Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

# АТЕСТАЦІЙНА РОБОТА
# Пояснювальна записка

рівень вищої освіти другий (магістерський)

Платіжні протоколи на основі Lightning Network
(тема)

Виконав: Сапожкова А.М.
(прізвище, ініціали)
студент 2 курсу, групи БІКСм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва освітньої програми)

Керівник проф. Олійников Р.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

# ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Сапожкової Анастасії Максимівни*
(прізвище, ім'я, по батькові)

1. Тема роботи *Платіжні протоколи на основі Lightning Network*
затверджена наказом по університету від "01" листопада 2019 р. № 1649Ст
2. Термін подання студентом роботи (проекту) 23.12.2019
3. Вихідні дані до роботи (проекту) Теоретичні дані про блокчейн
4. Зміст пояснювальної записки (перелік питань, що потрібно розробити)
*1. Актуальний стан та перспективи розвитку сучасних платіжних систем*
*2. Традиційні централізовані платіжні системи*
*3. Перша генерація децентралізованих платіжних систем*
*4. Архітектура Lightning Network*
*5. Подальше вдосконалення Lightning Network*
*6. Методика порівняння властивостей сучасних і перспективних платіжних систем*
*7. Застосування методики порівняння Lightning Network та інших платіжних систем*
8. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*
9. Основна література та джерела. Кравченко П. Блокчейн і децентралізовані системи / П. Кравченко, Б. Скрябін, О. Дубініна // сб. − 2018 – С. 430.

# КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів магістерської атестаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Отримання завдання* | *25.09.19* | |
| 2 | *Пошук літератури* | *25.09.19-28.09.19* | |
| 3 | *Аналіз властивостей схем анонімізації* | *28.09.19-15.10.19* | |
| 4 | *Методика порівняння схем анонімізації* | *15.10.19-11.11.19* | |
| 5 | *Аналіз рівня безпеки платіжних протоколів на основі Lightning Network* | *11.11.19-25.11.19* | |
| 6 | *Обґрунтування вибору мережі з найкращим рівнем безпеки і швидкодії* | *25.11.19-04.12.19* | |
| 7 | *Оформлення пояснювальної записки* | *04.12.19-16.12.19* | |

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ __проф. Олійников Р.В..____
(підпис) (посада, прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка містить: 83 сторінки, 4 рисунки, 16 таблиць, 3 додатки, 72 джерела.

Об’єктом дослідження є децентралізовані системи, методика порівняння сучасних централізованих платіжних систем з перспективними децентралізованими платіжними системами.

Предметом дослідження є технологія масштабування мережі Біткоін через протокол Lightning Network, методика порівняння протокола Lightning Network з іншими централізованими та децентралізованими рішеннями.

Метою даної роботи є отримання результату рівня безпеки платіжних протоколів на основі Lightning Network та отримання результату методики порівняння сучасних і перспективних платіжних систем з протоколом Lightning Network.

Робота містить теоретичні відомості про централізовані та децентралізовані платіжні системи, існуючі способи масштабування децентралізованих мереж, розроблену методику порівняння рівня безпеки сучасних і перспективних платіжних систем, результати порівняння сучасних і перспективних платіжних систем з мережою типу Lightning Network.

ДЕЦЕНТРАЛІЗОВАНА ПЛАТІЖНА СИСТЕМА, БІТКОІН МЕРЕЖА, LIGHTNING NETWORK, PLASMA

# РЕФЕРАТ

Пояснительная записка содержит: 83 страницы, 4 рисунки, 16 таблиц, 3 приложения, 72 источника.

Объектом исследования является децентрализованные системы, методика сравнения современных централизованная платежных систем с перспективными децентрализованными платежными системами.

Предметом исследования является технология масштабирования сети Биткоин используя протокол Lightning Network, методика сравнения протокола Lightning Network с другими централизованными и децентрализованными решениями.

Целью данной работы является получение результата уровня безопасности платежных протоколов на основе Lightning Network и получения результата методики сравнения современных и перспективных платежных систем с протоколом Lightning Network.

Работа содержит теоретические сведения о централизованных и децентрализованных платежных системах, существующих методах масштабирования децентрализованных сетей, разработанную методику сравнения уровня безопасности современных и перспективных платежных систем, результаты сравнения современных и перспективных платежных систем с сетью типа Lightning Network.

ДЕЦЕНТРАЛИЗОВАННАЯ ПЛАТЕЖНАЯ СИСТЕМА, БИТКОИН СЕТЬ, LIGHTNING NETWORK, PLASMA

# ABSTRACT

The explanatory note contains: 83 pages, 4 figures, 16 tables, 3 appendices, 72 sources.

The object of the study is decentralized systems, a methodology for comparing modern centralized payment systems with promising decentralized payment systems.

The subject of the study is Bitcoin network scaling technology that using Lightning Network protocol, a technique for comparing Lightning Network protocol with other centralized and decentralized solutions.

The aim of this work is to obtain the result of the security level of payment protocols based on Lightning Network, to obtain the result of a methodology for comparing modern and promising payment systems with Lightning Network protocol.

The work contains theoretical information about centralized and decentralized payment systems, existing methods for scaling decentralized networks, a developed methodology for comparing the security level of modern and promising payment systems, and results of comparing modern and promising payment systems with a network like Lightning Network.

DECENTRALIZED PAYMENT SYSTEMS, BITCOIN NETWORK, LIGHTNING NETWORK, PLASMA

ЗМІСТ

# СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

| | | |
|---|---|---|
| ІКС | – | Інформаційно-телекомунікаційна система |
| МАІ | – | Метод аналізу ієрархій |
| НОВП | – | Нормалізовані оцінки вектора пріоритету |
| ЦП | – | Цифровий підпис |
| | | |
| BTC | – | Bitcoin |
| CP | – | Core protocol |
| LN | – | Lightning Network |
| PoW | – | Proof-of-Work |
| PoS | – | Proof-of-Stake |
| P2P | – | Peer-to-Peer |
| SWIFT | – | Society for Worldwide Interbank Financial Telecommunications |

# ВСТУП

Останні кілька років технологія блокчейн все більше застосовується сучасним суспільством [1]. Блокчейн – розподілений електронний реєстр, в якій реєструється кожна транзакція, яка відбувається в системі [2]. Найбільш широка область застосування блокчейна – децентралізовані платіжні системи [3].

Як було вже зазначено, досить часто користувачами даної технології є цифрові валюти, а найвідоміша з них – Біткоін [3]. Ринок цифрових валют досить швидко розвивається, так, максимальна капіталізація ринку криптовалют складає 190 млрд. доларів [4], а курс Біткоіна у лістопаді перетнув відмітку 7000 доларів [4]. Проте це не єдине ефективне застосування цієї технології, так, ринок стартапів на базі використання технології блокчейн, за оцінками експертів, на початку 2019 року блокчейн-проекти залучили $3,38 млрд [5]. У минулому році інвестиції в цю сферу склали $12,86 млрд [5].

Варто звернути увагу, що використання технології блокчейн викликає зацікавлення і в Україні. Так стало відомо, що Україна уклала угоду з міжнародною технологічною компанією Bitfury Group про переведення всіх електронних державних даних на блокчейн [6].

Таким чином, технологія блокчейн є певною мірою революційною та може бути використана в різних сферах людської діяльності. Зокрема, мова йде про такі реалізації як криптовалюти, різного роду реєстри корпоративного або ж державного значення [1]. Але у криптовалют, зокрема у Біткойна, є великий недостаток – низька пропускна здатність. Через це запропоновується велика кількість технологій, що намагаються виправити цю проблему. Найперспективнішою з таких є технологія Lightning Network [7].

Метою даної магістерської роботи є аналіз безпеки та ефективності сучасних платіжних систем на прикладі Lightning Network, а також порівняння цих систем з сучасними та перспективними платіжними системами.

# 1 АКТУАЛЬНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ СУЧАСНИХ ПЛАТІЖНИХ СИСТЕМ

## 1.1 Огляд області застосування

У сучасному світі в зв'язку з динамічним розвитком технологій відбуваються значні зміни. Вони торкнулися практично всіх сфер життя, в тому числі і сферу грошових відносин. Питання подальшого розвитку системи індустрії платіжних систем активно обговорюється науковим співтовариством. Серед інноваційних технологій найчастіше називають технологію блокчейн, або децентралізовані платіжні системи [8], незаперечною перевагою яких є безпека даних. У більшості випадків впровадження децентралізованих технологій в сферу платежів трактується як позитивний варіант розвитку подій [8]. Аргументація експертів, які висловлюються за розвиток даного процесу, зводиться, перш за все, до можливості мінімізації ризиків, які притаманні сучасній системі платежів [2]. Властивості анонімності та захищеності від підробок призводять експертів до розуміння високої значимості криптовалют, а отже і до децентралізованих платіжних систем на основі яких вони працюють. Така позиція в ряді країн призводить до легалізації криптовалют як платіжний засіб (як, наприклад, в Японії [9], частково в Хорватії [10]). Однак, високі значні коливання курсу роблять криптовалюти занадто ризиковим активом, здатним вивести з рівноваги національну систему платежів. Наявність такої потенційної небезпеки призводить до повної заборони криптовалют в інших країнах, наприклад, у Китаї [11].

На сьогоднішній день ми маємо статті про технологію блокчейн від таких видань як The Wall Street Journal, щоденна газета, одне з найбільших і найвпливовіших американських видань [12]. А основні світові аудиторські компанії активно працюють у галузі розподіленого реєстру [13][14]. З огляду на величезне поширення індустрії блокчейн в світі, стало питання про

масштабування і поліпшення цієї системи [7]. Актуальним питанням залишаються способи збільшення швидкості, масштабування і повної безпеки з боку децентралізованих платіжних систем [7].

У 2015 році проект Біткоін, найпопулярніша у світі криптовалюта, зіткнувся з проблемою, яка полягала в масштабуванні [7]. Мережа не могла обробляти більшу кількість транзакцій щосекунди. Тож альтернативні рішення спрямовані на вирішення цієї проблеми, а саме Біткоін форки [15]. На рисунку 1.1 зображено біткоін форки.

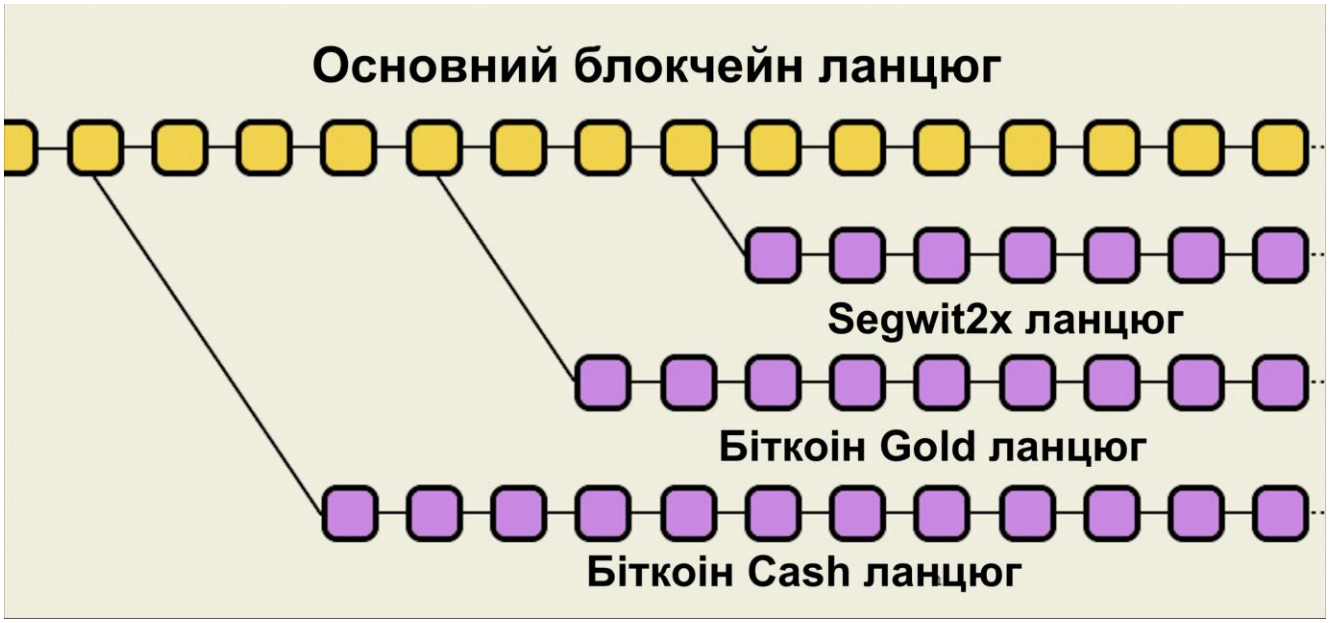


Рисунок 1.1 – Біткоін форкі

Таким чином, проект Lightning Network являє собою розробку, орієнтовану на підвищення пропускних показників біткоін-мережі при досягненні частоти операцій, яку можна порівняти з показниками мережі централізованої системи Visa [16].

## 1.2 Властивості сучасних платіжних систем

Ключова базова характеристика будь-якої сучасної платіжної системи, а саме децентралізованої системи – технологія узгодження загальної бази даних між сторонами, які не довіряють один одному [2].

Розглянемо деякі властивості децентралізованих платіжних систем [2,17]:

- Проведення платежів здійснюється на підставі прозорості історії транзакцій між учасниками. Наприклад, користувач системи може здійснювати транзакції – ініціювати і приймати платежі в глобальному масштабі і без обмежень. Це дозволяє децентралізованим платіжним системам виконувати в тому числі і функцію міжнародних переказів.
- Децентралізовані платіжні системи мають просту функціональність в використанні. Простота таких систем полягає в тому, що користувач може створити платіжний рахунок без реєстрації, при наявності лише комп'ютера або смартфона (на відміну від відкриття традиційного банківського рахунку, де потрібно оформлення паперів і особиста присутність у відділенні).

Однак система також має і недолік як складність обліку операцій та підвищення ризиків при збільшенні числа учасників системи [8].

## 1.3 Принципи побудови децентралізованих систем

Розглянемо способи взаємодії користувачів з системою. На рис. 1.6 зображені три підходи [14], що принципово відрізняються один від одного за своїм устроєм.

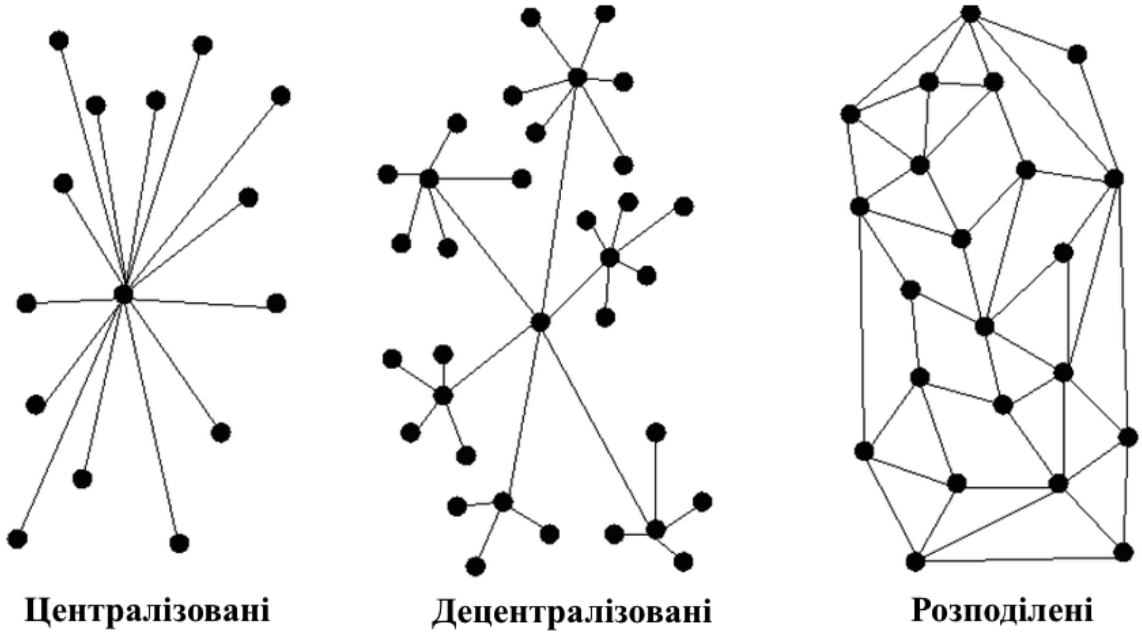


Рис. 1.1 – Види систем в залежності від способу взаємодії користувачів між собою

До централізованих систем можна віднести популярні соціальні мережі [18]. Порушення роботи бази даних в таких системах торкнеться всіх користувачів. До децентралізованих систем – банківську систему в цілому, бо її утворюють безліч локальних центрів, і несправності, наприклад, у банку Аргентини, не приведуть до затримок платежів у банках Німеччини [2]. До розподілених систем можна віднести mesh-мережі та систему зв'язку на основі кишенькових рацій, де система підтримується тільки пристроями користувачів, а відключення одного з пристроїв не вплине на взаємодію інших користувачів. Централізована платіжна система включає до себе базу даних, механізми її оновлення та керуючий центр, відповідальний за підтримку її роботи [19]. Керуючий центр не завжди може забезпечити достатній рівень безпеки обробки даних і надійності прийняття рішень.

