 |  |
|  | Інтеграція смарт контактів в існуючу мережі | 01.04 – 15.04 |  |
|  | Програмна реалізація децентралізованого зв’язку | 15.04 – 11.05 |  |

Студент ЦИМБАЛЕНКО І.М.

Науковий керівник МОСІЙЧУК В.С.

РЕФЕРАТ

Магістерська дисертація на здобуття магістерського ступеня за спеціальністю 172 «Телекомунікації та радіотехніка» (спеціалізація «Радіотехнічні інформаційні технології») — Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2020, Київ.

Магістерська дисертація складається з 76 сторінок, на яких розміщено 14 рисунків та 12 таблиць.

**Метою роботи** є дослідження підходів забезпечення реалізації децентралізованого VoIP зв’язку з використанням методів блокчейн.

**Об’єктом дослідження** є процеси встановлення з'єднання та автентифікації абонентів IP телефонії.

**Предметом дослідження** є методи та алгоритми публічної автентифікації абонентів IP телефонії на основі ланцюжків блоків транзакцій (блокчейн).

**Ключові слова**: *децентралізований зв’язок, IP телефонія, голосовий зв'язок через Інтернет, алгоритми блокчейн, автентифікація абонентів, кібербезпека*.

ABSTRACT

Dissertation for master’s degree in 172 "Telecommunications and Radio Engineering" (specialization "Radio Engineering Information Technologies") - National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 2019, Kiev.

The master's dissertation consists of 76 pages with 14 figures and 12 tables.

**The purpose** is to research approaches for providing realization decentralized VoIP using of blockchain methods.

**The object of the study** is process of establishing a connection for user authenticating.

**The subject of the study** are methods and algorithms of public authentication IP base on blockchain transaction.

**Keywords:** *decentralized connection, voice over Internet Protocols, blockchain algorithms, subscriber authentication, cyber security.*

**ЗМІСТ**

[РЕФЕРАТ 4](#_Toc40904999)

[ABSTRACT 5](#_Toc40905000)

[1 ПЕРЕЛІК ТЕРМІНІВ, ПОНЯТЬ ТА СКОРОЧЕНЬ 9](#_Toc40905001)

[ВСТУП 10](#_Toc40905002)

[1. ОГЛЯД ЦЕНТРАЛІЗОВАНИХ ТА ДЕЦЕНТРАЛІЗОВАНИХ VoIP МЕРЕЖ 12](#_Toc40905003)

[1.1 Переваги та недоліки централізованих мереж зв’язку 14](#_Toc40905004)

[1.1.1. Виклик/сеанс викрадення та уособлення 15](#_Toc40905005)

[1.1.2. Підслуховування на SIP-сигналізації 15](#_Toc40905006)

[1.1.3. Перехоплення на носії 16](#_Toc40905007)

[1.2. Можливості та проблеми децентралізованих систем зв’язку 16](#_Toc40905008)

[1.2.1. Характеристика P2P мережі 17](#_Toc40905009)

[1.2.1.1. Ступінь децентралізація 17](#_Toc40905010)

[1.2.1.2. Структура мережі 17](#_Toc40905011)

[1.2.1.3. Протокол підстановки 18](#_Toc40905012)

[1.2.1.4. Розповсюдження транзакцій 18](#_Toc40905013)

[1.2.1.5. Cистемні параметри 19](#_Toc40905014)

[1.2.1.6. Продуктивність маршрутизації 19](#_Toc40905015)

[1.2.1.7. Стан маршрутизації 20](#_Toc40905016)

[1.2.1.8. Вузли приєднуються і від’єднуються 20](#_Toc40905017)

[1.2.1.9. Безпека 22](#_Toc40905018)

[1.2.1.10. Надійність і відмовостійкості 22](#_Toc40905019)

[1.2.2. Проблеми безпеки в P2P-мережах 24](#_Toc40905020)

[1.2.3. Алгоритм блокчейн для P2P-МЕРЕЖ 24](#_Toc40905021)

[1.2.4. Перспективи створення деценталізованої системи VoIP зв’язку з використання алгоритмів блокчейн 29](#_Toc40905022)

[2. АРХІТЕКТУРА ДЕЦЕНТРАЛІЗОВАНИХ P2P МЕРЕЖ 33](#_Toc40905023)

[2.1. Опис біткойн P2P мережі 33](#_Toc40905024)

[2.2. Біткойн вузли 34](#_Toc40905025)

[2.3. Забезпечення безпеки VoIP звязку в P2P-мережах 37](#_Toc40905026)

[2.3.1. DoS Flooding 38](#_Toc40905027)

[2.3.2. Атака затемнення 39](#_Toc40905028)

[2.3.3. Профілювання користувачів 40](#_Toc40905029)

[2.3.4. ID атаки 42](#_Toc40905030)

[2.3.5. Атаки Сивілли 43](#_Toc40905031)

[2.3.6. Підроблене завантаження 43](#_Toc40905032)

[2.3.7. Несанкціонований доступ до ресурсів 44](#_Toc40905033)

[2.3.8. Управління шкідливими ресурсами 45](#_Toc40905034)

[2.3.9. Людина-в-середині (MITM) 45](#_Toc40905035)

[2.3.10 Висновки до підрозділу 2.3 46](#_Toc40905036)

[3. ЕКСПЕРИМЕНТАЛЬНЕ ПІДТВЕРДЖЕННЯ БЛОКЧЕЙН ДЕЦЕНТРАЛІЗОВАНОГО ЗВ’ЯЗКУ 47](#_Toc40905037)

[3.1 Програмна реалізація децентралізованого встановлення зв’язку 47](#_Toc40905038)

[3.2 Структура мобільного додатку VoIP-клієнта 48](#_Toc40905039)

[3.3 Заміна номерного ресурсу смарт-контрактами 50](#_Toc40905040)

[3.4 Реалізація VoIP пов'язаних мобільних додатків 53](#_Toc40905041)

[3.5 Session та Precence 54](#_Toc40905042)

[3.6 Рекомендації до створення систем децентралізованого VoIP зв’язку 56](#_Toc40905043)

[3.7 Результати створення системи децентралізованого зв’язку 57](#_Toc40905044)

[4. ОХОРОНА ПРАЦІ 58](#_Toc40905045)

[4.1 Технічні рішення та організаційні заходи з безпеки і гігієни праці та виробничої санітарії 59](#_Toc40905046)

[4.1.1 Електробезпека 59](#_Toc40905047)

[4.1.2 Розрахунок захисного відключення електромережі при аварійному режимі роботи електрообладнання 61](#_Toc40905048)

[4.1.3 Мікроклімат робочої зони 62](#_Toc40905049)

[4.1.4 Виробниче освітлення 63](#_Toc40905050)

[4.1.5 Виробничий шум 65](#_Toc40905051)

[4.1.6 Вимоги щодо організації комофортних та безпечних робочих місь користувачів ВДП ПЕОМ 66](#_Toc40905052)

[4.1.7 Організація оптимального режиму праці та відпочинку привикористанні ЕОМ 67](#_Toc40905053)

[4.2 Безпека в надзвичайних ситуаціях 68](#_Toc40905054)

[4.2.1 Вимоги щодо організації ефективної роботи системи оповіщення персоналу при НС 68](#_Toc40905055)

[4.2.2 Обов’язки та дії персоналу у разі виникнення надзвичайних ситуацій 72](#_Toc40905056)

[4.2.3 Пожежна безпека 73](#_Toc40905057)

[ЗАГАЛЬНІ ВИСНОВКИ 75](#_Toc40905058)

[ПЕРЕЛІК ПОСИЛАНЬ 76](#_Toc40905059)

ПЕРЕЛІК ТЕРМІНІВ, ПОНЯТЬ ТА СКОРОЧЕНЬ

OTP — Over the Top Provider

VoIP — Voice over Internet Protocol

CDR ­— Call Detail Records

P2P — Peer to Peer, один з архітектурних варіантів системи що базується на мережі рівноправних вузлів.

Однорангова мережа – мережа в якій кожен учасник є рівноправним, немає ієрархії і виділеного сервера.

SIP – Session Initial Protocol, протокол передачі даних, що описує спосіб встановлення та завершення сеансу користувача в термінологі P2P мереж

Блокчейн – розподілена база даних, що зберігає ланцюжок записів в певному порядку

Біткойн – електронна валюта, курс якої залежить від попиту та пропозиції і не регулюється законодавчими органами.

ВСТУП

***Актуальність теми***. Існуючі системи зв’язку зазвичай є централізованими, тобто вони мають у структурі базові станції, вузли концентрації та комутації каналів та пакетів даних. Проте поява та популяризація пірингових мереж (p2p) та mesh систем призвели до можливості створення нових підходів в організації VoIP зв'язку, зокрема розподілених та децентралізованих. Проте у разі децентралізованого зв’язку виникає цілий ряд проблем які мають мати якесь вирішення, зокрема, складність зберігання історії дзвінків, атрибутів сеансу виклику (джерело, призначення, часова мітка, характеристики мережі та медіа тощо), гарантування конфіденційнійності та підзвітності. Це стало навіть більш складніше в додатках на основі OTP (Over the Top Provider), оскільки вони працюють без центрального органу чи сервера додатків для моніторингу викликів. Щоб вирішити проблеми відстеження викликів та потоків медіа та гарантувати безпеку запису викликів від зміни, а також для автентифікації абонентів потрібно шукати нові підходи в організації таких систем,. зокрема перспективіним є використання алгоритмів блокових ланцюжків (блокчейн).

**Метою роботи** є дослідження підходів забезпечення реалізації децентралізованого VoIP зв’язку з використанням методів блокчейн.

Для досягнення цієї мети поставлені такі **задачі:**

* Проаналізувати особливості деценталізованих систем VoIP зв’язку;
* Провести теоретичний аналіз вразливосстей децентралізованого зв’язку;
* Дослідити та запропонувати архітектуру децентралізованого зв’язку на основі алгоритмів блокчейн;
* Створити тестовий додаток для для дослідження можливості реалізації VoIP мережі на основі BitCoin P2P мережі;
* Розглянути питання охорони праці .

***Об’єктом дослідження*** є процеси встановлення з'єднання та автентифікації абонентів IP телефонії.

***Предметом дослідження*** є методи та алгоритми публічної автентифікації абонентів IP телефонії на основі ланцюжків блоків транзакцій (блокчейн).

***Методи дослідження.*** Аналітичний пошук та аналіз літератоурних джерел, моделювання та аналіз стеку протоколів мережі Інтернет, аналіз даних.

***Наукова новизна.*** Удосконалено методику створення децентралізованої платформи VoIP зв’язку з використанням смарт-контрактів на основі алгоритмів блокчейн.

***Практичне значення.*** Підвищення безпеки та надійності в екосистемі VoIP зв’язку за рахунок використання потужностей алгоритмів блокового ланцюга (блокчейн).

1. ОГЛЯД ЦЕНТРАЛІЗОВАНИХ ТА ДЕЦЕНТРАЛІЗОВАНИХ   
VoIP МЕРЕЖ

Технологія VoIP (voice over IP – голос через IP) дозволяює здійснювати телефонні дзвінки через стек протоколів TC/IP в мережі Інтернет. Хоча Інтернет і робить VoIP можливим, вам не доведеться сидіти за комп'ютером, щоб здійснювати і приймати дзвінки. VoIP зв’язок може бути реалізованим як централізованим, так і розподіленим. Обидва типи VoIP допомагають нам спілкуватися, але вони функціонують дещо по-різному. Під час сеансу зв’язку, звичайний телефон перетворює звукові хвилі в електричні сигнали, які далі передаюються до іншого телефону через канали зв’язку з синхронізацією. Далі телефон перетворює сигнали назад в звукові хвилі. VoIP-телефони перетворюють звукові хвилі в цифрові пакети даних, які можуть передаватися через Інтернет. Цифрова передача даних дає змогу абонентам спілкуватися за допомогою гарнітури, комп'ютерів, смартфонів та інших пристроїв, які можуть отримувати цифрову інформацію.

Огляд систем IP телефонії

Мережа VoIP зв’язку складається з декількох компонентів. Один з найважливіших компонентів в мережі VoIP є вузлом. Вузол – це точка в мережі, в якій відбувається важливий процес. Наприклад, вузол може бути точкою підключення, де починається передача даних VoIP. Це також може бути кінцева точка, яка отримує дані і перетворює його в аудіо. Кінцева точка в системі VoIP може бути комп'ютер, телефон або інший пристрій, який може отримувати і декодувати VoIP даних.

Переваги VoIP систем зв’язку:

* низька вартість - ця технологія призводить до більшої фінансової економії. Це зменшує витрати на проїзд і навчання, завдяки веб-і відеоконференціям. Якщо у користувача присутнє широкосмугове підключення до Інтернету (DSL або кабельний), в нього є можливість здійснювати ПК-ПК телефонні дзвінки в будь-якій точці світу безкоштовно. Також є можливість здійснити дзвінок з компютера на телефон, як правило, дорожче для цього, але, ймовірно, набагато дешевше, ніж звичайний дзвінок використовуючи послуги будь якого оператора зв’язку;
* низькі податки – оскільки дзвінки здійснюються через Інтернет, уряди не сильно оподатковують VoIP телефонні послуги. Вибір VoIP провайдера може додати до значної економії для будь якого користувача;
* Відеоконференції
* Без зайвих кабелей та додаткових витрат. Номер телефону VoIP, на відміну від регулярного номера телефону, повністю портативний. Найбільш часто визначаються як віртуальними числами.

Недоліки VoIP систем зв’язку:

* Екстрені виклики – традиційна телефонна техніка в екстрених дзвінків може відстежувати ваше місцезнаходження. Однак, оскільки голос за IP-викликом по суті передачі даних між двома адресами IP, а не фізичними адреси, з VOIP в даний час жодним чином не визначити, де відбувається VOIP телефонний дзвінок.
* Надійність – оскільки VoIP спирається на підключення до Інтернету, VoIP сервіс буде залежати від якості та надійності широкосмугового Інтернет-провайдера, а іноді і обмеження комп'ютера. Погані інтернет-з'єднання і перевантаження може призвести до спотвореного або спотвореної голосової якості. Якщо використовується комп'ютер у той же час, як відбувається виклик з комп'ютера VOIP, можна виявити, що якість голосу різко погіршується.
* **Якість VoIP голосом –** VoIP має трохи поліпшити якість передачі голосу, але не у всіх випадках. VoIP QoS (якість обслуговування) залежить від багатьох чинників: широкосмугове підключення, обладнання, послуги, що надаються постачальником, призначення дзвінка і т. д.
* **Безпека –** найбільш помітні питання безпеки через VoIP є ідентифікація і служби крадіжки, віруси і шкідливі програми, відмова в обслуговуванні, спам, підробний виклик і фішинг-атак

1.1 Переваги та недоліки централізованих мереж зв’язку

Централізовані системи VoIP мають централізовані сервери, які приймають вхідні дані і маршрут до місця призначення. MyNetFone забезпечує гарний приклад того, як цей процес працює. Якщо використовується служба VoIP компанії, адаптер на комп'ютері може перетворити голос в цифрові дані і відправити його на сервер MyNetFone. Сервер буде пересилати, ці дані назад через Інтернет, де він в кінцевому підсумку досягає людину, з якою відбувається комунікація. У централізованій системі є централізований сервер який є критичною кінцевою точкою в мережі.

