НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

На правах рукопису
УДК 004.04

До захисту допущено
В. о. завідувача кафедри ММСА
О.Л.Тимощук
«___» _____ 2019 р.

Магістерська дисертація

на здобуття ступеня магістра за спеціальністю 122 Комп'ютерні науки
на тему: «Криптографічні алгоритми для генерації ключів на основі технології Blockchain»

Виконав:
студент II курсу, групи КА-83 мп
Панасюк Іван Вікторович _____

Керівник: доцент кафедри ММСА
к.ф.-м.н, доц. Шубенкова І.А. _____

Рецензент: _____

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

Київ
2019

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Рівень вищої освіти — другий (магістерський)
Спеціальність — 122 «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
В. о. завідувача кафедри ММСА
О. Л. Тимощук
«___» _____ 2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту Панасюку Івану Вікторовичу

1. Тема дисертації: «Криптографічні алгоритми для генерації ключів на основі технології Blockchain», науковий керівник дисертації Шубенкова Ірина Анатоліївна, к.ф.-м.н., доцент, затверджені наказом по університету від «08» листопада № 3862-с

2. Термін подання студентом дисертації: 13 грудня 2019 р.
3. Об'єкт дослідження: IT технологія Blockchain, з використанням якої створенні більшість теперішніх криптовалют
4. Предмет дослідження: технологія Blockchain та криптографія
5. Перелік завдань, які потрібно розробити:
1) дослідити технологію Blockchain та принципи роботи Bitcoin;
2) проаналізувати кирптографічні алгоритми, які використовує структура Bitcoin;
3) створити програму, що генерує bitcoin-адресу;
4) розробити стартап-проект з використанням Blockchain для вирішення потреб на сучасному ринку;
5) розробити концептуальні висновки за результатами наукового дослідження
6. Орієнтовний перелік графічного (ілюстративного) матеріалу:
30 слайдів
7. Дата видачі завдання: 05 вересня 2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації
1.	Ознайомлення з літературою за темами : економіка, фінанси, криптографія, інформаційна безпека	18.09.2019—20.09.2019
2.	Дослідження реалізації криптовалюти Bitcoin і технології Blockchain загалом	21.09.2019—30.09.2019
3.	Аналіз та дослідження криптографічних алгоритмів, які використовуються у криптоалюті Bitcoin	31.09.2019—16.10.2019
4.	Створення програми	17.10.2019—25.10.2019
5.	Аналіз використання технології Bloockchain у різноманітних сферах життєдіяльності	26.10.2019—02.11.2019
6.	П’ятий розділ. Стартап-проект	03.11.2019—06.11.2019
7.	Підготовка дисертації	07.11.2019—30.11.2019

Студент І.В.Панасюк

Науковий керівник дисертації І.А.Шубенкова

РЕФЕРАТ

Магістерська дисертація виконана на 66 сторінках, містить 11 ілюстрацій, 25 таблиць.

Тема – Криптографічні алгоритми для генерації ключів на основі технології Blockchain.

Мета дослідження – Проаналізувавши технологію Blockchain та принципи роботи криптовалюти Bitcoin, поглибленно і всебічно розглянути криптографію як спосіб захисту інвестиційних фінансів для збільшення довіри кінцевого користувача до технології Blockchain .

Об’єкт дослідження – технологія Blockchain основуючись на якій створенна більшість із криптовалют.

Предмет дослідження – криптографія.

Наукова новизна – розробка ПО для генерації біткойн адрес.

Продукт підлягає вдосконаленню шляхом прив’язки до будь-якого API(банку, біржи).

ABSTRACT

Master's thesis performed at 66 pages, contains 11 illustrations, 1 supplement.

Thesis – Cryptographic Key Generation Alghoritms in case of Blockchain Technology.

The aim - using the cryptographic algorithms of the blockchain technology, with.

The object of study – blockchain technology, which is base for modern cryptocurrencies.

Purpose of the study - modern cryptography.

Methods - the concept of creating a crypto currency, the principle of BTC.

Scientific novelty – developing software for generating bitcoin addresses

Improving project by connecting any API(banks, exchange).

Зміст

РОЗДІЛ 1 BLOCKCHAIN.....*11*

1.1 Системи керування 12

1.2. Концепція 16

1.2.1. Структура блоку транзакцій.....17

1.2.2.Заголовок.....17

1.2.3. Генезис.....19

1.3. Застосування.....20

1.4. Висновок.....20

РОЗДІЛ 2 BTC.....*21*

2.1. Причини появи криптовалюти 22

2.2. Властивості.....25

2.3. Принцип роботи Bitcoin.....27

2.3. Транзакції 28

2.4. Майнінг.....28

2.5. Висновок.....30

РОЗДІЛ 3 КРИПТОГРАФІЯ.....*31*

3.1. Симетричне шифрування 32

3.2. Асиметричне шифрування 33

3.3. Криптографія з відкритим ключем 35

3.3.1. Концепція приватних та публічних ключів.....36

3.4. Електронний цифровий підпис 41

3.5. Криптографічні хеш-функції.....42

РОЗДІЛ 4 BTC-АДРЕСА ТА ПРИНЦИПИ ЇЇ СТВОРЕННЯ *45*

4.1. Створення Біткоїн-адреси..... 46

4.1.1 Base58 48

4.2. Власна реалізація біткоїн-адреси на мові програмування Java 49

Висновок *52*

РОЗДІЛ 5 СТАРТАП-ПРОЕКТ *53*

5.1. Опис ідеї проєкту 53

5.2.Технологічний аудит ідеї проєкту 54

5.3. Аналіз ринкових можливостей запуску стартап-проєкту 54

5.4. Розроблення ринкової стратегії проєкту 60

5.4. Розроблення маркетингової програми стартап-проєкту 62

5.6. Висновки 64

ПЕРЕЛІК ПОСИЛАНЬ *65*

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

Blockchain

Ланцюжок з формованих блоків транзакцій, який побудований за певними правилами.

Bitcoin

P2P платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних [1].

Біткоїн-адреса

Біткоїн-адреса подібна до фізичної чи електронної адреси. Це єдина інформація, яку необхідно передати тому, хто надсилатиме Вам біткоїни, важлива відмінність полягає у тому, що кожна адреса повинна використовуватись тільки для однієї транзакції [1].

Блок

Це частина ланцюжку блоків, що містить та підтверджує багато транзакцій, що очікують підтвердження [1].

Криптовалюта

Цифрові рахункові одиниці, облік яких децентралізований.

Майнінг

Процес, що передбачає використання апаратних ресурсів комп'ютера з метою виконання математичних розрахунків для підтвердження транзакцій і

забезпечення безпеки мережі Біткоїн. Винагородою за свої послуги майнери можуть збирати комісії за підтверджені ними транзакції - новостворені біткоїни [1]

Ланцюжок блоків

Публічний запис біткоїн- транзакцій у хронологічному порядку. Ланцюжок блоків єдиний для усіх біткоїн-кристувачів [1].

Підпис

Криптографічний цифровий підпис - це математичний механізм, що дозволяє підтвердити право власності [1]

BTC

Загальноприйнята одиниця, що використовується для позначення одного біткоїну [1]

Приватний ключ

Це секретна послідовність певних даних, що дає вам право витрачати цифрову валюту з конкретного гаманця за допомогою криптографічного підпису[1].

P2P

Термін peer-to-peer означає системи, що працюють як організована спільнота, надаючи можливість кожному учаснику безпосередньо взаємодіяти з іншими [1].

ВСТУП

За останні пару років Blockchain почав стрімко набирати популярність.

На сьогоднішній день є успішно працюючі проекти побудовані на базі технології, як Bitcoin – перша децентралізована цифрова валюта без центрального банку або єдиного адміністратора, яку можна надсилати від користувача до користувача в одноранговій біткойн-мережі без необхідності посередників, Brave – захищений та анонімний браузер.

В простому розумінні блокчейн це розподілена бд, де будь-який користувач може підключитися і проводити тразакції. Вони зберігаються в блоках, створенних таким чином, що мінімізуеться вірогідність втручання та корекції інформації після потрапляння її в систему. Тобто головна проблематика яку вирішує блокчейн це безпечність, доступність та мобільність.

Криптовалюти – не один ефективний спосіб використання. Стартапи на базі технології блокчейн мають досить хороший потенціал с експертними оцінками інвестицій на приблизно в декілька мільярдів usd, що складає конкуренцію традиційним ввенчурним інвестиціям.

Саме ця технологія є революційною і може використовуватись у найрізноманітніших сферах життя людини.

РОЗДІЛ 1 BLOCKCHAIN

Blockchain можна охарактеризувати як структуру даних, яка зберігає записи про транзакції та забезпечує безпеку, прозорість та децентралізацію. Ви також можете вважати це ланцюжком або записами, що зберігаються у формах блоків, над якими немає одноосібного керівництввва. Блокчейн - це розподілена книга, яка повністю відкрита для всіх в мережі. Після того, як інформація зберігається в блокчейн, змінити або видалити її вкрай важко.

Кожна транзакція на блокчейні захищена цифровим підписом, що підтверджує її справжність. Завдяки використанню шифрування та цифрових підписів дані, що зберігаються в блокчейні, захищені від несанкціонованих дій і не можуть бути змінені.

Технологія Blockchain дозволяє всім учасникам мережі досягти домовленостей, загальновідомих як консенсус. Всі дані, що зберігаються в блокчейні, записуються цифровим шляхом і мають загальну історію, доступну для всіх учасників мережі. Таким чином усуваються шанси на будь-яку шахрайську діяльність або дублювання транзакцій без необхідності третьої сторони.

Щоб краще зрозуміти блокчейн, розглянемо приклад, коли ви шукаєте варіант відправити трохи грошей своєму другові, який живе в іншому місці. Загальним варіантом, яким ви зазвичай можете скористатися, може бути банк або через додаток для переказу платежів, наприклад PayPal або Paytm. Цей варіант передбачає третю сторону для того, щоб обробити транзакцію, завдяки якій додаткова сума ваших грошей віднімається як плата за переказ. Більше того, у таких випадках ви не можете забезпечити безпеку своїх грошей, оскільки цілком можливо, що хакер може порушити мережу та вкрасти ваші

гроші. В обох випадках страждає саме клієнт. Саме тут приходить на допомогу Blockchain.

