МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ

Кафедра комп'ютерних наук

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему: **«ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ТА ЦИФРОВИХ ТРАНЗАКЦІЙ»**

Виконав: студент 4 курсу, групи 6.1220-з
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)
освітньої програми Комп'ютерні науки
(назва освітньої програми)
Д. М. Власенко
(ініціали та прізвище)
Керівник завідувачка кафедри комп'ютерних наук, д.т.н., доцент, Шило Г.М.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент професор кафедри програмної інженерії, доцент, к.ф.-м.н. Кудін О.В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет математичний

Кафедра комп'ютерних наук

Рівень вищої освіти бакалавр

Спеціальність 122 Комп'ютерні науки

(шифр і назва)

Освітня програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувачка кафедри комп'ютерних наук, д.т.н., доцент
_____ Шило Г.М.
(підпис)
" ____ " _____ 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ

Власенку Дмитру Максимовичу

(прізвище, ім'я та по-батькові)

1. Тема: роботи Дослідження технологій блокчейн для забезпечення безпеки даних та цифрових транзакцій.

керівник роботи Шило Галина Миколаївна, д.т.н., професор

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

затверджені наказом ЗНУ від « 21 » грудня 2023 року № 2181-с

2. Строк подання студентом роботи 15.05.2024

3. Вихідні дані до роботи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз предметної області і постановка завдання
2. Основні теоретичні можливості і код написання блокчейна
3. Застосування blockchain у різних галузях.
4. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 22.12.2023

К А Л Е Н Д А Р Н И Й П Л А Н

№	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка плану роботи.	04.03.2024	
2.	Збір вихідних даних.	10.03.2024	
3.	Обробка методичних та теоретичних	15.03.2024	
	джерел.		
4.	Розробка першого та другого розділу.	25.03.2024	
5.	Розробка третього розділу.	05.04.2024	
6.	Оформлення та нормоконтроль	25.05.2024	
	кваліфікаційної роботи бакалавра.		
7.	Захист кваліфікаційної роботи.	30.05.2024	

Студент _____ Д.М. Власенко
(підпис) (ініціали та прізвище)

Керівник роботи _____ Г.М. Шило
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено

Нормоконтролер _____ О.Г.Спиця
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кваліфікаційна робота бакалавра «Дослідження технологій блокчейн для забезпечення безпеки даних та цифрових транзакцій»: 53 с., 1 рис., 2 табл., 11 джерел.

БЛОКЧЕЙН, ДОКАЗ ВІДОКРЕМЛЕННЯ, ДОКАЗ РОБОТИ, КРИПТОВАЛЮТА, МЕХАНІЗМ КОНСЕНСУСУ, ПРАВО ПІДТВЕРДЖЕННЯ БЛОКА, ХЕШ, GENESIS-БЛОК.

Об’єкт дослідження – технологій блокчейн та її вплив на різні сфери життя людини.

Мета роботи: аналіз та исследование технологій блокчейн для забезпечення високого рівня безпеки даних і цифрових транзакцій та розробка рекомендацій щодо їх застосування в різних сферах. Робота спрямована на дослідження різних аспектів використання блокчейн, включаючи його застосовність, ефективність, і потенційні проблеми, з метою запропонувати рекомендації щодо оптимального використання даної технології для різних сфер діяльності.

Метод дослідження – використання методу літературного огляду. За допомогою нього я відповів на такі питання: "основи технології блокчейн, застосування технології блокчейн, проблеми безпеки".

SUMMARY

Bachelor's Qualifying Theses «Research on blockchain technologies to ensure data security and digital transactions»: 53 pages, 1 figures, 2 tables, 11 references.

BLOCKCHAIN, PROOF OF STAKE, PROOF OF WORK, CRYPTOCURRENCY, CONSENSUS MECHANISM, HASH, RIGHT TO CONFIRM A BLOCK, GENESIS-BLOCK.

Object of the study – research on blockchain technology and its effect on different people's life spheres.