Децентралізована облікова система – це окремий випадок облікової системи, принциповою відмінністю якої є використання механізму досягнення консенсусу між декількома незалежними сторонами [19]. Кожна сторона будує власну базу даних, де алгоритм досягнення консенсусу гарантує, що кожна побудована база даних ідентична іншим копіям. В узгодженні кінцевого стану

всіх копій беруть участь безліч незалежних сторін (валідаторів), а не одна уповноважена сторона (центр) [19].

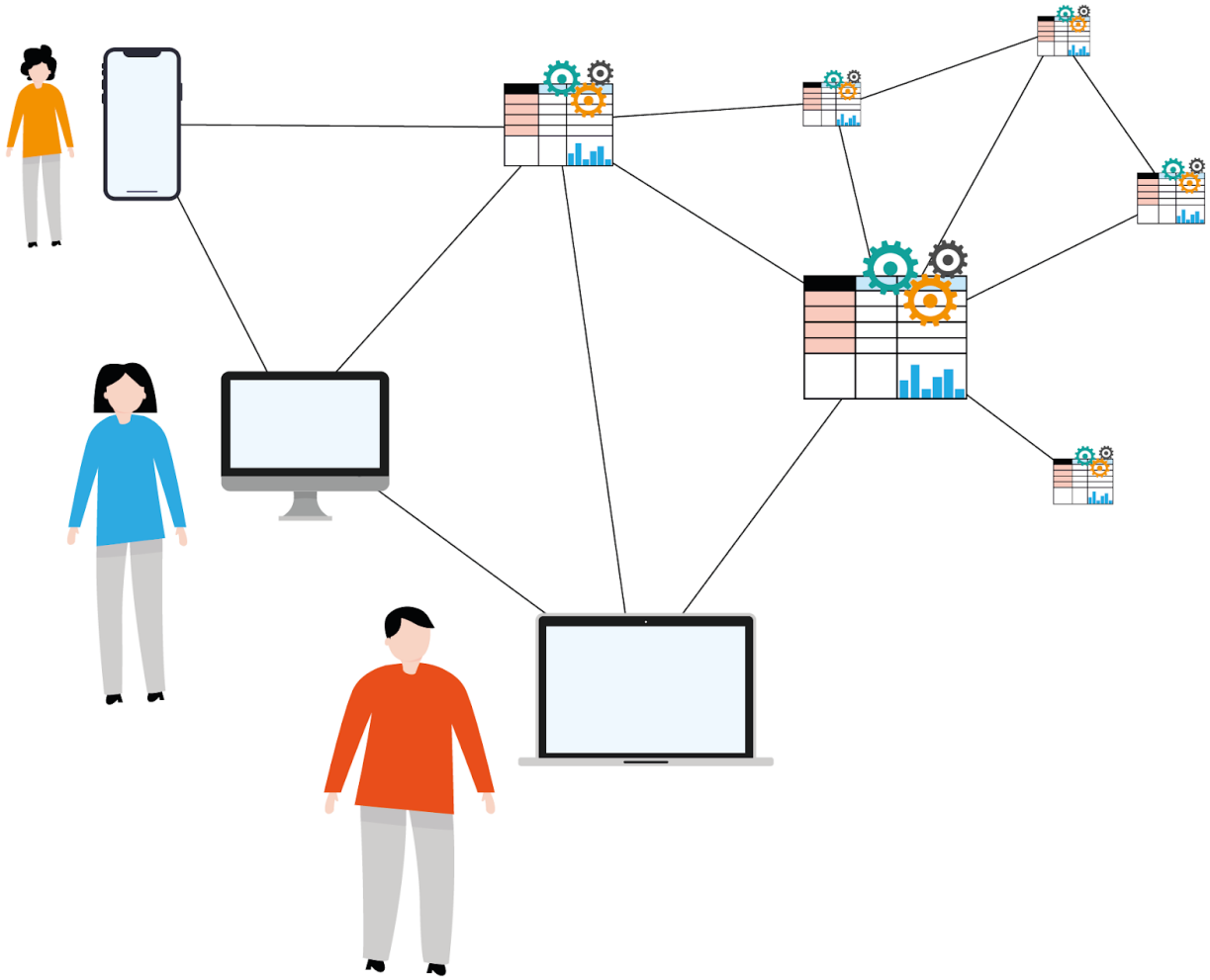

Рис. 1.2 – Архітектура децентралізованої облікової системи

## 1.4 Переваги децентралізованих систем

Децентралізована система передбачає, що учасники обмінюються інформацією безпосередньо, використовуючи p2p-протоколи та самостійно зберігають дані, що потрібні для них самих [19]. Для цього вони запускають спеціальне програмне забезпечення, яке підтримує необхідний p2p-протокол конкретної децентралізованої системи. У децентралізованих системах обліку фінансів, таких як криптовалюти, передбачається, що всі учасники зберігають

копії однієї і тієї ж бази даних й оновлюють їх, використовуючи алгоритми досягнення консенсусу.

Основні переваги децентралізованих систем [2,19]:

1) відмовостійкість;
2) незалежність від одноосібного контролю;
3) відсутня необхідність у довірі третій стороні;
4) вільне використання;
5) незмінність кінцевого стану бази даних;
6) гарантується додавання записів;
7) формальність протоколів

Відмовостійкість є властивістю системи, за якої система зберігає свою працездатність навіть після відмови одного або декількох її компонентів. У традиційній клієнт-серверної архітектурі основні зусилля спрямовуються на захист центрального серверу. Якщо атакуюча сторона заволодіє сервером та отримає доступ до бази даних, то вона може переписати історію на власний розсуд. Атакуючий децентралізованої системи оперуючи одним сервером отримує доступ до бази даних, але він не зможе завдати критичної шкоди системі. Принципи децентралізації багато років успішно застосовуються при проектуванні та побудові авіаційної та космічної техніки, а також при роботі високоточних обчислювальних систем. Наприклад, при роботі в нестабільних умовах дуже важливо, щоб основні системи (навігації, зв'язку, управління тощо) працювали надійно. У таких випадках проектувальники систем вдаються до використання надмірності.

Незалежність від одноосібного контролю є ще однією відмінною рисою децентралізованої системи [20]. За наявності великої кількості незалежних учасників ніхто, навіть дуже зацікавлена сторона, не може вплинути на прийняття рішення на свою користь.

Третя перевага полягає у відсутності необхідності довіряти системі щодо зберігання й обробки деяких даних або виконання деяких процесів [19]. Зазвичай вона досягається завдяки великій кількості незалежних учасників, що досягають згоди у прийнятті спільного рішення. З ростом кількості незалежних (незнайомих) учасників сильно знижується ймовірність їхньої змови.

Властивість “вільне використання” значить, що система доступна для роботи без будь-яких додаткових дозволів (відсутня ієрархія зумовлених ролей) [19]. Будь-який бажаючий може зчитувати та записувати дані, здійснювати їх аудит, а також брати участь у прийнятті спільного рішення, тобто у процесі управління. Однак в низці випадків, коли мова йде про рішення, що повинні прийматися експертами, загальнодоступна участь і навіть відкритість бази даних облікової системи вже не є перевагами. Також властивість permissionless буде недоліком у тому випадку, коли валідатори будуть обробляти конфіденційні дані.

Властивість “незмінність кінцевого стану бази даних” значить, що система зберігає незмінність кінцевого стану своєї базі даних навіть якщо вона повністю припинила свою роботу на деякий час [19].

Шоста властивість гарантує, що якщо всі чесні учасники бажають додати запис до спільної базі даних, то у результаті він буде до неї доданий.

Під формальністю протоколів мається на увазі, що всі учасники прийдуть до єдиного рішення якщо кожен з них дотримується встановленому алгоритму.

## 1.5 Огляд застосування децентралізованих систем

Використання децентралізованих систем можливо спричинить за собою зміну фінансової системи. Кілька років тому деякі фахівці в банківській сфері навіть не уявляли, що можливо створити децентралізовану фінансову систему. Зараз же ця система може задовольнити потреби банківських переказів, де особливо цінні властивості: простота, швидкість і прозорість. Прикладами сфер, де ці системи особливо добре зарекомендували себе, є міжнародні платежі і

перекази. Втім, як технологія узгодження загальної бази даних між сторонами, які не довіряють один одному, децентралізовані платіжні системи ще не повністю реалізували свій потенціал. У перспективі вони можуть застосовуватися фінансовими інститутами для підвищення ефективності взаєморозрахунків.

За останні кілька років зацікавлені в технології банки об'єдналися для її тестування і проведення з її допомогою взаєморозрахунків. Один із прикладів – консорціум R3 [21], який тестує можливості децентралізованих систем для фінансових операцій.

Технологія також знайшла застосування в платформі NASDAQ Linq [22], яка використовується для торгівлі акціями шести приватних компаній.

У перспективі децентралізовані платіжні системи доповнять світову фінансову систему, а не повністю замінять її. Ймовірно, принципи децентралізації зможуть застосовуватися для всіх без винятку облікових систем.

Цілком можливо, що національні банки разом з приватними банками будуть здійснювати спроби побудувати національні системи обліку електронних грошей, які могли б обслуговувати потреби населення в масштабах країн.

Такі платіжні системи дуже нагадують криптовалюти, тому що використовують подібні електронні гаманці та цифрові ключі, але насправді не є криптовалютами.

У 2014 році обговорювались перспективи того, що децентралізовані платіжні системи будуть використовувати єдину валюту – біткоін, яка стане світовою валютою і буде використовуватися в повсякденних транзакціях [8]. Однак цього не сталося.

Очевидно, виникають питання регуляції подібних систем. Наприклад, вже сьогодні регулятори американського і китайського фінансових ринків приймають дії щодо децентралізованих платіжних систем і криптовалют [23]. Розуміючи, що в ці ринки залучається все більше роздрібних споживачів, державні органи прагнуть регулювати дії учасників ринку і створити єдині стандарти роботи, щоб обмежити ризики для населення. За словами регуляторів, для того щоб

децентралізовані платіжні системи стали використовувати масово, потрібно повністю визначити їх юридичний статус (поки що немає єдиної думки щодо правової природи криптовалют), умови ліцензування учасників ринку, а також систему оподаткування [8]. На сьогоднішній день ці питання викликають багато суперечок на національних і міжнародних рівнях.

## 1.6 Постановка задач досліджень

Визначивши актуальність та важливість для сучасного суспільства децентралізованих платіжних систем, метою магістерської роботи стали способи досягнення швидкодії при проведенні транзакцій в децентралізованій мережі, аналіз платіжних систем, порівняння характеристик безпеки та швидкодії сучасних і перспективних платіжних систем.

У розділі «Традиційні централізовані платіжні системи» виконано аналіз функціональності децентралізованих систем, розділ «Перша генерація децентралізованих платіжних систем» присвячено анализу та візначенню переваг децентралізованих платіжних систем. У розділі «Архітектура Lightning Network» проведено аналіз властивостей мережі. У розділі «Подальше вдосконалення Lightning Network» запропоновано до розгляду подібну до Lightning Network мережу. У шостому розділі «Методика порівняння властивостей сучасних і перспективних платіжних систем» розроблено методіку порівняння розглядаємих мереж, в сьомому розділі «Застосування методики порівняння Lightning Network та інших платіжних систем» застосовано методики порівняння сучасних і перспективних платіжних систем з мережою Lightning Network.

# 2 ТРАДИЦІЙНІ ЦЕНТРАЛІЗОВАНІ ПЛАТІЖНІ СИСТЕМИ

## 2.1 Платіжна система PayPal

PayPal — міжнародна електронна платіжна система. Це найпоширеніший у світі спосіб розрахунків в Інтернеті [24].

Платіжна система PayPal була створена в США у 1998 році [24], саме за кордоном переклади через PayPal мають статус найбільш швидких, вигідних і популярних. Десятки мільйонів людей щодня користуються системою, через яку проводять сотні мільярдів доларів [25]. В Україні система PayPal все ще не працює в повному режимі. Україна дозволяє витрачати кошти на товари і послуги в Інтернеті, але не дозволяє знімати готівку, виводити їх на інші рахунки або приймати перекази для себе [26].

Використання системи PayPal несе безліч переваг, серед яких варто назвати наступні [24]:

- миттєві перекази в будь-яку країну світу без традиційних банківських перевірок;
- високий рівень контролю користувачів з боку PayPal, що значно в рази зменшує відсоток шахраїв при здійсненні онлайн-покупок, в порівнянні з традиційними методами;
- проста реєстрація, яка прив'язана до адреси електронної пошти;
- забезпечення збереження особистих даних користувача. PayPal не надсилає відомості продавцеві про банківські рахунки і кредитні картки, тому що розрахунки між учасниками здійснюються всередині системи;
- можливості PayPal з купівлі в іноземних інтернет-магазинах;
- безкоштовне обслуговування аккаунта, відсутність внутрішньої комісії за перекази;

- швидка доступність коштів в будь-який час і в будь-яке місце з будь-якого пристрою (смартфона, планшета, комп'ютера).

Недоліки системи PayPal [24][25]:

- У кожної країни свої правила для комісії при переведенні між рахунками;
- для здійснення фінансових операцій PayPal передає дані клієнтів третім особам. Сервера, де зберігається вся інформація про користувачів, розташовуються на території США, і при реєстрації кожен дає згоду на передачу своєї персональної інформації за кордон;
- існує мінімальне і максимальне обмеження на виведення грошей;
- система вимагає прив'язки до внутрішнього рахунком банківської карти для верифікації особистості власника. Для виведення коштів додатково потрібно надсилати паспортні дані.

Платіжна система PayPal – популярний інструмент для здійснення покупок в інтернеті і переказу грошових коштів. Але ця система має низку технічних недоліків та обмежень, як, наприклад, комісії між рахунками, втручання третьої стороні, час переказу, та інше які істотно впливають на зручність використання платежі.

## 2.2 Платіжна система SWIFT

SWIFT – міжнародна міжбанківська система передачі інформації та здійснення платежів [27].

Заснована система у 1973 році за участю 239 банків з 15 країн світу [27]. В даний момент головний офіс спільноти також розташований в Брюсселі. Кожному банку в цьому співтоваристві присвоюється свій унікальний код, який називається SWIFT-BIC або SWIFT-ID, а кожній юридичній або фізичній особі, яка бере участь в платежах, присвоюється унікальний код, іменований IBAN. Щоб

перевести гроші в цій платіжній системі, досить знати всього 2 реквізиту: SWIFT код банку одержувача і IBAN самого адресата.

З моменту заснування SWIFT став найпопулярнішою міжнародною платіжною системою. Щодня в співтоваристві SWIFT здійснюється кілька мільйонів платежів, а щорічно через цю систему проходить понад 2,5 млрд. транзакцій [28]. Мережа SWIFT включає в себе більше 10 000 банків і фінансових установ в більш ніж 200 країнах.

Перерахуємо переваги платіжної системи SWIFT в точки зору традиційних централізованих систем [28]:

- відсутність обмежень по сумі платежу;
- надійність в збереженні персональної інформації клієнта, яка забезпечується центральним органом;
- популярність у світі, що дозволяє здійснювати платежі майже в будь-яку країну;
- гарантії своєчасної доставки перекладу. У разі порушення терміну доставки, SWIFT покриває виникли збитки клієнтів [29].

Недоліки платіжної системи SWIFT:

- необхідність надання в банк великого пакета документів;
- необхідність перебування у банку під час реєстрації;
- необхідність комунікації з третьою сторону;
- моніторинг платежів з боку державних структур;
- платіж може йти від 3 до 7 днів;
- SWIFT не надсилає гроші, він відправляє повідомлення між банками. Через це для перекладу фактичних коштів необхідно використовувати інші системи, що вимагають більшого втручання людини, а це, в свою чергу, уповільнює перекази SWIFT;
- збори, пов'язані з здійсненням переказів SWIFT: кожен з банків-посередників має право на комісію, забраних із суми переказу;
- обмеження вибір валют, якими оперує система [29].

Платежі в системі SWIFT швидкі та зручні для способу оплати товарів і послуг за кордоном. Багато банків по всьому світу використовую SWIFT, в тому числі українські банки [29]. Але ця система має ряд технічних недоліків та обмежень, як, наприклад, комісії між рахунками, втручання третьої стороні, час переказу, та інше які істотно впливають на зручність використання платежі.

## 2.3 Основні властивості централізованих платіжних систем

В основі централізованих систем закладено централізоване управління процесами. У деяких випадках подібний підхід може забезпечити більшу ефективність функціонування системи. Яскравим прикладом можна навести можливість простого та швидкого оновлення правил протоколу. Наприклад, якщо у централізованій обліковій системі виявляється вразливість, розробники швидко з'ясовують причину проблеми та випускають відповідне оновлення. В результаті всі користувачі, що хочуть надалі взаємодіяти з обліковою системою, змушені оновити своє програмне забезпечення [19].

Властивості, притаманні централізованим платіжним системам:

- база даних зберігається на головному сервері (хмарі чи кластері);
- система керується централізовано;
- користувачі відправляють запити до системи для проведення транзакцій.