Переваги централізованих мереж зв’язку:

* легко менеджити
* легко підтримувати традиційні та додаткові сервіси

Недоліки централізованих мереж зв’язку:

* ліміт маштабування обмежений об’ємом серверу

Недоліками данного типу мережі є також що мережа є дуже вразлива до різних типів атак.

* + 1. Виклик/сеанс викрадення та уособлення

Механізм дайджест HTTP, визначений в RFC 2617 [3], використовується між користувачами для проксі-серверів і користувачів. Цей метод використовується для зменшення загроз викрадення і уособлення. Він забезпечує шлях для сервера або UA (User Agent) для виклику інших UAs або серверів для аутентифікації. Коли сервер отримує запит від клієнта, він генерує значення поточного часу і відправляє його до клієнта як виклик. Клієнт обчислює відповідь, за допомогою хешування поточного часу, ім'я користувача, паролю і області, потім надсилає його на сервер. Нарешті, сервер обчислює хеш і порівнює його з отриманою відповіддю. Основним недоліком цього механізму є ризик викрадення облікових даних SIP-клієнта, який може призвести до того що зловмисник може видавати себе за користувачів без будь-яких підтверджень, і це буде означати що законний клієнт фактично використовує ці облікові дані.

* + 1. Підслуховування на SIP-сигналізації

Зловмисна сторона може відстежувати та записувати, з якою користувач спілкується, дотримуючись SIP-повідомлень. Для уникнення цієї загрози використовуються наступні механізми:

1. Шифрування на IP-шарі (IPSec). IPsec [4] може бути встановлений між двома Інтернет хостами і виконується в операційній системі. Це складно для додатків таких як SIP знати чи IPsec на місці.
2. Транспортний рівень безпеки (TLS):

SIP може використовувати TLS для шифрування сигнальних повідомлень як шифрування на транспортному шарі маскує дані рівня програми. TLS надає лише один стрибок конфіденційності для аутентифікації між UA і проксі-сервером; таким чином, конфіденційність не виконується, якщо один із стрибків, не захищений TLS. Основною проблемою з TLS є вимога сертифікатів і шифрування одного із стрибків. Як правило, існує більше ніж один стрибок між двома UAs.

**3.** Конфіденційність за допомогою S/MIME

Використання S/MIME [5] захищає тільки протокол опису сесії (SPD) [6] частина SIP-повідомлення, оскільки частина заголовка повинна бути відправлена ясно, щоб мати можливість для проксі-сервера, щоб направити повідомлення в правильному напрямку. S/MIME дає змогу шифрувати тіло SPD в SIP і безпечні дані, не впливаючи на заголовок повідомлення.

* + 1. Перехоплення на носії

Шкідливі сторони можуть відстежувати медіарозмову між кінцевими користувачами. Безпечний протокол реального часу (SRTP) [7] використовується для забезпечення RTP медіа потоків і, отже, пом'якшення цієї загрози. Основним обмеженням у цьому методі є вимога до головного сеансу розподілу ключа механізму. SIP може допомогти встановити захищений сеанс медіа, обмінюючись мастер ключем через SPD частину SIP повідомлень. Мультимедійний Інтернет-кеїнг (MIKEY) використовує поле SPD для транспортування медіа ключа, який може передаватися в SPD a = Key-mgt-attributes. ZRTP є ще одним протоколом для обміну в медіа сеансі за допомогою RTP заголовків розширення механізму.

* 1. Можливості та проблеми децентралізованих систем зв’язку

Якщо ви коли-небудь обмінялися файлами через однорангові мережі, ви використовували метод обміну даними, подібний до одного з розподіленого використання систем VoIP. Розподілені системи VoIP користуються перевагами P2P архітектури, яка координує потік цифрових даних між кінцевими точками. P2P мережі VoIP не покладаються в значній мірі на централізовані серверні вузли для полегшення спілкування. Натомість потоки даних між іншими вузлами системи – такі як точка підключення та кінцева точка. Ці дві точки можуть бути вашим комп'ютером і комп'ютером телефонної сторони.

* + 1. Характеристика P2P мережі

Для того, щоб охарактеризувати нову мережеву P2P парадигму, що мережа криптовалюти представляє, ми проводемо аналіз мережі Bitcoin P2P за допомогою таксономії, визначеної Lua та ін. [10] для порівняння різних P2P мереж. Після тієї ж таксономії, ми зможемо підкреслити відмінності таких нових мереж у порівнянні з існуючими. Наступний аналіз спрямований тільки на досяжну мережу Біткойн, оскільки вона є єдиною повною частиною P2P мережі Bitcoin.

* + - 1. Ступінь децентралізація

Децентралізація оцінює, що поширення проаналізованої мережі представляє собою розподілений характер або, навпаки, його конфігурація показує деякі централізовані характеристики. У цьому сенсі мережа Bitcoin є неструктурованим P2P накладенням з деякими збіжностями з Gnutella. З лінійною топологією вузлів. У мережі Bitcoin, кожен вузол є сервером або клієнтом і система не надає ні централізованих послуг, ні інформації про топологію мережі.

* + - 1. Структура мережі

Архітектура описує організацію системи по відношенню до її експлуатації. Як ми вже вказали, мережа Біткойн представляє плоску архітектуру без шарів і особливих вузлів. Мережа формується вузлами, що приєднанні до мережі після деяких визначених основних правил, де випадковість є важливим компонентом. Така випадкова поведінка в мережі створення має намір генерувати непередбачувану і рівномірну мережеву топологію, невідому своїм користувачам. Як ми побачимо в розділі 2 така нестача знань про топологію необхідна з міркувань безпеки.

* + - 1. Протокол підстановки

Однією з головних проблем в P2P-мережах, особливо тих, які використовуються для розповсюдження контенту, є протокол запитів пошуку, прийнятий накладанням для пошуку потрібного вмісту. Однак, незважаючи на те, що мережа Bitcoin може розглядатися як мережа розподілу вмісту (де вміст є транзакціями і блоками), інформація, що надходить у мережу, повністю реплікується в кожному вузлі. Таким чином, немає необхідності в такому протоколі підстановки, оскільки інформація завжди доступна в останньому вузлі. Тим не менш, розповсюдження інформації повинно бути виконано з метою синхронізації всіх вузлів по мережі з однаковими даними. Таке розповсюдження виконується через протокол контрольованого затоплення. Головним чином, контрольований протокол затоплення працює по принципу рush, дані розповсюджуються в такому порядку в якому вони були створені. Замість того, щоб бути безпосередньо надісланими, доступність даних оголошується обраним вузлам, а у випадку, якщо не вистачає деяких відомостей, він просить його повернутися до диктора. Через мережу розповсюджуються два типи структур даних: *транзакції* та *блоки*.

* + - 1. Розповсюдження транзакцій

Транзакції – це базова структура даних, яка проходить через мережу Біткойн і одна з найбільш частих структур яку можна помітити. Кожен вузол може взяти участь у транзакції, просто використовуючи гаманець, незалежно від його типу. Потік транзакцій через мережу, спрямованих на досягнення кожного вузла, в кінцевому рахунку, буде включено до блоку. Середня кількість операцій за день протягом вересня 2019 року склала 222 458 близько 1 808 009 біткоїнів між різними рахунками (необроблені дані отримані з <https://blockchain.info/charts>).

* + - 1. Cистемні параметри

Різні P2P мережі вимагають набір системних параметрів для роботи такої системи. Наприклад, структуровані P2P-мережі вимагають, щоб зберігати інформацію про розподіл вузлів в мережі, для того щоб поліпшити продуктивність маршрутизації. Тим не менш, мережа P2P, відповідно до інших неструктурованих P2P, не вимагає особливих параметрів системи для нормальної поведінки мережі. Кожен вузол може приєднатися до мережі без попереднього знання про неї. Крім того, деякі параметри за замовчуванням використовуються вузлами, наприклад, максимальний ліміт підключення яких встановлено на 125, хоча таке значення не є обмеженням, і кожен вузол може вибрати кількість підключень, які він хоче зберегти.

* + - 1. Продуктивність маршрутизації

На відміну від традиційних мереж P2P (таких як Gnutella [11]), Bitcoin не відповідає багатоінтервальній схемі маршрутизації. Як вже зазначалося раніше, вузли в мережі зберігають копію всієї інформації, яка протікає через систему до дати, а саме блокчейн.

Таким чином, ніякі запити не перенаправляються між вузлами, оскільки вся інформація повинна бути розташована в одному вузлі максимуму. Таким чином, дані гарантовано буде розташовано, якщо мережа синхронізується, а протокол маршрутизації не потрібен, крім протоколу синхронізації.

Таким чином, для досягнення синхронізації в будь-який момент часу затримка розповсюдження є основним фактором для мережі біткойн. Таким чином, Декер і Ваттенгофер [12] проаналізував час розповсюдження блоку для 10 000 блоків і виявили, що після експоненційної кривої, середній час розповсюдження блоку 6,5 секунди, а середнє значення було розташовано в 12,6 секунд. Однак розподіл показав, що невеликому відсотоку вузлів (5%) потрібно більше 40 секунд, щоб отримати блоки. Крім того, було також проведено аналіз впливу на розмір блоку на затримку розповсюдження. Вони досягли висновку, що для невеликої кількості даних, тобто менше 1 КБ, є величезні накладні витрати під час розповсюдження, оскільки протокол включає в себе кілька повідомлень при узгодженні інформаціх, яка повинна бути переслана. Це відноситься в основному до транзакцій, насправді до величезної кількості з них (96%), а не до блоків. Для розміру даних більше 20 КБ, додаткові затримки незначні (близько 80 мс).

* + - 1. Стан маршрутизації

Незважаючи на те, що мережа розповсюдження контенту, стан маршрутизації біткойн не може бути безпосередньо визначений через випадковість і динамічність його топології і той факт, що він не відомий. Крім того, як ми вказали раніше, багатоадресна маршрутизація не виконується, оскільки дані можуть бути знайдені не більше чим на одному вузлі стрибка.

* + - 1. Вузли приєднуються і від’єднуються

Як побудувати мережу? Це класична проблема P2P мережі з якою їй доводиться мати справу. Побудова мережі від її ядра і до того, як вузли мають бути підключеними з іншими вузлами, P2P-мережі повинні бути дуже адаптовані, щоб уникнути поділу. Для того, щоб впоратися з цією проблемою, а також забезпечити справедливий і безпечний спосіб обрання вузла вузол що буде підключений до мережі, біткойн мережа виконує конкретний механізм виявлення вузлів.

За замовчуванням усі вузли зберігають до 125 з'єднань з іншими вузлами. Кожен вузол буде починати 8 з цих з'єднань з іншими вузлами (що називаються вихідними з'єднаннями) і прийме до 117 від потенційних вузлів (так звані вхідні з’єднання). Незважаючи на назву, всі з'єднання є дванаправленими. Для того, щоб вибрати вихідні з'єднання, кожен окремий вузол буде шукати підмножину вузлів, які він зберігає в локальній базі даних. Ця база даних формується за двома різними таблицями: *пробна* і *нова*. *Пробна* таблиця містить адреси від вузлів, до яких вже підключено вузол, і *нова* таблиця містить адреси, про які вузол тільки чув. Крім того, коли вузол намагається встановити підключення до мережі в перший раз, він запитує відомий список DNS-вузлів, які будуть надавати набір онлайнових потенційних вузлів (більш детальну інформацію про те, як вузли зберігаються і вибираюттся може бути знайдено в [13]).

Вузли намагаються завжди підтримувати свої 8 вихідних з'єднань, вибираючи нові вузли з бази даних, якщо будь-яке з встановлених з'єднань буде припинено. Вузли зберігаються і вибираються з бази даних після псевдовипадних процедур, що забезпечує високу динамічність мережі і зберігає свою структуру невідомою. Інформація про вузли може бути отримана вузлом двома способами. Перш за все, вузол може просити такі дані своїх сусідів, з тим щоб поповнити свою базу даних, шляхом відправки повідомлення *getaddr* , або може отримати таку інформацію спонтанно від одного з його вузлів без будь-якого запиту. В обох випадках, інформація відправляється з використанням набору повідомлень *addr*, що містять до 2 500 однорангових адрес з *пробної* і *нової* таблиці сусідів. Такі адреси зберігаються в *новій* таблиці локального вузла. З іншого боку, повідомлення *addr*, що містить одну адресу, можна надіслати до вузла, коли вузол хоче розпочати зв'язок з потенційним вузлом.

Надсилаючи свою адресу, вузол сповіщає одержувача про те, що його було отримано як вузол, і якщо останній має місце для вхідних підключень, то зв'язок встановлюється. Однорангові адреси, отримані таким чином, зберігаються у *пробних* таблцях.

Всі адреси зберігаються в базі даних разом з часовою позначкою, яка допомагає вузлу оцінити свіжість такої адреси при виборі інших вузлів.

* + - 1. Безпека

Безпека в P2P-мережах завжди була широка тема, оскільки численні загрози безпеці можуть бути ідентифіковані в різних реалізацій P2P. Зацікавлений читач може послатися на обстеження Уоллах [14] для введення в тему безпеки в цілому P2P-мереж, на роботи Белловвіна [15] де опис зосереджено на питаннях безпеки, що зачіпають конкретні протоколи P2P, такі як Napster і Gnutella, і до [16] введення в проблеми безпеки в P2P SIP комунікаціях.

Однак, в P2P криптовалютних мереж, безпека має інший зміст. На перший погляд, можна повірити, що загрози з якими стикається P2P криптовалютні мережі є підмножиною загроз, знайдених в стандартних мережах P2P. Однак, як ми побачимо детально в наступному розділі, більшість загроз, що зустрічаються в цілому в P2P-мережах, не застосовуються безпосередньо до P2P криптовалютних мереж через криптографічні механізми, що використовуються валютами рівнем безпеки запропонованими їхніми протоколами. Крім того, можна також повірити, що кілька нових загроз також можуть виникнути в криптовалютах через чутливістьь яку вони мають як мережі грошових переказів. Однак, як ми побачимо в наступному розділі, це ще не так.

У наступному розділі (розділ 2) ми надаємо детальний огляд найпоширеніших загроз безпеки, виявлених для типових мереж P2P, і обговоримо, в якій мірі вони впливають на мережу біткойн.