Замість використання банку для переказу грошей, якщо ми використовуємо блокчейн у таких випадках, процес стає набагато простішим та безпечнішим. Ніякої додаткової плати не передбачається, оскільки кошти безпосередньо обробляються вами, тим самим усуваючи потребу в третій стороні. Більше того, база даних blockchain є децентралізованою і не обмежується будь-яким єдиним місцеположенням, тобто вся інформація та записи, що зберігаються на blockchain, є загальнодоступними та децентралізованими. Оскільки інформація не зберігається в одному місці, жоден хакер не може зіпсувати інформацію.

1.1 Системи керування

Blockchain – розподілена система, але що ж мається на увазі під цією назвою? Спробуємо розібратися .

На сьогоднішній день є такі системи:

- централізовані;
- децентралізовані;
- розподіленні.

Централізовані системи

Мають єдину точку в якій сконцентрований весь контроль над системою,так звана точка управління (рис. 1.1). Все виконується у цій точці, усі процеси та усі рішення. Такі системи надзвичайно не стійкі, адже деякий збій приводить до повної супинки системи[5].

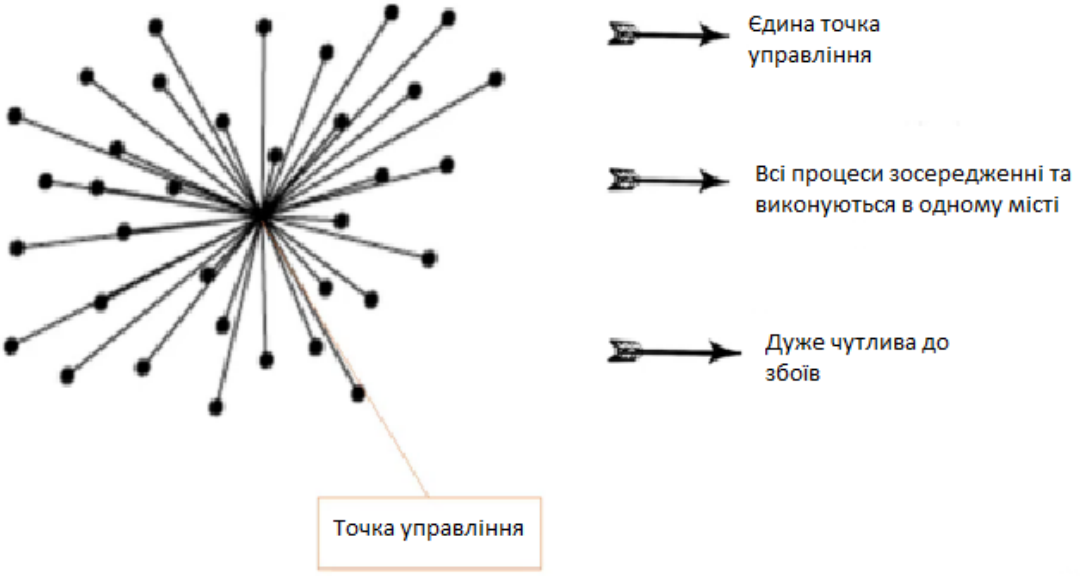

Рисунок 1.1 – Централізована система

Плюси централізованої системи:

1. Легка реалізація, шввидкість рішень через відсутніть конфліктів між точками управління
2. Простота масштабування

Мінуси централізованої системи:

1. Ненадійність через використання лише однієї точки управвління
2. Бюрократичність.
3. Непрозорість.

Децентралізовані системи

Наявні декілька точок управління і присутня диверсифікація повноважень (рис. 1.2). Система стійкіша, вимкненя точки управління не зламає систему.

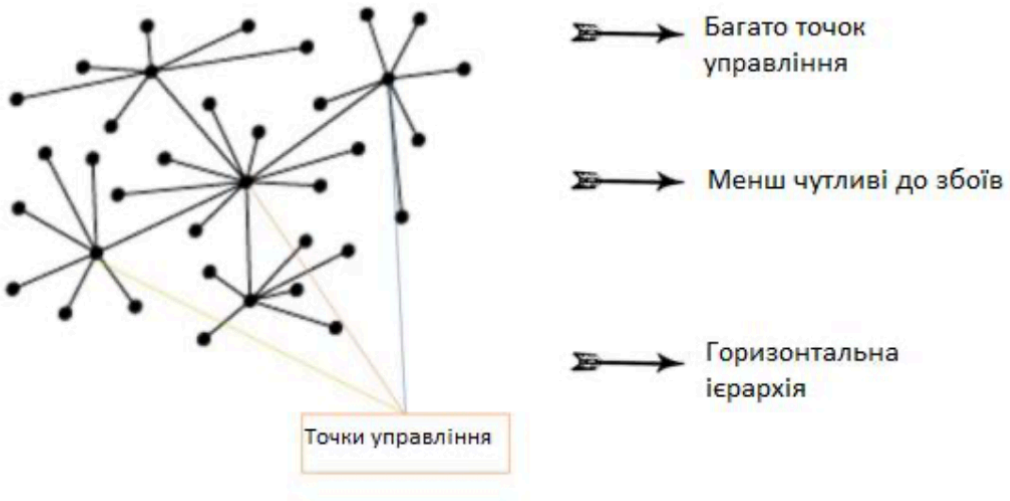

Рисунок 0-1.2 – Децентралізована система

Плюси децентралізованої системи:

1. Більше наближення рішень до користувача.
2. Стійкість.

Мінуси децентралізованої системи:

1. При масштабуванні може з’явитись ефект «дублювання».
2. Більша надійність ніж у централізованих, але не ідеал.

Розподілені системи

Будь-яка точка являється точкою управління (рис. 1.3). Це робить систему майже незворушною. Для виведення з ладу або внесення коректив зловмисники повинні зламати більш ніж 50% точок управління, що практично не можливо.

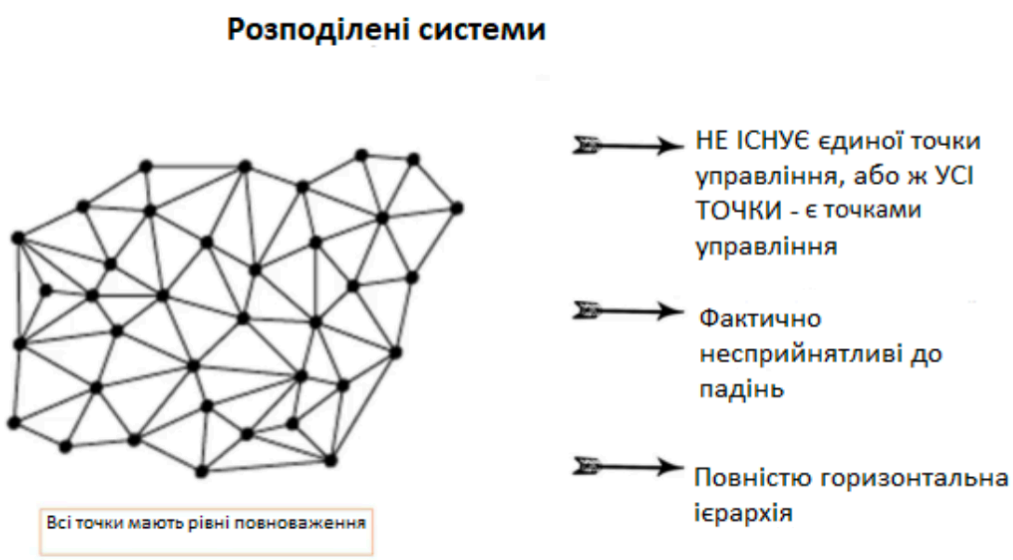

Рисунок 1.3. – Розподілена система

Плюси розподіленої системи:

1. Немає посередників.
2. Через економічну невигідність зламу, найнадійніша.
3. Повна прозорість.

Мінуси централізованої системи:

1. Новітність технології і її постійний розвиток.
2. Дороговизна стабілізації.

Засновуючись на вище ввказаному можна виділити. Blockchain являє собою цифровий децентралізований реєстр, який дає можливість провводити транзакції без участі посередника. Перевагами у порівнянні з іншими платіжними системами є:

- **Відкритість;**
- **Зменшення коммісійних;**
- **Розподіл управління.**

1.2. Концепція

Структура – розподілена база данних, яка зберігає впорядкований ланцюжок блоків, який постійно збільшуеться. Кожен наступний блок зсилаеться на попередній. Blockchain візуалізується як вертикальний стовпчик блоків які знаходяться один на одному та першим блоком, що являє основу для вищестоячих блоків. Така візуалізація приводить до термінів "висота" і "вершина"

Кожен блок оттотожнюється хешем, що створюеться криптографічним алгоритмом SHA256, при застосуванні до заголовка. Кожен блок містить хеш свого попереднього блоку всередині власного заголовка. Хеші, що зв'язують блоки створюють ланцюг до першого блоку (блок генезису). Блок може мати тільки одного батька, але кількість дочірніх блоків не обмежуеться одним.

Зміни хешу блоку потребують зміни хешів попередніх блоків що привводить до так званого каскадного ефекту, тобто якщо блок має за собою велику кількість блоків то він не може бути заміненим без перерахунку хешів наступних блоків, що в свою чергу потребує надзвичайно великих об’ємів перерахунків. Це нас привводить до секрету безпеки.

1.2.1. Структура блоку транзакцій

Найпростіша одиниця в blockchain - блок. Блок складається із Head(заголовок), у ньому метадані та списку транзакцій (Рис.1.4.).

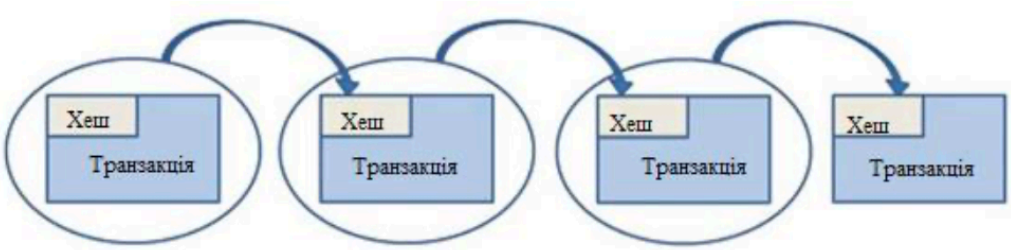

Рисунок 1.4. – Блок транзакцій

Записані в блокчейн блоки змінити неможливо, а редагування інформації (транзакцій) заборонено. Дозволено тільки дописувати нові блоки. Це важлива властивість надійності.

1.2.2.Заголовок

Заголовок блоку вміщає в себе:

- версію блоку;
- дату і час створення блоку;
- хеш-код заголовка блоку;
- хеш-код попепереднього блоку;
- хеш-код всіх транзакцій в блоці;
- спеціальні параметри nonce і bits, які записуються при Майнінгу.