Однак такі системи мають певні ризики. Одним з них є можливість повної відмови системи. При виникненні такої ситуації, ключові компоненти системи можуть відмовити і тим самим призвести до повної втрати її функціональності. Наявність систем резервування допомогає в такому випадку, однак і такий підхід не завжди може гарантувати безперебійну роботу сервісу [19].

Традиційні фінансові інструменти працюють по принципу, згідно з яким внутрішню облікову систему необхідно захищати з допомогою грубої сили. Мається на увазі, що центральний сервер, на якому знаходиться база даних,

захищений тільки вздовж периметру. Якщо подолати зовнішній захист, то сама база даних залишиться незахищеною. В цьому і криються деякі недоліки. З однієї сторони, якщо атакующий подолає ций захист, то він може отримати повний доступ до даних та можливість їх модифікації. З іншого боку, такий підхід не дозволяє користувачам особисто перевіряти дані. Користувач може тільки відправити запит до серверу, який в свою чергу обробить цей запит і згодом надішле відповідь. Для звичайного користувача внутрішня структура такої системи обліку не прозора та відсутні будь-які гарантії правильності її роботи, однак у випадку збою чи відмови в обслуговуванні є людина, яка несе за це відповідальність. Крім того, централізована облікова система має єдину точку відмови.

Якщо необхідно провести перевірку облікової системи, то треба робити це вручну чи використовувати інструменти автоматизації. До 2009 року так працювали всі облікові системи.

Потенційна можливість цензурування дій користувача у системі також є одним з недоліків. Централізована система передбачає повну і беззастережну довіру користувача до власника і керівництва організації. Такий підхід містить у собі загрозу, що правила протоколу взаємодії в системі можуть бути порушені, якщо власнику системи це буде вигідно.

# 3 ПЕРША ГЕНЕРАЦІЯ ДЕЦЕНТРАЛІЗОВАНИХ ПЛАТІЖНИХ СИСТЕМ

Підхід до зберігання даних у зв'язаному вигляді не є чимось новим, однак блокчейн став новим способом організації бази даних цілої облікової системи. І це сталося не в результаті теоретичних наукових розробок, а при спробі відповісти на загрози учасників анонімної розподіленої мережі. Існуючі до цього облікові системи часто спиралися на не технологічні способи захисту інформації та вирішення конфліктів – це було можливо в неанонімному середовищі, де існують вже визначені сторони, призначені регулювати проблемні ситуації, такі як суди, поліція тощо. Сатоши Накамото, автор Біткоін, як деякі інші інженери, робив спроби створення системи обліку фінансів, в якій би всі стали рівноправними і могли зберігати приватність [30]. У цьому випадку вже неможливо звернутися за допомогою до суду.

Анонімна розподілена мережа, до того ж стійка до цензури, вимагала зовсім інших підходів до вирішення проблем – у звичайному світі багато небажаних речей просто не відбуваються, тому що існує ризик розкриття злочину, подальшого розголосу, втрати репутації і навіть тюремного ув'язнення. Тому захист від багатьох атак просто відсутній – суспільство, в якому закони працюють ефективно, їх просто не вимагає. Наприклад, в США при втраті банківської карти і PIN-коду до неї банк все одно поверне вам вкрадені гроші – так як усе застраховано [31]. І навіть якщо близько 4% прибутку банків витрачається на страхування, це все одно виявляється дешевше, ніж безпосередній захист від усіх можливих сценаріїв шахрайства. У випадку Біткоін багато конфліктів нікому вирішувати. Тому він спроектований таким чином, щоб уникати появі конфліктів, а не створювати механізми їх розглядів постфактум. У Біткоін неможливо відправити неіснуючі монети, але є загроза проведення успішної атаки double spending [32].

Блокчейн є ланцюжком блоків даних, які створюються і зберігаються на комп'ютерах учасників ланцюжка. Всі учасники мережі діляться на дві категорії:

звичайні користувачі, які створюють нові записи, і майнери, які створюють блоки. Майнери перевіряють записи, які створюють звичайні користувачі, формують з них блоки, а потім розсилають ці блоки по мережі. Звичайні користувачі отримують ці блоки і зберігають їх у себе в комп'ютері. Учасники блокчейн-мережі мають доступ до інших комп'ютерів мережі, завдяки чому можна обмінюватися даними. Кожен користувач перевіряє коректність нових даних. Якщо вони достовірні, він зберігає їх і передає далі по мережі [32].

Технологія блокчейн може успішно використовуватися банками для проведення внутрішніх взаєморозрахунків і здійснення міжбанківських операцій, а також при проведенні мікроплатежів між фізичними особами. При цьому блокчейн здатен значно спростити відстеження підозрілих транзакцій і в цілому підвищити прозорість угод. По суті це технологія розподіленого підтвердження транзакцій, яка представляє собою розподілену базу даних. При цьому перевіркою достовірності транзакцій займаються самі учасники, вони ж підтверджують їх справжність та формують блоки записів.

Такий підхід важливий для платіжної системи перш за все тим, що відсутня необхідність у посередниках, що здійснюють обробку транзакцій і, як наслідок, підвищується швидкість обробки транзакцій і знижується вартість для кінцевого споживача.

За деякими оцінками [28], використання блокчейн дозволить банкам заощаджувати близько 20 мільярдів доларів за рахунок відмови від послуг посередників при здійсненні транзакцій. Блокчейн може стати реальною альтернативою системі SWIFT, яка на даний момент є не дуже гнучкою і досить дорогою [28].

## 3.1 Принцип роботи Біткоін

Біткоін – це протокол, що реалізує незалежну валюту та платіжну систему [2]. Якщо розглядати інші електронні гроші чи платіжні системи, наприклад,

PayPal, SWIFT – це платіжні системи, які оперують вже існуючими валютами: долар, євро, фунт тощо. Біткоін є як окремої валютою, так і платіжною системою, яка керує цією валютою, це незалежна платіжна система, тобто немає організації, яка б контролювала її роботу [30].

Розробник Біткоін, Сатоші Накамото, спробував відтворити всі властивості золота, такі як: обмежена кількість, складність видобутку, незалежність від єдиної організації, неможливість його штучного відтворення [30]. Біткоін відтворює всі перераховані властивості у цифровому вигляді, тому багато людей вважають це великим проривом у комп'ютерних науках.

Використовуючи Біткоін, можна відправити платіж кому завгодно і куди завгодно. Для цього потрібен доступ до мережі, цифровий гаманець та адреса отримувача. Обмеження, характерні для звичайного міжнародного переказу відсутні. Ніяких додаткових дозволів для здійснення платежу не потребується. Тому Біткоін зацікавив людей, які підтримували сводобу системи без цензорування.

Як тільки ціна біткоіну стала зростати, він почав привертати увагу підприємців і спекулянтів, що намагалися заробити на коливанні курсу. Для звичайної людини інтерес представляють відсутність необхідності реєструватися і можливість здійснювати платежі без залучення третіх сторін. Якщо розглядати такі платіжні системи, як PayPal або SWIFT, то вони керуються конкретними компаніями, де можуть проводитись обшуки, що призводить до конфіскації серверів та заблокування рахунків [33]. У разі Біткоін не існує компанії Біткоін, яка здійснює облік монет або підтверджує транзакції. Це означає, що транзакції не схильні до цензури.

Ніхто не знає хто вперше запропонував дану технологію і назвав її Біткоін. Офіційно відомо, що це був хтось під псевдонімом Сатоші Накамото [30]. Можливо, цей хтось – одна людина, але є припущення, що за псевдонімом може стояти і група людей. Сатоші зареєстрував домен bitcoin.org в 2008 році, випустив

першу статтю, опублікував початкову версію вихідного коду протоколу [30]. До 2011 року від псевдоніма Сатоші Накамото на відповідних форумах і в email-розсилках з'являлися повідомлення. Пізніше він написав, що вирішив займатися іншими справами та припинив публічні комунікації. Проте ідея створення Біткоін виникла у Сатоші Накамото після публікації статті «Bitcoin: A Peer-to-Peer Electronic Cash System» [30], де він згадав два інших ключових проекта.

Це були попередні спроби створити незалежну цифрову валюту: HashCash доктора Адама Бека (Adam Back) [34] і B-Money інженера Вей Дая (Wei Dai) [35]. У першому з'явився підхід proof-of-work [36], спочатку створений для боротьби зі спамом в електронних листах, а в іншому – модель мережі для розподіленого зберігання даних про транзакції та використання криптографічних підписів для відправки грошей. Таким чином, Сатоші задіяв вже існуючі концепції для реалізації Біткоін, зумівши вирішити проблеми, що залишилися на ранніх етапах, чого не вдалося зробити їх творцям.

Перша публікація документації про Біткоін “Bitcoin White Paper” відбулась – 31 жовтня 2008 року. Перший вихідний код був опублікований в 3 січня 2009 році [37], тоді ж був сформований і перший блок – в Біткоін з'явилися перші 50 монет. Тому можна вважати цю дату запуском цифрової валюти. У лютому 2010 року відбувся перший обмін біткоіну на гроші.

На момент 2019 року по всьому світу Біткоін користуються мільйони людей, а сотні тисяч компаній приймають його в якості оплати [38]. Деякі країни, зокрема Японія, визнали його законним засобом платежу [9].

## 3.2 Блок транзакцій

Поняття «блокчейн» в контексті Біткоін – це база даних, яка містить транзакції, і вона загальна для всіх вузлів, залучених до системи Біткоін. Особливість її полягає в тому, що кожен наступний блок підтверджує цілісність

попереднього блоку, який в свою чергу підтверджує цілісність попереднього по відношенню до нього блоку і таким чином до genesis block [19]. Забезпечується односторонній зв'язок всіх блоків і підтверджується факт того, що блок був створений після появи попереднього. Така організація даних гарантує, що кожен блок був створений при наявності визнання всієї історії транзакцій за весь час існування Біткоін. Кожен блок складається з двох частин: заголовка блоку та включених транзакцій.

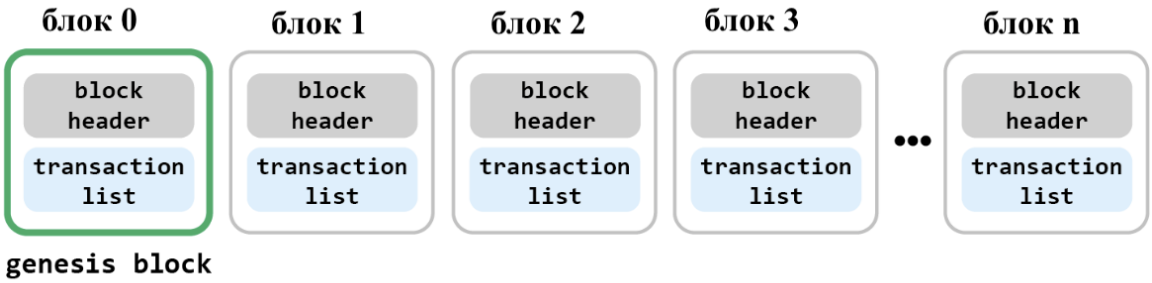


Рис. 3.1 – Структура ланцюга блоків

Для того, щоб транзакція вважалась достовірною («підтвердженою»), її формат і підписи повинні перевірити майнери і потім групу транзакцій записати в спеціальну структуру - блок [19]. Інформацію в блоках можна швидко перевірити ще раз. Кожен блок завжди містить інформацію про попередній блок. Всі блоки можна побудувати в один ланцюжок, яка містить інформацію про всіх скоєних коли-небудь операціях в цій базі. Найперший блок в ланцюжку – Genesis block, за яким учасники можуть створювати наступні блоки. Особливість genesis block полягає в тому, що він не розповсюджується при синхронізації вузлів, так як він закладений до програмного забезпечення вузла мережі і має порядковий номер 0 [19].

Там, де необхідно провести верифікацію, що здійснюється малоресурсным клієнтом, децентралізованої облікової системи, вузлу досить завантажити тільки заголовки блоків. Це дозволяє перевірити час створення блоку, геш-значення попереднього блоку, зміну параметра складності з часом. Однак для більш

серйозної перевірки, наприклад перевірки на double-spending, вузлу знадобиться і тіло блоку з транзакціями, тобто повний блок [2].

Блок складається з заголовка і списку транзакцій. У системі біткойнів першої транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок. Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоці використовується деревоподібне хешування, аналогічне формування хеш-суми для файлу в протоколі BitTorrent. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію з попереднім станом даних (в системі біткойнів, наприклад, дається посилання на ту транзакцію, по якій були отримані витрачаються біткойни). Комісійні транзакції можуть містити в атрибуті будь яку інформацію (для них це поле зветься англ. Coinbase parameter), оскільки у них немає батьківських транзакцій.

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка одно або нижче певного числа, величина якого періодично коригується. Так як результат хешування (функції SHA-256) є незворотним, немає алгоритму отримання бажаного результату, крім випадкового перебору. Якщо хеш не задовольняє умові, то в заголовку змінюється параметр nonce і хеш перераховується. Зазвичай потрібна велика кількість перерахунків. Коли варіант знайдений, вузол розсилає отриманий блок іншим підключеним вузлів, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш [2].

## 3.3 Структура блоку

В таблиці 3.1 надана структура блоку, що передається мережею Біткоін. Відповідний порядок даних вказаний у таблиці.

Таблиця 3.1 – Структура блоку в Біткоін

| Поле | Значення | Розмір (у байтах) |
|---|---|---|
| MagicNo | 0xD9B4BEF9 | 4 |
| BlockSize | значення кількості байтів у блоці, включаючи всі дані транзакцій | 4 |
| BlockHeader | складається з шести полів | 80 |
| TxCounter | кількість транзакцій у блоці | 1-9 |
| Transactions | Перелік транзакцій | N/A |

У блоці передбачається декілька полів, перше з них – *MagicNo – є* спеціальним константним числом. Для протоколу Біткоін воно завжди має саме таке значення і займає 4 байта. Використовується воно для ідентифікації потоку даних. Припустимо, є канал передачі, де проходять дані від різних протоколів. Щоб ідентифікувати, що в певний проміжок часу почався блок Біткоін, можна використовувати пошук по цьому значенню. Відповідно, для інших протоколів значення буде іншим [2].

Після нього йде поле *blockSize* (розмір блоку), яке займає також 4 байта і містить значення кількості байтів у цьому блоці, включаючи всі дані транзакцій. За ним йде заголовок блоку, він складається з шести полів і завжди дорівнює 80 байтам [2].

Нижче розташовується лічильник транзакцій. Кількість транзакцій у блоці може бути настільки великою, що лічильник може мати розмір від 1 до 9 байт. Після йдуть дані самих транзакцій, їх розмір не визначений. На практиці блок може мати розмір від 100 байт і до 1 MB: набір транзакцій теж може бути різним за кількістю [2].

Ключовою складовою блоку є його заголовок (*block header)*. Тема блоку містить 6 полів. Їх перевіряють всі вузли мережі, навіть полегшені. Верифікація кожного поля виконується за суворо визначеними правилами, основні з яких навряд чи будуть змінені у майбутньому.

Розглянемо структуру заголовку блоку. У першому полі записується версія – це 4 байта. Вона відповідає версії протоколу, за якою працював валідатор (творець блоку). Далі йде геш-значення попереднього блоку, тобто геш-значення від заголовку попереднього блоку, яке має довжину 256 біт. Важливо відзначити, що геш-значення було отримано у результаті застосування подвійного гешування за допомогою геш-функції SHA-2. Це поле містить 32 байта даних. Нижче знаходиться отримане спеціальним чином (*Merkle tree*) геш-значення від усіх транзакцій у блоці – теж 32 байта, після чого слідує часова позначка (Unix Timestamp), яку зазвичай встановлюють рівній часу створення блоку, – 4 байта. Після цього йде стислий параметр складності – так званий *bits* – 4 байта. Останній параметр – *nonce*, який називають рішенням завдання PoW конкретно для цього блоку. Він теж має розмір 4 байта. В результаті заголовок блоку в Біткоін завжди займає 80 байт [2].

## 3.4 Підтвердження транзакцій

Поки транзакція не включена в блок, система вважає, що кількість біткойнів на якомусь адресу залишається незмінним. У цей час є технічна можливість оформити кілька різних транзакцій з передачі з однієї адреси одних і тих же біткойнів різним одержувачам. Але як тільки одна з подібних транзакцій буде включена в блок, інші транзакції з цими ж біткойнів система буде вже ігнорувати. Є невелика ймовірність, що при розгалуженні дві подібні транзакції потрапляють в блоки різних гілок. Кожна з них буде вважатися правильною, лише при відмирання гілки одна з транзакцій стане вважатися помилковою. При цьому не буде мати значення час здійснення операції.

Таким чином, попадання транзакції в блок є підтвердженням її достовірності незалежно від наявності інших транзакцій з тими ж біткойнів. Кожен новий блок вважається додатковим «підтвердженням» транзакцій з попередніх блоків. Якщо в ланцюжку 3 блоку, то транзакції з останнього блоку

будуть підтверджені 1 раз, а поміщені в перший блок матимуть 3 підтвердження. Досить дочекатися декількох підтверджень, щоб звести ймовірність скасування транзакції до мінімуму.