* + - 1. Надійність і відмовостійкості

Наскільки надійна система при впливі на несправності? Як правило, такі виміри надійності пов'язані з ненавмисними збоями, наприклад, шляхом масового відключення вузлів мережі або збільшення обсягу інформації, що передається через мережу, але не включають навмисні атаки, які будуть класифіковані всередині властивостей безпеки мережі. Біткойн реалізує протокол розподіленого консенсусу, який є стійким від так званих візантійський помилок. Тобто протокол стійкий до довільних несправностей, що виробляються у вузлів-учасників, від помилок програмного забезпечення а також від атак противника. Головна ідея цього протоколу полягає у використанні системи доказів роботи для створення публічної книги, де зберігаються транзакції. Додавання нової інформації в публічну книгу вимагає величезної кількості обчислювальної потужності, таким чином запобігаючи зловмисникам монополізувати книгу і давати під сумнів транзакції. Подібним чином, зміну змісту блокчейну також обчислювати доволі складно, аж до того, що транзакції вважаються безпечними, коли вони мають 6 підтверджень (тобто п'ять блоків були створені на вершині блоку, який включав транзакцію). Крім того, блокчейн реплікується на всіх повних вузлах blockchain, сприяючи відмовостійкості системи та забезпечуючи високу доступність даних про книги. Припускаючи, цю класифікацію, мережа біткойн P2P була розроблена з високим рівнем надійності, завдяки надмірності, яка має на увазі зберігання всієї відповідної інформації мережі в кожному вузлі мережі. При такому підході високий рівень неефективності в термінах дискового простору переводиться на високу стійкість мережі, оскільки наявність одного вузла в мережі містить інформацію, щоб зберегти систему в живих. Крім того, доказ роботи системи дозволяє вузлам (в кінцевому рахунку) досягти консенсусного стану, навіть у присутності зловмисників, що намагаються підірвати систему. Як недолік, узгоджений протокол, трішки повільний, з операціями, які потребують 9 хвилин (медіана часу підтвердженна станом на 13 жовтня 2016 [17]), що вимагає споживання великої кількості енергії для кожного видобутого блоку.

* + 1. Проблеми безпеки в P2P-мережах

Безпека в P2P-мережах була широко вивчена в літературі. У цьому розділі ми пропонуємо широкий огляд основних проблем безпеки, які виникають в мережах P2P, ми переглядаємо, як кожна з проблем безпеки може впливати на мережу біткойн, і якщо це так, ми пояснюємо конкретні контрзаходи які біткойн забезпечує для того, щоб захищатися від кожної атаки.

Список розглянутих атак переходить на найбільш типові типи атак і недоліки безпеки, знайдені в загальних мережах P2P. Очевидно, що конкретні мережі і додатки можуть представляти спеціалізовані напади, але в більшості випадків їх можна розглядати як специфікацію нападів, представлених тут.

Таким чином, щоб забезпечити чітке уявлення про те, як звичайні P2P атаки впливають на біткойн, ми спочатку розглянемо три види атак, які будуть показані, що явно застосовані до біткойн. Після цього, ми включаємо список атак, виявлених для загальних мереж P2P, але це не має такого високого впливу на біткойн, огляд того, чому напади не поширюються на конкретну мережу біткойн і деталізація конкретних випадків, коли ці напади (або деякі варіації) можуть якимось чином ставитися до біткойн.

* + 1. Алгоритм блокчейн для P2P-МЕРЕЖ

У цьому розділі ми звернемо увагу на основні ідеї, щоб зрозуміти основну функціональність криптовалюти біткойн. Такі знання необхідні для розуміння базової мережі P2P, яка підтримує зв'язок між біткойн -компаніями. Тим не менш, складність біткойн робить неможливим, щоб забезпечити повний опис системи в цьому огляді, тому більш детальну інформацію можна отримати з книги Narayanan та ін. [2] для більш розширеного пояснення про систему біткойн.

Біткойн - це криптовалюта на основі бухгалтерських записів [5]. Тому біткойни не повинні розглядатися як цифрові токени, а як баланс облікового запису біткойн. *Обліковий запис біткойну* визначається еліптичною кривою криптографічної пари ключів. Обліковий запис біткойну публічно ідентифікується своєю *біткойн-адресою*, отриманим з публічного ключа. Використовуючи цю публічну інформацію, користувачі можуть відправляти біткоїни на цю адресу (терміни "Публічний ключ", "адреса" або "Біткойн-акаунт" відносяться до тієї ж концепції). Потім відповідний закритий ключ потрібен для витрачання біткойнів рахунку. Спеціальне програмне забезпечення, яке зазвичай називають *гаманці*, було розроблено для створення та керування цими приватними ключами та адресами.

Платежі в системі біткойн здійснюються через транзакції між біткойн аккаунтами. *Біткойн-транзакція* вказує на рух біткойн з вихідних адрес до адрес призначення. Адреси джерел відомі як *вхідні адреси* в транзакції, а адреси призначення називаються *вихідними адресами*. Як видно на рисунку 1.1, одна транзакція може мати одну або кілька вхідних адрес і одну або кі ька вихідних адрес.

A screenshot of a cell phone

Description automatically generated

Рис. 1.1 Інформація про біткойн транзакцію

Деталі транзакції - точна кількість біткойнів, які будуть переведені з кожної вхідної адреси. Те ж саме стосується і вихідних адрес, з зазначенням загальної кількості біткойнів, які будуть переведені на кожен рахунок (хоча в даному випадку специфікація явно зроблена). У протоколі біткойн введені адреси, щоб витрачати точну суму раніше отриманої транзакції ( на рисунку 1.1 дві вхідні адреси, які точно однакові, що свідчить про те, що біткоїни прибули до цього облікового запису біткойн в дві окремі транзакції). Тому кожен вхід повинен однозначно вказувати на попередній ідентифікатор транзакції (в системі біткойн ідентифікується транзакція) і індекс виходу, де були отримані біткоїни. Як наслідок, в будь-який момент, вихід може бути у двох станах: або вже витрачені або ще не витрачені. Вивід, який не було витрачено, відомий як невитрачений вивід транзакції або *UTXO*.

Нарешті, власник вхідних адрес повинен виконати цифровий підпис, використовуючи його приватні ключі для авторизації передачі біткойн, довівши, що він є справжнім власником таких рахунків (хоча це cтандартна форма біткойн перевірки для регулярних операцій з переказами біткойн, перевірка транзакції може бути набагато складнішим і ґрунтується на виконанні стек скриптової мови.

Перед прийняттям платежу з стандартної транзакції, отримувач повинен

* перевірити правильність цифрових підписів;
* перевірити, що біткоїни вхідних адрес не були раніше витрачені.

Перша перевірка може бути виконана з інформацією, включеною до самої транзакції (поле *ScriptSig*) разом з інформацією про транзакцію, ідентифікована в попередньому виході (index) (поле *scriptPubKey*). Друга перевірка запобігає подвійного витрачання в системі біткойн, і вона виконується через загальну книгу, блокчейн, де записані всі попередні транзакції.

*Блокчейн* — це загальна книга тільки для додавання, яка містить усі транзакції біткойн, що виконуються з часу початку роботи системи (ще в 2009), і вона вільно реплікована та зберігається в різних вузлах мережі біткойн, що робить біткойн повністю розподіленою системою.

Операції включаються в блокчейн на проміжки часу, а не в потоці, а таке доповнення виконується шляхом збору всіх нових операцій системи, компілювання їх разом у структурі даних, що називаються блоком, і в тому числі блок у верхній частині блокчейну. Щоразу, коли блок, що містить певну транзакцію, включений до блокчейну, така транзакція вважається *підтвердженою транзакцією* , оскільки вона вже включена в блокчейн і може перевірятися на запобігання подвійного витрачання коштів.

*Блоки-* це структури даних, які в основному містять набір операцій, які були виконані в системі (рис. 1.2). Для досягнення властивості тільки для додавання, включення блоку в блокчейн є досить важкою проблемою, тому додавання блоків до блокчейну є часом і трудомістким. Крім того, кожен блок індексується з використанням його хеш-значення, і кожен новий блок містить хеш-значення попереднього (див. поле *попереднього блоку* на рисунку 1.2). Такий механізм гарантує, що модифікація блоку з середини ланцюга буде означати зміну усіх блоків ланцюга, що залишилися з цього пункту до вершини, для того щоб відповідати всім хеш-значенням.

A screenshot of a cell phone

Description automatically generated

Рис. 1.2. Загальна інформація про блок

Додавання блоку до блокчейну відоме як *процес видобування(mining* *process)*, процес, який також розподіляється, і який може виконувати будь-який користувач мережі біткойн з використанням конкретного цільового програмного забезпечення (і устаткування). Mining процес використовує систему хеш суми як систему підтвердження, що була спочатку запропонована як механізм захисту від спаму [6]. Доказ роботи складається з знаходження хешу нового блоку з значенням нижче визначеної мети (значення цілі визначає складність mining процесу. Біткойн налаштовує цільове значення залежно від хеш-потужності майнерів для того, щоб встановити пропускну здатність нових блоків 1 раз на 10 хвилин (середнє значення)). Цей процес виконується звичайним перебором варіюючи одноразове значення блоку. Після того, як значення було знайдено, новий блок стає верхнім блоком блокчейну, і всі майнери скидують свою роботу на цей блок і рухаються до наступного.

Видобуток нових блоків є структурним завданням в системі біткойн, оскільки це допомагає підтвердити транзакції системи. З цієї причини, а також припускаючи, що видобуток припускає важку роботу, майнери повинні бути належним чином винагороджені. У системі біткойн майнери винагороджуються двома механізмами. Перший з них надає їм новостворені біткойни. Кожен новий блок включає в себе спеціальну транзакцію, так звану *транзакцію генерації* або монетобазову транзакцію (див. першу транзакцію на рисунку 1.2), в якій немає будь-якої вхідної адреси і вихідна адреса визначається майнером, який створює блок, який явно вказує на один з його власних адрес (сума транзакції генерації не є постійною, і вона визначається системою біткойн. Таке значення, почалося в 50 біткойнів, вдвічі скорочувалася кожні чотири роки, фіксуючи асимптотично до 21 000 000 загальної кількості біткойнів, які коли-небудь будуть створюватися).

Система біткойн має поширювати різні види інформації, по суті, транзакції та блоки. Оскільки обидва генеруються в розподіленій формі, система передає таку інформацію через Інтернет через мережу P2P, що ми детально описуємо в наступному розділі.

* + 1. Перспективи створення деценталізованої системи VoIP зв’язку з використання алгоритмів блокчейн

Криптовалюти дійсно є потужним інструментом для розробки нових децентралізованих додатків (в даний час найкращим відомим додатком для P2P-мереж є технологія розподілу контенту [49]), завдяки розподіленому довірчому механізму, на якому вони базуються. Три відповідні властивості криптовалют можуть використовуватися як будівельний блок для таких застосувань:

1. Захищений механізм розподіленого платежу
2. Розподілене сховище з цілісністю за дизайном
3. Безпечне перенесення та розповсюдження цифрових активів

Очевидний випадок використання криптовалют, звичайно, прийняти їх як платіжний рівень в будь-якій системі, де є необхідність перерахування грошей від платника до одержувача платежу в повністю розподілених (і без цензури) способом. Кілька додатків можуть скористатися гнучкою платіжною системою, від P2P розподілених схем зберігання, де користувачі можуть найняти локальний дисковий простір для економічного стимулювання, до більш складних сценаріїв, таких як мобільного кравзондування [50]. Мобільне кравзондування (МКС) –розподілена програма, де сила натовпу, разом з можливостями розпізнавання смартфонів які вони носять, забезпечує потужний інструмент для сприйняття даних, особливо в тих сценаріях, що стосуються поведінки користувачів або тих, які покладаються на мобільність користувачів, де стандартні сенсорні мережі можуть бути не придатні. Однак, в тому числі участь людини в задачах зондування несе, принаймні, три критичні проблеми [51]: участь користувачів, якість даних і анонімність користувача.

Участь користувачів є надзвичайно важливою в МКС, оскільки продуктивність і корисність таких датчиків значною мірою залежать від готовності натовпу до участі в процесі збору даних. Таким чином, стимулюючі механізми мають першорядне значення в сценаріях МКС для залучення багатьох датчиків натовпу і надання центру збору даних з значною кілкістю даних.Участь користувача може бути підвищена шляхом надання плати за сприйняття. Однак, стандартні платіжні схеми мають кілька недоліків у оплаті за змістом заявки. Перш за все, реєстрація користувачів в платіжній системі спряжена з тягарем для участі користувача. По-друге, заставні витрати стандартних платіжних систем (в основному у вигляді зборів) запобігають їх використанню в оплаті за змістом сценарію. Нарешті, стандартні платіжні механізми не забезпечують збереження приватності властивостями, особливо актуальними, коли такі платежі можуть ідентифікувати дані з конкретної особи, чия ідентичність не повинна бути розкрита. Криптовалюти можуть успішно використовуватися в сценаріях визначення натовпу мобільних пристроївяк корисний механізм, оскільки вони дозволяють забезпечити доступну за змістом схему з відповідними властивостями збереження конфіденційності, оскільки вона була запропонована в системі Paysense [52].

Розподілене сховище також є дуже цікавим властивістю, запропонованою криптовалютами на основі блокчейн, але, незважаючи на інші розповсюджені пропозиції, його основна перевага полягає у цілісності дизайну, що робить його таким привабливим для декількох застосувань. Наприклад, кільком P2P-мережам необхідний маханізм розширення IP/Name, і криптовалюти спеціального призначення можуть вирішити цю проблему. Прикладом такої ідеї є криптовалюта Namecoin [53].

Криптовалюти були призначені для передачі грошей, але його використання може бути продовжено для передачі інших видів цифрових активів. Використовуючи криптовалюту як транспортний рівень, цифрові активи можуть бути пов'язані з криптографічними ключами і можуть бути продані, використовуючи безпечну інформацію, включену до блокчейну, щоб визначити законного власника кожного активу в кожен конкретний час. Можна знайти кілька прикладів таких цифрових активів, від акцій компанії до DRM, де властивість медіаоб'єкта може бути визначена [54]. Крім того, розширення трохи концепції активів, криптовалюти також можуть бути використані для зберігання репутації, концептуалізований як актив, який користувачі можуть зберігати і передавати. Повертаючись до прикладу мобільного сприйняття натовпу, нагадаємо, що якість даних-зондування була однією з важливих проблем такого сценарію. У системах МКС немає контролю над датчиками натовпу, і не можна припустити, що всі особи будуть вести себе точно таким же чином або будуть однаково чесними. Таким чином, загальна якість показань датчика може погіршитися, якщо підроблені дані отримані від зловмисників. Таким чином, методи перевірки даних повинні бути правильно розгорнуті, і широко використовуваний підхід полягає в перевірці даних в залежності від рівня довіри датчика натовпу, що повідомляє про це. У цьому конкретному випадку криптовалюти можуть використовуватися як механізм анотації [52], за допомогою якого користувачі заробляють або втрачають репутацію в залежності від правильності попередніх дій, враховується сума винагород, отриманих раніше.