Хеш заголовка блоку є зв’язківцем між попереднім і подальшим блоком.

Хеш транзакцій вираховується за допомогою алгоритму - дерево Меркла (Merkle tree) (Рис.1.5.)

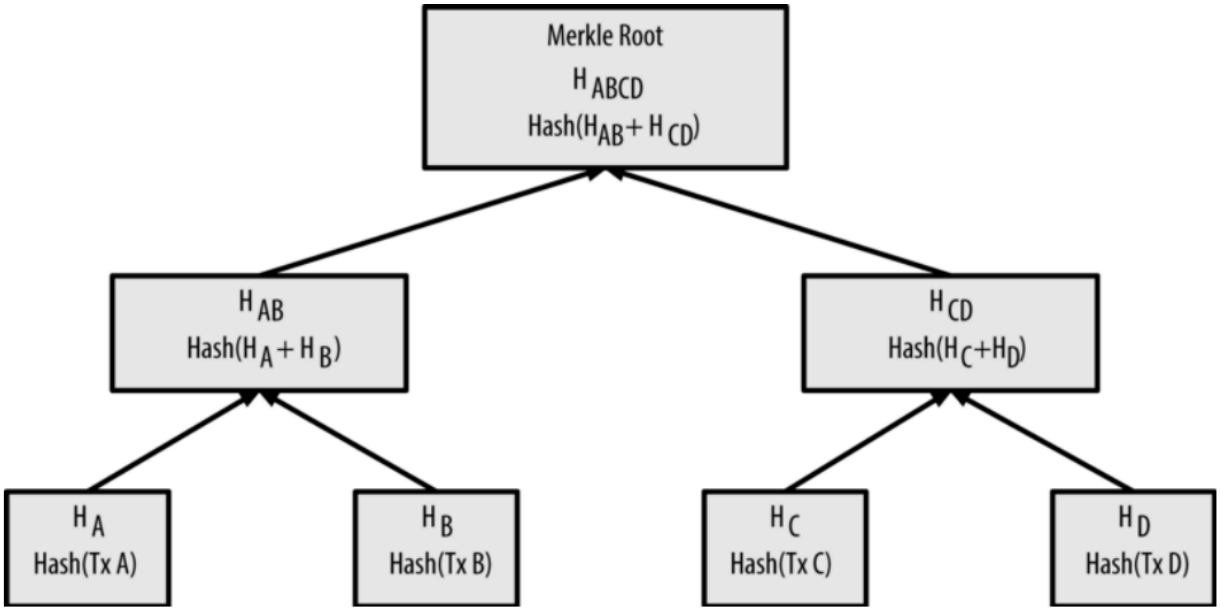

Рисунок 1.5 – дерево Меркла

Працює це так:

1. Підраховуються хеші всіх транзакцій.
2. Рахується сума від усіх хеш пар транзакцій.
3. Рахуються хеші від суми отриманих хеш пар і так далі по тій же системі, поки не отрмаємо один єдиний хеш-код, який і буде хешем транзакцій в блоці.

Заголовки дають змогу відслідкувати цілісність вмісту блоків.

Транзакція схематично виглядає так:

3 < address 1> відправник <N> біткоїнів на < address 2>¶

1.2.3. Генезис

3 січня 2009 року анонімний розробник під іменем Satoshi Nakamoto створив історію, коли він (або вона, або вони) випустили на Sourceforge блок Genesis, оригінальний блок, що містить перші 50 біткойнів. На відміну від будь-якого з 502 000+ блоків, які з’явилися після, Накамото залишив повідомлення в коді блоку:

"The Times 03 / січня / 2009, канцлер на межі другого порятунку для банків"

Цей рядок випливає із заголовка статті London Times від 3 січня 2009 р. Хоча Накамото ніколи чітко не висловлював сенс повідомлення, багато хто трактував це як посилання на те, чому Накамото розробив біткойн: вирізати банки та посередників, які він вважав корумпованими та недостовірними, вирішивши створити валюту, керовану людьми.