Транзакція вважається достатньо підтвердженою, якщо вона включена до найдовшого ланцюга і після блоку, в якому вона міститься, є ще 5 блоків. Інакше кажучи, потрібно дочекатися 3 – 6 підтверджень [2]. Якщо врахувати, що блок з'являється в середньому 1 раз в 10 хвилин, нескладно розрахувати, що повне підтвердження транзакції займає до однієї години.

Відповідь на питання, чому необхідно саме 6 підтверджень, надає математичний розрахунок: якщо один ланцюг випереджає інший на 5 блоків, при тому ж розподілі обчислювальної потужності, ймовірність «обігнати» той, що довший вкрай мала. У своїй статті Сатоші Накамото математично доводить це на підставі наступного положення [30]:

$$q_z = \begin{cases} 1, & \text{якщо } p \le q \\ \frac{q^z}{p}, & \text{якщо } p > q \end{cases}$$

$p$ – ймовірність, що наступний блок буде знайдений чесним вузлом;

$q$ – ймовірність, що наступний блок буде знайдений атакуючим;

$q^z$ – ймовірність, що атакуючий коли-небудь наздожене основний ланцюг, якщо він почав альтернативний z блоків назад.

Наприклад, якщо зловмисник володіє 10% обчислювальної потужності всіх валідаторів, а чесні вузли працюють в мережі з швидкою доставкою повідомлень, то ця ймовірність буде менше 1/1000 [2].

## 3.5 Принцип роботи Біткоін

Біткойн існує тільки у вигляді записів в розподіленої базі, в якій в загальнодоступному відкритому (нешифрованому) вигляді зберігаються всі

транзакції, із зазначенням біткойн-адрес відправників / одержувачів, але без інформації про реального власника цих адрес. У базі немає окремих записів про поточну кількість біткойнів у будь-якого власника. Лише на підставі ланцюжків транзакцій стає зрозумілим поточну кількість біткойнів, пов'язаних з тим чи іншим біткойн-адресою. Тобто можна побачити, що на адресу надійшов 1 біткойн, а по інший транзакції на цю ж адресу надійшло 2 біткойна, третя транзакція відправила з цієї адреси 1 біткойн. Але в базі не зберігається окремого запису, скільки всього зараз біткойнів числиться за даними адресою - просто надається можливість будь-якої миті це легко порахувати. Такі підрахунки автоматично роблять клієнтські програми, користувач може і не помічати роздробленості інформації [37].

## 3.6 Ключі

Кожен користувач системи може генерувати необмежену кількість пар ключів (алгоритм ECDSA [39]). Розмір закритого ключа - 256 біт, а відповідного йому відкритого ключа - 512 біт [2].

Основне використання ключів - створення біткойн-адреси і підтвердження правомочності формування транзакцій. Але вони можуть використовуватися і для цифрового підпису або шифрування при листуванні.

Створення нової пари ключів автономно і не вимагає підключення до мережі або Інтернетом. Створені ключі зазвичай зберігають в спеціальному зашифрованому файлі wallet.dat («гаманці»). Користувач придумує пароль тільки для доступу до інформації з файлу «wallet.dat», тобто для доступу до своїх парам ключів. Для розпорядження біткойнів наявність цього файлу не є обов'язковим - в більшості випадків буде достатньо будь-яким чином отримати закритий ключ [2].

Зберігати ключі можна на будь-якому носії, не тільки на карті пам'яті, але і в паперовому вигляді. Існують онлайн гаманці, наприклад, Blockchain.info [40]

або Coinbase [41], які досить прості у використанні. Але проблеми з сайтом такого сервісу можуть призводити до втрат.

## 3.7 Адресація

Адреси створюються за допомогою генерації асиметричною пари криптографічних ключів для чого не потрібне підключення до інтернету. Людина може мати необмежену кількість адрес, створюючи їх за своїм бажанням. Кожному потенційному адресою відповідає баланс, виражений в біткойнів. Всі адреси з ненульовим балансом записані в децентралізовану ланцюжок блоків транзакцій, захищену від змін. При створенні адреси, його баланс завжди нульовий і може бути поповнений або відправкою біткойнів з інших адрес, або шляхом створення нових біткойнів і комісійних зборів за рахунок майнінгу [2].

Біткойн-адреса є послідовністю байт, отриманих в результаті перетворення відкритого ключа. Найчастіше кодуванням Base58 адресу записують як рядок довжиною до 34 літер латинського алфавіту і цифр. Перший символ адреси є завжди одиницею для звичайних адрес або трійкою для адрес створених з використанням мультипідпісу. Частина символів є контрольною сумою, яка перевіряє правильність основної частини адреси, яка, в свою чергу, є повністю випадковим результатом операцій хешування відкритого ключа.

Адреси також можуть бути відображені у вигляді QR-кодів і інших штрихкодів, придатних для машинного зчитування, наприклад, мобільними пристроями [2].

Якщо секретний ключ загублений, біткойн-мережа не прийме ніяких інших доказів права власності. Створити для існуючого адреси новий ключ неможливо, так як унікальної парі ключів завжди відповідає свою адресу. Біткойни, пов'язані з адресою, для якого немає закритого ключа, стають недоступними, фактично втрачаються. В кінці листопада 2013 року на BBC пройшов сюжет про британця, який на місцевому звалищі шукав викинутий ним раніше свій старий комп'ютерний жорсткий диск з секретним ключем до адресою,

на якому ще з 2009 року зберігалося 7,5 тис. біткойнів [42]. З новин британець дізнався про значне зростання курсу біткойнів і «усвідомив, що накоїв». На момент пошуку вартість втрачених біткойнів перевищила 7,5 млн доларів.

## 3.8 Транзакції

Біткойни можуть бути передані будь-кому, хто повідомить коректний біткойн-адресу або відкритий ключ. Мінімальна передана величина біткойнів отримало назву «сатоши» - на честь творця Сатоши Накамото [2]. Для передачі біткойнів поточний власник створює нову транзакцію, яка крім вказівок про кількість переданих біткойнів містить підписаний ініціатором хеш попередньої транзакції, по якій біткойни були отримані. Попередня транзакція стає «входом» поточної транзакції. Також вказується публічний ключ або біткойн-адреса нового одержувача («вихід»). Транзакція широкомовною запитом по відкритих каналах без шифрування відправляється в мережу. Решта вузли мережі, перш ніж прийняти транзакцію до обробки, перевіряють підписи. Правильність підпису свідчить, що ініціатор дійсно є власником секретного ключа для адреси «виходу».

Транзакції підтримують будь-яку кількість «входів» (посилань на попередні транзакції, в тому числі на користь різних адрес) і «виходів» (вказівки про одержувачів). Значення з усіх «входів» підсумовуються, і сума розподіляється по «виходів» [2].

Особливістю протоколу є неможливість взяти лише деяку частину біткойнів з «входу». Якщо на адресу було передано 2 біткойнів однієї транзакцією, то при наступній операції із зазначенням цієї транзакції в якості «входу» автоматично буде матися на увазі передача 2 біткойнів. Однак їх можна розподілити на кілька «виходів», один з яких може вказувати на цю ж адресу, тобто частина біткойнів будуть передані самому собі ( «здача»). Але залишок не обов'язково відправляти на адресу з вхідного списку. Наприклад, «Bitcoin-qt» відправляє кожен залишок на новий біткойн-адреса з резерву заздалегідь створених адрес [2].

Скасувати стандартну транзакцію неможливо, навіть при явній помилці або шахрайстві. Однак передбачено використання мультипідписів, в тому числі для угод за участю арбітра, що може забезпечити повернення біткойнів при невиконанні контрагентами обумовлених умов.

Передача біткойнів зводиться до вказівкою умов подальшого розпорядження ними. Умови формуються із застосуванням відкритих ключів. Для наступної операції з цими біткойнів потрібна відповідна електронний підпис із застосуванням секретних ключів (див. Асиметричні алгоритми шифрування), що і буде виконанням умов. Мережа перевіряє підписи парними відкритими ключами. Таким чином, розпорядитися біткойнами зможе тільки власник секретного ключа. Найбільш типовим умовою є просте зазначення біткойнадреси, який формують на основі відкритого ключа. Умови можуть бути і іншими. Наприклад, можна зажадати використати більше цифрових підписів (тобто отримати згоду декількох сторін) або вказати відкритий ключ і IP-адреса - тоді цифровий підпис треба буде виконати на комп'ютері з обумовленим IP адресою [2].

Окремі транзакції об'єднують разом з іншими транзакціями в спеціальну структуру - блок. Інформація в блоках відкрита, не шифрується, її можна швидко перевірити ще раз. Кожен блок завжди містить свій порядковий номер і хеш попереднього блоку. Всі блоки можна побудувати в один ланцюжок, яка містить інформацію про всіх скоєних коли-небудь операціях з біткойнів . З ними можна ознайомитися, наприклад, на спеціалізованих сайтах - браузерах ланцюжків блоків.

Перша транзакція в блоці завжди формується автоматично і передає винагороду за створення блоку. Решта наповнення блоку беруть з черги транзакцій, які ще не були записані в попередні блоки. Створює блок учасник може сам відібрати включаються в блок транзакції, наприклад, не взяти в блок транзакції без комісії.

Не всякий сформований блок буде прийнятий іншими учасниками. Потрібно, щоб числове значення хешу заголовка не перевищувало встановленого значення (параметр «складність»). Чим менше задано значення, тим менше

ймовірність виконання умови. У службовій області блоку виділено місце для довільних значень. Якщо хеш заголовка не задовольняє вимогам, довільні значення замінюються на нові і розрахунок хешу повторюється. Результат хешування (функції SHA-256) непередбачуваний, тому немає алгоритму цілеспрямованої зміни довільної області для досягнення бажаного результату. Зазвичай потрібна велика кількість перерахунків. Параметр «складність» приблизно раз в два тижні автоматично встановлюється так, щоб підтримувати постійної середню швидкість створення блоків (приблизно 1 блок в 10 хвилин). Якщо блоки формуються швидше, то після перерахунку «складності» досягти мети стає важче, і навпаки. Тому зміна сумарною обчислювальною потужності мережі лише дуже незначно змінює кількість створюваних блоків.

Коли підходящий варіант хешу знайдений, вузол розсилає отриманий блок іншим підключеним вузлів для перевірки. Якщо помилок немає, то кожен вузол мережі отримав блок записує його в свій екземпляр бази.

При формуванні блоків можуть виникнути ситуації, коли кілька нових блоків вважають попереднім один і той же блок. Це явище називається розгалуженням і відбувається через одночасне формування блоків «майнер» [2].

До включення транзакції в блок є технічна можливість оформлення кількох різних транзакцій з передачі з однієї адреси одних і тих же біткойнів різним одержувачам. Як тільки транзакція буде включена в блок, інші транзакції з цими ж біткойнів  система буде вже ігнорувати, тобто в ланцюжку блоків залишиться тільки одна транзакція. Але якщо контролювати більше 50% сумарною обчислювальною потужності мережі, то існує теоретична можливість при будь-якому порозі підтверджень формувати паралельну більш довгий ланцюжок блоків, в якій ті ж біткойни будуть передані іншому одержувачу (проблема «подвійного витрачання») [2]. Коли мережу отримає відомості про другий ланцюжку блоків, вона стане основною, а транзакція в ній - підтвердженої, перша ж транзакція втратить підтвердження і буде вважатися помилковою. В результаті не відбудеться подвоєння біткойнів , але зміниться їх поточний

власник, при цьому перший одержувач втратить біткойни без будь яких компенсацій.

# 4 АРХІТЕКТУРА LIGHTNING NETWORK

Lightning Network – це спосіб надійної маршрутизації платежів через велику кількість p2p двонапрямлених платіжних каналів [43].

Ця технологія, дозволяє трансформувати будь-яку криптовалюту в швидкий і надійний платіжний засіб з мінімальними комісіями. Lightning Network розробили в 2015 році, активна фаза тестування і запуску почалася тільки в кінці 2017 року [44]. Зараз Lightning Network використовується для проведення мікроплатежів у Біткоін. Завдяки використанню цієї технології кількість транзакцій в секунду збільшилась в сотні тисяч разів, а комісія за переказ - менша ніж без використання Lightning Network [45].

Типова транзакція в мережі біткоін виглядає так: відправник хоче перевести певну суму в BTC одержувачу і щоб переконатись, що транзакція пройде в визначений час, він повинен заплатити комісію, яка йде іншому учаснику мережі в якості нагороди за включення транзакції в блок. Транзакція стає в чергу - відправник і одержувач чекають, поки вона запишеться в блок, і тільки тоді отримують кінцевий результат [43].

Lightning Network вирішує цю проблему за допомогою так званих «каналів оплати». Технологія дозволяє налаштувати окремі мережі між двома учасниками основної мережі, внутрішні транзакції яких не будуть записуватися в блокчейн, а тільки зберігатися в рамках мережі каналу. Це означає, що користувачі можуть здійснювати скільки завгодно транзакцій між собою, не завантажуючи основну мережу [43].

При роботі за такою схемою в блокчейн записується тільки факт відкриття і закриття каналу с вказаним початковим і кінцевим балансом сторін, а всі транзакції, що пройшли по каналу, не займають місце у блокчейні. Така мережа може працювати не тільки з двома учасниками - вона запросто масштабується до будь-якого розміру, поєднуючи відправників і одержувачів ланцюжком в один канал, вибираючи оптимальний маршрут [43]. Важливий

момент: мережа пересилає по каналам не кошти, а тільки інформацію про володіння ними, тобто, згадану вище розписку, адже для відкриття каналу потрібне внесення сторонами певного депозиту.

## 4.1 Платіжні канали

Платіжний канал – це довірчий механізм обміну біткоінами між двома сторонами за межами Біткоін блокчейну, тобто це метод проведення платежів без додавання транзакції в блокчейн [19]. При цьому учасники каналу взаємодіють тільки один з одним. Наявність додаткових валідаторів або третіх довірених сторін не потрібно. У спрощеному варіанті роботу платіжного каналу можна зобразити як на рисунку 4.1.

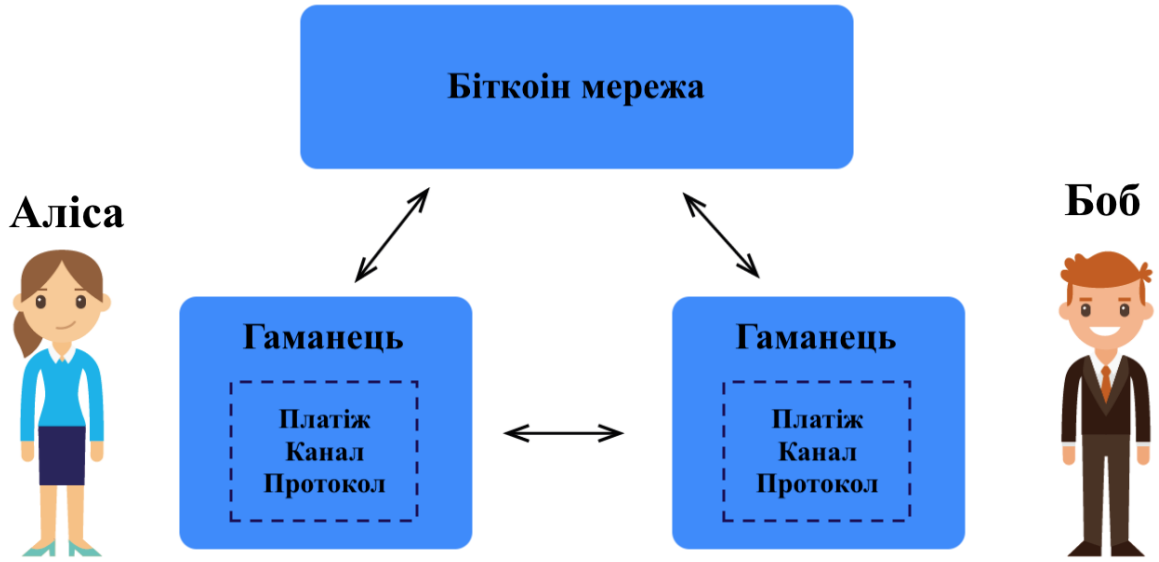


Рис 4.1 - Робота платіжного каналу

Для розуміння Lightning Network необхідно попереднє розуміння влаштування двонаправлених платіжних каналів. Тож детальніше розглянемо цей термін.

Двосторонній платіжний канал – канал оплати який дозволяє здійснювати обмін між двома або більше сторонами. Основна перевага двонаправлених каналів полягає в тому, що учасники можуть передавати монети в обидві сторони, при цьому не довіряючи один одному і не транслюючи проміжні транзакції до мережі. Якщо одна зі сторін спробує зшахраювати, то згідно з протоколом вона втрачає всі свої монети. Важливо відзначити, що при цьому не потрібно ніякого втручання з боку третьої сторони.

У разі використання платіжного каналу такого типу, сторони, що взаємодіють, можуть обмінюватися монетами один з одним необмежену кількість разів. При цьому в мережу буде необхідно публікувати тільки дві транзакції: funding, яка блокує монети в мережі і відкриває канал, і refunding, яка повертає монети сторонам по результату взаємодії між ними [19].