Aim of the study: analyze and evaluate the potential of blockchain technology to ensure a high level of data security and digital transactions. The work aims to explore various aspects of the use of blockchain, including its applicability, efficiency, and potential challenges, in order to offer recommendations on the optimal use of this technology in the context of data security and digital transactions..

Method of research – using the literary review method. With it, I answered the following questions: "the basics of blockchain technology, the use of blockchain technology, security issues".

ЗМІСТ

ВСТУП

В епоху цифрової революції, де величезний потік інформації та здійснення транзакцій відбувається в онлайн просторі, головною необхідністю стає забезпечення високого рівня безпеки даних та ефективності цифрових операцій. У цьому контексті технології блокчейн набувають особливого значення, оскільки вони пропонують інноваційний підхід до забезпечення конфіденційності, цілісності та доступності інформації.

Ця кваліфікаційна робота бакалавра спрямована на глибоке вивчення технологій блокчейн, розкриття їхнього потенціалу в забезпеченні безпеки даних та покращенні ефективності цифрових транзакцій. Буде проаналізовано технічні аспекти функціонування блокчейну, визначено можливості та обмеження його застосування. Дослідження також охопить практичні приклади впровадження блокчейн технологій у різних сферах, від фінансів до ланцюжка постачання, для детального вивчення позитивного впливу цих інновацій на забезпечення кібербезпеки в сучасному суспільстві.

Робота має на меті розширити розуміння про переваги та виклики використання блокчейн технологій, а також визначити їхній потенціал у побудові надійних та безпечних цифрових середовищ для інформаційного обміну та здійснення електронних операцій.

Технологія блокчейн, в основі якої лежить розподілена база даних та концепція децентралізації, зробила революційний внесок у сферу фінансів, надаючи можливість уникнути централізованих посередників, таких як банки. Одним із ключових викликів у цифрових фінансових транзакціях була проблема "Double spend", яка полягає в можливості подвійного використання одних і тих же цифрових активів. Завдяки технології блокчейн та концепції консенсусу, ця проблема ефективно вирішується.

Блокчейн використовує розподілену мережу вузлів, які підтверджують та реєструють транзакції. Кожна транзакція включається у блок, який

ланцюгується з попередніми блоками. Таким чином, взаємодія між учасниками мережі відбувається без посередництва централізованої сторони. Метою цієї роботи є аналіз та дослідження технологій блокчейн для забезпечення високого рівня безпеки даних і цифрових транзакцій, а також розробка рекомендацій щодо їх застосування в різних сферах. Цей підхід не лише ефективно вирішує проблему подвійного використання, але також забезпечує високий рівень безпеки та невідмовності від маніпуляцій. Таким чином, технологія блокчейн стала каталізатором для нового етапу в розвитку фінансової сфери, підвищуючи ефективність та довіру в електронних транзакціях. Робота спрямована на вивчення різних аспектів використання блокчейн, включаючи його застосовність, ефективність та потенційні проблеми, з метою запропонувати рекомендації щодо оптимального використання цієї технології у різних сферах діяльності.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І ПОСТАНОВКА ЗАВДАННЯ

У цьому розділі ви зможете прочитати про історію створення блокчейн системи і класифікація блокчейн систем.

1.1 Класификация блокчейна

В 1991 році Хабер та Стоннетта розповіли про своє відкриття в статті "Як датувати цифровий документ", опублікованій у журналі, присвяченому криптографії. Технологія отримала назву "блокчейн", оскільки розподілена електронна книга зберігає елементи даних у цифрових групах із часовими відмітками, які називаються блоками. Кожен блок включає буквено-цифровий код, який називається "хеш", і сумує свої дані. Хеш кожного завершеного блоку також з'являється у наступному блоку, що означає, що для зміни одного блоку потрібно змінити і всі пов'язані з ним. Ці криптографічні "доміно" працюють разом, щоб захистити від підробки або шахрайства.

У системі було використано криптографічно пов'язану ланцюг блоків для зберігання документів з міткою часу, а в 1992 році до розробки були включені "дерева Меркла", що зробило її більш ефективною, дозволивши збирати кілька документів в один блок. Однак впровадження цієї технології так і не відбулося.