Блок Генезису – не може бути зміненим, тому це початкова лінія для всіх подальших блоків, йому у відповвідність іде такий хеш[2](Рис 1.6)

```
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

Рисунок 1.6 – хеш блока генезису

1.3. Застосування

Наразі у більшості людей технологія блокчейн ассоціюється тільки з криптовалютами, але чи це є правдою? Авжеж – ні.

Данна техннологія має постійний шалений розвиток і має потенціал застосування у сферах де необхідні меньші витрати, ефективність та надійність:

- ***управління ідентифікаційної інформацією;***
- ***цифрові активи і токенізація;***
- ***міжнародні платежі;***
- ***захист авторського права;***
- ***смарт-контракти;***
- ***електронне голосування.***

1.4. Висновок

Данний розділ привідкриває базові поняття блокчейн, аналізує його переваги та недоліки, та дає відповвіді на те чому блокчейн перспективна автономна та надійна система

РОЗДІЛ 2 BTC

Біткоїн відрізняється від усього що ви знаете і використовуете щодня.

BTC - це абревіатура Bitcoin. Тобто, Bitcoin називають BTC. Біткойн - це цифрова валюта або онлайн фінансова система. Біткойни також відомі як криптовалюта. Біткоїни використовують криптографію для заходів безпеки. Криптографія захищає біткойни від заходів підробки. Криптографія також дозволяє біткоінам працювати незалежно від центрального банку.

Термін Bitcoin походить від двох слів, біт і монета. Біткойни - це платіжна система з цифровим керуванням, яка працює в системі P2P. Передача або транзакції біткойнів здійснюються з одного гаманця Bitcoin в інший Bitcoin гаманець. Жоден посередник не потрібен для передачі або транзакції біткойнів, і він може бути переданий безпосередньо від однієї особи до іншої особи.

Кожен гаманець Bitcoin має секретний фрагмент даних, який називається seed, необхідний для підписання трансакції Bitcoin, відкривши конкретний гаманець Bitcoin. Також служить для того, щоб математично довести, що біткойни були передані з конкретного гаманця Bitcoin.

Записи транзакцій вводяться в блоки Bitcoin. Ланка Bitcoin Blocks служить ланцюжком. Цей ланцюжок блоків Bitcoin називається Blockchain. Кожен запис, зроблений у блоці Bitcoin, є постійним. Вони безповоротні і не руйнуються.

2.1. Причини появи криптовалюти

Для розуміння причин створення, а також перспективності та революційності цифрових криптовалют потрібно розглянути концепції інших платіжних систем і виявити їх сильні та слабкі сторони.

Бартерна платіжна система

Система бартеру - старий метод обміну. Ця система використовується століттями і задовго до винайдення грошей. Люди обмінялися послугами та товарами на інші послуги та товари. Сьогодні бартер повернувся з використанням прийомів, які є більш досконалими для сприяння торгівлі, наприклад, Інтернет. Цінність предметів бартеру може бути узгоджена з іншою стороною. Бартер не передбачає грошей, що є однією з переваг. Ви можете придбати предмети, обмінявши предмет, який у вас є, але більше не потрібний. Як правило, торгівля таким чином здійснюється через Інтернет-аукціони та ринки своп.

Як і у більшості речей у бартеру, є і недоліки, і переваги. Ускладненням бартеру є визначення надійності людини, з якою ви торгуєте. Інша особа не має жодних доказів чи сертифікатів, і немає захисту споживачів чи гарантій. Це означає, що послуги та товари, якими ви обмінюєтесь, можна обміняти на погані або несправні товари. Ви б не хотіли обмінювати іграшку, яка є майже новою та в ідеальному робочому стані на іграшку, яка не працює взагалі? Для хорошого бартеру потрібні навички та досвід. Часом легко вважати, що потрібний вам предмет коштує більше, ніж є насправді, і недооцінювати цінність вашого власного предмета.

З позитивної сторони є великі переваги для бартеру. Як згадувалося раніше, вам не потрібні гроші для бартеру. Ще однією перевагою є те, що є

гнучкість у бартерному обміні. Наприклад, пов'язаними товарами можна торгувати, такими як портативні планшети в обмін на ноутбуки. Або предметами, які є абсолютно різними, такими як газонокосарки та телевізори. Зараз будинки можна обміняти, коли люди подорожують, що може заощадити гроші обох сторін. Наприклад, якщо у ваших батьків є друзі в іншому штаті, і їм потрібно десь залишитися, перебуваючи у сімейних канікулах, їхні друзі можуть обміняти свій будинок на тиждень або близько того в обмін ваші батьки дозволяють їм користуватися вашим домом.

Ще одна перевага бартеру полягає в тому, що вам не доведеться розлучатися з матеріальними предметами. Натомість ви можете запропонувати послугу в обмін на товар. Наприклад, якщо у вашого друга є скейтборд, який ви хочете, і його велосипед потребує ремонту, можете запропонувати поправити їх велосипед в обмін на скейтборд. За допомогою бартеру дві сторони можуть отримати одне від когось, що хочуть або потребують, не витрачаючи грошей.

Монетна платіжна система

Ця система вирішувала кардтинальну проблему бартерної системи – відсутність стабільної одиниці.. Золоті запаси обмежені, що приводить до постійного росту попиту, через вічну обмеженість пропозиції. Золото просто транспортувалось, і відпала потреба у транспортуванні речей для бартера.

Проте суттєві мінуси перешкоджували подальшому використанню золота. Головним недоліком є добування самого ресурсу, досить тяжка праця. Іншим недоліком являється гнучкість, яка не досягала того рівня, що мають паперові гроші в сьогоденні. І нарешті, останнім але не найменш важливим недоліком є безпека, адже монети досить легко вкрасти, таким чином не вирішувалась найголовніша проблематика бартеру, а саме - безпека

Це призвело до появи посередників у вигляді банків, які почали давати розписки, котрі людина могла обміняти на товари чи послуги, проте все одно не вирішувалась проблема зав’язки на золоті.

Паперова платіжна система

Ця система стала популярною через вирішення багатьох проблематик попередніх. Більш просте виробництво і підкріплення таким ресурсом як довіра уряду що їх випускає.

Проте суттєввими недоліками стала та ж сама безпека, адже підробка та викрадення паперових грошей це не досить складна справа. Ще одною проблемою стала інфляція, так як не існує фізичного ресурсу, який підкріплює їх цінність уряд може випустити необмежену їх кількість що буде їх знецінювати.

На мою думку найголовніший недолік паперової системи вв тому, що таким чином не можливо відсліткувати рух грошей.

Чекова платіжна система

Наступною ланкою розвитку платіжних систем стала чекова система. З’явилась найпростіша форма криптографії у вигляді підпису, що давало хоч і невелику, але гарантію безпеки.

Основними недоліками є те, що підпис доволі легко підробити, що кардинально негативно впливає на безпеку. Гнучкість цієї системи далека від досконалості через так зване підтвердження транзакції, що займало доволі тривалий проміжок часу. Також значним недоліком є відсутність гарантій присутності коштів на рахунку виписника чека для завершення угоди.

Платіжна система електронних гаманців

Ця система виглядає досить стабільно та безпечно, адже засоби захисту інформації в сьогоденні продовжують розвиватись. Майже кожен новітній пристрій має засоби захисту, такі як сканер обличчя або сканнер відбитків, що може бути прекрасним засобом ідентифікації для проведення банківських операцій. Досить гнучка та швидка система у порівнянні с іншими. Найголовніше надає можливості відслітковування потоків грошей, що негативно впливає на можливі грошові махінації. Тож в чому недоліки? Основною проблематикою цієї системи є її зав'язка на існуючій фінансовій системі, котра далека від єффективності і «котиться з гори». Саме цей факт сприяв появі криптовалюти біткоїн. Адже наслідком фінансової кризи стала невіра людей у банки, які виступали гарантом і третьою стороною, вони перестали бути непорушною альтернативою для збеігання гошей. Звідци і з'явилася потеба у новій безпечній і гарантованій альтенативі для зберігання грошей. У 2008 році був опублікований документ про біткоін. Він кинув виклик нині існуючій фінансовій системі та показує подуманість цієї концепції

2.2. Властивості

Хочу виділити 5 найважливіших, на мою думку, властивостей біткойна

1. Незворотність - Після підтвердження транзакцію неможливо змінити. Ніким. Не ви, не ваш банк, не президент, не сатоші, не ваш майнер. Якщо ви надсилаєте гроші, ви надсилаєте їх. Ніхто не може вам допомогти, якщо ви направили свої кошти аферистам або якщо хакер викрав їх з вашого комп'ютера.

2. Анонімність - ні транзакції, ні рахунки не пов’язані з реальними особами. Ви отримуєте біткойни за так званими адресами, які випадковим чином представляються ланцюжками приблизно 30 символів. Хоча, як правило, можливо проаналізувати потік транзакцій і з'єднати реального користувача з цими адресами.
3. Швидкість та Глобальність - транзакція майже миттєво поширюється в мережі та підтверджується через пару хвилин. Оскільки вони потрапляють у глобальну мережу комп’ютерів, вони абсолютно байдужі до вашого фізичного місцезнаходження. Не має значення, чи надсилаю я біткойн своєму сусідові чи комусь з іншого боку світу.
4. Безпека - кошти Bitcoin заблоковані в криптографічній системі відкритого ключа(public key). Лише власник приватного ключа може надсилати криптовалюту. Сильна криптографія та магія великих чисел унеможливлює порушення цієї схеми. Біткойн-адреса більш безпечна, ніж форт Нокс.
5. Дозволеність - Вам не потрібно нікого просити використовувати криптовалюту. Це просто програмне забезпечення, яке кожен може завантажити безкоштовно. Після його встановлення ви можете отримувати та надсилати біткойни чи інші криптовалюти. Ніхто не може вам завадити. Тут немає воротаря та третіх сторін.

2.3. Принцип роботи Bitcoin

Як новий користувач, ви можете розпочати роботу з Bitcoin, не розуміючи технічних деталей. Щойно ви встановите на свій комп’ютер або мобільний телефон гаманець Bitcoin(рис 1.7), він генерує вашу першу адресу Bitcoin, ви зможете створити більше, за необхідністю. Ви можете розкрити свої адреси своїм друзям, щоб вони могли вам заплатити або навпаки. Насправді це дуже схоже на те, як працює електронна пошта, за винятком того, що адреси Bitcoin слід використовувати лише один раз.

Рисунок 1.7 – програма-гаманець

Блокчейн - це спільна публічна “книга”, на яку покладається вся мережа Bitcoin. Всі підтверджені транзакції включаються в нього. Це дозволяє гаманцям Bitcoin обчислювати свій витрачений баланс, щоб можна було перевірити нові транзакції, тим самим гарантуючи, що вони фактично належать витратнику. Цілісність та хронологічний порядок блокчейну забезпечуються за допомогою криптографії.

2.3. Транзакції

Транзакція - це передача вартості Bitcoin, яка транслюється в мережу і збирається в блоки. Зазвичай транзакція посилається на попередні результати транзакцій як нові входи транзакції і присвячує всі вхідні значення Bitcoin новим результатам. Операції не шифруються, тому можна переглядати кожну зібрану транзакцію в блоці. Після того, як транзакції отримають достатню кількістю підтверджень, їх можна вважати незворотними.

Усі транзакції видно в блокчейн і їх можна переглядати. Веб-переглядач блоку - це веб-сайт, на якому кожну транзакцію, включену до блокчейну, можна переглядати в людському розумінні. Це корисно для перегляду технічних деталей перевірки платежів.

2.4. Майнінг

Майнінг - це розподілена консенсусна система, яка використовується для підтвердження транзакцій шляхом включення їх у блокчейн. Він здійснює хронологічний порядок, захищає нейтралітет мережі та дозволяє різним комп'ютерам домовлятися про стан системи. Для підтвердження, транзакції повинні бути упаковані в блок, який відповідає дуже суворим криптографічним правилам, які будуть перевірені мережею. Ці правила запобігають зміні попередніх блоків, оскільки це призведе до недійсності всіх наступних блоків. Майнінг також створює еквівалент конкурентної лотереї, яка заважає будь-якій людині легко додавати нові блоки послідовно до ланцюга блоків. Таким чином,

жодна група чи особи не можуть контролювати те, що входить до ланцюга блоків, або замінювати частини ланцюга блоків, щоб відкотити власні витрати.

Випуск нових біткойнів децентралізований, не залежить від будь-якого регулюючого органу (Рис 1.8).

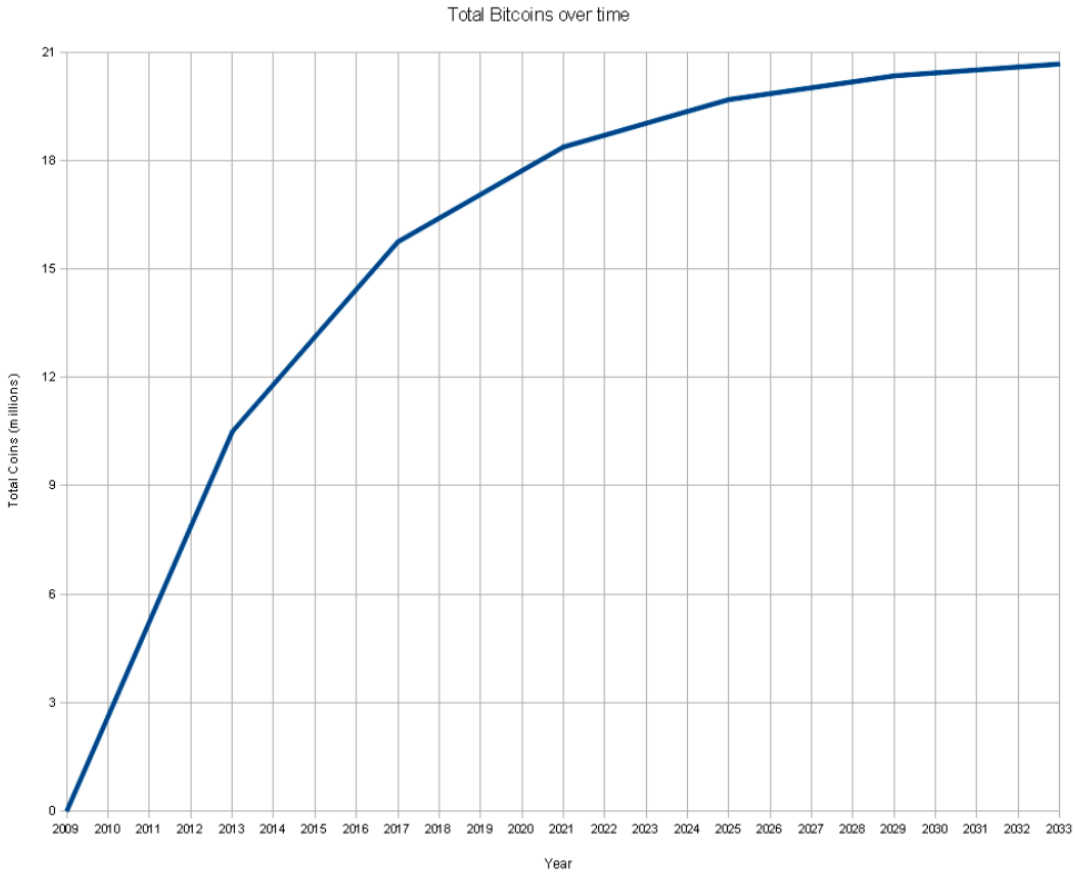

Рисунок 1.8 – кількість BTC

Наразі існує 18 097 475 біткойнів. Це число змінюється приблизно кожні 10 хвилин, коли видобуваються нові блоки. Зараз кожен новий блок додає в обіг 12,5 біткойнів. Максимальна і загальна кількість біткойнів, які коли-небудь можуть існувати, - 21 мільйон. У середньому видобувається 144 блоки в день, а в блоці - 12,5 біткойнів. 144 х 12,5 - 1800, тож це середня кількість нових біткойнів, що видобуваються на день.