## 4.2 Опис Lightning Network

Lightning Network – це peer-to-peer платіжна мережа для проведення мікротранзакцій, що підтримує такі криптовалюти, як Біткоін, Ethereum, Litecoin [43]. Завданням цієї мережі є прискорення кріптовалютних платежів без делегування володіння грошима третій стороні, а також об'єднання різних криптовалют в єдину мережу з прикордонними точками у вигляді децентралізованих бірж.

На рисунку 4.3 зображено приклад передичі платежу за протоколом Lightning Network для мережі Біткоін. Протягом 3 днів Боб пред'являє Алісі платіж R. Аліса може довести, що переслала кошти Дейву. Аліса і Боб погоджуються відновити баланси в каналі, а не передавати інформацію про операції в блокчейні біткоін.

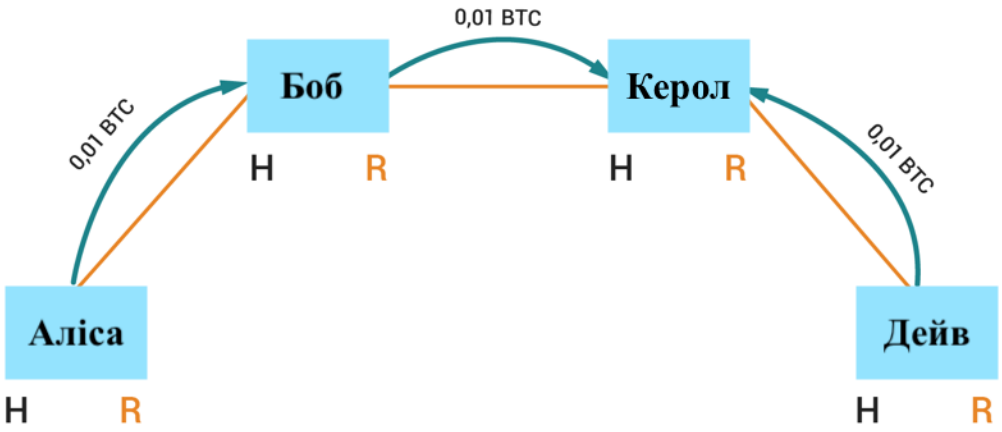


Рисунок 4.3 – Передача платежу за протоколом Lightning Network

Двома елементами будь-peer-to-peer мережі є вузол і з'єднання [44]:

- Під вузлом в Lightning Network може розумітися мобільний додаток / десктоп програма / серверне ПЗ, яке підтримує протокол спілкування Lightning Network.
- Під з'єднанням в Lighting Network розуміється платіжні канал - відношення між учасниками, яке реєструється в блокчейне і регулюється смарт-контрактом.

Кожен вузол має можливість приймати і відправляти платежі, отримуючи за це комісію. Надіслати платіж від одного учасника мережі до іншого можна тільки в разі наявності маршруту, що складається з платіжних каналів, які з'єднують одержувача і відправника.

За допомогою можливості взяття комісії за проведення платежу, в мережі стимулюється створення вузлів, які з'єднують між собою безліч інших користувачів.

Відмінність Lightning Network від таких мереж як Visa і MasterCard полягає в тому, що приєднатися до неї може будь-хто [45]. Варто врахувати, що в

Lightning Network вбудовані алгоритми, подібні мережі Tor [46], тому одержувач і відправник платежу не відомі вузлам-провідникам.

## 4.3 Переваги Lightning Network

Основною перевагою Lightning Network є збільшення пропускної здатності облікових систем. Фактично пропускна здатність каналів не обмежена і залежить безпосередньо від засобів комунікації користувачів між собою. Користувачі можуть щомиті відправляти платежі один одному і не чекати підтвердження транзакцій валідаторами (за винятком funding і refunding транзакцій) [47].

Друга перевага – конфіденційність переказів між користувачами в каналі. Фактично деталі всіх транзакцій видно тільки сторонам, які беруть в цьому участь. Якщо ви використовуєте тільки платіжний канал, то валідатори мережі бачать лише деталі funding і refunding транзакцій. Деталі всіх інших транзакцій можуть бути приховані. Якщо ж ви використовуєте Lightning Network для передачі монет іншим сторонам, то про транзакції знають всі посередники, через яких ви проводите платежі. При цьому вузли Біткоін не обробляють ці транзакції і не знають їх деталей (зрозуміло, якщо ніхто з посередників не розкриє деталі транзакцій) [47].

Третя перевага полягає в економії на комісіях. За кожен канал, його учасники в сумі платять комісію лише двічі (за його відкриття і закриття). Решта транзакцій можуть бути безкоштовними (в разі Lightning Network комісії можуть бути мінімальними і сплачуватися тільки посередникам за зміну стану каналів) [19].

Ще одна важлива перевага Lightning Network є неможливість однієї зі сторін шахраювати, так як це може призвести до втрати всіх її монет в каналі.

Тож ключові переваги Lightning Network [19]:

- Рішення проблем з пропускною спроможністю облікових систем.

- Швидкість. Транзакції Біткоін з використанням мережі Lightning надсилаються за мілісекунди, а не за хвилини, оскільки HTLC видаляються без здійснення транзакцій до блоку.
- Конфіденційність перекладів учасників каналів.
- Економія на комісіях для підтверджень транзакцій.
- Неможливість сторін шахраювати.

Як згадувалося раніше, протокол мережі Lightning Network - це не єдиний спосіб запровадження маршрутизованих платіжних каналів. Інші пропоновані системи включають Tumblebit [48] і Teechan.[49] Однак у цей час Lightning Network вже була розгорнута на тест-мережі. Кілька різних команд розробили конкуруючі реалії Lightning Network і працюють над єдиним стандартом сумісності (так званий BOLT). Цілком імовірно, що Lightning Network буде першою мережею каналів розрахункових каналів, яка буде розгорнута у виробництві [45].

## 4.4 Області застосування Lightning Network

Всі наступні приклади виходять з можливості зробити платіжний канал за допомогою технології Lightning Network.

Децентралізовані біржі. Швидкість децентралізованих бірж буде порівняна з їх централізованими аналогами. Одним з недоліків є те, що вона може оперувати тільки з криптовалютами, поверх яких побудована Lightning Network (дивись рис. 4.4) [19].

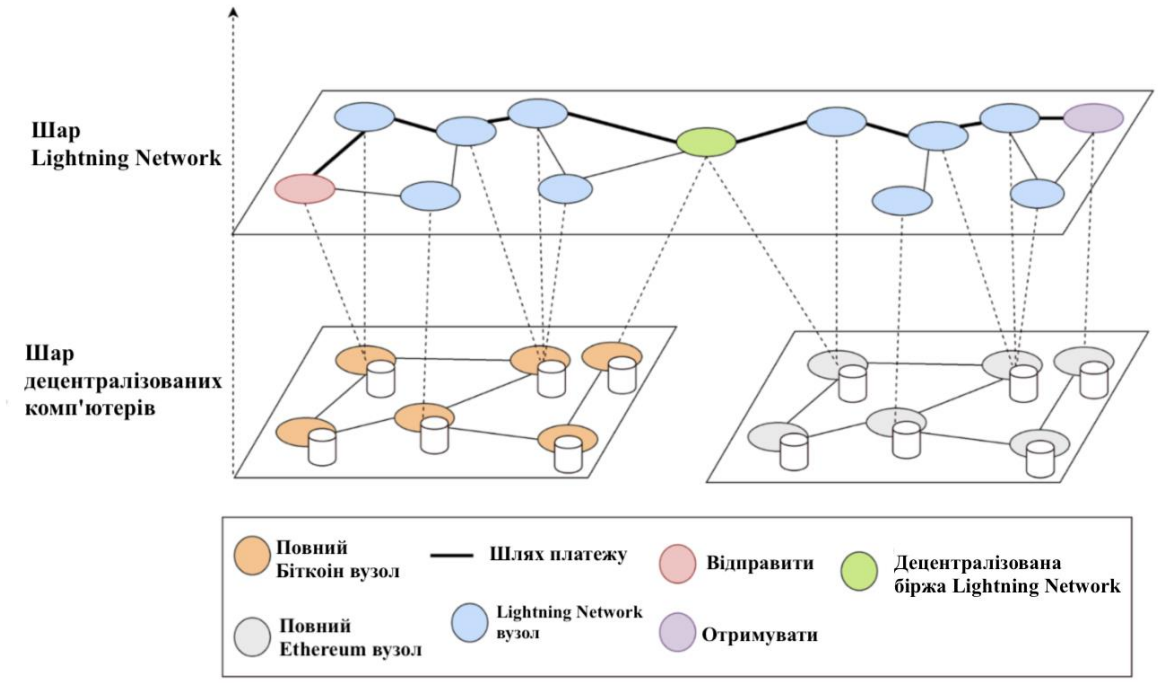


Рисунок 4.4 – Схематичний опис децентралізованої біржі

Браузерний гаманець. На поточний момент оплата послуги/товару в мережі біткоін відбувається через віджети онлайн-гаманців. Для того щоб зробити оплатиту за допомогою біткоіна, необхідно бути зареєстрованим на сайті онлайн гаманця. Кожен онлайн-гаманець надає доступ тільки до підмножини онлайн-магазинів, які зареєстровані в їх системі. З'єднавшись в одну Lightning Network онлайн-гаманці нададуть доступ до більшої кількості онлайн-магазинів, які приймають оплату в криптовалюті. Для користувачів це означає, що їм не потрібно буде переживати за втрату своїх коштів, внаслідок закриття або злому сервісу, тому що доступ до грошей може зберігається локально [19].

Банківські канали. Так як для реалізації каналу необхідно три базові елементи, то за допомогою розробки банківської системи смарт-контрактів поверх звичайної бази даних можливо створити канали, в яких можна оперувати електронним доларом. На відміну від кріптовалютних каналів, гарантом виконання смарт-контракту в даному випадку буде не майнерское співтовариство,

а внутрішня процесингова система банку. Таким чином можна буде створити децентралізовані біржі, які оперують не тільки криптовалютою [19].

Платний торрент. За допомогою технології Lightning Network і IPFS можлива монетизація Torrent. У термінології Torrent [50] існуєте два поняття:

– peer - вузол, який викачує файл;
– seed - вузол, який роздає файл.

Застосовуючи ці технології разом з peer можна зробити покупця, а з seed продавця. В системі Torrent файли розбиті на маленькі частини, і якщо один і той же файл є на двох комп'ютерах, то скачування буде відбуватися одночасно з обох. Так як файли розбиті на частини і розподілені по декількох комп'ютерів, а Lightning Network дозволяє робити мікроплатежі, то можна платити за скачування частки файлу. Якщо вузол, який роздає файл, вийшов з мережі, то оплата прожовжиться з іншого вузла у якого є необхідний файл. Оперуючи маленькими платежами знижується втрата при ненадання частки файлу [19].

Використання в чаті. Використання платежів в месенджерах на даний момент отримало широке поширення в країнах Азії. У мессенджере WeChat [51], призначена для користувача база якого складає близько 900 мільйонів чоловік, кожен третій використовує внутрішню платіжну систему чату. Незважаючи на величезні розміри населення Китаю, юань не володіє потенціалом поширитися на інші країни на відміну від криптовалют. Впровадження клієнта Lightning Network в месенджер дасть можливість використання біткоіну в якості внутрішньої валюти.

OpenBazaar [52]. На OpenBazaar, peer-to-peer ринку товарів і послуг, транзакції відбуваються за допомогою біткоіна. Комісії в мережі біткоіни можуть стати перешкодою для покупки товарів і послуг, вартість яких порівнянна з самою комісією. Впровадження клієнта Lightning Network може вирішити цю проблему.

## 4.5 Аналіз рівня безпеки протокола Lightning Network

Існуюче застосування протоколу Біткойн дозволяє проводити лише сім транзакцій в секунду, в той час як Visa регулярно обробляє 2 000 транзакцій в секунду [53]. Існуюча реалізація біткойн має високий рівень безпеки, але не може бути масштабуватна і перетворена в глобальну мережу для транзакцій. Мережа Lightning пропонує потенційне рішення масштабування протоколу Біткойн до мільйона транзакцій в секунду і зменшення комісій за транзакції до центів при цьому покращуючи безпеку для учасників системи [44].

Застосувати технологію Lightning Network можна не тільки до протоколу Біткойн. Експерти вважають, що мережа блокчейн може бути на рівні з платіжними системами Visa і Mastercard, якщо використовувати надстройку Lightning Network [44]. Крім того, дана розробка пропонує підвищені заходи безпеки, що дуже важливо при роботі з фінансами. Відбувається це завдяки тому, що всі транзакції між каналами заплутані і зрозуміти який користувач кому кому відправив гроші важко.

25 вересня 2019 була успішно проведена перша формальна перевірка специфікації мережі Lightning Network на безпеку, яка називається «A Composable Security Treatment of the Lightning Network» [54]. Його проводили вчені з Единбурзького університету [55], за підтримки компанії IOHK [56]. Вчені вивчили основоположну криптографію, створену для забезпечення роботи мережі Lightning Network, і високо оцінили її надійність. Висновок дослідження такий, що чесний учасник мережі може втратити свої кошти тільки в разі, якщо будуть пошкоджені підпис або хеш-функція, що використовуються у біткоіні. Все критично важливі для системи частини надійні.

Була представлена функціональність $F_{PayNet}$, яка абстрагує властивості безпеки, що надаються Lightning Network. Використовуючи $F_{PayNet}$, сторони можуть відкривати і закривати канали, здійснювати платежі по каналах мережі, а

також опитувати його статус. Важливо відзначити, що ця функціональність відстежує всі off-chain і on-chain баланси зареєстрованих сторін, які гарантують, що при закритті каналу on-chain баланси відповідають off-chain балансам. Найважливішою характеристикою безпеки, яку Lightning Network надає своїм учасникам: від чесних сторін очікується опитування про функціональність, що відповідає рівню їхньої участі в мережі і властивостями базової мережі. Якщо сторона не виконує цю вимогу, вона визначається як недбала по функціональності і може втратити кошти.

Функціональність відкриття каналу $F_{PayNet}$:

1) При отриманні $(openChannel, \text{Аліса}, \text{Боб}, x, tid)$ від Аліси:
2) $tid$ забезпечує достовірність, що Аліса не відкриває інший канал
3) Обирає унікальний канал *ID fchid*
4) Очікує на відкриття *(fchid) ← (Аліса, Боб, x, tid)*
5) Надсилає $(openChannel, \text{Аліса}, \text{Боб}, x, fchid, tid)$до $S$
6) При отриманні

$(ChannelAnnounced, \text{Аліса}, p_{\text{Аліса},F}, p_{\text{Боб},F}, fchid, pchid, tid)$ від $s$:

7) Переконуємось, *що pendingOpen (fchid)* запис з тимчасовим id *tid*
8) Додаємо Аліса Announced, $p_{\text{Аліса},F}, p_{\text{Боб},F}, fchid$ до $pendingOpen\ (fchid)$
9) При отриманні $(CheckForNew, \text{Аліса}, \text{Боб}, tid)$ від Аліси:
10) Переконуємось, що є відповідність channel та $pendingOpen\ (fchid)$
11) (funder, fundee, $x$ , $p_{\text{Аліса},F}, p_{\text{Боб},F}$ ) ← $pendingOpen\ (fchid)$
12) Надсилає *(Читати) до* $G_{Ledger}$ і зберігає відповідь $\sum_{\text{Аліса}}$
13) *checkClosed*($\sum_{\text{Аліса}}$)
14) Переконуємось, *що TX* $F \in \sum_{\text{Аліса}}$ з (x, ($p_{funder,F}$ ^$p_{fundee,F}$))
15) Позначаємо $channel$ як $FundingLocked$ (фінансування заблоковано)
16) Надсилає $(FundingLocked, \text{Аліса}, \sum_{\text{Аліса}}, fchid)$ до $S$

17) При отриманні ($FundingLocked, fchid$) від $S$:

18) Переконуємось, що $channel$ дорівнює $pendingOpen\ (fchid)$

19) Змінюємо позначку чекає на $FundingLocked$ на чекає на $ChannelOpen$

20) Надсилає *(Читати) до* $G_{Ledger}$ Бобу і зберігає відповідь $\sum_{\text{Боб}}$

21) *checkClosed* ($\sum_{\text{Боб}}$)

22) Переконуємось, *що TX* $F \in \sum_{\text{Боб}}$ з (x, ($p_{funder,F}$ ^$p_{fundee,F}$))

23) Додаємо *receipt(channel)* до *newChannels(Боб)*

24) Надсилає ($FundingLocked$, Боб, $\sum_{\text{Боб}}, fchid$) до $S$

25) При отриманні ($ChannelOpen, fchid$) від $S$:

26) Переконуємось, що $channel$ дорівнює $pendingOpen\ (fchid)$. Змінюємо позначку чекає на $ChannelOpen$

27) *offChainBalance (funder)* ← *offChainBalance (funder)+x*

28) *onChainBalance (funder)* ← *onChainBalance (funder)-x*

29) $channel$ ←*(funder,fundee,x,0,0,fchid,pchid)*

30) Додаємо $channel$ до $channels$

31) Додаємо *receipt(channel)* до *newChannel(Аліса)*

32) Видаляємо *pendingOpen(*$fchid$*) запис*

Функціональність здійснення платежів по каналу $F_{PayNet}$:

1) При отриманні ($PAY$, Боб, $\xrightarrow[path]{}$) від Аліси:

2) Обирається унікальний ID платежа *payid*

3) Додається $\left(\text{Аліса, Боб}, x, \xrightarrow[path]{}, payid\right)$ до $pendingPay$

4) Надсілається $\left(PAY, \text{Аліса, Боб}, x, \xrightarrow[path]{}, payid, state, \sum\right)$ до $S$

5) При отриманні ($update, receipt$, Аліса) від $S$:

6) Додаємо *receipt* до *updatesToReport(Аліса)*

7) Надсилаємо *(continue)* до $S$

Функціональність закриття каналу $F_{PayNet}$:

1) При отриманні $(CloseChannel, receipt, tid)$ від Аліси:
2) Переконуємось, що $channel \in channels : receipt\ (channel) = receipt$ з $ID\ tid$
3) Отримаємо $fchid$ з $channel$
4) Додаємо $(fchid, receipt(channel))$ до $pendingClose$(Аліса)
5) Не служить жодному іншому ($PAY$ чи $CloseChannel$) повидомлення від Аліси до цього каналу
6) Надсилаємо отриманні $(CloseChannel, receipt, tid,$ Аліса) від $S$

У звіті вперше були визначені точні вимоги до опитування, які пред'являються Lightning Network для чесних сторін. Чесні сторони беруть участь в опитуваннях, для того, щоб не втратити кошти, в залежності від базових параметрів функціональних можливостей реєстру, на які накладається Lightning Network. У роботі «A Composable Security Treatment of the Lightning Network» описується $F_{PayNet}$ з урахуванням функціональності глобальної учетної системи (блокчейн Біткоіну). Функціональність забезпечує явні гарантії безпеки щодо узгодженості і життєздатності, які, в свою чергу, впливають на гарантії, що надаються $F_{PayNet}$.