Слід зазначити, що в цьому розділі ми вказали кілька можливих застосувань криптовалют у розподілених додатках, щоб показати широкий перетин між обома полями. Однак для подальшої роботи оставлено поглиблене досліження того як оптимально виконати взаємодію між криптовалютами і конкретними сценаріями.

1. АРХІТЕКТУРА ДЕЦЕНТРАЛІЗОВАНИХ P2P МЕРЕЖ

Термін «peer-to-peer», або P2P, означає, що комп'ютери, які беруть участь в мережі, є рівними один з одним, це означає, що немає "спеціальних" вузлів, і що всі беруть однакову участь в наданні мережевих послуг. Мережеві вузли з'єднання в сітчастій мережі з лінійною топологією. Немає сервера, немає централізованої служби, і немає ієрархії в мережі. Однорангові мережі є за своєю суттю стійкими, децентралізованими і відкритими. Видатний приклад архітектури мережі P2P був ранній Інтернет сам, де вузли в IP-мережі були рівними. Сьогоднішня архітектура Інтернету є більш ієрархічною, але Інтернет-протокол досі зберігає свою лінійну топологію. біткойн мережа структурована як однорангова мережа у верхній частині стеку протоколів Інтернет. Розглянемо мережу P2P та її характеристики на основі блокчейн мережі біткойн.

* 1. Опис біткойн P2P мережі

Біткойн вперше був представлений публіці описавши основні поняття. Через кілька місяців було випущено відкрите джерело біткойн-клієнта, що дало початок криптовалюті, яку ми тепер знаємо, і мережу P2P, яка підтримує його. Такі визначення мережі P2P і впровадження були клоновані в декількох нових криптовалют, які випливають з впровадження біткойн. У таких нових криптовалютах, конфігурація мережі була реалізована майже однаково. Наприклад, як описано в [3], Litecoin, Dogecoin, Dash, і Peercoin мають однакові типи мережевих повідомлень біткойн, які в результаті мереж для цих криптовалют дуже схожі, а в деяких випадках ідентичні до Bitcoin One.

З моменту розгортання в 2009, де єдиним біткойн-клієнтом був доступний референт-клієнт, мережа біткойн тепер складається з дуже різнорідних вузлів, чиї апаратні можливості та програмні реалізації відрізняються значною мірою один від одного. Крім того, було створено навіть нові протоколи з метою оптимізації певних завдань, які потребують екосистеми Біткойн.

Щоб описати існуючу мережу біткойн, ми спочатку визначимо деякі властивості, які характеризують вузли Біткойну. Після цього ми розглянемо найпоширеніші конфігурації вузлів, використовуючи властивості, описані раніше. Нарешті, ми опишемо склад поточної мережі біткойн.

* 1. Біткойн вузли

Як ми вже згадували, біткойн вузли є неоднорідними, що представляють помітні відмінності як у своєму апаратному, так і в програмному забезпеченні. У цьому розділі ми зосереджуємося на описі основних властивостей, які визначають вузол біткойн: точну частину блокчейну, що зберігається, її основні функціональні можливості, її підключення та протоколи, які він використовує для зв'язку з іншими вузлами. Рисунок 2.1 підсумовує таку класифікацію.

Точка прослуховування

Точка не прослуховування

Біткойн вузол

Блокчейн

Функціональність

Зв’язок

Імплементація протоколу

Повний Блокчейн

Урізаний Блокчейн

Лише заголовки

Майнери

Валідація

Гаманець

Об’єкти: DNS, блок, сервіси, міксини

Біткойн

Getblocktemplate

Stratum

Falcon

FIBRE

Рис.2.1. Класифікація вузлів біткойн

Вузли, що беруть участь у мережі, зберігають деякі дані про *блокчейн*. Однак точні дані, які вони зберігають, відрізняються значною мірою від кількох мегабайт до десятків гігабайтів. *Повні* вузли блокчейну зберігають повну і актуальну версію блокчейн (2016 вересня загальний розмір блокових заголовків і транзакцій складається з 80 ГБ даних). *Урізані* вузли блокчейн зберігають актуальну версію блокчейну з повними даними блокчейн, принаймні за останні 2 дні (кількість днів, за які для зберігання повних даних блокчейн може бути налаштована користувачами. Режим «урізання» оцінюється для зменшення використання диску близько до 2 Гб [7]). Хоча повні дані зберігаються тільки декілька днів, урізані вузли здатні надійно перевіряти транзакції, тому що вони дійсно зберігають необхідну інформацію з їхньої попередньої історії блокчейн, тобто метадані про всі відомі блоки і набір UTXO. *Спрощена перевірка платежів (SPV) клієнта* має актуальну версію блокчейн заголовків (заголовок блоку є 80-байтна структура. 2016 вересня блокчейн біткойн має 432 000 блоків, таким чином потребується близько 33 МБ дискового простору). Крім того, клієнти SPV можуть зберігати деякі транзакції що цікавлять юзера. SPV клієнти, як правило, розгорнуті в мобільних пристроях, таких як смартфони, де повний блокчейн, як правило, є недоступним.

Вузли також можуть бути класифіковані на основі їх функціональності. Існує три функції, необхідні для роботи системи біткойн. Майнінг є обчислювально-затратне завдання створення блоків. Нові блоки додаються до кінця блокчейну що призводить до зростання загальної книги. Вузли які виконують операцію майнінгу називаються майнерами. Деякі вузли виконують *перевірку та ретрансляцію* операцій і блоків, які вони отримують, тобто ретранслюють до інших вузлів дійсні транзакції і блокують дані, разом з мережевими даними. Деякі вузли також мають функціональність *гаманця* , тобто зберігають набір ключових пар, вони відстежують кількість біткойнів, що є за адресами, пов'язаними з цими ключами, і здатні створювати транзакції, які витрачають ці біткоїни. Ці функціональні можливості не обов'язково виключають один одного, тобто вузол може виконувати більше однієї функціональності одночасно. Крім того, хоч і не строго необхідні для роботи біткойн, деякі ввузли можуть надавати інші функціональні можливості. Наприклад, вони можуть надавати службу *DNS* , яка надає інформацію про існуючих вузли; *служба блокування блоків*, де можна запитувати транзакції та блокувати дані за допомогою графічного інтерфейсу; служба обміну, де користувачі можуть купувати або продавати біткоіни в обмін на інші валюти; і *змішані послуги*, де користувачі можуть заплутати історію своїх монет.

Залежно від їх *підключення*, вузли можуть бути класифіковані у вузли, що прослуховуються і вузли, що не прослуховуються. Прослуховуванні однорангові вузли – це вузли, які приймають вхідні з'єднання, в той час як вузли, що не прослузовуються не роблять цього. Хоча більшість біткойн повних реалізацій прослуховують вхідні з’єднання, деякі конфігурації мереж не дозволяють щоб такі з'єднання були створені (наприклад, вузли позаду NAT).

Хоча оригінальний біткойн Сатоші передбачалося, що вузли будуть використовувати тільки один *протокол*, економіка біткойн виросла набагато більшою, ніж оригінальна специфікація, що дає місце для виникнення багатьох протоколів. Ми будемо використовувати термін "*біткойн* - протокол", щоб посилатися на мережевий протокол, що використовується поточною стандартною реалізацією, клієнтом Сатоші. Інші протоколи, які в даний час існують в системі біткойн в основному орієнтовані на оптимізацію басейну майнінгу і прискорення розповсюдження даних. *Шаблон getblock* – це новий біткойн протокол (замінює попередній протокол *getwork*) у якому дані блоку відправляються майнерам. Це дозволяє майнерам змінювати зміст блоку самим, таким чином отримати автономію по відношенню до пулл серверів. *Stratum* являє протокол спочатку спроектований для легких клієнтів, а потім розширені для обробки майнінгу в пуллі. Що стосується майнінгу, то він не надсилає повні блоки майнеру, тим самим краще масштабування з кількістю операцій, але надає меншу автономію майнерам, щоб вирішити, що включити в блоки. *Мережа ретрансляції біткойну* має протокол для зв'язку з магістральною мережею швидкої ретрансляції Corallo, 6-вузлова мережа, призначена для прискорення ретрансляції даних біткойн. Аналогічно, *Falkon* також є основою вузлів, призначених для пришвидшення розповсюдження біткойн-даних. Вузли можуть підключатися до Falcon, використовуючи протокол біткойн або спеціально розроблений мережевий протокол, що ретранслює пакети як отримані (замість того, щоб чекати, поки всі пакети повного блоку повинні бути отримані перед тим, як почати ретранслювати цей блок). Знову з метою прискорення поширення блоку, *FIBRE* (Fast Internet біткойн Relay Engine) являє собою протокол, який використовує UDP з прямим виправлення помилок, щоб зменшити затримки, зроблені втратою пакетів. Він також використовує стиснення для зменшення обсягу даних, що надсилаються по мережі. Швидкісна мережа як одне з рішень обмеження розширення Біткойн мережі. У цьому контексті *FLARE* є новою пропозицією для протоколу маршрутизації для швидкісної мережі.

* 1. Забезпечення безпеки VoIP звязку в P2P-мережах

Безпека в P2P-мережах була широко вивчена в літературі. У цьому розділі ми пропонуємо широкий огляд основних проблем безпеки, які виникають в мережах P2P, ми переглядаємо, як кожна з проблем безпеки може впливати на мережу біткойн, і якщо це так, ми пояснюємо конкретні контрзаходи які біткойн забезпечує для того, щоб захищатися від кожної атаки.

Список розглянутих атак переходить на найбільш типові типи атак і недоліки безпеки, знайдені в загальних мережах P2P. Очевидно, що конкретні мережі і додатки можуть представляти спеціалізовані напади, але в більшості випадків їх можна розглядати як специфікацію нападів, представлених тут.

Таким чином, щоб забезпечити чітке уявлення про те, як звичайні P2P атаки впливають на біткойн, ми спочатку розглянемо три види атак, які будуть показані, що явно застосовані до біткойн. Після цього, ми включаємо список атак, виявлених для загальних мереж P2P, але це не має такого високого впливу на біткойн, огляд того, чому напади не поширюються на конкретну мережу біткойн і деталізація конкретних випадків, коли ці напади (або деякі варіації) можуть якимось чином ставитися до біткойн.

* + 1. DoS Flooding

Атаки типу «відмова в обслуговуванні» (DOS) можливі в більшості сценаріїв P2P і особливо актуальні, наприклад, в P2P потокових додатках [20–22]. З огляду на їх динамічний характер, P2P-мережі, як правило, більш стійкі до загальних атак DoS, ніж статичні мережі. Цільові DoS атаки на конкретні частини мережі P2P (даний вузол) або послуги, як правило, більш важливі. Так існує кілька потенційних DoS атак в біткойн, але система має контрзаходи за замовчуванням. *Флуд транзакії* запобігаються тим що, не ретранслююються неприпустимі транзакції. З одного боку, операції підписані відправниками для того, щоб продемонструвати, що вони мають правопередавати ці біткоїни. Якщо підписи транзакції неправильні, транзакція вважається неприпустимою і не передається в мережу. З іншого боку, протокол за замовчуванням не передає транзакції без комісій (за винятком декількох дуже конкретних випадків, які також призводять до дуже дорогих атак). Крім того, збори за транзакцію збільшуються для більш низького віку введення (тобто для біткоїнів, які були переміщені останнім часом), тому зловмисник намагається генерувати величезну кількість операцій, які ружають одні і ті ж біткоїни, буде змішений платити збільшену комісію. *Block flooding* перешкоджається тільки передачею лише дійсних блоки, які повинні містити дійсний доказ роботи. Для того, щоб блок містив дійсний доказ роботи, його хеш повинен бути нижчим за дану ціль. Отримання блоку з таким хешом є обчислювально дорогим завданням, таким чином, виконуючи DOS атаку звикористанням даних блоку неможливо. *Переповнення даних в мережі* простіше, ніж в попередніх двох випадках, тому що це дійсно можливо, щоб створити дійсні мережеві повідомлення без сплати комісії, або витрат за обчислення циклів. Однак, Біткойн має протокол заборони: одногрангові вузли можуть заборонити інших однорангові вузли протягом усього дня, якщо їх оцінка поведінки перетинає певний поріг. Оцінка неправильної поведінки збільшується при надсиланні однакових повідомлень, надсилання великих повідомлень і надсилання неприпустимих блоків. Зважаючи на природу біткойн, *використання ЦП DOS* можливо, якщо змусити піри витрачати багато часу на перевірку транзакції або блоку. З метою запобігання такого роду атак, Біткойн намагається зловити помилки перед початком перевірки транзакції, обмежуючи кількість операцій підпису за одну транзакцію та за блок, а також обмежуючи розмір скрипту. Нарешті, попередні версії клієнта Біткойну були також схильні до *безперервного читання із жорсткого диска*, де зловмисник неодноразово послав двічі транзакції щр були вже проведені, які пройшли початкові перевірки і необхідні для отримання даних з диска для того, щоб бути повністю перевіреними. Цієї атаки можна уникнути, перевіряючи, що вхідні дані транзакції знаходяться в наборі UTXO Set (тобто перевіряються, чи є транзакція подвійною витратою), перш ніж отримати інформацію з диска.

* + 1. Атака затемнення

Атака затемнення відбувається, коли зловмисник створює (або контролює) велику кількість різних вузлів, які заповнюють весь район вузла-жертви [23]. Зловмисник може потім *зетемнити* вигляд мережі, який має жертва. Для захисту від атак затемнення, як правило, загальні рішення для атак Сивілли не є достатніми проти атак затемнення [24]. У криптовалютніх мережі ізоляція вузла від решти мережі може дозволити двом іншим видам атаки на затемнений вузол. По-перше, затемнениий вузол може зазнати цензурної атаки, тому що транзакції жертви повинні проходити через вузли нападники, щоб досягти мережі. Таким чином, зловмисник може вирішити, не пересилати ці операції, піддаючи цензурі операції жертви. По-друге, якщо затемнена жертва є майнером, зловмисник може відмовитися або затримати поширення нових блоків, знайдених іншою частиною мережі. Як наслідок, жертва витрачає час обчислення, намагаючись майнити на вершині старих блоків. Біткойн має багато захисних механізмів для запобігання атак затемнення, деякі з яких були додані нещодавно, після дослідження, що показали деякі недоліки, тієї реалізації [13]: клієнт обмежує кількість вихідних підключень до адресатів у тій самій мережі, рандомізує процедуру вибору адреси та підтримує великий список вузлів, серед інших.