Оскільки багато майнерів додають нові хеш-потужності, за останні кілька років блоки часто виявлялися з інтервалом 9,5 хвилини, а не 10. Це створює

нові біткойни швидше, тому в більшості днів насправді створено більше ніж 1800 нових біткойнів.

2.5. Висновок

Виділемо такі риси біткойна.

1. **Низька комісія.**
2. **Завжди доступний.**
3. **Швидкість трранзакцій.**
4. **Безпечність у порівнянні з іншими фінансовими системами.**
5. **Новітність технологій.**
6. **Потенціал можливостей..**
7. **Простота використання.**
8. **Інтернаціональність.**
9. **Відкритість..**
10. **Обхід заборон та санкцій..**
11. **Відсутність посередників.**
12. **Контроль власних коштів**
13. **Анонімність.**
14. **Прозорість.**

РОЗДІЛ 3 КРИПТОГРАФІЯ

Криптографія - це метод захисту інформації та комунікацій за допомогою використання кодів, щоб лише ті, для кого інформація призначена, могли її читати та обробляти.

У комп’ютерних науках під криптографією розуміються захищені інформаційно-комунікаційні методи, отримані з математичних концепцій та набору обчислень, заснованих на правилах, що називаються алгоритмами для перетворення повідомлень способами, які важко розшифрувати. Ці детерміновані алгоритми використовуються для генерації криптографічних ключів, цифрового підписання та перевірки для захисту конфіденційності даних, веб-перегляду в Інтернеті та конфіденційного зв’язку, такого як транзакції кредитними картками та електронною поштою.

Криптосистеми використовують набір процедур, відомих як криптографічні алгоритми або шифри, для шифрування та дешифрування повідомлень для захисту зв'язку між комп'ютерними системами, пристроями, такими як смартфони та додатки. Набір шифрів використовує один алгоритм для шифрування, інший алгоритм аутентифікації повідомлень та інший для обміну ключами. Цей процес, вбудований у протоколи та записаний у програмне забезпечення, яке працює на операційних системах та мережевих комп'ютерних системах, передбачає генерацію відкритих та приватних ключів для шифрування / дешифрування даних, цифрового підпису та перевірки аутентифікації повідомлень та обміну ключами.

У сучасних технологіях широко використовуються три форми шифрування:

- симетричне;
- асиметрична;
- хеш.

3.1. Симетричне шифрування

Симетричне шифрування - це метод криптографії, коли за шифрування та розшифрування даних відповідає один ключ. Зацікавлені сторони діляться цим ключем, паролем або парольною фразою, і вони можуть використовувати його для розшифрування або шифрування будь-яких потрібних повідомлень. Відповідно до проекту безпеки Open Web Application (OWASP), деякі найпоширеніші алгоритми, які використовуються для симетричної криптографії, включають Стандарт шифрування даних (DES), який використовує 56-бітні клавіші, Triple DES, який тричі використовує алгоритм DES з різними ключі; та Розширений стандарт шифрування (AES) - алгоритм, за яким Національний інститут стандартів і технологій США рекомендує нові можливості для безпечного зберігання та передачі даних.

Переваги

- Простота: Цей тип шифрування легко здійснити. Все, що потрібно зробити, - це вказати та поділитися секретним ключем, а потім почати шифрувати та розшифровувати повідомлення.
- Шифруйте та розшифровуйте власні файли: Якщо ви використовуєте шифрування для повідомлень або файлів, до яких

ви самі маєте намір отримати доступ, не потрібно створювати різні ключі. Шифрування одним ключем найкраще для цього.

- Швидкість: Симетричне шифрування ключів набагато швидше, ніж асиметричне шифрування ключа.
- Використовується менше комп’ютерних ресурсів: для шифрування одним ключем не потрібно багато комп'ютерних ресурсів у порівнянні з шифруванням відкритого ключа.

Недоліки

- Необхідність безпечного каналу для обміну секретними ключами: обмін повинен пройти таким чином, щоб ключ залишався таємним.
- Забагато ключів: для спілкування з різними сторонами повинен бути створений новий спільний ключ. Це створює проблему з керуванням та забезпеченням безпеки всіх цих ключів.
- Неможливо гарантувати походження та автентичність повідомлення: оскільки і відправник, і одержувач використовують один і той же ключ, повідомлення не можуть бути підтверджені від конкретного користувача. Це може бути проблемою, якщо є суперечка.

3.2. Асиметричне шифрування

Цей метод шифрування повідомлень використовує два ключі: відкритий ключ та приватний ключ. Публічний ключ стає загальнодоступним та використовується для шифрування повідомлень будь-ким, хто бажає надіслати повідомлення людині. якій належить ключ. Приватний ключ зберігається в

таємниці і використовується для розшифровки отриманих повідомлень. Прикладом асиметричної системи шифрування ключа є RSA.

Переваги

- Зручність: це вирішує проблему розповсюдження ключа для шифрування. Кожен публікує свої відкриті ключі, а приватні ключі зберігаються в секреті.
- Забезпечує автентифікацію повідомлення: шифрування відкритого ключа дозволяє використовувати цифрові підписи, що дає можливість одержувачу повідомлення перевірити, чи є повідомлення справді від певного відправника.
- Виявлення підробок: використання цифрових підписів при шифруванні відкритого ключа дозволяє одержувачу виявити, чи було змінено повідомлення під час транзиту. Цифрово підписане повідомлення не може бути змінено без відміни підпису.
- Невідхильність: цифрове підписання повідомлення схоже на фізичне підписання документа. Це підтвердження повідомлення, і, отже, відправник не може його відмовити.

Недоліки

- Публічні ключі повинні бути засвідчені автентичністю: ніхто не може бути абсолютно впевнений, що відкритий ключ належить особі, яку він вказав, і тому кожен повинен перевірити, що їхні відкриті ключі належать їм.
- Повільне: шифрування відкритого ключа повільне порівняно з симетричним шифруванням. Неможливо використовувати для розшифрування масових повідомлень.

- Використовується більше комп’ютерних ресурсів. Це вимагає набагато більше комп'ютерних запасів порівняно з шифруванням з одним ключем.
- Можливий широкий компроміс із безпекою: Якщо зловмисник визначає приватний ключ людини, його повідомлення можуть бути прочитані.
- Втрата приватного ключа може бути непоправною: втрата приватного ключа означає, що всі отримані повідомлення не можуть бути розшифровані.

3.3. Криптографія з відкритим ключем

Криптографія відкритого ключа - це криптографічна система, яка спирається на пару ключів, приватний ключ, який зберігається в таємниці, і відкритий ключ, який транслюється в мережу. Ця система допомагає забезпечити справжність та цілісність повідомлення, спираючись на передові криптографічні методи.

Ось приклад того, як криптографія відкритого ключа використовується на практиці. Скажімо, користувач A хоче надіслати повідомлення B через ненадійний канал зв'язку, як Інтернет. A використовує криптографію відкритого ключа, генеруючи набір відкритих та приватних ключів. Потім він розміщає свій відкритий ключ до B. Тепер, коли A хоче спілкуватися з B, він додає цифровий підпис до свого повідомлення за допомогою свого приватного ключа. Це доводить, що A є творцем цього повідомлення. B може підтвердити те саме, використовуючи отримане повідомлення та відкритий ключ від A.

Криптографія відкритого ключа є важливою частиною протоколу Bitcoin і використовується в декількох місцях для забезпечення цілісності повідомлень, створених у протоколі. Створення гаманця та підписання транзакцій, які є основними компонентами будь-якої валюти, значною мірою залежать від криптографії відкритого ключа. Протокол Bitcoin використовує алгоритм цифрового підпису Еліптичної кривої (ECDSA) для створення нового набору приватного ключа та відповідного відкритого ключа. Потім відкритий ключ використовується з хеш-функцією для створення публічної адреси, яку користувачі Bitcoin використовують для надсилання та отримання коштів. Приватний ключ зберігається в таємниці і використовується для підписання цифрової транзакції, щоб переконатися, що походження транзакції є законним.

3.3.1. Концепція приватних та публічних ключів

Загальна мета PKC - забезпечити безпечне та приватне спілкування за допомогою цифрових підписів на загальнодоступному каналі, де можуть бути потенційно зловмисні підслуховувачі. У контексті криптовалют метою є довести, що витрачена транзакція справді була підписана власником коштів і не підроблялася, і все це відбувається через загальнодоступну мережу блокчейн.

Коли ви володієте криптовалютами, то, що ви насправді володієте, - це "приватний ключ". Ваш "приватний ключ" відкриває право його власнику витрачати пов'язані з ним криптовалюти. Оскільки він забезпечує доступ до ваших криптовалют, він повинен, як випливає з назви, залишатися приватним.

Окрім приватного ключа, існує також відкритий ключ і існує криптографічний зв’язок між відкритим ключем та приватним ключем. Відновити відкритий ключ можна, якщо у вас є приватний ключ. Однак неможливо знайти приватний ключ, використовуючи лише відкритий ключ.

Відкриті та приватні ключі аналогічні адресі електронної пошти та паролю відповідно.

Користувач А теоретично може створити мільярди відкритих ключів (адрес) зі свого приватного ключа, який у нього є лише один, і функціонує як приватний пароль, який знає лише він - його секрет. Після того як А створює адресу відкритого ключа, ця адреса стає загальнодоступною для всіх користувачів мережі як адреса, куди вони можуть надсилати криптовалюти, такі як Bitcoin. Лише А може отримати доступ до криптовалют, надісланих на цю адресу, оскільки він має відповідний ключ до загальнодоступної адреси.

Приватні ключі створюються досить простим алгоритмом

Крок 1: Створення випадкового набору даних

Нам потрібен криптографічно захищений генератор чисел, щоб генерувати наше число. Для задоволення цієї вимоги нам потрібно генерувати випадковий набір даних, ми перетворимо ці дані в число пізніше.

Наприклад: klajsdnflasdnclksdjanx`knk`bliu3o2ueq[i21pru[qojml;sam`piupo
Крок 2: Перетворення випадкових даних у 256-бітне число

Тепер, коли у нас є випадковий набір даних, ми можемо використовувати SHA256 для перетворення нашого випадкового набору даних у 256 біт.

SHA256 - алгоритм хешування, який отримує будь-які вхідні дані, наші випадкові дані та створює 256-бітний хеш.

Ось SHA256 хеш наших випадкових даних:

526ea43fb1057bb3d2725f17406030c1e1b3a45d126a1de5252e861f1fb957e2

Крок 3: Перевірка номера

Тепер, коли ми створили криптографічно захищене 256-бітове випадкове число, остаточне, що нам потрібно зробити, - це перевірити, чи є наш номер від 1 до 2^{256}.

Наша кількість, хоча і дуже велика, все ж набагато менша за ліміт Bitcoin в 2^{5656}. Це означає, що наш номер відповідає критеріям і тепер його можна використовувати як приватний ключ на Bitcoin.

Крок 4: Додати номер версії

У Bitcoin кожен приватний ключ від основної мережі починається з "5". Це полегшує ідентифікацію приватного ключа. Для того, щоб наш приватний ключ починався з «5», нам потрібно додати 80 до початку нашого шістнадцяткового.

80526ea43fb1057bb3d2725f17406030c1e1b3a45d126a1de5252e861f1fb957e2

Крок 5: Додати 32-бітну контрольну суму

Введення нашого приватного ключа, оскільки він настільки великий, може бути схильним до помилок. Додавання контрольної суми дозволяє виявити будь-які помилки введення тексту, використовуючи наш приватний ключ. Щоб додати контрольну суму до нашого приватного ключа, нам потрібно отримати подвійний хеш SHA256 нашого нового шістнадцяткового числа.

80203d631b56c32d701162a421111315607f87fd704288a81c95b795d18be68217

Крок 6: Перетвореня у base58

Для подальшого запобігання помилок введення тексту нам потрібно перетворити наш приватний ключ із шістнадцяткової у base58. Base58 видаляє легко помилкові буквено-цифрові символи o, O, L та I. Результат - 58 символів, які можна використовувати для представлення нашого приватного ключа.

Ось наш перетворений приватний ключ base58, який включає "5", необхідний для кожного приватного ключа в Bitcoin.

5NtM4AqHpky4pSE7DeonMQRTxCXvBL8PfmXQeWartMFJoNnJQNoJuC
KtWsj4mh2ZbjCaCisYuWFiHXesLbCmo8xCKWN

Криптографія еліптичної кривої

Що таке еліптична крива? Еліптична крива складається з усіх точок, які задовольняють рівнянню наступної форми:

$y^2 = x^3+ax+b$

де $4a^3 + 27b^2 \neq 0$ (це потрібно для уникнення точок сингулярності).

Ось кілька прикладів еліптичних кривих(рис 3-1)

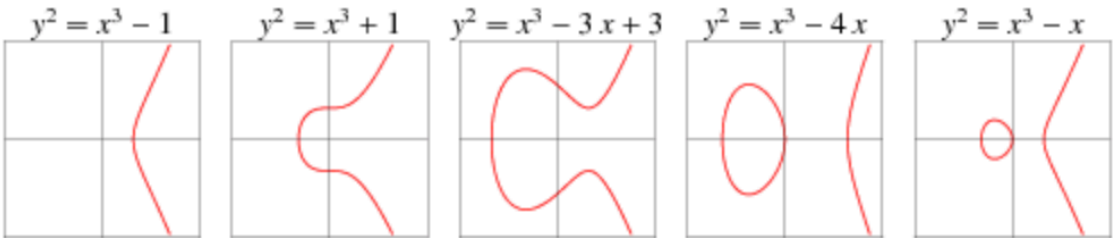

Рисунок 3-1 – еліптичні криві

Приватні та відкриті ключі в криптографії еліптичної кривої

Скажімо, я обчислюю x * P, де x - випадкове 256-бітове ціле число. Результатом буде деяка точка на кривій. Давайте назвемо цю точку X.