Вимоги до опитування для кожної сторони є двоякими: перший тип опитування відноситься до моніторингу закриття каналів, що сторона є однією з кінцевих точок і визначається обраної користувачем затримкою параметру, другий тип опитування відноситься до моніторингу конкретних подій, пов'язаних з отриманням і передачею платежів. Зокрема, для кожного платежу, в якому сторона виступає в якості посередника, опитування має проводитися двічі протягом періоду часу, коли ланцюжок з точки зору сторони виходить з висоти блоку *h* в *h' - a*, де *h*, *h'* - це два параметри висоти блоку, зазначені в конкретному платіжному шляху, і *a* - це параметр облікової системи, який є верхньою межею кількості блоків, які можуть бути завершені в системі з моменту видачі певної

транзакції до моменту її завершення. Крім того, два опитування повинні бути розділені часовим вікном, яке дозволяє ланцюжку рости як мінімум на $a$ блоків.

Реалізація $F_{PayNet}$ доводиться у протоколі Lightning Network $\Pi_{LN}$ при певному наборі криптографічних припущень. Щоб висловити $\Pi_{LN}$ коротким способом, був ідентифікований ряд базових криптографічних примітивів, які використовувалися в базовій специфікації Lightning Network. Деякі з цих криптографічних примітивів є стандартними (вони включають в себе PRF [57], схему цифрового підпису та схему підписи на основі ідентифікації [57]), також додатковий примітив - комбінований цифровий підпис [58]. Комбінований цифровий підпис є окремим випадком асиметричного двостороннього примітиву цифрового підпису з характеристикою, згідно з якою одна з двох сторін, "акціонер", генерує і зберігає частку ключа підпису, в той час як відкритий ключ комбінованого підпису визначається не інтерактивно на основі інформації відкритого ключа, створеного обома сторонами. Для видачі підписів потрібна наявність "акції", яка піддається перевірці з урахуванням публічної інформації, наданої "акціонером". У схемі формалізується примітив цифрового підпису. Ця конструкція лежить в специфікації Lightning Network і реалізує її при стандартних криптографічних припущеннях. Таким чином, реалізація $F_{PayNet}$ досягається за умови безпеки базових примітивів [54].

Більшість криптовалют в повному обсязі анонімні. Переходи все ще можна простежити від одного гаманця до іншого. Так як більшість угод Lightning Network відбувається поза основного блокчейна, все мікроплатежі через Lightning Network буде майже неможливо відстежити.

# 5 ПОДАЛЬШЕ ВДОСКОНАЛЕННЯ LIGHTNING NETWORK

Plasma є способом проведення транзакцій поза мережею, при цьому безпеку таких транзакцій спирається на базовий ланцюг ефіріум блокчейна [59]. Основним завданням, яке вирішує Plasma, є перенесення виконання операцій за основну мережу і повернення результату в mainchain. Plasma має схожість з функціонуванням Lightning Network. Однак, особливість технології Plasma полягає в можливості створення дочірніх блокчейнов, прикріплених до mainchain. Більш того, дочірні ланцюжки блоків в свою чергу можуть породжувати власні дочірні ланцюжки [59].

Масштабованість є однією з головних проблем ефіріум блокчейна. Існуючі обмеження, з якими стикається мережу з точки зору пропускної здатності та швидкості, не дозволяють використовувати її в більш глобальному масштабі. Ефіріум Plasma була запропонована одним із засновників криптовалюти Ефіріум в серпні 2017 року як метод вирішення проблем масштабування для ефіріум блокчейна [59]. Хоча Plasma і Lightning Network були запропоновані як рішення масштабування блокчейнів, у кожного з них є свій власний механізм і особливості.

## 5.1 Опис Plasma

Основна ідея Plasma складається в створенні фреймворка sidechains, які будуть якомога рідше взаємодіяти з основним ланцюгом [59]. Такий фреймворк призначений для роботи в вигляді блокчейн дерева, яке ієрархічно організовано таким чином, що безліч дрібних ланцюжків може бути створено поверх

основного. Ці маленькі ланцюги також називають як Plasma ланцюги або малі ланцюги (child chains).

Структура Plasma побудована з використанням смарт-контрактів і дерев Меркла, що дозволяє створювати необмежену кількість малих ланцюжків, які є меншими копіями основного блокчейна. У верхній частині кожного малого ланцюга, також може створюватися велика кількість інших ланцюжків, і саме це створює деревоподібну структуру. Кожний малий Plasma ланцюг являє собою настроюваним смарт-контрактом, який може бути розроблений так, щоб працювати єдиним чином, служачи різним потребам [59]. Це означає, що ланцюги можуть співіснувати і працювати незалежно. Зрештою, Plasma дозволить підприємствам і компаніям впроваджувати масштабовані рішення різними способами відповідно до їх конкретним потребам.

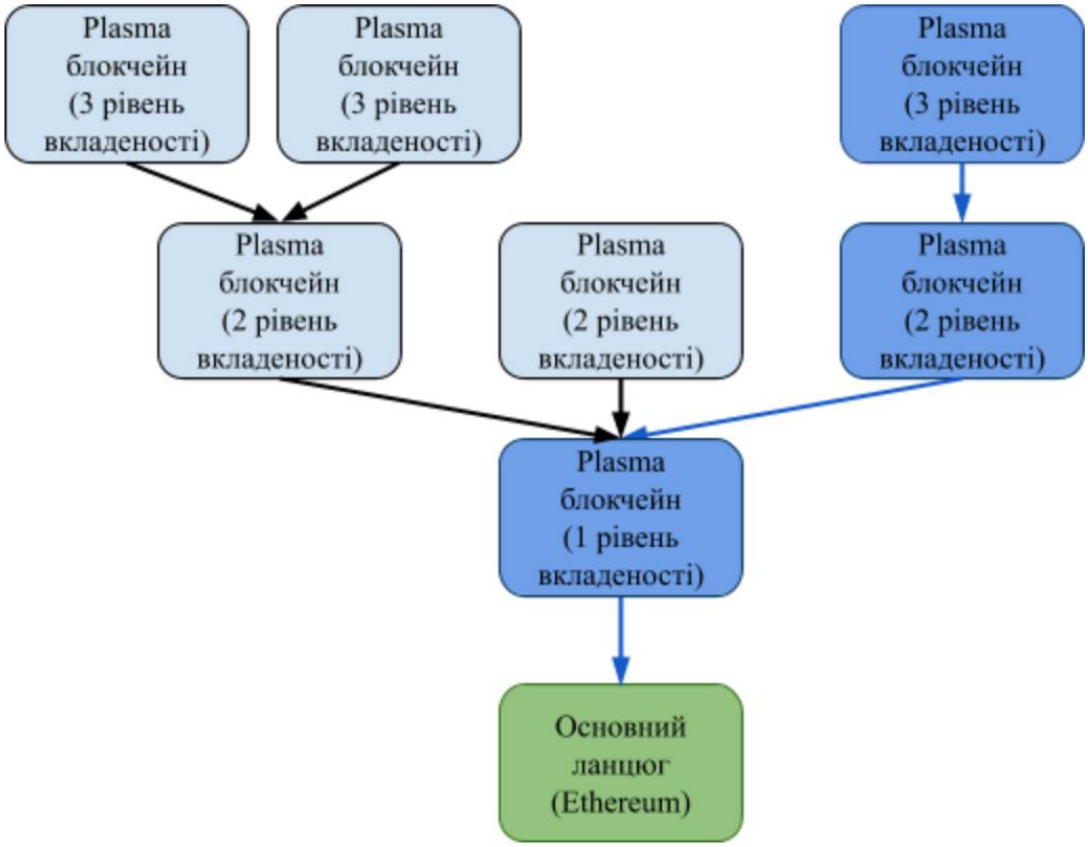


Рисунок 5.1 - Будова протоколу Plasma

За допомоги Plasma ймовірність того, що головна ланцюг буде перевантажен, буде менше, оскільки кожний малий ланцюг буде розроблен для роботи певним чином, для досягнення своїх конкретних цілей, які не обов'язково пов'язані с основним ланцюжком. Таким чином малі ланцюга полегшать загальну роботу основного ланцюжка [60].

## 5.2 Переваги Plasma

Зараз користувачам системи доводиться завантажувати і підтверджувати кожен смарт-контракт, однак Plasma - це спосіб значно зменшити обсяг необхідних даних. Основна перевага Plasma в тому, що обсяг оброблюваних клієнтів даних значно зменшений. Замість завантаження повної історії Plasma, користувачі зможуть генерувати так звані «Plasma coins» шляхом відправки коштів на смарт-контракт. Таким чином, замість завантаження і верифікації всіх даних, користувачі можуть лише відстежувати маркери, створені всередині системи [62].

Основна ідея Plasma полягає у використанні sidechains для підвищення пропускної здатності мережі Ethereum. Plasma представляє із себе структуру з великою кількістю деревовидних ланцюжків блоків, стан яких прив'язується до основних ланцюжків блоків. Кожна з дочірніх ланцюжків може мати власний механізм досягнення консенсусу і метод зв'язку з батьківським ланцюжком (до кореневої). Учасникам системи потрібно тільки перевіряти доступність і коректність ланцюга Plasma лише для спеціального індексу, пов'язаного з монетами, які вони хочуть витратити, якими володіють [62].

Така оптимізована система знайшла безліч корисних застосувань, включаючи захист бірж від великомасштабних хакерських атак. Замість прямого використання коштів користувачів біржі можуть за допомогою смарт-контрактів

Plasma забезпечувати роботу книги ордерів. Також за допомогою цієї системи можна страхувати можливі збитки [63].

Однак, найбільш важливим є те, що нове рішення може значно сприяти вирішенню актуальної проблеми масштабованості мережі Ethereum [63]. Це спосіб зробити Plasma більш масштабованої і значно знизити вимоги для її використання звичайними користувачами.

## 5.3 Області застосування Plasma

Децентралізовані біржі. Біржа Altcoin [64] грунтується на блокчейне ефіріум, використовуючи для цього технологію Plasma. Обмін активами відбувається за допомогою atomic swap. Перед тим, як зробити обмін, Plasma блокує кошти і надає доказ блокування коштів (proof of locked value) в sidechain. Якщо кошти заблоковані в смарт-контракті, вони стають доступними для користувачів для проведення транзакцій в sidechain.

Процес обміну на біржі відбувається наступним чином [65]:

- відбувається переказ коштів в дочірній блокчейн;
- створювані orders записуються безпосередньо в дочірній блокчейн. На цьому етапі всі дочірні order books рекурсивно зводяться в єдиний order book, представлену цим ланцюжком, поки не буде досягнутий найвищий батьківський Plasma блокчейн;
- користувач вибирає потрібний йому order і за допомогою технології atomic swap відбувається обмін активами;
- результат обміну записується в дочірній блокчейн. Після синхронізації з батьківським блокчейном, результат обміну буде і в батьківському блокчейні, і через деякий час буде записаний в кореневій блокчейн.

## 5.4 Аналіз рівня безпеки Plasma

Як і Lightning Network, Plasma являє собою набір смарт контрактів, що виконуються позакореневого блокчейна. Кореневої контракт обробляє лише невелику кількість запитів від дочірніх блокчейнов, які у більшості випадків, самі виконують основний обсяг обчислень [66].

Однак, оскільки дані передаються не всім вузлам (а тільки тим, які бажають підтверджувати конкретний стан), зацікавлені сторони мають самостійно контролювати конкретний sidechain, і за допомогою окремого механізму карати спроби шахрайства. Ще один запобіжний механізм: в разі атаки, учасники sidechain можуть швидко і дешево здійснити масовий вихід з sidechain в кореневу мережу.

Sidechains можуть об'єднуватися в ієрархію дерева: це дозволить створити збалансовану систему з співвідношеннями доступність даних, безпека (по теоремі CAP), і мінімумом цін. Повна надійність забезпечується тільки майнінгом кореневого блокчейна, який передає доказ достовірності даних дочірнім блокчейнам[66].

Будь який sidechain (він же дочірній блокчейн) може створити власний токен. У цих токенах валідатори sidechain можуть отримувати виплати за роботу своїх вузлів, і в них же створюються депозити валідаторів. При виявленні недобросовісної поведінки валідаторів (перешкода доступності даних, або інших атак) залишок депозиту згорає. В sidechains немає свого PoW - в них використовується PoS, в якому депозити, відкриті в платіжному каналі, одночасно є і страховкою від несумлінної поведінки валідатора.

Кореневий ланцюг обробляє невелику кількість запитів від дочірніх ланцюжків, так що кореневий ланцюжок виступає в якості найбільш безпечного та остаточного шару для зберігання всіх проміжних станів. Кожний дочірній ланцюжок функціонує як свій блокчейн зі своїм власним консенсусом[66].

Валідатори мають економічні стимули діяти чесно, і відправляють запити в кореневий ланцюг - фінальна установка транзакції. В результаті учасники

системи, що працюють в childchain, взагалі не повинні взаємодіяти з кореневим ланцюгом. Крім того, вони можуть вивести свої гроші в кореневий ланцюг, коли захочуть, навіть якщо childchain зламаний. Ці виходи з childchain дозволяють користувачам безпечно зберігати свої кошти за допомогою Merkle Proof, що підтверджує право власності на певну суму коштів.

Ітак в Plasma особливий акцент зроблено на безпеку - депозити платіжних каналів одночасно служать гарантією чесної поведінки валідаторів, а «Докази Шахрайства» (Proof of Fraud) [67] забезпечуються логікою смарт-контрактів, яка дозволяє в разі атаки швидко вивести кошти з sidechain в основний блокчейн, захищений майнінгом. Proof of Fraud дозволяє будь-якій особі на основному ланцюжку уявити деталі транзакцій, які, на його думку, є шахрайськими. Якщо виклик буде успішним, ставки сторін, що беруть участь в шахрайстві, будуть скорочені, а претендент отримує винагороду в якості стимулу для виявлення шахрайства [66].

# 6 МЕТОДИКА ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ СУЧАСНИХ І ПЕРСПЕКТИВНИХ ПЛАТІЖНИХ СИСТЕМ

## 6.1 Визначення критеріїв для порівняння

Визначається система, характеристики якої відображають основну функціональність системи і присутні в тій чи іншій мірі в кожній платформі.

При виборі системи, що найбільше задовольняє критеріям безпеки і швидкодії необхідно зробити оцінку по комплексному набору показників. Для цього потрібна формалізована методика, показниками якої виступають критерії для забезпечення безпеки. Визначимо критерії: відкритість, децентралізація, анонімність, швидкість, надмірність, прийняття. Оцінка виконується по найбільш важливим критеріям безпеки.

## 6.2 Сучасні та перспективні системи для порівняння

Для проведення ефективного аналізу обираються для порівняння платформи Біткоін, Lightning Network, Plasma, PayPal, SWIFT, Visa - вони відповідають заданим характеристикам.

## 6.3 Обґрунтування вибору схеми з найкращим рівнем безпеки

Перед тим, як заглиблюватися в порівняльний аналіз технічних характеристик продукту, розберемо деякі найпопулярніші класичні платіжні системи та порівняймо їх між собою.

Алгоритм такого аналізу виглядає наступним чином:

- визначимо основну функціональність системи;
- проведемо пошук подібних продуктів зі схожим інтерфейсом;
- визначємо критерії для порівняння, які дозволять виявити загальні риси і відмінності між системами;
- проведемо порівняльний аналіз.