У 2004 році Хел Фінні (Гарольд Томас Фінні II) представив систему під назвою Reusable Proof of Work (далі – RPoW). Система працювала, отримуючи незамінний токен Hashcash, заснований на доказі роботи та підписаний в RSA, який потім міг бути переданий від особи до особи.

RPoW вирішила проблему подвійного витрачання, зберігаючи право власності на токени, зареєстровані на довіреному сервері, який був

розроблений з метою надання можливості користувачам по всьому світу перевіряти його правильність та цілісність в реальному часі.

31 жовтня 2008 року о 14 годині 10 хвилин за нью-йоркським часом кілька сотень криптографічних спеціалістів, що входили в закритий список розсилки, отримали на свої електронні адреси лист від невідомого, що називав себе Сатоші Накамото.

3 січня 2009 року о 18:15:05 за часовим поясом Гринвіча була запущена мережа біткоїн і створений генезис-блок, який був здобутий Сатоші Накамото. Першим одержувачем біткоїна був Хал Фінні, який отримав 10 біткоїнів від Сатоші Накамото у першій у світі біткоїн-транзакції 12 січня 2009 року.

Мережа біткоїн була першою практичною реалізацією мережі блокчейн у сучасному розумінні цієї технології. З моменту запуску пройшло понад 10 років. За цей час технологія блокчейн значно еволюціонувала і пройшла кілька етапів, так званих поколінь: Блокчейн 1.0, Блокчейн 2.0 і Блокчейн 3.0.

Блокчейн, на якому була реалізована мережа біткоїн, відноситься до покоління Блокчейн 1.0 – піринговой децентралізованої електронної мережі, призначеної для прямого обміну віртуальними грошима (криптовалютою). Незважаючи на "революційність" технології, Блокчейн 1.0 має суттєві обмеження: складність інтеграції з зовнішніми системами, порівняно низька пропускна здатність, обмеженість практичного застосування. Основне призначення Блокчейн 1.0 полягає в використанні його як платіжної системи, в якій відсутні посередники, а об'єктами операцій виступають віртуальні валюти (криптовалюти).

Особливість Блокчейн 2.0 полягає в інтеграції моделі розумних контрактів. Розумний контракт представляє собою цифровий протокол, який автоматично виконує заздалегідь визначені процеси транзакції і не потребує участі третьої сторони (наприклад, банку). По суті, мережі блокчейн покоління 2.0 представляють собою блокчейн-платформи для створення та реалізації розумних контрактів. На основі технології блокчейн 2.0 був реалізований проект Ethereum. Ethereum є платформою блокчейн, яка дозволяє створювати

розумні контракти і децентралізовані додатки (DApps). Цей проект відкрив нові можливості для розробників, дозволяючи їм створювати програми на базі блокчейн безпосередньо на платформі Ethereum. Ethereum використовує власну криптовалюту, єфір (ETH), для здійснення транзакцій у мережі та виконання розумних контрактів. Цей проект став кроком вперед у розвитку технології блокчейн, розширюючи її можливості і застосування.

Блокчейн 3.0 – це етап розвитку технології з подальшим удосконаленням концепції розумного контракту з метою створення децентралізованих, автономних організаційних одиниць, які керуються власними законами і діють практично автономно.

Отже, технологія блокчейн, як і будь-яка інша технологія у світі, постійно еволюціонує, розширюючи при цьому спектр свого застосування та інтеграції.

Системи, які використовують технологію блокчейн, можуть мати різні варіації, які відрізняються за способом організації, конфігурацією та метою використання. Ось кілька основних варіацій:

За об'єктами транзакцій:

- інформація;
- віртуальна вартість (вартість, якої немає в реальному світі, наприклад, біткоїни).

За типом доступу до мережі:

- необмежений (учасники мають можливість здійснювати будь-яку діяльність);
- обмежений (мережі, що обмежують види діяльності учасників).

За вимогами до ідентифікації:

- анонімний;
- псевдоанонімний;
- повна ідентифікація.