Якщо я дам вам X, ви могли б визначити x? Іншими словами, чи можете ви визначити, скільки разів я додав P до себе, щоб отримати точку X на кривій? Припустимо, що ви знаєте, що таке P, і ви знаєте, яку криву я використовував.

Виявляється, вам неможливо визначити x, навіть якщо у вас є суперкомп'ютер. Неіснує алгоритму визначення x, тому ваш єдиний варіант - продовжувати додавати P до себе, поки ви не отримаєте X, або продовжувати віднімати P від X, поки не отримаєте P. В середньому, x буде десь від 0 до 2^{256}-1. Таким чином, вам знадобиться в середньому 2^{128} операції додавання точок, щоб визначити x, незалежно від вашого підходу. Навіть якби ваш комп’ютер міг робити один трильйон операцій додавання за секунду, а ви працювали з комп'ютером з початку Всесвіту, ви б уже зробили лише 2^{98} операції додавання. $2^{98} / 2^{128} = 1/1073741824$.

Припустимо ви почали з середини, ви можете обчислити 2^{128} * P за 510 кроків або менше. В середньому x не ближче до 2^{128} ніж до 2^{256}-, тому що x – рандомне, тож не має різниці де починати, все одно доведеться провести близько 2^{128} операцій.

Тож через те, що ніхто не може x при данному X, де X=x*P, доцільно зробити x приватним ключем, а X публічним ключем. Тоді ваш приватний ключ буде випадковим 256-бітним цілим числом, а ваш відкритий ключ - це координати x- і y- точки на еліптичній кривій. Це може задовольнити таку властивість приватних та відкритих ключів: "Обчислювально неможливо отримати приватний ключ, відповідний даному відкритому ключу".

3.4. Електронний цифровий підпис

Цифрові підписи досить схожі на фактичні підписи на документі. Вони допомагають гарантувати, що автором транзакції є власне особа, яка має приватний ключ. Цифрові підписи є основою Bitcoin і кожна транзакція має різний цифровий підпис, що залежить від приватного ключа користувача. Також, враховуючи повідомлення, відкритий ключ користувача та підпис нетривіально перевіряється чи підпис справжній. Більш формально цифрові підписи залежать від двох функцій:

Знак/Sign(повідомлення, приватний ключ) -> Підпис

З огляду на повідомлення, яке ми хочемо підписати, та приватний ключ, ця функція створює унікальний цифровий підпис для повідомлення.

Перевірити/Verify (повідомлення, відкритий ключ, підпис) -> True / False

Враховуючи повідомлення, яке ми хочемо перевірити, підпис та відкритий ключ, ця функція дає двійковий вихід залежно від того чи підпис справжній

Після підписання власником транзакції транзакція відправляється в пул пам’яті, де вона обробляється майнерами. Майнери використовують відкритий ключ відправника, щоб гарантувати справжність цифрового підпису, щоб хакер не міг витрачати кошти користувача без їх згоди. Якщо право власності та цифровий підпис проходять перевірку, вони включають транзакцію в наступний блок, а гроші надсилаються з одного гаманця в інший.

3.5. Криптографічні хеш-функції

У Bitcoin та більшості інших криптовалют вхід для хеш-функції включає дані про транзакції разом із часовими позначками та іншими відповідними даними. Довжина вихідного хеша визначається відповідно до специфікацій алгоритму. Наприклад, SHA-256 завжди видає хеш довжиною 256 біт.

Хоча хешинг лише нещодавно почав набирати популярність через підвищення популярності блокчейну, цей процес вже використовується і для кількох інших програм, що не відносяться до блокчейн. Зберігання паролів веб-сайту фактично одне з найпоширеніших застосунків криптографічного хешування. Тобто, сучасні веб-сайти виконують процес хешування, щоб запобігти збереженню точної копії пароля користувача на своїх серверах. Таким чином, у разі порушення безпеки, зловмисники просто отримають копію хешей паролів, зменшуючи збитки, заподіяні повномасштабним витіком данних.

Як і більшість математичних процесів, хеш-функції, як правило, різняться за складністю. Більш складний алгоритм хешуваннявання, зробить повний перебір набагато складнішим.

Хоча використання найбільш безпечного в даний час алгоритму може здатися найкращим способом, важливо відзначити, що підвищена складність часто вимагає значно більше часу та обчислювальної потужності. Враховуючи те, що велика кількість криптовалютних ентузіастів вже вважають, що спеціалізований майнінг ASIC негативно впливає на децентралізацію, необхідний баланс між безпекою та зручністю.

Bitcoin використовує криптографічну хеш-функцію SHA-256, яка є абревіатурою для 256-бітного алгоритму Secure Hash. Спочатку алгоритм був розроблений Агенцією національної безпеки США (NSA), ,без намірів

використовувати його для криптовалют. Переваги безпеки цього вільно доступного математичного алгоритму зробили його ідеальним для мережі Bitcoin.

Функція хешування SHA-256 - це насправді один із найскладніших криптографічних алгоритмів, який використують цифрові валюти. Звичайно, конкуренти, що використовують простіший алгоритм, не обов'язково роблять їх менш захищеними. Додаткова складність, ймовірно, є причиною того, чому біткойн встиг простояти вже майже десятиліття і досі, мабуть, є найбільш надійною криптовалютою на ринку.

Незважаючи на те, що SHA-256 є складним за своєю суттю, це не ускладнює впровадження в апаратному відношенні. За своєю суттю виконання хешування за допомогою функції передбачає не що інше, як просту булеву алгебру та 32-бітове додавання, дві задачі, які обчислювальні пристрої надзввичайно ефективвно виконують. Насправді такі кроки є настільки простими, що будь-яка звичайна людина може зробити це також, хоча і набагато повільніше, ніж сучасне майнінг обладнання.

Як було зазначено раніше, не всі криптовалюти розроблені для використання алгоритму хешування SHA-256. Інші криптографічні хеш-функції можуть бути навіть енергоефективвнішими через меншу складність. Scrypt - найвідоміша альтернатива, яку використовують у валютах, таких як Litecoin та Dogecoin.

Алгоритм хешування Scrypt був випущений в 2009 році, того ж року, що і біткойн, і, як правило, віддається перевазі новим криптовалютам, оскільки він швидший і простіший, ніж перевірений SHA-256.

Замість того, щоб покладатися на цифрову логіку, він поєднує 1024 різних хеш-значень у ряді перестановок, щоб в кінцевому підсумку знайти дійсний результат. Мінусом цього підходу є те, що для зберігання такої

кількості значень необхідних для алгоритму призводить до використання великої кількості системної пам'яті, що збільшує витрати на обладнання.

Scrypt, звичайно, не єдиний доступний алгоритм хешу, який часто використовується. Інші альтернативи включають X11, Cryptonight і Dagger Hashimoto, причому один з них має свої унікальні характеристики.

Хоча X11 налаштований в основному на енергоефективність, вимагаючи меншої потужності, Cryptonight призначена для майнінгу виключно за допомогою настільних комп'ютерних процесорів. Існує багато причин, які пояснюють, чому ці альтернативні алгоритми зазвичай обирають для досягнення певної цілі. Наприклад, у випадку Cryptonight, опір на ASIC був важливим фактором при розробці алгоритму, імовірно, щоб тримати децентралізацію в руках користувачів валюти.

Незважаючи на те, що алгоритми криптографічного хешуваннявання розроблені таким чином, щоб протистояти атакам, існує кілька векторів атак, які можуть поставити під загрозу всю мережу криптовалют. З цієї причини нові комп'ютери та математики постійно розробляють та досліджують нові хеш-функції.

РОЗДІЛ 4 BTC-АДРЕСА ТА ПРИНЦИПИ ЇЇ СТВОРЕННЯ

Біткойн-адреса - це 160-бітний хеш публічної частини публічного / приватного ключа ECDSA. Використовуючи криптографію з відкритим ключем, ви можете "підписувати" дані своїм приватним ключем, і кожен, хто знає ваш відкритий ключ, може перевірити, що підпис дійсний.

Для кожної адреси створюється нове ключове слово. Відкритий ключ та пов’язані з ними приватні ключі зберігаються у файлі даних гаманця. Це єдиний файл, який користувачі повинні зберегти. Щоб "надіслати" транзакцію на певну адресу, bitcoin вимагає, щоб відповідний гаманець знав приватний ключ, що їй відповвідає. Якщо ви створите адресу та отримаєте монети за цією адресою, при відновленні гаманця із попередньої резервної копії, до генерації адреси, монети, отримані за цією адресою, втрачаються. Це не проблема для HD-гаманців, де всі адреси генеруються з одного елемента. Адреси додаються до пулу адресних ключів перед тим, як використовуватись для отримання монет. Якщо ви повністю втратите свій гаманець, всі ваші монети будуть втрачені і їх неможливо відновити.

Біткойн дозволяє створювати стільки адрес, скільки вам потрібно, і використовувати нову для кожної транзакції. Немає "головної адреси". Пункт "Ваша біткойн-адреса" в деяких інтерфейсах гаманця не має значення. Це тільки для вашої зручності, і він повинен автоматично змінюватися при використанні.

Біткойн-адреси містять вбудований контрольний код, тому, як правило, не можна надсилати біткойни на неправильну адресу. Однак якщо адреса добре сформована, але її ніхто не має (або власник втратив wallet.dat), будь-які монети, надіслані на цю адресу, будуть загублені назавжди.

Значення хеша та дані контрольної суми перетворюються в алфавітно-числовий вигляд за допомогою спеціальної схеми: схеми кодування Base58Check. У розділі Base58Check адреси можуть містити всі буквено-цифрові символи, крім 0, O, I та l. Нормальні адреси в даний час завжди починаються з 1 (адреси скрипт хешів з 3), хоча це може змінитися в майбутній версії. Адреси тестових мереж зазвичай починаються з m або n. Основні адреси можуть бути довжиною 25-34 символи, а адреси тестової мережі можуть бути довжиною 26-34 символи. Більшість адрес мають довжину 33 або 34 символи.

Оскільки біткойн-адреси в основному є випадковими числами, можливо, хоча і вкрай малоймовірно, що двоє людей самостійно згенерують одну і ту ж адресу. Це називається колізією. Якщо це станеться, то і початковий власник адреси, і власник, що зіткнувся, можуть витратити гроші, надіслані на цю адресу. Але оскільки простір можливих адрес настільки великий, то більша ймовірність, що Земля буде знищена в найближчі 5 секунд, ніж колізія в наступному тисячолітті.

4.1. Створення Біткоїн-адреси

Правильний спосіб створити адресу Bitcoin - це використання добре перевіреного програмного забезпечення з відкритим кодом та програмним забезпеченням для гаманців, що перевіряється. Ручне керування ключами призводить до втрати коштів знову і знову. На відміну від інших централізованих систем, втрати в Bitcoin зазвичай не підлягають відшкодуванню.

Ось короткий огляд того, як працює генерація адрес:

1. наявність приватного ключа ECDSA
2. Візьміть відповідний відкритий ключ, згенерований ним (33 байти, 1 байт 0x02 (y-координата є рівним) і 32 байти, що відповідають координаті X)
3. Виконайте хешування SHA-256 на відкритому ключі
4. Виконайте хешування RIPEMD-160 за результатом SHA-256
5. Додати байт версії перед хешем RIPEMD-160 (0x00 для основної мережі)
6. Виконайте хеш SHA-256 на розширеному результаті RIPEMD-160
7. Виконайте хеш SHA-256 за результатом попереднього хешу SHA-256
8. Візьміть перші 4 байти другого хешу SHA-256. Це контрольна сума адреси
9. Додайте 4 байти контрольної суми з етапу 8 наприкінці розширеного хешу RIPEMD-160 зі стадії 5. Це 25-байтова двійкова біткойн-адреса.
10. Перетворіть результат з байтового рядка в рядок base58 за допомогою кодування Base58Check. Це найпоширеніший формат адреси Bitcoin

4.1.1 Base58

Для подачі числа компактніше комп'ютерні системи застосовують численні системи. Десяткова система використовує 10 цифр від 0 до 9, шістнадцяткова - 16 символів, з цифрами від 0 до 9 та з буквами від A до F. Таке число буде коротшим ніж еквівалентне йому в звичайному вигляді. Для більшої лаконічності використоввують base64. Алфавіт містить 26 великих літер, 26 малих літер, 10 цифр, "+", "/". Base64 застосовують для кодуввання, наприклад, е-пошти. Формат Base58 розроблений для використання в блокчейн та криптовалютах. Надає зручність, компактність та помилкостійкість, за рахунок виключення деяких символів. Є підмножиною base64 і вигляда.ьб практично однаково, проте у base58 відсутні 6 символів: 0, O, L, I, +, /. Це зроблено для надання дотаткової безпеки, адже саме ці символи досить легко сплутати.Base58Check - це Base58 з однією відмінністю, містить вбудований код перевірки помилок.

Найпоширеніші формати ключів, що використовуються у системі (Таблиця 4.1).

Таблиця 4.1 - формати кодування

Тип	Префікс	Опис
Шістнадцятковий	Не має	64 шістнадцятковий чисел
WIF	5	Кодування Base58Check: Base58 з префіксом версії 128 і 32-бітною контрольною сумою
Стислий WIF	K чи L	Те що й вище, але з додаванням суфіксу 0x01 перед кодуванням

4.2. Власна реалізація біткоїн-адреси на мові програмування Java

Зробимо аналіз коду програми реалізованої програми

Використовується ECDSA для генерування ключів.

Тому робимо генератор для еліптичних крривих