* + 1. Профілювання користувачів

У деяких мережах P2P, легко записати всі дії вузла дозволяючи зловмисникам легко створювати ідентифікації профілів користувачів і їх діяльності. Це актуально в анонімних системах або системах, які хочуть гарантувати певний рівень анонімності [16, 25].

Біткойн забезпечує псевдоанонімність, дозволяючи користувачам отримувати платежі за їхніми адресами, які спочатку не є пов'язаними з їхніми особистостями. Використання нових адрес для кожної транзакції в системі призначене для забезпечення незв’язаності між різними діями, які виконує один користувач через Біткойн. Таким чином, профілювання користувачів у Біткойн, як правило, полягає в нападі на незв'язаність між різними адресами одного користувача. Необхідно виконати три різні підходи для виконання кластеризації адрес: використання даних мережного рівня [26], виконання аналізу графу транзакції [27–29] та аналіз фільтрів Блума [30]. Ідея використання даних мережного рівня для кластерних адрес проста: якщо зловмисник може підключитися до всіх вузлів по мережі, перший вузол, який посилає йому дану транзакцію має бути творцем цієї транзакції. Таким чином, якщо зловмисник спочатку отримує дві різні транзакції з одного боку, він може зробити висновок, що вихідні адреси обох операцій належать до одного користувача. Однак, як проста атака може здатися концептуальною, але це не так легко виконати на практиці. Це не тривіально підключатися до всіх вузлів мережі, оскільки більшість з них не приймають вхідні з'єднання. Крім того, деякі вузли анонімізують свої зв'язки за допомогою Tor. Нарешті, зібрані дані дуже шумні, і тому, це не легко зробити сильні визновки при його аналізі. Що стосується аналізу графіків транзакції, існують послуги змішування, які здатні ефективно розірвати відносини між адресою і її минулим. Крім того, використання захищеного гаманця, який намагається звести до мінімуму витік інформації про адреси кластера допомагає пом'якшити наслідки такого аналізу. Нарешті, щодо використання фільтрів Блума, користувачі повинні бути дуже обережними при виборі параметрів фільтра і при створенні різних фільтрів, які відповідають одному набору адрес і спільних ключів. Крім того, розробляються нові протоколи, які дозволяють полегшеним клієнтам отримати свої транзакції, зберігаючи конфіденційність. Проблеми з маштабованістю біткойну викликали пошук нових рішень, що дозволили б збільшити пропускну здатність мережі. Деякі пропозиції передбачають механізми створення неланцюгових платіжних каналів, такі, що безпечні операції між користувачами біткойн можуть виконуватися без необхідності включати всі транзакції в блокчейн. У свою чергу, ці рішення можуть також тягни за собою проблеми з конфіденційністю, які ще не ретельно вивчені [5].

* + 1. ID атаки

У цій категорії можна визначити дві різні підатаки:

1. *Атака зіставлення ідентифікаторів*: коли вузол змінює свій власний ідентифікатор із зловмисними цілями. Як приклад, у DHT на основі P2P-мереж, вузол може отримати контроль над ресурсами, змінивши свій власний ідентифікатор [31]. Ці типи атак є складнішими в мережах, де ідентифікатор отриманий від публічного ключа [32].
2. *Атака зіткнення ідентифікаторів*: Подібно до попередніх атак, тут напад вважається, коли є дубльовані ідентифікатори. Зазвичай проблема вирішується забезпеченням унікальності ідентифікаторів [16].

Немає чіткого поняття про однорангові ідентифікатори в біткойн. Дві різні властивості можна розглядати як ідентифікатори в біткойн, в залежності від точної сутності, яку хочеться визначити: IPs і Біткойн-адреси. IPS дозволяє ідентифікувати колег, тоді як адреси пов'язані з користувачами. Зловмисний вузол може отримати вигоду від зміни IP, якщо він заборонений за неправильну поведінку. Кожен вузол підтримує banscore для кожного з його сусідів. Цей banscore збільшується, кожного разу, коли вузол поводить себе неправильно. Якщо banscore перевершує певний поріг, вузол є забороненим протягом 24 годин. Таким чином, будучи в змозі змінити IP дозволяє одноранговому вузлі ефективно скинути його banscore. Що стосується другого роду ідентифікаторів, Біткойн-адреси, рекомендується для користувачів дійсно змінювати їх часто. Фактично, пропонується не використовувати повторно адреси, тобто створювати нову адресу для кожної транзакції, зроблену в системі. Це дозволяє захистити конфіденційність користувачів.

* + 1. Атаки Сивілли

Атака Сивілли - це добре відома атака в мережах P2P, де шкідливий користувач створює кілька посвідчень для керування системою або частинами системи [33]. Це було дуже широко вивчено в літературі в контексті декількох технологій P2P [34, 35].

Атака Сивілли може бути проблемою в Біткойн, якщо вона може затемнити всі з'єднання з вузлами (див. розділ 1 для подробиць атаки затемнення). Однак, крім свого розширення на атаку затемнення, одноранговий вузол з декількома посвідченнями не може зашкодити системі щодо основного вмісту мережі: транзакції та блоків. Блоки не можуть бути підробками без відповідного підтвердження роботи, а генерація транзакцій тягне за собою пов'язану плату. Тим не менше, якщо багато вузлів Сивілли починають виконувати величезну кількість підключень до існуючої мережі, вони можуть монополізувати всі доступні слоти підключення, і системна децентралізація може бути зменшена.

* + 1. Підроблене завантаження

Доступ до мережі в P2P-середовищах починається з підключення до одного або кількох вузлів мережі. Цей перший контактний вузол відомий як вузол початкового завантаження. Зловмисний вузол початкового завантаження може впливати на вигляд мережі для нового користувача [23]. Кілька рішень вже існують для цієї проблеми, такі як не ретрансляції в одному вузлі початкового завантаження, використання кешування вузлами для наступних підключень, випадкові адреси зондування, використання зовнішніх механізмів, використання конкретних послуг завантаження, або використання мережевого шару рішень (наприклад, використання спеціальної багатоадресної групи для завантаження) [16, 36, 37].

Біткойн вирішує проблеми початкового завантаження шляхом визначення локальної бази даних на кожному вузлі, яка запитується за псевдовипадковим протоколом, щоб отримати підмножину потенційних однорангових вузлів (див. розділ 4.7 для подробиць).

Таким чином, біткойн застосовує більшість рішень для фіктивного протоколу, наприклад, *не ретранслюючи в простому вузлі початкове завантаження*, встановивши 8 вихідних з'єднань на кожному завантаженні, *використання кешованих вузлів для подальших з'єднань*, за допомогою однорангових вузлів, збережених у *перевірочній* таблиці, використовуючи *випадкові адреси*, за допомогою псевдовипадкового протоколу для зберігання та отримання однорангових адрес з бази даних, а також *за допомогою зовнішніх механізмів* , що є в списоку відомих DNS-вузлів або навіть за допомогою списку жорстко закодованих вузлів, якщо DNS не може бути досягнуто.

* + 1. Несанкціонований доступ до ресурсів

P2P-мережі часто використовують якісь приватні дані, які повинні бути захищені від несанкціонованого доступу. Загальними рішеннями є ті, які зазвичай використовуються для розподіленого контролю доступу [38, 39].

Біткойн базується на криптокриптографії з відкритим ключем, де необхідні приватні ключі для авторизації платежів. Таким чином, приватні ключі повинні зберігатися в таємниці, і два методи, як правило, використовуються: шифрування і оффлайн зберігання. За допомогою шифрування приватні ключі залишаються захищеними, навіть якщо зловмисник може отримати ключ файлу, поки ключ шифрування залишається секретним. Що стосується офф-лайн зберігання, різні підходи можуть бути прийняті з різними технічними рівнями складності, від використання спеціалізованих апаратних пристроїв для паперових гаманців. Зверніть увагу, що на відміну від інших застосувань криптографія публічного ключа, де приватні ключі повинні бути в мережі (наприклад, у процесі TLS), Біткойн-мережа не залучає приватну інформацію, оскільки перевірки виконуються з використанням публічної інформації. З цієї причини, офф-лайн зберігання спільних ключів не впливає на продуктивність мережі.

* + 1. Управління шкідливими ресурсами

Зловмисний вузол може заперечувати існування даного ресурсу під його відповідальністю або заявляти, про ресурс якого немає. Це особливо актуально у додатках для розповсюдження контенту, а спільні рішення – це реплікація ресурсів [40], або використання кодів виправлення помилок для реконструкції відсутніх частин ресурсу [41]. Мережа біткойн захищена від управління шкідливими ресурсами, з одного боку, велика кількість інформації про надмірність даної мережі, а з іншого боку, кілька сусідів до яких підключений вузол. Завдяки тому, що вузли встановлюють з'єднання (за замовчуванням) до 8 інших однолітків, якщо даний сусід заперечує існування певного ресурсу, то одноранговий вулол може дізнатися її від інших сусідів. Крім того, якщо сусід каже, що він має деякий ресурс, якого він насправді не має, однорангові вузли помітять це, коли вони будуть намагатися отримати його (так як транзакції та блоки визначаються їх хеш).

* + 1. Людина-в-середині (MITM)

У контексті P2P-мереж, напад MITM зазвичай вважається атакою маршрутизації, схожу на класичну мережеву MITM атаку. P2P-мережі, які вимагають маршрутизацію з декількома прийомами, повинні включати заходи, аналогічні до цибулевої маршрутизації, з тим щоб забезпечити з'єднання між усіма вузлами по шляху [45, 46].

MITM атаки в Біткойн не є проблемою для транзакції і цілісності блоків, оскільки транзакції криптографічно підписані і блоки повинні містити дійсний доказ роботи. Гнучкість транзакцій може бути проблемою в дуже конкретних сценаріях, але рішення в даний час розгортається. Цензура не є проблемою, тому що один пір зберігає різні з'єднання. Зловмисник має бути посередині всіх, щоб приховати інформацію про однорангові вузли (таким чином, вдаючись до атак *затемнення*).

2.3.10 Висновки до підрозділу 2.3

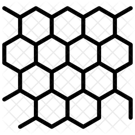
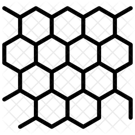
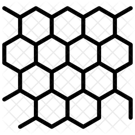
Як бачимо існує багато різноманітних типів атак які можуть бути використані для того щоб порушити правильність функіонування мережі або ж з цілью отримання приватної інформації. Але деякі типи атак можуть бути заблоковані або взагалі неможливі завдяки внутрішній реалізації мережі біткойн. Тобто якщо порівнювати звичайну централізовану мережу VoIP, яка незахищена від таких типів атак, P2P мережа на основі біткойну має значну перевагу в цьому.

3. ЕКСПЕРИМЕНТАЛЬНЕ ПІДТВЕРДЖЕННЯ БЛОКЧЕЙН ДЕЦЕНТРАЛІЗОВАНОГО ЗВ’ЯЗКУ

Для того, щоб перевірити ефективність децентралізованого VoIP зв’язку на основі парадигми біткойн P2P необхідно створимо мобільний додаток для отримування публічних ключів, зашифрований за допомогою методів блокчейн.

3.1 Програмна реалізація децентралізованого встановлення зв’язку

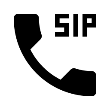
Головна проблема з вищезгаданими механізмами безпеки – вимога наявності публічної ключової інфраструктури (PKI) для забезпечення жорсткої безпеки. Таким чином, сертифікати є обов'язковими для перевірки автентичності клієнта та сервера. У нашому рішенні ми маємо намір виключити використання PKI, замінивши їх на мережу блокчейн для зберігання та управління публічним ключами абонентів. Рисунок 3.1 ілюструє архітектуру та інтерфейси системи.



BTC блокчейн

Мобільний девайс

Модуль клієнта



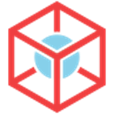
SIP клієнт

BTC гаманець

BTC клієнт



Платформа менеджменту застосунку



Повний вузол

BTC гаманець

Підтвердження

Операції гаманця

SiP сервер



1

Отримати публічний ключ

2

TLS-PSK

[Address,Token]

3

Зберегти публічний ключ

4

5

6

Рис 3.1 – Архітектура системи та інтерфейс зв’язку

Користувач завантажує мобільний додаток з магазину Google Play в операційну систему Android (1). Додаток включає інтерфейс до мережі блокчейн біткойн. Додаток генерує порожній гаманець біткойн і надійно просить ефір з функції управління Wallet на сервері (2,3) . Після успішної передачі ефіру, мобільний додаток генерує і зберігає ключову пару в захищеному Android keystore. Крім того, він зберігає публічний ключ у Блокчейн через смарт-контракт (4), а потім запитує схвалення від сервера керуванням Wallet (3). Сервер перевіряє транзакцію запиту, звернувшись до служби Google Play, щоб перевірити справжність програми (5). Якщо запит є достовірним, то керування гаманцем схвалить транзакцію зберігання в Блокчейн (6). Для автоматизації конфігурації SIP-облікових даних (7) визначається новий інтерфейс між керуванням гаманця і сервером SIP.

Основними компонентами, які задіяні в даній системі є: 1) мобільний додаток, 2) сервер управління Wallet і 3) біткойн Smart контракт.

3.2 Структура мобільного додатку VoIP-клієнта

Мобільний додаток складається з наступних компонентів: стандартний SIP клієнт, легкий клієнт Ethereum, який використовує Ethereum Subprotocol (LES) [8] для інтерфейсу Blockchain, і виділений модуль для взаємодії з функцією управління Wallet на сервері. Послідовність подій, що відбуваються після установки програми по телефону, зображена на рис. 3.2.

Додаток генерує порожній гаманець біткойн на своєму першому запуску, і пропонує користувачеві заповнити його достатнньою кількість BTC, щоб мати можливість зберігати ключ у мережі блокчейн. Передача ефіру клієнту є обов'язковою як зберігання даних або зміна стану контракту в блокчейн вимагає плати за транзакцію, які оцінюються в ефірі. Щоб спростити цей процес для кінцевих користувачів, додаток надає діалогове вікно покупки в програмі, що пропонує користувачу платити за передачу ефіру у валюті.

Старт

Генерувати BTC гаманець

Запитати про BTC

Старт

 Генерувати ключ пару

SIP реєстрація

Завершити

Зберегти ключ пару у BTC

Зберегти у захищеному місці

SIP конфігурація для юзера

Перший запуск?

Підтверджено?

Рис. 3.2 – Блок-схема для послідовності дій після встановлення програми

Після завершення покупки мобільний додаток надсилає нову адресу гаманця, квитанцію про покупку та номер мобільного телефону в управління гаманця як шифроване корисне навантаження. Потім програма генерує пару ключ абонента і зберігає його в захищеному Android keystore. Управління Wallet перевіряє запит і передає достатній ефір для клієнта. Після успішної передачі клієнт зберігає свій публічний ключ у смарт-договорі разом із маркером отримання та абонентом.