## 6.4 Визначення функціональності системи

Проект Lightning Network в даній роботі буде розглядатися в якості платіжної системи. Тому основні функції інтерфейсу полягають в наступному:

- прийом платежів;
- відправка платежів;
- створення акаунтів.

### 6.4.1 Показники відкритості

Характеристика «показники відкритості» [68] описує здатність підключення в роботу мережі інших систем при обробці операцій і отримання оплати за використання ресурсів. Ця властивість характеризує ступінь стійкості системи по відношенню до зовнішніх чинників: видалення вузла, який займається обробкою операції, не може призвести до збою роботи всієї системи. У ролі вузла в даному випадку виступають сервери, які знаходяться під контролем однієї компанії.

Оцінка проводиться таким чином:

- 0 - властивість відсутня. Це говорить про нездатність системи нормально функціонувати при зупинці роботи конкретного вузла, який займається обробкою операції;
- 1 - показники середньої відкритості. При блокуванні вузла, який займається обробкою операції, використання системи буде недоступно деякій кількості користувачів;
- 2 - показники сильної відкритості. Система буде недоступна користувачам тільки за умови масової зупинки вузлів, що обробляють транзакції.

### 6.4.2 Показники децентралізованності

Критерій «показники децентралізованності» [68] характеризує працездатність системи з точки зору незалежності мережі від центральної складової в ході прийняття остаточних рішень з питання зміни балансу. Оцінка:

- 0 - критерій відсутній;

– 1 - критерій присутній.

### 6.4.3 Показники анонімності

Властивість показників анонімності [68] визначає рівень складності процесу отримання конфіденційних даних про учасників транзакції. Оцінка проводиться так:

– 0 - властивість відсутня;
– 1 - слабкий рівень анонімності. Властивість припиняє свою дію при запиті державних структур;
– 2 - середній рівень анонімності, або псевдоанонімності. Операції доступні всім користувачам мережі, але при цьому не розкривається прив'язка до акаунтів та учасникам транзакції;
– 3 - високий рівень анонімності. Інформація про учасників транзакції відсутня, як і дані про самі операції.

### 6.4.4 Показники швидкості, надмірності

Показники швидкості - оцінка проводиться за шкалою від 0 до n. Цей критерій дозволяє відобразити пропускну здатність мережі, описує швидкість роботи з прикордонними і внутрішньодержавними операціями .

Показники надмірності - оцінюються за шкалою від 0 до 9. Дозволяють характеризувати проекту з точки зору використовуваних обсягів даних і ресурсів для забезпечення системі працездатності. Цей критерій також свідчить про наявність інерційності, а саме описує обсяги витрат користувачів мережі, які виражаються в сплаті комісій за використовуваний функціонал.

Показники прийняття - оцінюються за шкалою від 0 до 9. Дозволяють характеризувати використовуваність продукту в умовах реального часу [68].

## 6.5 Вибір схеми з найкращим рівнем безпеки

Тепер приведемо безпосередньо порівняльний аналіз, результати якого будуть виражені в числових показниках (таблиця 6.1, таблиця 6.2, таблиця 6.3, таблиця 6.4, таблиця 6.5).

Таблиця 6.1 – Результати аналізу мережі Біткоін

| Мережа Біткоін | |
|---|---|
| Відкритість | 2 |
| Децентралізація | 1 |
| Анонімність | 5 |
| Швидкість | 7 |
| Надмірність | 4 |
| Прийняття | 3 |

Такі показники відкритості та децентралізації аргументуються використанням в даній мережі технології блокчейн, в яку закладені механізми розподілу можливості внесення змін в роботу системи безліччю користувачів, а в прийнятті кінцевих рішень центральний сервіс не бере участь. Поряд з цими характеристиками блокчейн технології властиві високі показники надмірності, які значно впливають на швидкість роботи мережі - прийняття консенсусу знижує швидкість проведення транзакцій.

Таблиця 6.2 – Результати аналізу платіжної системи PayPal

| Платіжна система PayPal | |
|---|---|
| Відкритість | 0 |
| Децентралізація | 0 |
| Анонімність | 1 |
| Швидкість | 4 |
| Надмірність | 2 |
| Прийняття | 8 |

Платформа PayPal має зрозумілу функціональність, оскільки в її базу закладені стандартні принципи роботи і технології, що не припускають використання відкритості та децентралізації. Це дає можливість територіально обмежувати функціонування продукту. При цьому мережа відрізняється дуже високою швидкістю проведення операцій, оскільки за обробку даних відповідає єдиний центр.

Таблиця 6.3 – Результати аналізу платіжної системи SWIFT

| Платіжна система SWIFT | |
|---|---|
| Відкритість | 0 |
| Децентралізація | 0 |
| Анонімність | 1 |
| Швидкість | 2 |
| Надмірність | 2 |
| Прийняття | 8 |

Таблиця 6.4 – Результати аналізу системи Lightning Network

| Система Lightning Network | |
|---|---|
| Відкритість | 3 |
| Децентралізація | 1 |
| Анонімність | 5 |
| Швидкість | 9 |
| Надмірність | 5 |
| Прийняття | 2 |

Таблиця 6.5 – Результати аналізу системи Plasma

| Система Lightning Plasma | |
|---|---|
| Відкритість | 3 |
| Децентралізація | 1 |
| Анонімність | 5 |
| Швидкість | 9 |
| Надмірність | 5 |
| Прийняття | 2 |

Результати проведено, на цьому доцільно підтверджено що Lightning Network задовольняє найбільшій кількості властивостей для забезпечення безпеки мережі. У попередньому розділі були отримані порівняння на основі яких можна стверджувати що платіжна система Lightning Network показала найліпші результати з усіх інших запропонованих систем.

## 6.6 Розробка і застосування методики порівняння рівня безпеки розглядаємих систем

Для вирішення завдань подібного роду в аналітичному плануванні широко застосовується метод аналізу ієрархій (MAI), розроблений Т.Сааті [69]. Першим етапом застосування MAI є структурування проблеми вибору у вигляді ієрархії. В даному випадку, ієрархія будується з вершини, через проміжні рівні до самого нижнього рівня, де враховуються вимоги до експлуатаційних характеристик.

Після ієрархічного відтворення проблеми встановлюються пріоритети критеріїв і оцінюється кожна з альтернатив за критеріями. У MAI елементи завдання порівнюються попарно по відношенню до їх впливу на загальну для них характеристику [70]. Система парних відомостей призводить до результату, який може бути представлений у вигляді асиметричної матриці. Елементом матриці a (i, j) є інтенсивність прояву елемента ієрархії і щодо елемента ієрархії j, оцінюється за шкалою інтенсивності від 1 до 9, запропонованої автором методу

[70]. Оцінка інтенсивності елементів представлена у таблиці 6.6.

Таблиця 6.6 – Оцінка інтенсивності елементів

| |
|---|
| 1 – рівна важливість |
| – помірна перевага одного над іншим |
| – істотна перевага одного над іншим |
| – значна перевага одного над іншим |
| – дуже сильна перевага одного над іншим |
| 4, 6, 8 – відповідні проміжні значення |

Корисним елементом теорії є так званий індекс узгодженості (ІС), який дає інформацію про ступінь порушення узгодженості. Разом з матрицею парних порівнянь існує міра оцінки ступеня відхилення від узгодженості. Якщо такі відхилення перевищують встановлені межі (більше 10%), то тому, хто проводить судження, слід ще раз перевірити їх в матриці [71].

Оберемо критеріїв та альтернатив, у таблиці 6.7.

Таблиця 6.7 – Критерії

| |
|---|
| Відкритість |
| Децентралізація |
| Анонімність |
| Швидкість |
| Надмірність |
| Прийняття |

Таблиця 6.8 – Альтернативи

| |
|---|
| Мережа Біткоін |
| PayPal |
| SWIFT |
| Мережа Lightning Network |
| Мережа Plasma |

Визначивши матриці попарних порівнянь для альтернатив, застосуємо обраний метод для порівняння платіжних каналів у підрозділі 6.7.

## 6.7 Результати застосування методики порівняння Lightning Network та інших платіжних систем

Наведемо відношення узгодженості для таблиці 6.6. Далі побудуємо матриці попарних порівнянь для альтернатив. Для цього побудуємо 6 матриць (по числу критеріїв) розмірністю 6x6 (по числу альтернатив). Матриці попарних порівнянь для альтернатив зображені у таблицях 6.9 – 6.14.

Числові значення в матрицях попарних порівнянь розраховувались як середнє значення п'яти експертів з кафедри «БІТ» та експертів з компанії «Distributed Lab». Також враховувались додаткові вимоги до вузла мережі, підтримки операційних систем, експлуатаційних характеристик пристроїв на яких можливе використання певної криптовалюти. Такий фактор як наявність зручних клієнтів був невід'ємним при оцінках, бо незручність користуванням системою може стати відмовою до застосування системи зовсім.

Таблиця 6.9 – Властивість відкритість

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 7 | 7 | 7 | 1/7 | 1/7 | 1,383088 | 0,128402 |
| PayPal | 1/7 | 1 | 3 | 1/3 | 1/9 | 1/9 | 0,347592 | 0,032270 |
| SWIFT | 1/7 | 1/3 | 1 | 1/3 | 1/9 | 1/9 | 0,241007 | 0,022374 |
| Visa | 1/7 | 3 | 3 | 1 | 1/9 | 1/9 | 0,501314 | 0,046541 |
| Мережа Lightning Network | 7 | 9 | 9 | 9 | 1 | 1 | 4,149263 | 0,385207 |
| Мережа Plasma | 7 | 9 | 9 | 9 | 1 | 1 | 4,149263 | 0,385207 |
| Сума | 15,4286 | 29,333 | 32,000 | 26,667 | 2,4762 | 2,4762 | 10,77152 | |

Відношення узгодженості (ВУ) = 12,99%

Таблиця 6.10 – Властивість децентралізація

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 9 | 9 | 9 | 1 | 2 | 3,367386 | 0,335394 |
| PayPal | 1/9 | 1 | 1 | 1 | 1/9 | 1/9 | 0,333333 | 0,033200 |
| SWIFT | 1/9 | 1 | 1 | 1 | 1/9 | 1/9 | 0,333333 | 0,033200 |
| Visa | 1/9 | 1 | 1 | 1 | 1/9 | 1/9 | 0,333333 | 0,033200 |
| Мережа Lightning Network | 1 | 9 | 9 | 9 | 1 | 1 | 3,000000 | 0,298802 |
| Мережа Plasma | 1/2 | 9 | 9 | 9 | 1 | 1 | 2,672696 | 0,266203 |
| Сума | 2,8333 | 30,000 | 30,000 | 30,000 | 3,3333 | 4,3333 | 10,04008 | |

Відношення узгодженості (ВУ) = 1,44%

Таблиця 6.11 – Властивість анонімність

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 5 | 5 | 5 | 1/3 | 1/3 | 1,550403 | 0,170290 |
| PayPal | 1/5 | 1 | 1 | 1 | 1/7 | 1/7 | 0,399766 | 0,043909 |
| SWIFT | 1/5 | 1 | 1 | 1 | 1/7 | 1/7 | 0,399766 | 0,043909 |
| Visa | 1/5 | 1 | 1 | 1 | 1/7 | 1/7 | 0,399766 | 0,043909 |
| Мережа Lightning Network | 3 | 7 | 7 | 7 | 1 | 1 | 3,177381 | 0,348992 |
| Мережа Plasma | 3 | 7 | 7 | 7 | 1 | 1 | 3,177381 | 0,348992 |
| Сума | 7,6000 | 22,000 | 22,000 | 22,000 | 2,7619 | 2,7619 | 9,104461 | |

Відношення узгодженості (ВУ) = 1,97%

Таблиця 6.12 – Властивість швидкість

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 3 | 3 | 3 | 1/7 | 1/7 | 0,905443 | 0,086976 |
| PayPal | 1/3 | 1 | 2 | 1 | 1/9 | 1/9 | 0,449335 | 0,043163 |
| SWIFT | 1/3 | 1/2 | 1 | 2 | 1/9 | 1/9 | 0,400312 | 0,038454 |
| Visa | 1/3 | 1 | 1/2 | 1 | 1/9 | 1/9 | 0,356638 | 0,034258 |
| Мережа Lightning Network | 7 | 9 | 9 | 9 | 1 | 1 | 4,149263 | 0,398575 |
| Мережа Plasma | 7 | 9 | 9 | 9 | 1 | 1 | 4,149263 | 0,398575 |
| Сума | 16,0000 | 23,500 | 24,500 | 25,000 | 2,4762 | 2,4762 | 10,41025 | |

Відношення узгодженості (ВУ) = 2,92%

Таблиця 6.13 – Властивість надмірність

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 1/7 | 1/7 | 1/7 | 1/3 | 1/3 | 0,262066 | 0,035746 |
| PayPal | 7 | 1 | 3 | 1 | 1/3 | 1/3 | 1,151674 | 0,157088 |
| SWIFT | 7 | 1/3 | 1 | 1 | 1/3 | 1/3 | 0,798526 | 0,108918 |
| Visa | 7 | 1 | 1 | 1 | 1/3 | 1/3 | 0,958979 | 0,130804 |
| Мережа Lightning Network | 3 | 3 | 3 | 3 | 1 | 1 | 2,080084 | 0,283722 |
| Мережа Plasma | 3 | 3 | 3 | 3 | 1 | 1 | 2,080084 | 0,283722 |
| Сума | 28,0000 | 8,4762 | 11,143 | 9,1429 | 3,3333 | 3,3333 | 7,331413 | |

Відношення узгодженості (ВУ) = 10,38%

Таблиця 6.14 – Властивість прийняття

| | Мережа Біткоін | PayPal | SWIFT | Visa | Мережа Lightning Network | Мережа Plasma | | НОВП |
|---|---|---|---|---|---|---|---|---|
| Мережа Біткоін | 1 | 1/3 | 1/5 | 1/5 | 3 | 3 | 0,702312 | 0,105444 |
| PayPal | 3 | 1 | 2 | 1 | 1/5 | 1/5 | 0,788319 | 0,118357 |
| SWIFT | 5 | 1/2 | 1 | 1 | 1/5 | 1/5 | 0,681292 | 0,102288 |
| Visa | 5 | 1 | 1 | 1 | 1/5 | 1/5 | 0,764724 | 0,114815 |
| Мережа Lightning Network | 1/3 | 5 | 5 | 5 | 1 | 1 | 1,861936 | 0,279548 |
| Мережа Plasma | 1/3 | 5 | 5 | 5 | 1 | 1 | 1,861936 | 0,279548 |
| Сума | 14,6667 | 12,833 | 14,200 | 13,200 | 5,6000 | 5,6000 | 6,660520 | |

Відношення узгодженості (ВУ) = 51,88%

Проаналізувавши значення попарних альтернатив, і переконавшись, що аналіз зроблено правильно, можна приступати до наступного кроку – вибору схеми з найкращим рівнем безпеки та швидкодії. Результати обчислень глобальних пріоритетів на підставі яких робиться висновок про схему з найкращим рівнем безпеки та швидкодії приведені у таблиці 6.15.

Таблиця 6.15 – Результати обчислень глобальних пріоритетів

| Альтернативи | Критерії | | | | | | Глобальні пріоритети |
|---|---|---|---|---|---|---|---|
| | Відкритість | Децентралізація | Анонімність | Швидкість | Надмірність | Прийняття | |
| | Чисельне значення вектора пріоритету | | | | | | |
| | 0,086067 | 0,111783 | 0,182226 | 0,343619 | 0,209322 | 0,066983 | |
| Мережа Біткоін | 0,128402 | 0,335394 | 0,170290 | 0,086976 | 0,035746 | 0,105444 | 0,124006 |
| PayPal | 0,032270 | 0,033200 | 0,043909 | 0,043163 | 0,157088 | 0,118357 | 0,070131 |
| SWIFT | 0,022374 | 0,033200 | 0,043909 | 0,038454 | 0,108918 | 0,102288 | 0,056502 |
| Visa | 0,046541 | 0,033200 | 0,043909 | 0,034258 | 0,130804 | 0,114815 | 0,062561 |
| Мережа Lightning Network | 0,385207 | 0,298802 | 0,348992 | 0,398575 | 0,283722 | 0,279548 | 0,345222 |
| Мережа Plasma | 0,385207 | 0,266203 | 0,348992 | 0,398575 | 0,283722 | 0,279548 | 0,322853 |

Обчислення були зроблені в окремому документі-таблиці [52], яка містить усі використані формули. На підставі цієї таблиці можна обчислювати будь-які матриці попарних порівнянь для альтернатив.

Відповідно до отриманих результатів можна зробити висновок, що мережа з кращим рівнем безпеки та швидкодії – Lightning Network.

Для об'єктивної оцінки доцільності використання тієї чи іншої платіжної системи необхідно враховувати контекст використання мережі для конкретного випадку - це варто залишити користувачам продуктів. Мережа Lightning Network дозволяє успішно оперувати кріптовалютнимі активами, проте отримані децентралізованості і відкритості досягаються за допомогою використання інших механізмів. Виходячи з проведеного порівняльного аналізу проект Lightning Network характеризується більш безпечними показниками за всіма критеріями ніж подібні системи.