```
KeyPairGenerator keyGen = KeyPairGenerator.getInstance("EC");
```

Викорристовуючи *secp256r1(еліптична крива)*

```
ECGenParameterSpec ecSpec = new ECGenParameterSpec("secp256r1")
keyGen.initialize(ecSpec);
```

Після цього отримується приватний і публічний ключі.

```
KeyPair kp = keyGen.generateKeyPair();
PublicKey pub = kp.getPublic();
PrivateKey pvt = kp.getPrivate();
```

Потрібно зберегти тільки приватний ключ, адже з нього завжди можна отримати публічний.

```
ECPrivateKey epvt = (ECPrivateKey) pvt;
String sepvt = adjustTo64(epvt.getS().toString(16)).toUpperCase();
System.out.println("s[" + sepvt.length() + "]: " + sepvt);
```

Заповнюється рядок довжиною 64, 16-річною системою числення

```
    private static String adjustTo64(String s) {
        switch (s.length()) {
            case 62:
                return "00" + s;
            case 63:
                return "0" + s;
            case 64:
                return s;
            default:
                throw new IllegalArgumentException("not a valid key: " + s);
        }
    }
}
```

Приклад такого заповнення:

```
AE45F0644349D91697750D01990DF2427204338ED7549B1AF650E68253F78514
```

Ключ ECDSA це точка, де x та y ствворюють публічний ключ.

```
ECPublicKey epub = (ECPublicKey)pub;
ECPoint pt = epub.getW();
String sx = adjustTo64(pt.getAffineX().toString(16)).toUpperCase();
String sy = adjustTo64(pt.getAffineY().toString(16)).toUpperCase();
String bcPub = "04" + sx + sy;
System.out.println("bcPub: " + bcPub);
```

Виконуємо шифрування алгоритмом SHA-256, після чого ще й алгоритмом RIPEMD-160.

```
MessageDigest sha = MessageDigest.getInstance("SHA-256");
byte[] s1 = sha.digest(bcPub.getBytes("UTF-8"));
System.out.println(" sha: " + bytesToHex(s1).toUpperCase());

MessageDigest rmd = MessageDigest.getInstance("RipeMD160", "BC");
byte[] r1 = rmd.digest(s1);
```

Додаємо на початок 0x00.

```
byte[] r2 = new byte[r1.length + 1];
r2[0] = 0;
for (int i = 0 ; i < r1.length ; i++) r2[i+1] = r1[i];
System.out.println(" rmd: " + bytesToHex(r2).toUpperCase());
```

Далі два рази хешуемо.

```
byte[] s2 = sha.digest(r2);
System.out.println(" sha: " + bytesToHex(s2).toUpperCase());
byte[] s3 = sha.digest(s2);
System.out.println(" sha: " + bytesToHex(s3).toUpperCase());
```

Додаємо контрольну суму.

```
byte[] a1 = new byte[25];
for (int i = 0 ; i < r2.length ; i++) a1[i] = r2[i];
for (int i = 0 ; i < 5 ; i++) a1[20 + i] = s3[i];
```

Виводимо фінальну адресу