3.3 Заміна номерного ресурсу смарт-контрактами

Смарт-контракт – це об'єкт, що містить розподілений код, що має біткойн блокчейн автономно. Будь-який користувач, що володіє гаманцем з достатньою кількістю валюти, може розгорнути смарт-контракт на Блокчейн, надіславши його як підписану транзакцію. Код контракту написаний на Solidity[9], мовою високого рівня з синтаксисом, схожим на JavaScript, призначений для використання з біткойн віртуальної машини (EVM).

У системі смарт-контракт, який містить загальнодоступні ключі абонентів за допомогою картографічної структури даних, індексованих жетонами отримання. Рисунок 3.3 ілюструє основні функціональні можливості смарт-контракту:

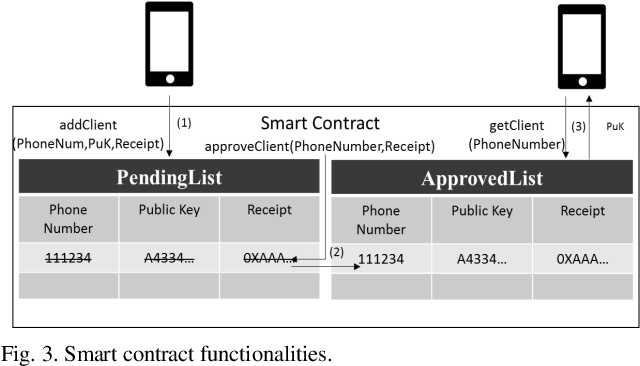


Рис. 3.3 – Основні функції і можливості смарт-контрактів

Універсальний протокол для протоколів безпеки PSK (PreShared ключем)

Важливим внеском цієї платформи (смарт-контракту в Ethereum) є ліквідація інфраструктури публічного ключа (PKI) і сертифікації (CA), а також здійснення загальних протоколів для PSK (попередньо спільний ключ) на основі протоколу безпеки, як TLS-PSK, DTLS-PSK, SRTP і т. д.. ..

Це з групи загальний протокол відповідає за розповсюдження PSK ключ між двома сутностями. Цей протокол реалізує метод Нідгема – Шредера [12] для розповсюдження ключа сеансу за допомогою асиметричного шифрування.

Після того, як канал зв'язку між клієнтом SIP і SIP-сервер захищений, наскрізне шифрування між кінцевими точками може бути встановлено. Клієнт VoIP вибирає публічний ключ від викликається від біткойну Blockchain і, отже, генерує випадковий сеанс ключ для використання в якості головного ключа в протоколі SRTP з метою шифрування RTP голосових пакетів між двома кінцевими точками. Майстер ключ шифрується за допомогою публічного ключа призначення, а потім за допомогою протоколу MIKEY через SPD частину SIP запросити, як показано на рис 3.3.

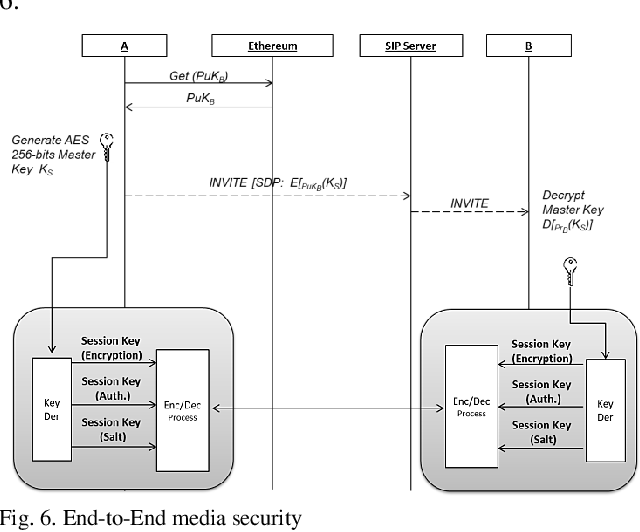


Рис. 3.3 – End-to-end медіа захист через RTCP

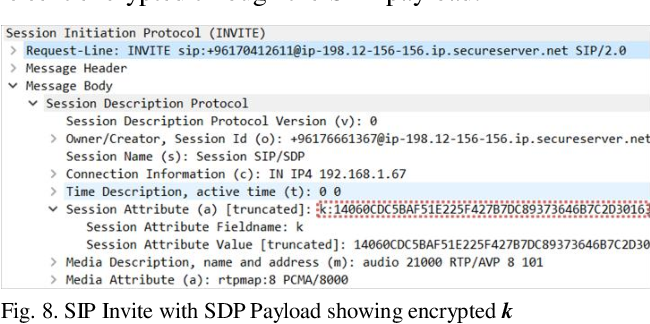
Для перевірки запропонованої системи ми реалізували рішення з використанням таких компонентів: a) Kamailio: SIP-сервер з відкритим вихідним кодом [15], b) RTPProxy: Високопродуктивний медіа-проксі для RTP потоків, c) Geth легкий клієнт (Ethдроїд) [16]: простий у використанні Bitcoin Geth обгортку для android, d) Solidity: Контрактне програмування мови для написання смарт-контрактів, e) NodeJS: серверні клієнтські сценарії (сервер управління Wallet), f) SIPDroid як клієнт SIP Android [17]. Рис. 3.4 демонструє SIP запити повідомлення, в якому майстер Key k відправляється зашифрований через SPD корисного навантаження. 

Рис. 3.4. SIP Invite з SDP Payload що показують зашифрований k

Таблиця показує час, який було зроблено для настроювання виклику під час надсилання ключа в частині SPD повідомлення SIP. Зберігання публічного ключа в Блокчейн Bitcoin Testnet зайняв 11,5 секунди для перевірки. На цей раз витрачається тільки раз на конфігурацію. Отримання публічного ключа з іншого боку тільки 507ms; Ця кількість часу витрачається на налаштування кожного виклику.

Загальний час установки виклику складається з: отримання ключа з Блокчейн, симетрична генерація ключа, шифрування публічного ключа, SIP сигналізація, закритий ключ дешифрування, і SRTP диференціювання ключа. Знадобилося 1218 ms для установки безпечного виклику між сторонами.

3.4 Реалізація VoIP пов'язаних мобільних додатків

Основні класи полягають у наступному: користувач, сесія, присутність і конференція.

Користувач представляє локального користувача, який прослуховує SIP-повідомлення і прив'язується до одного адреса запису. Сеанс це - SIP запрошення на основі сеансу, який створюється неявно бібліотекою, кол User.connect або User.accept викликається для вихідних або вхідних дзвінків. Об'єкт Preserve використовується для представлення стану присутності користувача і створюється неявно в бібліотеці, коли User.watch або User.approve викликається для перегляду віддаленого користувача або затвердження наявності підписки від віддаленого користувача. Об'єкт Conf створюється програмою або для нової конференції для запрошення нових учасників конференції або прийняття вхідного запрошення на конференцію. Conf, Session або Presence пов'язаний з одиним локальним об'єктом User, який постачає локальні облікові дані та локальну адресу запису для різнb[ SIP-повідомлень. Є деякі спрощення в дизайні API. Зокрема, один сокет для прослуховування пов'язана з одним об’єктом User, отже, може зробити тільки одну вихідну реєстрацію. Мить повідомлення може бути частиною встановленого сеансу обміну миттєвими повідомленнями на основі сеансу або може бути надіслано незалежно від об'єкту користувача для пейджингового режиму IM.

Існує деяка аналогія між UNIX сокет API і цим API. Використовується семантика сокета такі функції, як bind, accept, recv, send, connect і close.

3.5 Session та Precence

Коли створюється об'єкт сеансу або присутності, подальші події для цього сеансу або присутність направлені до цього об'єкта. Застосування робить цикл обробки для отримання подій з об'єкта наступним чином:A screenshot of a cell phone

Description automatically generatedЗастосунок може змінити стан присутності на об'єкті користувача так, що всі затверджені віддалені спостерігачі отримують оновлення стану.

За межами цього модуля цей модуль буде обробляти медіацикл. Зокрема, програма повинна зробити щось подібне до такого, щоб відправляти і отримувати медіа на msock. Це зовнішній, таким чином, бібліотеці не потрібно мати справу з надсилання та отримання носія на створений сеанс.

A screenshot of a cell phone

Description automatically generated

Об'єкт конференції може бути побудований з назви конференції, ідентифікатора та локального User об’єкта наступним чином:

ID є унікальним ідентифікатором, який використовується в заголовку conf-ID на децентралізованих сигнальних конференціях.

Після того, як об'єкт conf створюється, можна обробити об'єкт користувача, за винятком того, що він дозволяє лише сеанс і серед декількох віддалених контактів. Зокрема, можна скористатися способом підключення та прийняття на conf запросити контакт у конференції або прийняти вхідний запит на підключення до конференції.

A screenshot of a cell phone

Description automatically generated

Різниця між confinvite і confconnect в тому, що confinvite відправляється на нову конференцію запрошення, яка може вимагати створення conf перед прийнятям виклику, в той час як confconnect, щоб вказати, що деякі члени запросили іншого члена B і що інші члени A повторне з'єднання з нами, тому ми повинні негайно викликати погодитися на conf , і нехай бібліотека турбується про статуси кожного члена конфереції.

3.6 Рекомендації до створення систем   
децентралізованого VoIP зв’язку

Функції-генератори працюють в багатозадачному контексті складніше. Більшість методів визначено як генератори тому семантика виглядає як блокуючий виклик функції але всередині це звичайний багатозадачний режим. Наприклад,



Є й інші альтернативні проекти для API, наприклад, орієнтований на події і зворотного виклику, провайдер і прослуховувач і т. д. Майже всі інші API SIP, як правило, є зворотним викликом або слухачі подій. Було вибрано синхронний стиль генератора з кооперативної багатозадачності, оскільки вона знижує накладні витрати з точки зору обслуговування та розуміння різних розрізнених частин вихідного коду. Існує ще один підводний камінь, якого потрібно уникати у разі використання цього API. Якщо метод генератора викликається, потрібно бути обережними у використанні "yield". Якщо ви використовуєте "yield" метод остаточне повернення значення, що повертається з заяви про прибутковість. Якщо ви не використовуєте "yield", то він повертає генератор, який пізніше може бути використаний для отримання всіх проміжних значень, а також остаточні значення. Це також корисно для того, щоб скасувати генератор функції, просто викликавши за близькою close() на ньому. В загальному можна завжди використовувати "yield" для простих застосунків.

3.7 Результати створення системи децентралізованого зв’язку

У даному розділі було розглянуто новий підхід щодо довірчого управління ключами на основі алгоритмів блокчейн, щоб вирішити складність безпеки SIP сигналу та сторонні питання довіри. Наша реалізація була випробувана на платформі Ethereum Testnet. Результати показали, що за критерієм часу встановлення сеансів зв’язку розроблене рішення є задовільним у порівнянні з централізованими системами зв’язку.

4. ОХОРОНА ПРАЦІ

У ході цього дослідження існує багато виробничих факторів, які загрожують життю та здоров’ю людини. У цьому розділі визначено основні потенційно шкідливі та небезпечні виробничі фактори, пов'язані з використанням комп'ютерних апаратних засобів та електронного обладнання у дослідницькій діяльності та підтверджено умови праці, які відповідають вимогам безпеки та гігієни. Також передбачені відповідні технічні рішення та організаційні заходи щодо охорони праці, гігієни праці та основних надзвичайних заходів.

Визначення основних потенційно небезпечних i шкідливих виробничих чинників при виконанні науково-дослідної роботи

Магістерська робота досліджує можливість створення розподілених систем для обробки великих даних та передачі даних через Wi-Fi. Так як при розробці даного пристрою згідно ТЗ були враховані усі вимоги ДСНіП №476 і ДСНіП №239 щодо захисту персоналу і населення від негативного впливу електромагнітного випромінювання радіочастотного діапазону, то ці питання в даному розділі не розглядаються.

Оскільки дослідження базуються на електронних комп'ютерах та лабораторному обладнанні, існує ризик ураження електричним струмом. В ході експериментальних досліджень електромагнітне випромінювання може негативно впливати також. Існують також небезпеки пожежі з електричних причин.

Небезпечні та шкідливі фактори для наукових досліджень:

* + - небезпека ураження електричним струмом;
    - недостатнє освітлення на робочому місці;
    - наявність електромагнітного випромінювання ВДТ ПЕОМ;
    - погані параметри мікроклімату в робочій зоні;
    - Підвищений шум;
    - Величезне психофізіологічне навантаження..

4.1 Технічні рішення та організаційні заходи з безпеки і гігієни праці та виробничої санітарії

4.1.1 Електробезпека

Лабораторне приміщення, що розглядається, розташоване в будівлі з 5-ти провідною 3-х фазною електромережою із зануленням. Температура в серединв приміщення не буде перевищувати +26 °С, а вологість повітря не перевищує 60%. Приміщення не є хімічно активним середовищем, що може руйнувати ізоляційні і електричні матеріали або струмопровідний пил. У приміщенні є можливість одночасного дотикання декількох або однієї людини до металевих корпусів електричного обладнання та металевих конструкцій будівлі що є заземленими. Таким чином, згідно з ОНТП 24-86 та ПУЕ, умови приміщення за рівнем електронебезпеки можна віднести до умов з підвищеною небезпекою.

Використовуване в данній дослідницькій роботі електроустаткування живиться від мережі напругою 220 В. Електромережа належить до класів 0І та І за електрозахистом ДСТУ ІЕС 61140:2015.Апаратура що використовуєтся для визначення характеристик досліджуваних зразків відноситься до першого класу за електрозахистом, тобто мається наувазі що буде використовано трьохпровідний шнур з заземленими та робочим нульовим дротами. Під час роботи з електронно-обчислювальним обладнанням є можливість доторкання до деяких частин електроустаткування, що перебувають під напругою. Оцінка ризику контакту з струмопровідними частинами полягає у визначенні струму, що протікає через тіло, та порівнянні його з допустимим значенням згідно ПУЕ-2017. Взагалі допустиме значення струму, що протікає через тіло людини, залежить від схеми з'єднання електрообладнання та електромережі, характеру та розміру напруги живлення, схеми включення.

Щоб правильно визначити необхідні засоби та заходи запобігання ураження електричним струмом, необхідно знати допустимі значення контактної напруги та струму через тіло людини..