На основі результатів проведеного порівняльного аналізу проект Lightning Network характеризується більш безпечними показниками та кращими показниками скорості ніж подібні сучасні та перспективні платіжні системи.

# ВИСНОВКИ

Централізована платіжна система система має низку корисних властивостей. Керувати такою системою легко та зазвичай відомо, хто несе відповідальність за її роботу. Рішення в таких системах зачасту приймаються швидко. Найбільшого поширення в області централізованих платіжних систем отримав PayPal, одна одна із найбільших електронних платіжних систем у світі, яка володіє такими властивостями як: миттєві перекази в будь-яку країну світу; реєстрація клієнта за допомоги його адреси електронної пошти; забезпечення збереження особистих даних користувача, розрахунки між учасниками здійснюються всередині системи; можливості PayPal з купівлі в іноземних інтернет-магазинах. Наразі послугами PayPal користуються 164 мільйони клієнтів. Та є і ряд проблем такі як відсутність одного правила перерахунку комісій, дані клієнтів надаються третім особам, обмеження на виведення грошей, прив'язка до особистості (при виведенні коштів потрібно надсилати паспортні дані), які потребують вирішення, а саме за допомогою децентралізації.

Децентралізовані платіжні системи мають великий потенціал використання сучасним суспільством. Із використанням технології для забезпечення анонімності в таких системах сучасні соціальні, економічні та фінансові механізми здатні кардинально змінити свій підхід до роботи.

Найпопулярніша криптовалюта на сьогодні – біткоін, є псевдоанонімною, здатна внести свій вклад в розвиток фінансової індустрії. Найважливішими властивостями Біткоін є: прозора історія транзакцій, колективне оновлення бази даних з транзакціями, самостійне управління ключами доступу, ризики роботи з ключами і ПО користувачі несуть самі. Біткоін працює без деяких обмежень, які властиві традиційним платіжним системам і цифровим валютам. Він доповнює фінансову систему, показуючи, що альтернативні варіанти архітектури можуть існувати без головної керуючої організації. Але враховуючи потреби країн, що розвиваються, ця криптовалюта не може задовольнити їх у всіх сферах. Крім

цього біткоін не має ряду важливих для цих стран властивостей, зокрема забезпечення швидкодії при здійсненні платежів.

В ході проведеної роботи здійснено аналіз нововведеної технології Lightning Network. Технологія Lightning Network, дозволяє мережі Біткоін виконувати мільйони транзакцій у секунду (зараз 5).

У магістерській роботі порівнянно властивості сучасних і перспективних систем. Була розроблена формалізована методика, показниками якої виступають критерії для забезпечення безпеки та швидкодії. В якості основних критеріїв для порівняння було обрано: відкритість, децентралізація, анонімність, швидкість, надмірність, прийняття. Для проведення ефективного аналізу для порівняння було обрано платформи Біткоін, Lightning Network, Plasma, PayPal, SWIFT, Visa.

За результатами досліджень було виявлено та доцільно підтверджено, що Lightning Network задовольняє найбільшій кількості властивостей для забезпечення безпеки та швидкодіх мережі. Отримані результати демонструють, що платіжна система Lightning Network показала найліпші результати з усіх інших запропонованих систем.

Крім цього була розроблена методика порівняння вище описаних мереж. Для вирішення цього завдання було застосовано метод аналізу ієрархій Т.Сааті. Проаналізувавши результати розрахунків методу ієрархій був зроблений висновок, що показники Lightning Network є найкращими, тож ця схема забезпечує найвищий рівень безпеки. Також проведені аналізи дозволяють зробити висновки про те, що проект  Lightning Network характеризується більш кращими показниками скорості проведення транзаукцій ніж подібні сучасні та перспективні платіжні системи.

Подальшими перспективними завданнями для дослідження є оптимізація протоколу Lightning Network, що дозволить реалізувати головну Біткоін мережу. Технологія  Lightning Network має перспективу привести світове співтовариство до масового прийняття Біткоін, демонструючи функціональність і надійність мережі. У разі успіху, який Біткоін Lightning Network зможе втілити ідею Сатоши Накамото про p2p-гроші з миттєвими перекладами і низькими комісіями.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Blockchain 101. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.coindesk.com/learn/blockchain-101/what-is-blockchain-technology (01.07.19)
2. Кравченко П. Блокчейн і децентралізовані системи / П. Кравченко, Б. Скрябін, О. Дубініна // сб. − 2018 – С. 47. (05.07.19)
3. Top 5 Blockchain Use Cases In Real World. 2019. // [Електронний ресурс]. – Режим доступу URL: https://dev.to/decipherzonesoft/top-5-blockchain-use-cases-in-real-world-47l6 (10.07.19)
4. CoinMarketCap. 2019. Top 100 Cryptocurrencies by Market Capitalization. // [Електронний ресурс]. – Режим доступу URL: https://coinmarketcap.com/ (12.07.19)
5. Blockchain And Crypto Deals Are Down Sharply In 2019. // [Електронний ресурс]. – Режим доступу URL: https://news.crunchbase.com/news/blockchain-and-crypto-deals-are-down-sharply-in-2019/ (14.07.19)
6. Ukraine launches big blockchain deal with tech firm Bitfury. 2016. // [Електронний ресурс]. – Режим доступу URL: https://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2 (17.07.19)
7. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments / Joseph Poon, Thaddeus Dryja – K. : 2016. – С. 5 – 54. (25.07.19)
8. Павел Кравченко. 2017. Как криптовалюты и блокчейн изменят персональные финансы. Fi.новости. // [Електронний ресурс]. – Режим доступу URL: https://news.finance.ua/ru/news/-/410285/pavel-kravchenko-kak-kriptovalyuty-i-blokchejn-izmenyat-personalnye-finansy (27.07.19)
9. Regulation of Cryptocurrency: Japan. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.loc.gov/law/help/cryptocurrency/japan.php (01.08.19)

10. License for Operation with Cryptocurrency in Croatia. 2019. // [Електронний ресурс]. – Режим доступу URL: https://lawstrust.com/en/licence/finance/crypto-license/hr (98.08.19)
11. Центробанк Китая запретил криптовалюты. 2017. // [Електронний ресурс]. – Режим доступу URL: https://korrespondent.net/business/economics/3882967-tsentrobank-kytaia-zapretyl-kryptovaluity (10.08.19)
12. The Wall Street Journal. 1889. // [Електронний ресурс]. – Режим доступу URL: https://www.wsj.com/ (15.08.19)
13. Deloitte. 1845. // [Електронний ресурс]. – Режим доступу URL: https://www2.deloitte.com/ (16.08.19)
14. PricewaterhouseCoopers. 1998. // [Електронний ресурс]. – Режим доступу URL: https://www.pwc.fr/ (17.08.19)
15. All Bitcoin Forked Coins List With Dates & Tips To Claim Them. 2019. // [Електронний ресурс]. – Режим доступу URL: https://coinsutra.com/bitcoin-forked-coins-list-dates-claim/ (21.08.19)
16. Visa. 1958. // [Електронний ресурс]. – Режим доступу URL: http://www.visa.com/ (28.08.19)
17. Don Tapscott, Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott, Alex Tapscott Blockchain – K. : Information Systems, 2016 – С. 100 – 150. (01.09.19)
18. Social Networking Sites // [Електронний ресурс]. – Режим доступу URL: https://makeawebsitehub.com/social-media-sites/ (03.09.19)
19. Кравченко П. Блокчейн і децентралізовані системи. Частина 2 / П. Кравченко, Б. Скрябін, О. Дубініна // сб. − 2019 – С. 55. (05.09.19)
20. Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6 (07.09.19)
21. R3. 2018. Blockchain for business. // [Електронний ресурс]. – Режим доступу URL: https://www.r3.com/ (08.09.19)

22. Nasdaq. 2015. Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology. // [Електронний ресурс]. – Режим доступу URL: http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326 (08.09.19)
23. Blockchain Laws and Regulations | USA | GLI. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa (09.09.19)
24. PayPal Developer Documentation. 2019. // [Електронний ресурс]. – Режим доступу URL: https://developer.paypal.com/ (11.09.19)
25. PayPal spikes 7% as company teases future of Venmo, adds 6.6 million active users. 2016. // [Електронний ресурс]. – Режим доступу URL: https://venturebeat.com/2016/01/27/paypal-spikes-7-as-company-teases-future-of-venmo-adds-6-6-million-active-users/ (11.09.19)
26. Когда в Украине появится Paypal. 2019. // [Електронний ресурс]. – Режим доступу URL: https://nv.ua/opinion/paypal-v-ukraine-kogda-poyavitsya-vozmozhnost-vyvesti-dengi-novosti-ukrainy-50033726.html (12.09.19)
27. SWIFT – The global provider of secure financial messaging services. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.swift.com/ (14.09.19)
28. How the SWIFT System Works / Shobhit Seth - K.: 2016. - C. 25. (14.09.19)
29. Что такое SWIFT платежи. 2016. // [Електронний ресурс]. – Режим доступу URL: http://privatbank-card.com.ua/article/chto_takoe_swift_platezhi (14.09.19)
30. Satoshi Nakamoto. Bitcoin.org 2015. Bitcoin: A Peer-to-Peer Electronic Cash System. // [Електронний ресурс]. – Режим доступу URL: https://bitcoin.org/bitcoin.pdf (17.09.19)
31. What to do when your credit card is lost. 2018. // [Електронний ресурс]. – Режим доступу URL: https://www.creditcards.com/credit-card-news/emergency-credit-card-replacement-1267.php (18.09.19)

32. Ghassan O. Karame. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin / Ghassan O. Karame, Elli Androulaki, Srdjan Capkun – K. : 2010 – С. 2 – 17. (20.09.19)
33. Соглашения с пользователем в отношении услуг PayPal. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.paypal.com/ru/webapps/mpp/ua/useragreement-full (21.09.19)
34. Adam Back. Hashcash - A Denial of Service Counter-Measure / Adam Back – K. : 2002. – С. 1 – 10. (22.09.19)
35. Wei Dai. B-Money / Wei Dai – K. : 1998. – С. 1 – 2. (22.09.19)
36. Ben Laurie. “Proof-of-Work” Proves Not to Work / Ben Laurie, Richard Clayton – K. : 2004. – С. 1 – 9. (22.09.19)
37. bitcoin/bitcoin: Bitcoin Core integration/staging tree. 2019. // [Електронний ресурс]. – Режим доступу URL: https://github.com/bitcoin/bitcoin (24.09.19)
38. 10 Best Bitcoin Payment Gateways for 2020. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.devteam.space/blog/10-best-bitcoin-payment-gateways/ (25.09.19)
39. D. Brown. Generic groups, collision resistance, and ECDSA. «Codes and Cryptography» / D. Brown – K. : 2005. – С. 2 – 21. (25.09.19)
40. Blockchain.info. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.blockchain.com/explorer (26.09.19)
41. Coinbase. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.coinbase.com/ (26.09.19)
42. Британец случайно выбросил жесткий диск с биткойнами на сумму в 75 млн долларов. 2017. // [Електронний ресурс]. – Режим доступу URL: https://thebusinesscourier.com/ru/britanec-sluchajno-vybrosil-zhestkij-disk-s-bitkojnami-na-summu-v-75-mln-dollarov (28.09.19)
43. Joseph Poon. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments / Joseph Poon, Thaddeus Dryja – K. : 2016. – С. 2 – 59. (02.10.19)

44. Lightning Network. Scalable, Instant Bitcoin/Blockchain Transactions. 2019. // [Електронний ресурс]. – Режим доступу URL: https://lightning.network/ (02.10.19)
45. What Is Lightning Network And How It Works. 2018. // [Електронний ресурс]. – Режим доступу URL: https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works (04.10.19)
46. Tor/ 2018. // [Електронний ресурс]. – Режим доступу URL: https://www.torproject.org/ (05.10.19)
47. What Is Lightning Network? 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.binance.vision/blockchain/what-is-lightning-network (06.10.19)
48. Ethan Heilman. TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub / Ethan Heilman, Leen AlShenibr, Foteini Baldimtsi – K. : 2016. – С. 2 – 36. (08.10.19)
49. Joshua Lind. Teechan: Payment Channels Using Trusted Execution Environments / Joshua Lind, Ittay Eyal, Peter Pietzuch – K. : 2016. – С. 2 – 14. (10.10.19)
50. Hendrik Schulze. Internet Study 2008/2009 / Hendrik Schulze, Klaus Mochalski – K. : 2008. – С. 2 – 14. (12.10.19)
51. WeChat. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.wechat.com/ (12.10.19)
52. OpenBazaar. 2019. // [Електронний ресурс]. – Режим доступу URL: https://openbazaar.org/ (12.10.19)
53. Платежные системы: Visa против Bitcoin. 2019. // [Електронний ресурс]. – Режим доступу URL: https://decenter.org/ru/platezhnye-sistemy-visa-protiv-bitcoin (14.10.19)
54. Aggelos Kiayias. A Composable Security Treatment of the Lightning Network / Aggelos Kiayias, Orfeas Stefanos Thyfronitis Litos1 – K. : 2019. – С. 1 – 84. (16.10.19)

55. The University of Edinburgh. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.ed.ac.uk/ (16.10.19)
56. IOHK: Input Output. 2019. // [Електронний ресурс]. – Режим доступу URL: https://iohk.io/en/ (16.10.19)
57. Katz J. Introduction to Modern Cryptography, Second Edition / Katz J., Lindell Y – K. : 2015. – С. 1 – 84. (23.10.19)
58. Nicolosi A. Proactive Two-Party Signatures for User Authentication. In Proceedings of the Network and Distributed System Security Symposium / Krohn M. N., Dodis Y., Mazières D. – K. : 2003. – С. 1 – 106. (25.10.19)
59. Joseph Poon. Plasma: Scalable Autonomous Smart Contracts / Joseph Poon, Vitalik Buterin – K. : 2017. – С. 1 – 45. (03.11.19)
60. Simplifying the Plasma Whitepaper. 2017. // [Електронний ресурс]. – Режим доступу URL: https://medium.com/@robertgreenfieldiv/simplifying-the-plasma-whitepaper-3b8a4be2bc57 (05.11.19)
61. White paper on the future of plasma science and technology in plastics and textiles. 2018. // [Електронний ресурс]. – Режим доступу URL: https://onlinelibrary.wiley.com/doi/full/10.1002/ppap.201700228 (10.11.19)
62. Plasma как решение проблемы масштабирования Ethereum. 2018. // [Електронний ресурс]. – Режим доступу URL: http://chainmedia.ru/articles/how-plasma-works/ (12.11.19)
63. Виталик Бутерин представил решение для масштабирования системы Plasma. 2018. // [Електронний ресурс]. – Режим доступу URL: https://forklog.com/vitalik-buterin-predstavil-reshenie-dlya-masshtabirovaniya-sistemy-plasma/ (14.11.19)
64. Altcoin - White Label Decentralized Exchange. 2018. // [Електронний ресурс]. – Режим доступу URL: https://altcoin.io/ (16.11.19)
65. Test the future of crypto trading with our latest Plasma DEX. 2018. // [Електронний ресурс]. – Режим доступу URL: https://blog.altcoin.io/test-the-future-of-crypto-trading-with-our-latest-plasma-dex-c2580449af43 (18.11.19)

66. Plasma - Definition | Binance Academy. 2019. // [Електронний ресурс]. – Режим доступу URL: https://www.binance.vision/glossary/plasma (19.11.19)
67. Elements of Proof of Fraudulent Practices. 2019. // [Електронний ресурс]. – Режим доступу URL: https://guide.iacrc.org/elements-of-proof-of-fraudulent-practices/ (21.11.19)
68. Предпосылки создания Lightning Network и сравнительный анализ с другими платежными системами. 2017. // [Електронний ресурс]. – Режим доступу URL: https://forklog.com/predposylki-sozdaniya-lightning-network-i-sravnitelnyj-analiz-s-drugimi-platezhnymi-sistemami/ (22.11.19)
69. Томас Л. Саати. 2015. Об измерении неосязаемого. Подход к относительным измерениям на основе главного собственного вектора матрицы парных сравнений. // [Електронний ресурс]. – Режим доступу URL: https://cloudofscience.ru/sites/default/files/pdf/CoS_2_5.pdf (24.11.19)
70. Stud. 2018. Метод аналізу ієрархій Т. Сааті. // [Електронний ресурс]. – Режим доступу URL: http://stud.com.ua/25063/menedzhment/metod_analizu_iyerarhiy_saati (24.11.19)
71. ADX.semestr. 2018. Метод анализа иерархий. // [Електронний ресурс]. – Режим доступу URL: https://axd.semestr.ru/upr/hierarchies.php (26.11.19)
72. Обґрунтування вибору схеми з найкращим рівнем безпеки та швидкодії. // [Електронний ресурс]. – Режим доступу URL: https://docs.google.com/spreadsheets/d/1sgWcsJ-kYxajp1XQn0IlgodNADtquOpcwa74LqxbywI/edit?fbclid=IwAR39-soU4OH2d5bGs4C7wwWqCTYNs1lKBtoqvk2I_z4S8LwZDJbanQILJc4#gid=169314180 (06.12.19)