```
System.out.println(" adr: " + Base58.encode(a1));
```

Висновок

В роботі проведене дослідження криптографічних алгоритмів, що використовуються в технології блокчейн. Незважаючи на те, що данна область перебуває у постійному розвитку, технологія ще не повністю вивчена, що надає безкрайні перспективні можливості росту та розвитку.

Синергія таких складових як розподілена бд, хеші, і цифрові підписи дають ффоррму обміну відмінну від усіх інших, а саме без посередників, органах нагляду чи дорогих процессів.

Найголовнішою ціллю дисертації було доведення надійності цієї технології, адже в сьогоденні, більшістю людей вона приймається доволі скептично. Її основною рисою є базовваність на математиці, що і дає віру в неї, адже “2+2” ніхто не ставить під сумнів.

В результаті роботи, було створено програму для генерації адрес. Проект підлягає ввдосконаленню шляхом розробки API та подальшої підв’язки до системи.

Технологія приховує в собі ще багато цікавостей, але на мою думку, блокчейн може розкрити свій безмежний потенціал тільки у синергіх з іншими технологіями, що дасть новітні неочікувані результати.

РОЗДІЛ 5 СТАРТАП-ПРОЕКТ

У даному розділі буде розглянуто ключові особливості розробленої системи як майбутнього стартап-проекту. Проект розглядатиметься як сервіс для обміну підписками на NFT.

5.1. Опис ідеї проєкту

Спочатку проаналізуємо та подамо у вигляді таблиці зміст ідеї стартап-проекту, можливі напрямки застосування та основні вигоди, які може отримати користувач товару. Ці характеристики стартап-проекту зображено в таблиці 5.1.

Таблиця 5.1 - Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Second-hand market of subscriptions with NFT .	1.Застосування як системи куплі/продажу діючих підписок.	Можливість придбати підписку по нижчій ціні за ринкову
		Збут вже існуючих підпискок

5.2.Технологічний аудит ідеї проєкту

Визначимо технологічну здійсненність ідеї проекту за допомогою аналізу таких складових, як технології, за якою буде виготовлено товар згідно ідеї проекту, існування таких технологій, чи їх необхідно розробити / доробити, доступність таких технологій авторам проекту. Результати даного аналізу зображено в таблиці 5.3.

Таблиця 5.3 – Технологічна здійсненність ідеї проекту

Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
Second-hand market of subscriptions with NFT.	Технологія Blockchain	Так	Дані технології доступні
	Технологія NFT	Так	Дані технології доступні
	Технологія ASP	Так	Дані технології доступні.

5.3. Аналіз ринкових можливостей запуску стартап-проєкту

Проведемо аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку. Результати даного аналізу зображено в таблиці 5.4.

Таблиця 5.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1	Кількість головних гравців, од	1
2	Загальний обсяг продаж, грн/ум.од	300 000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Немає
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі (або по ринку), %	80

Таким чином, за попереднім оцінюванням, ринок є привабливим для входження.

Надалі визначимо потенційні групи клієнтів, їх характеристики, та сформуємо орієнтовний перелік вимог до товару для кожної групи. Ці дані зображено в таблиці 5.5.

Таблиця 5.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1	Простоювання підписки	Малий бізнес Великий бізнес Фізичні особи тощо	Бізнесу потрібна нова модель залучення клієнтів для швидкого росту Фізичним особам та іншим потрібно повернути кошти.	Клієнти прагнуть збереженню їх особистих коштів. Також прагнуть простоти та надійності ринку збуту.

Після визначення потенційних груп клієнтів проведемо аналіз ринкового середовища: складемо таблиці факторів, що сприяють ринковому впровадженню проекту (таблиця 5.6), та факторів, що йому перешкоджають (таблиця 5.7).

Таблиця 5.6 – Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1	Відсутність попиту	Бізнес може не оцінити переваги продукту, або ж у цілому відмовитися від ведення нарад	Акцентувати увагу на клієнтах, що вже скористалися продуктом, якщо такі є, навести інфографіку результативності (очікувану).
2	Молодість технології	Технологія досить нова і не широко використовується у повсякденному житті	Перенести розгляд можливостей застосування на необмежений період часу

Таблиця 5.7 – Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1	Перспективність технології та ідеї	Розроблення патенту та подальший його продаж іншим компаніям	Висока зацікавленість у використанні даного способу реклами та розвитку

Тепер визначимо та обґрунтуємо фактори конкурентоспроможності, які зображені в таблиці 5.9.

Таблиця 5.9 – Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*
1	Невибагливість до апаратних ресурсів
2	Швидкодія
3	Інтеграція
4	Модульність
5	Гнучкість

Таблиця 5.10 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Складові аналізу	Динаміка галузі, продуктова лінія, бар'єри проникнення	Наявність товарних знаків, доступ до ресурсів, патенти на продукти	Концентрація постачальників, диференціація витрат	Рівень чутливості до зміни цін, прибутки, контроль якості	Ціна, лояльність споживачів
Висновки:	Конкуренція не є інтенсивною, адже даний ринок ще ніким не зайнятий.	Для входу на ринок необхідно створити товарний знак та написати бета-версію програмного продукту. На даний момент потенційних конкурентів немає.	Постачальники не диктують умови роботи на ринку, бо програмному продукту не потрібно постачання.	Клієнти диктують умови роботи на ринку, бо вони є єдиним джерелом прибутку компанії.	При наявності товарів замінників необхідно буде зменшувати ціну програмного продукту чи створювати ПЗ для інших технічних систем.

За визначеними факторами конкурентоспроможності проведемо аналіз сильних та слабких сторін стартап-проекту. Результати даного аналізу зображено в таблиці 5.11.

Таблиця 5.11 – Порівняльний аналіз сильних та слабких сторін системи «BioM»

№ п/п	*Фактор конкуренто-спроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з BioM*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1	Інтеграція	15					*		
2	Модульність	16			*				
3	Гнучкість	18			*				

Тепер проведемо SWOT-аналіз на основі виділених загроз і можливостей, та сильних і слабких сторін проекту. SWOT-матриця зображено в таблиці 5.12.

Таблиця 5.12 – SWOT-аналіз стартап-проекту

Сильні сторони:невибагливість до обчислювальних ресурсів, швидкодія	Слабкі сторони: Інтеграція має пройти із залученням розробників на стороні замовника
Можливості: Кобрендінг	Загрози: відсутність попиту, порушення прав конфеденційності споживачів (GDRP)

На основі SWOT-аналізу розробимо альтернативи ринкової поведінки для виведення стартап-проекту на ринок та орієнтований оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок. Дані альтернативи зображено в таблиці 5.13.

Таблиця 5.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1	Реалізація можливості використання системи не тільки на веб-сайтах, а й телефонних додатках	Середня	18 місяців
2	Розробка MVP	Висока	12 місяців

Серед даних альтернатив було обрано другу альтернативу, адже строки її реалізації найменші та є ймовірність отримання ресурсів.

5.4. Розроблення ринкової стратегії проєкту

Для розроблення ринкової стратегії першим кроком необхідно описати цільові груп потенційних споживачів, які можна побачити в таблиці 5.14.

Таблиця 5.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Малий бізнес	Низька	5-10 підприємств в рік	Слабка	Середня
2.	Середній бізнес	Готові	5-10 підприємств в рік	Слабка	Середня
3.	Великий бізнес	Готові	3-5 закладів в рік	Слабка	Середня
Було обрано цільову групу підприємств групи Великого бізнеса.					

Для роботи в обраних сегментах ринку необхідно сформувати базову стратегію розвитку, яку ображено в таблиці 5.15.

Таблиця 5.15 – Визначення базової стратегії розвитку

Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Концентрація на потребах одного цільового сегменту – веб-сайтах.	Створений продукт є дешевим у використанні та іноваційним	Стратегія спеціалізації.

Наступним кроком є вибір стратегії конкурентної поведінки, яку зображено в таблиці 5.16.

Таблиця 5.16 – Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохід-цем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
Так.	Компанія буде шукати нових споживачів, але і, за потреби, буде намагатися забирати існуючих у конкурентів.	Компанія, за потреби, буде копіювати характеристики конкурентів.	Стратегія заняття конкурентної ніші.

Тепер розробимо стратегію позиціонування, що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект. Її зображено в таблиці 5.17.

5.4. Розроблення маркетингової програми стартап-проєкту

Сформуємо маркетингову концепцію товару, який отримає споживач. В таблиці 5.18 зображено результати попереднього аналізу конкурентоспроможності товару.

Таблиця 5.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1.	Простота	Прозора та зрозуміла система	Доступність для компаній з невеликим капіталом.
2.	Невибагливість до апаратних ресурсів	Невибагливість до апаратних ресурсів клієнта	Доступність для компаній з невеликим капіталом.
3.	Швидкодія	Швидкодія системи	Більша швидкість

Надалі розробимо трирівневу маркетингову модель товару: уточнимо ідею продукту, його фізичні складові, особливості процесу його надання. Дана модель зображена в таблиці 5.19.

Тепер визначимо цінові межі, якими необхідно керуватись при встановленні ціни на потенційний товар, яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів. Аналіз проводився експертним методом і його результати зображено в таблиці 5.20.

Таблиця 5.20 – Визначення меж встановлення цін

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
3000-5000 $/рік	5000-6000 $/рік	12000-50000 $/рік	Нижня межа – 3000 $/рік, верхня межа - 5000 $/рік

Надалі визначимо оптимальну систему збуту, в межах якого приймається рішення. Дану систему зображено в таблиці 5.21.

Таблиця 5.21 – Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Клієнт виплачує гроші на рік, тоді до нього приходить спеціаліст із впровадження інформаційних систем і встановлює ПЗ на комп’ютер клієнта.	Встановити програмний продукт на комп’ютери клієнтів.	Один посередник – спеціаліст по впровадженню інформаційних систем.	Канал збуту одного рівня.

5.6. Висновки

В даному розділі було повністю виконано перший етап розроблення стартап-проекту, а саме, виконано маркетинговий аналіз стартап-проекту.

За допомогою нього можна сказати, що існує можливість ринкової комерціалізації проекту, адже на ринку програм систем біометрії наявний попит на системи голосової біометрії, до того ж рентабельність роботи є досить високою.

З огляду на потенційну групу клієнтів, а саме, малий бізнес, що має вебсайт з приватним контентом для своїх клієнтів, та інноваційність технології є великі перспективи впровадження даного програмного забезпечення.

Для ринкової реалізації проекту доцільно обрати таку альтернативу впровадження: створення MVP та впровадження його в невелику кількість веб-сайтів середніх бізнесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Біткоїн-терміни URL: https://bitcoin.org/uk/vocabulary
2. Украина переведет все государственные данные на блокчейн URL: https://hightech.fm/2017/04/14/us-ukraine-bitfury-blockchain
3. Andreas M. Antonopoulos Mastering Bitcoin: Unlocking Digital Cryptocurrencies : NGITS, 2014. URL: https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
4. Don Tapscott, Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World: Information Systems, 2016. URL: https://www.academia.edu/39300279/Blockchain_Revolution_How_The_Technology_Behind_Bitcoin_Is_Changing_Money_Business_And_The_World
5. Технологія блокчейн та страхування URL: http://www.insa.com.ua/uk/blog/tehnologiya-blockchain- i-strahovanie/
6. Blockchain: Приклади використання технології на практиці URL: https://stocx.org/blockchain- tehnologii-na-praktitsi/
7. Bitcoin Wiki URL: http://ru.bitcoinwiki.org
8. Melanie Swan Blockchain: Blueprint for a New Economy: Economic, 2015. URL: https://epdf.pub/blockchain-blueprint-for-a-new-economy.html
9. Основы блокчейн и криптовалюты URL: https://www.intuit.ru
10. Введение в криптовалюты и блокчейн URL: https://www.intuit.ru
11. Биткоин и технологии криптовалюты URL: https://www.intuit.ru
12. Навчальні відео-матеріали від компанії URL: https://distributedlab.com/

13. Майнінг. Процес майнінгу URL: https://pingblockchain.com/majning-proces-majningu/
14. Paul Vigna The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order K.: Economic. 2016
15. Bitcoin Forum URL: https://bitcointalk.org
16. Pandia: Вибір криптогрфічно стійких еліптичних кривих URL: http://pandia.ru/text/80/176/51044.php
17. Лекториум, Криптографические Хэш-функции URL: https://www.lektorium.tv/course/22746
18. BitNovosti: Математика Биткойна: Теория URL: https://bitnovosti.com/2014/10/23/bitcoin- math/
19. habr: Хэш-алгоритмы: URL: https://habr.com/post/93226/
20. Nathaniel Popper Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money: Economic, 2016. URL: https://www.semanticscholar.org/paper/Digital-Gold%3A-Bitcoin-and-the-Inside-Story-of-the-Popper/b56acc81e2986f211ad1e73b845df70bfacba241