Табл. 4.1 – гранично-допустимі значення напруги доторкання та сили струму IL, для нормального режиму електроустановки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| t(сек) | до 0,1 | 0,2 | 0,5 | 0,7 | 0,9 | > 1 сек.  до 5 сек. |
| Uдоп.дот. | 500 | 400 | 200 | 130 | 100 | 65 |

Основною причиною ураження електричним струмом є контакт із голими струмопровідними деталями, які є пристроями, що працюють під напругою через збій ізоляції. Нижче наведені деякі групи технічних рішень щодо запобігання електротравм згідно ПУЕ. «Правила улаштування електроустановок. Розділ 1 Загальні правила. Гл.1.7 Заземлення і захисні заходи електробезпеки»:

Технічні рішення для запобігання ураження електричним струмом під час переходу напруги до електропровідного обладнання, яке, як правило, не проводить електричний струм (аварійний режим роботи електрообладнання, наприклад, поломка робочої ізоляції): занулення, тобто навмисне електричне з’єднання нормально не струмоведучих елементів електроустаткування із заземленою нейтраллю електромережі за допомогою нульового дроту і автоматичне вимкнення живлення. В аварійному режимі спрацює захист від короткого замикання (пристрій захисту максимального струму або запобіжник), а пошкоджене електрообладнання відключено від електроживлення.

4.1.2 Розрахунок захисного відключення електромережі при аварійному режимі роботи електрообладнання

Проведемо деякі розрахунки ланцюга захисного відключення фазного проводу при короткому замиканні. Струм короткого замикання можна обчислити за наступною формулою:

де UF = 220 В - напруга фазного проводу,

R0 = 1,8 Ом - опір нульового проводу,

RF = 2,3 Ом - опір фазного проводу,

*ZTR*= 0,1 Ом - еквівалентний опір трансформатора.

Струм для спрацьовування автоматів захисту з електромагнітним розпилювачем повинен бути в 1,4 рази менше струму короткого замикання при струмі короткого замикання меншим 100 А. Проведемо деякі розрахунки для визначення необхідного струму для спрацювання автомату струмового захисту.

Таким чином струм для спрацьовування автомату повинен бути не більше 15,6 А.

Автомати, які встановлені в дослілжуваному приміщенні мають Іспр= 10 А, що задовольняє заданим умовам.

Розрахуємо напругу дотику до корпусів електрообладнання при короткому замиканні ():

В

Відповідно до ПУЕ-2017 (табл. 4.1) максимально допустима напруга дотику при часі спрацьовування автомату струмового захисту < 0,1 с дорівнює 500В.

4.1.3 Мікроклімат робочої зони

Для нормалізації мікроклімату, згідно з ДСН 3.3.6.042-99. «Державні санітарні норми параметрів мікроклімату у виробничих приміщеннях», приміщення з ЗОТ є обладнаним системою опалення, а також системою для кондиціювання повітря з температурним регулюванням та об'єму повітря, що буде подаватися, у відповідності до СНиП 2.04.05-91 «Отопление, вентиляция и кондиционирование». Для запобігання перегріву та радіаційного охолодження в теплу пору року - взимку приміщення обладнують жалюзі та екранами.

Робота на робочому місці виконується сидячи і тому не потребує фізичного навантаження. Таким чином її можна віднести до категорії Іа, що о види діяльності з витратами енергії до 120 ккал/год.

Відповідно до ДСН 3.3.6.042-99 «Державні санітарні норми параметрів мікроклімату у виробничих приміщеннях» параметри мікроклімату, що нормуються: температура (t°С) і відносна вологість (W,%) повітря, швидкість руху повітря (V, м/с).

Допустимі та оптимальні параметри мікроклімату для умов, що розглядаються на данний момент (категорія робіт та період року) показані в табл. 4.3.

Фактичні параметри мікроклімату в зоні для виконання роботи відповідають приведеним нормам ДСН 3.3.6.042–99 що були описані вище.

*Таблиця 4.3* – *Параметри мікроклімату.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Період року | Оптимальні | | | Допустимі | | |
| t °С | W,% | V,м/с | t°С | W,% | V,м/с |
| Теплий | 23-25 | 40-60 | 0,1 | 22-28 | 55 | 0,2-0,1 |
| Холодний | 22-24 | 40-60 | 0,1 | 21-25 | 75 | ≤ 0,1 |

4.1.4 Виробниче освітлення

Для пітримки працездатності протягом тривалого проміжку часу, підвищення продуктивності праці, суттєвим фактором є забезпечення норм освітленості на місці роботи. Значення освітленості регулюється нормами ДБН В.2.5-28-2018. Приміщення з ЕОМ, відповідно до ДБН В.2.5–28–2018. «Природне і штучне освітлення. Норми проектування», відноситься до класу кабінетів інформатики та обчислювальної техніки. Розряд і підрозряд зорової роботи Б-2.

Нормування штучного освітлення також відбувається за допомогою ДБН В.2.5-28-2018. Для загального освітлення використовується в основному люмінесцентні лампи, через їхн переваши. Для обрахунку штучного освітлення використовують метод коефіцієнта використання потоку:

де Ф – світловий потік;

E – нормована мінімальна освітленість;

К – коефіцієнт запасу;

S – освітлювана площа;

Z – коефіцієнт нерівномірності освітлення;

С – коефіцієнт використання випромінюваного світильниками світлового потоку на розрахунковій площі;

N – число світильників.

Згідно ДБН В.2.5-28-2018 обрахуємо норму освітленості. E = 300 лк; K = 1,4; S = 6,4∙4 = 25,6 м2; Z = 1,2. Кількість необхідних люмінесцентних ламп визначається за наступною формулою:

Найбільш підходящим для приміщення є люмінесцентна лампа ЛД (денного світла) потужністю 40 Вт. Світловий потік лампи ЛД-40 дорівнює Ф = 2340 люмен (лм). Величиною *i*, індекс приміщення можна визначити за допомогою наступної залежністі від площі приміщення та його висоти:

де A = 5м – довжина приміщення;

B = 4м – ширина приміщення;

h – висота підвісу;

де H = 2,75 м – висота приміщення;

hр = 0,8 м – висота робочої поверхні;

hс = 0,4 м – висота від стелі до нижньої частини лампи;

Коефіцієнт використання світлового потоку на площі

C = 0,3. В результаті кількість ламп буде дорівнює:

Для штучного освітлення в робочому приміщенні достатньо бцде використовувати 2 люмінесцентні лампи денного світла ЛД – 40, зі світловим потоком Ф = 2340 лм кожна.

4.1.5 Виробничий шум

Розглянуті в проекті умови та характер роботи можна класифікувати як роботу комп'ютерних програмістів у лабораторії з теоретичної роботи та обробки даних, де рівні шуму визначені за допомогою ДСН 3.3.6.037-99. Допустимі рівні звукового тиску в октавних смугах частот представлені у таблиці 4.4.

*Табл. 4.4* – *Допустимі рівні звукового тиску і рівні звуку для постійного (непостійного) широкосмугового (тонального) шуму*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Характер  робіт | Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах частот із середньогеометричними значеннями (Гц) | | | | | | | | | Допустимий рівень звуку (ДБА) |
| 1,5 | 3 | 125 | 250 | 500 | 1000 | 2000 | 4000 | 8000 |
| програміст обчислювальної машини | 86 | 71 | 61 | 54 | 49 | 45 | 42 | 40 | 38 | 50 |

Джерелами шуму на робочому місці, що розглядаються під час роботи, є вентилятор охолодження (джерело живлення, процесор та вентилятор відеокарти) внутрішньої системи персонального комп’ютера та системи кондиціонування.

Очікуваний рівень звукового тиску та рівня звуку на основі шумових характеристик цих джерел звуку:

* + - рівень шуму, що створюється внутрішніми елементами ПК рівний 35 дБ;
    - рівень шуму низькочастотної / високочастотної системи кондиціонування повітря становить 25/30 дБ.

Оскільки рівень звуку потенційного джерела шуму нижчий за прийнятний рівень, робоче середовище відповідає вимогам.

4.1.6 Вимоги щодо організації комофортних та безпечних робочих місь користувачів ВДП ПЕОМ

Вимоги до робочого місця робіт з використанням ЕОМ регулює нормативний документ ДСанПіН 3.3.2.007-98 та «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» .

Дизайн робочого столу відповідає сучасним вимогам ергономіки та забезпечує розміщення на робочому столі найкращого обладнання (монітора, клавіатури, принтера) та документів.

Роботчий стілець - підйомно-поворотне крісло, що має можливість регульованя за висотою, за кутом і нахилу сидіння та спинки. Кожен параметр коригується незалежно, легко та безпечно. Фіксовані підлокітники з регульованою висотою над сидінням зменшують статичне напруження м’язів. Поверхня сидіння і спинки крісла напівм'яка з нековзним покриттям.

Дисплей розташований на відстані від очей користувача що є оптимальною зважаючи на розмір знаків і символів.Дисплей розташовано так що він знаходиться у вертикальній площині під кутом +300 до лінії погляду працюючого . Клавіатура знаходиться на поверхні стола на відстані 100...300 мм від його краю. В констукції клавіатори присутній опорний пристрій, за допомогою якого є можливість змінювати кут нахилу клавіатури по відношенню до горизонтальної ділянки робочої поверхні у межах 5...150. Дане розташування клавіатури в просторі є оптимальніми для праці обома руками.

Комп'ютерна кімната має природне та штучне освітлення. Природне освітлення повинно забезпечуватися через світловий отвір. Внутрішнє освітлення забезпечується загальною уніфікованою системою освітлення. Люмінесцентні лампи ЛБ слід використовувати як штучні джерела світла.

Працівники з ЕОМ мають обов'язково проходити попередній медичний оглядам перед влаштуванням на роботу і періодичним – близько одного разу на два роки медичного огляду де у складі присутні терапевт, невропатолог та офтальмолог. Метою медогляду є перевірка стану здоров'я конкретного працівника і підтвердження відсутності у нього медичних протипоказань, які можуть заважати правильному виконанню роботи з ПК.

4.1.7 Організація оптимального режиму праці та відпочинку привикористанні ЕОМ

Організовуючи роботу, пов’язану з використанням комп’ютерів, з метою збереження здоров’я працівників, запобігання професійним захворюванням та збереження працездатності слід вказати встановлений період часу відпочинку. Згідно з ДСанПіН 3.3.2.007-98 характер трудової діяльності відповідає роботі оператора електронно-обчислювальних машин – це робота, що є пов'язаною з інформацією що одержана з дисплея за деяким запитом, або іншої, що надходить з робітника, супроводжується перервами на відпочинок різної тривалості, пов'язана також з виконанням іншої роботи і характеризується як робота з напруженням зору, не дуже великими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у вільному темпі.

Тривалість регламентованих перерв під час роботи з ЕОМ становить 15 хвилин через кожні дві години роботи.

4.2 Безпека в надзвичайних ситуаціях

Аварійну безпеку регулює ПЛАС. Однією з головних складових ПЛАС є розробка технічних рішень та організаційних заходів для оповіщення, евакуації та експлуатації персоналу у випадку надзвичайних ситуацій та визначення активних заходів пожежної безпеки.

4.2.1 Вимоги щодо організації ефективної роботи системи оповіщення персоналу при НС

Для збільшення рівня безпеки в надзвичайних ситуаціях (НС) рекомендується встановити систему оповіщення (СО) виробничого персоналу.

Оповіщення робочого персоналу у разі виникнення деякої НС, наприклад пожежі, здійснюється відповідно до вимог НАПБ А.01.003-2009.

Необхідність обладнання виробничих приміщень певним типом СО визначається згідно з додатком Е до ДБН В.1.1-7-2016 "Захист від пожежі. Пожежна безпека об'єктів будівництва".

Коли виробнича будівля обладнана системою попередження, вони повинні бути розділені на зони сповіщення, і в той же час слід враховувати рішення щодо планування приміщення, будинку евакуації та пожежного відділення., а також з урахуванням вимог, що наведені в примітці 1 таблиці Е.1 додатка Е до ДБН В.1.1-7-2016.

Розмір зони тривоги, пріоритет тривоги та час початку видачі тривоги людям у кожній зоні визначаються відповідно до умов для забезпечення безпечної та своєчасної евакуації персоналу в надзвичайній ситуації..

Повідомлення про надзвичайні ситуації та контроль евакуації здійснюються одним або комбінацією наступних методів:

* + - поданням сигналів (звукових і (або) світлових) в усі робочі приміщення будівлі де можливе постійне або тимчасове перебування людей;
    - трансляція текстів евакуації, маршрутів евакуації, вказівки щодо руху та інші заходи з безпеки людини;
    - трансляція спеціально розробленого тексту для запобігання паніки та інших ускладнень евакуації;
    - розміщенням на шляхах евакуації знаків безпеки згідно з ДСТУ ISO 6309;
    - ввімкненням евакуаційних знаків "Вихід";
    - ввімкненням світла що сигнлізує про проведення евакуації та світлових вказівників що вказують напрямок евакуації;
    - віддаленим відкриттям дверей евакуаційних виходів;

Як правило, система сповіщення має вмикатися автоматично від сигналу про пожежу, складається з пожежної сигналізації або системи пожежогасіння. Також з приміщення чергового (оперативного) персоналу системи сповіщення (диспетчера пожежного поста) слід продумати можливість запуску СО вручну, що буде забезпечувати більшу надійну роботу СО не тільки при пожежі, а і при виникненні будь-якої іншої НС.

Відповідно до вимог ДБН B.1.1-7-2016, необхідно транслювати голосові повідомлення та команди управління в режимі реального часу через мікрофон, щоб швидко реагувати, коли ситуація змінюється або настає нормальна ситуація евакуації виробничого персоналу.

Повідомлення про аварійний персонал / пожежу / тривогу видаються за допомогою світлових та / або звукових сповіщувачів - усі виробничі приміщення.

СО має розпочати трансляцію сигналу про оповіщення НС /пожежу/, не пізніше чим після трьох секунд з моменту отримання сигналу про НС /пожежу/.

Аварійні / пожежні / попереджувальні сигнали повинні відрізнятися від сигналів інших цілей.

Панель управління СО повинна бути розміщена у пожежній станції, диспетчерській або іншій спеціальній зоні (за наявності). Ці приміщення повинні відповідати вимогам ДБН В.2.5-56-2014 .

Кількість звукових і голосових детекторів, їх розташування та потужність повинні забезпечувати необхідний рівень звуку в усіх місцях, де виробничий персонал постійно або тимчасово знаходиться.

Якщо існує небезпека механічного пошкодження детектора, слід передбачити заходи захисту, які не пошкодять працездатність детектора.

Встановлення звукових і голосових детекторів на виробничому майданчику повинно виключити можливість концентрації та нерівномірного розподілу звуку.

Звукові сповіщувачі слід використовувати в поєднанні із світловими в наступних випадках:

- у приміщенні, де люди носять звукоізоляцію;

- у приміщеннях з рівнем шуму понад 95 дБ.

Світлові покажчики "Вихід" потрібно вмикати одночасно з основними приладами робочого освітлення.

Дозволяється використовувати евакуаційні світлові покажчики, автоматиного зразку при отриманні СО імпульсу про початок НС /пожежі/ та (або) аварійному вимкненні робочого освітлення.

Вимоги до світлових покажчиків "Вихід" приймаються відповідно до ДБН В.2.5-28-2006 "Інженерне обладнання будинків і споруд. Природне і штучне освітлення".

Заземлення, електропостачання, вибір та прокладання мереж оповіщення, занулення застосовуються відповідно до вимог систем пожежної сигналізації за ДБН В.2.5-56-2014 "Протипожежний захист".

Вимоги до освітлення по евакуацію приймаються відповідно до ДБН В.2.5-28-2006 "Природне та штучне освітлення".

У режимі «Тривоги» сигнал тривоги повинен бути активним протягом часу, необхідного для евакуації людини з дому, але не менше 15 хвилин.

Вихід з ладу одного з детекторів не повинен викликати вихід з ладу ланки, до якої він підключений.

За даними ПУЕ-2006, згідно першого типу надійності, CO живиться від двох незалежних джерел енергії: основного - від мережі змінного струму та резервного - від акумулятора. У разі виходу централізованого джерела живлення перехід від основного джерела живлення до резервного джерела живлення повинен бути автоматичним. Це ж саме має діяти у звоотньому напрямку при відновленні основного джерела живлення.

Час роботи СО від резервного джерела енергії у режимі очікування має бути не меншим чим двадцять чотири години.

У режимі тривоги час роботи СО від резервного джерела живлення повинен бути не менше 15 хвилин.

Звукові оповіщувачі повинні відповідати вимогам ДСТУ EN 54-3:2003 "Системи пожежної сигналізації. Частина 3. Оповіщувачі пожежні звукові".

Звукові сигнали СО мають забезпечити загальний рівень звуку не менший ніж 75 дБ на відстані близько 3 м від оповіщувача, але в той же ж час не більше 120 дБ у будь-якій іншій точці приміщення. Однак для наочності рівень звуку звукового сигналу СО повинен бути на 15 дБ вище, ніж допустимий рівень звуку постійного шуму в захищеному приміщенні. Такі виміри проводяться на висоті близько 1,5 м від підлоги.

Світлові оповіщувачі у режимі спалахування, мають бути червоного кольору, мати частоту мерегтіння в межах від 0,5 Гц до 5 Гц та бути розташованими у області прямої видимості з постійних робочих місць.

4.2.2 Обов’язки та дії персоналу у разі виникнення надзвичайних ситуацій

Якщо виявлені аварійні знаки, працівники, які помічають ці знаки, повинні:

* + - Як умога швидше повідомити про це службою зв’язку відповідні органи, зазначивши у своєму повідомленні адресу, кількість поверхів, місце виникнення НС, можливість наявності людей, а також свої контактні дані;
    - повідомити керівника підприємства з надзвичайних ситуацій, , пожежну охорону підприємства, адміністрацію;
    - організувати оповіщення персоналу про виникнення НС;
    - вжити відповідних заходів для евакуації персоналу та майна;
    - вжити заходів для усунення наслідків НС використовуючи інуючі поблизу засоби.

Голова призначеного відомства та пожежна служба даного підприємства повинні:

* + - перевірити, чи викликані підрозділи ДСНС;
    - вимкнути струмоприймачі та вентиляцію у разі необхідності;
    - якщо життю людей загрожує небезпека, мають негайно організувати евакуацію та порятунок, а всіх працівників, які не залучені до ліквідації надзвичайних ситуацій, вивести із небезпечної зони;
    - перевірити чи отримують люди попередження про НС;
    - прослідкувати за дотриманням техніки безпеки працівниками, що беруть участь в усуненні НС;
    - організувати зустріч підрозділів Державної пожежної охорони, надати їм допомогу у локалізації та ліквідації НС.

Після прибуття на НС підрозділів ДСНС повинен бути забезпечений безперешкодний доступ їх до місця, де виникла НС.

4.2.3 Пожежна безпека

У робочому приміщенні виконані всі вимоги НАПБ А.01.001-2004 «Правил пожежної безпеки України».

У дослідницькій лабораторії є велика кількість твердих горючих речовин та матеріалів (дерев’яні меблі, вироби з пластику, гума, папір, які вбирають покриття на стіни). Згідно ДСТУ Б.В.1.1-36:2016 «Визначення категорій приміщень та споруд з вибухопожежної та пожежної безпеки», науково-дослідницька лабораторія відноситься до пожежонебезпечних приміщень категорії В (тверді горючі й важкогорючі речовини й матеріали, речовини й матеріали, які при взаємодії з водою, киснем, повітря або один з одним здатні тільки горіти).

Відповідно до класифікації робочої зони, згідно з робочою зоною ДНАОП 0.00-1.32-01 науково-дослідної лабораторії, вона належить до зони класу П-ІІа - небезпека від пожежі, містить тверді горючі речовини і не може перейти у суспендований стан.

Причиною пожежі можуть бути порушення ізоляції дроту, коротке замикання, куріння в приміщенні та порушення правил експлуатації приладу. Тому на місці потрібно вживати заходів щодо запобігання пожежам: використовувати запобіжники в електромережі, користуватися пиловидними роз'єднувальними коробками та розподільними коробками, проводити навчання пожежної безпеки.

Відповідно до ДСТУ 3675-98 та ISO 3941-2017, у дослідницькій лабораторії є два типи вогнегасників: вуглекислий тип "OУ-5" та порошок "OП-2". "OУ-5" розташований на підлозі поруч із виходом на висоті 1,5 м.

У коридорі знаходяться коробки, в середині яких знаходиться пожежний гідрант і рукав, а також вогнегасник типу «ОХП-2».

В обох кінцях коридору є телефони, а над телефонами – відповідні номери телефонів для виклику внутрішніх та міських пожежних відділів.

Тому науково-дослідна лабораторія забезпечує технічні та організаційні рішення щодо пожежної безпеки.

ЗАГАЛЬНІ ВИСНОВКИ

У даній роботі охарактеризовано найбільш поширені види P2P мереж, із забезпеченням глибокого аналізу найбільш релевантної криптовалюти в даний час: біткойн. Характеризуючи P2P криптовалютні мережі, ми можемо зробити висновок, що такі мережі представляють нову парадигму у зв'язку з основними властивостями, що криптовалюта повинна забезпечити: надійність і безпеку інформації що передається.

Для забезпечення надійності VoIP P2P мережі додано сильний надлишковий механізм щодо системної інформації. В результаті кожен вузол мережі зберігає всю необхідну інформацію системи. При такому підході наявність одного вузла в мережі, що містить інформацію, достатньо для того щоб зберегти всю систему для подальшого функціонування.

Для того, щоб підвердити можливість реалізації децентралізованого зв’язку через P2P мережі було розроблено тестовий застосунок за допомогою якого було встановлено зв’язок між двома абонентами. Як результат було встановлено зв'язок між двома пристроями з парою ключів, що були згенеровані за допомогою біткойн мережі. Налаштування з’єднання зайняло 11.5 секунд у разі першого сеансу з’єднання і 1.2 секунди під час всіх наступних. У порівнянні з централізованим VoIP зв’язком, отриманий результат є гіршим всього на 20%. Це є відмвінним результатом, враховуючи, що для встановлення зв'язку додатково проходять наступні процедури, зокрема отримання ключа-пари з блокчейну, запуск симетричного шифрування для цієї пари ключів, відправлення SIP сигналу, розшифрування за допомогою приватного ключа. Всі ці дії відсутні у традиційному VoIP зв’язку. Написане програмне забезпечення було протестовано за допомогою засобів BTC Testnet.

ПЕРЕЛІК ПОСИЛАНЬ

1. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, <https://bitcoin.org/bitcoin.pdf>.
2. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, Princeton, NJ, USA, 2016.
3. J. A. D. Donet and J. Herrera-Joancomartí, “Cryptocurrency P2P networks: a comparison analysis,” J. L. Ferrer and M. Payeras, Eds., pp. 423–428, Menorca, Illes Balears, Spain, 2016.
4. M. Lischke and B. Fabian, “Analyzing the bitcoin network: the first four years,” *Future Internet*, vol. 8, no. 1, p. 7, 2016.
5. J. Herrera-Joancomartí and C. Pérez-Solà, “Privacy in bitcoin transactions: new challenges from blockchain scalability solutions,” in in *Modeling Decisions for Artificial Intelligence*, c. 26–44, Springer, Berlin, Germany, 2016.
6. A. Back, *Hashcash-A Denial of Service Counter-Measure*, 2002.
7. Bitcoin Core, *Bitcoin Core Version 0.12.0 Released*, 2016, <https://bitcoin.org/en/release/v0.12.0>.
8. Bitcoin Core, *Bitcoin Core Version 0.13.0 Released*, 2016, <https://bitcoin.org/en/release/v0.13.0>.
9. Bitnodes, 2016, <https://bitnodes.21.co/>.
10. E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, “A survey and comparison of peer-to-peer overlay network schemes,” *IEEE Communications Surveys and Tutorials*, vol. 7, no. 2, с. 72–93, 2005.
11. P. Kirk, *Gnutella Protocol Development*, 2011.
12. C. Decker і R. Wattenhofer, “Information propagation in the bitcoin network,” in *Proceedings of the IEEE Internation Conference on Peer-to-Peer Computing (P2P)*, Trento, Italy, 2013.
13. E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in *Proceedings of the 24th USENIX Conference on Secrity Symposium (SEC’15)*, pp. 129–144, USENIX Association, Berkeley, CA, USA, 2015,
14. D. S. Wallach, “A survey of peer-to-peer security issues,” in in *Software Security—Theories and Systems*, pp. 42–57, Springer, Berlin, Germany, 2003.
15. S. Bellovin, “Security aspects of Napster and Gnutella,” in *Proceedings of the 2001 Usenix Annual Technical Conference*, Boston, MA, USA, June 2001.
16. D. S. Touceda, J. M. Sierra, A. Izquierdo, and H. Schulzrinne, “Survey of attacks and defenses on P2PSIP communications,” *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 750–783, 2012.
17. Bitcoin Core, *Blockchain Info Website*, <https://blockchain.info/>.
18. M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, “On the instability of bitcoin without the block reward,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS’16)*, pp. 154–167, ACM, Vienna, Austria, 2016.
19. M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking bitcoin: routing attacks on cryptocurrencies,” in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392, San Jose, CA, USA, 2017.
20. K. Suto, H. Nishiyama, N. Kato, T. Nakachi, T. Fujii, and A. Takahara, “THUP: a P2P network robust to churn and DoS attack based on bimodal degree distribution,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 247–256, 2013.
21. W. Wang, Y. Xiong, Q. Zhang, and S. Jamin, “Ripple-stream: safeguarding P2P streaming against DoS attacks,” in *Proceedings of the 2006 IEEE International Conference on Multimedia and Expo*, pp. 1417–1420, Toronto, ON, Canada, July 2006.
22. M. Brinkmeier, G. Schäfer, and T. Strufe, “Optimally DoS resistant P2P topologies for live multimedia streaming,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 6, pp. 831–844, 2009.
23. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach, “Secure routing for structured peer-to-peer overlay networks,” *SIGOPS Operating Systems Review*, vol. 36, pp. 299–314, 2002.
24. A. Singh, M. Castro, P. Druschel, and A. Rowstron, “Defending against eclipse attacks on overlay networks,” in *Proceedings of the 11th Workshop on ACM SIGOPS European Workshop (EW’11)*, ACM, Leuven, Belgium, 2004.
25. N. Borisov and J. Waddle, “Anonymity in structured peer-to-peer networks,” Tech. Rep. UCB/CSD-05–1390, Computer Science Division (EECS), University of California, Oakland, CA, USA, May 2005
26. P. Koshy, D. Koshy, and P. McDaniel, “An analysis of anonymity in bitcoin using P2P network traffic,” in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds., vol. 8437, of Lecture Notes in Computer Science, pp. 469–485, Springer, Berlin, Germany, 2014.
27. D. Ron and A. Shamir, “Quantitative analysis of the full bitcoin transaction graph,” in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed., vol. 7859, of Lecture Notes in Computer Science, pp. 6–24, Springer, Berlin, Germany, 2013.
28. E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun, “Evaluating user privacy in bitcoin,” in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed., vol. 7859, of Lecture Notes in Computer Science, pp. 34–51, Springer, Berlin, Germany, 2013.
29. M. Ober, S. Katzenbeisser, and K. Hamacher, “Structure and anonymity of the bitcoin transaction graph,” *Future Internet*, vol. 5, no. 2, pp. 237–250, 2013.
30. A. Gervais, S. Capkun, G. O. Karame, and D. Gruber, “On the privacy provisions of Bloom filters in lightweight bitcoin clients,” in *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC’14)*, pp. 326–335, ACM, New Orleans, LA, USA, December 2014.
31. D. Cerri, A. Ghioni, S. Paraboschi, and S. Tiraboschi, “ID mapping attacks in P2P networks,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM’05)*, vol. 3, pp. 1785–1790, St. Louis, MO, USA, 2005.
32. E. Sit and R. Morris, “Security considerations for peer-to-peer distributed hash tables,” in *First International Workshop on Peer-to-Peer Systems (IPTPS 2002)*, Cambridge, MA, USA, vol. 2429 of Lecture Notes in Computer Science, pp. 261–269, Springer, Berlin, Germany, 2002.
33. J. J. Douceur, “The sybil attack,” in *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, Cambridge, MA, USA, March 2002.
34. J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis and defenses,” in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN’04)*, pp. 259–268, Berkeley, CA, USA, April 2004.
35. B. N. Levine, C. Shields, and N. B. Margolin, “A survey of solutions to the sybil attack,” Tech. Rep. 2006-052, University of Massachusetts Amherst, Amherst, MA, USA, October 2006.
36. J. Dinger and O. P. Waldhorst, “Decentralized bootstrapping of P2P systems: a practical view,” in *Proceedings of the 8th International IFIP-TC 6 Networking Conference on NETWORKING 2009*, pp. 703–715, Springer, Aachen, Germany, May 2009.
37. C. Cramer, K. Kutzner, and T. Fuhrmann, “Bootstrapping locality-aware P2P networks,” in *Proceedings of the 12th IEEE International Conference on Networks, 2004 (ICON’04)*, vol. 1, pp. 357–361, Singapore, 2004.
38. H. Tran, M. Hitchens, V. Varadharajan, and P. Watters, “A trust based access control framework for P2P file-sharing systems,” in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, p. 302c, Washington, DC, USA, 2005.
39. Y. Zhang, X. Li, J. Huai, and Y. Liu, “Access control in peer-to-peer collaborative systems,” in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS’05)*, pp. 835–840, Columbus, OH, USA, June 2005.
40. A. Ghodsi, L. O. Alima, and S. Haridi, “Symmetric replication for structured peer-to-peer systems,” in *Proceedings of the International Workshops on Databases, Information Systems, and Peer-to-Peer Computing (DBISP2P 2005/2006)*, pp. 74–85, Springer, Trondheim, Norway, August 2006.

1. [↑](#footnote-ref-2)