За протоколом досягнення консенсусу мережі:

- PoW (Proof-of-Work) – право підтвердження блока отримується учасником на основі виконання ним певної достатньо складної роботи, яка відповідає заздалегідь визначеним критеріям;
- PoS (Proof-of-Stake) – право підтвердження блока отримується власником рахунку, коли кількість його коштів та строк володіння ними відповідають заданим критеріям;
- PoS + PoW – гібрид PoW і PoS, коли блоки можуть підтверджуватися як через розрахункові критерії PoS, так і PoW-перебором;
- PBFT (Practical Byzantine Fault Tolerance), Paxos, RAFT – алгоритми багатоступеневого досягнення консенсусу мережі;
- Non-BFT (Non Byzantine Fault Tolerance) – алгоритми консенсусу, нестійкі до неблагонадійної поведінки деяких учасників.

За наявністю центрального адміністратора:

- існує центральний адміністратор(Private blockchain) – право на запис інформації має лише один учасник або вузли, уповноважені цим єдиним адміністратором. Це централізовані персоніфіковані системи, оскільки існує ієрархія повноважень. Помилки можна швидко виправити вручну. Немає сенсу застосовувати доказ виконання роботи або доказ володіння часткою – інформація без затримки потрапляє в блоки, формовані за необхідності, і не вимагає додаткового підтвердження, що максимізує швидкість роботи мережі і мінімізує вартість транзакцій. Проте зберігається розподілений характер зберігання даних, при якому вузли містять повні копії у вигляді взаємопов'язаних ланцюгів блоків. Доступ до інформації може бути загальним або мати довільні обмеження. Найчастіше мова йде про систему передачі інформації всередині однієї компанії, яка не потребує загального доступу до всієї інформації, але може передбачати загальнодоступну можливість аудиту;

– відсутній центральний адміністратор (Public blockchain) – загальнодоступні. Будь-хто може переглядати блоки, надсилати до них інформацію та брати участь у механізмі консенсусу. При цьому користувачі можуть залишатися анонімними. Такі блокчейни зазвичай є повністю децентралізованими, тобто вони не мають адміністраторів чи центрів довіри. Незмінність та цілісність інформації забезпечують економічні стимули та криптографічні перевірки з використанням таких механізмів, як доказ виконання роботи або доказ володіння часткою;
– консорціумні блокчейни – це тип блокчейнів, у яких участь беруть обмежена група учасників або організацій, зазвичай заздалегідь визначених і довірених. Ці блокчейни можуть бути як приватними, так і публічними, але вони зазвичай керуються групою компаній або організацій, які спільно приймають рішення про те, як вони будуть функціонувати та яким чином будуть вирішуватися питання безпеки та конфіденційності.

1.2 Основні принципи технології блокчейн

Основні принципи технології блокчейн включають:

– децентралізація: Блокчейн працює на основі децентралізованої мережі вузлів (комп'ютерів), які розташовані по всьому світу. Це означає, що немає центрального органу або сервера, який контролює всю систему. Замість цього, дані розподіляються та зберігаються на всіх вузлах мережі;
– криптографічна безпека: Криптографічні методи забезпечують безпеку та недоступність даних у блокчейні. Кожен блок має унікальний хеш, який відображає дані у блоку і включає інформацію з попереднього блоку, утворюючи ланцюг хешів. Це робить

надмірно складним зміну даних у блоках без зміни всієї ланцюга, що забезпечує надійність та непереборність системи;

– прозорість та імутабельність: Дані, які занесені у блокчейн, є відкритими для всіх учасників мережі. Кожен учасник може перевірити історію транзакцій та стан будь-якого блоку. Крім того, імутабельність означає, що коли інформація занесена у блокчейн, вона не може бути змінена або видалена, що дозволяє створювати довіру в систему;
– спільний консенсус: Щоб забезпечити єдність даних у децентралізованій мережі, учасники мережі повинні домовитися про те, який блок буде доданий до ланцюга наступним. Це досягається за допомогою механізмів консенсусу, таких як "доказ роботи" (Proof of Work), "доказ відокремлення" (Proof of Stake) або інші протоколи консенсусу;
– смарт-контракти: Деякі блокчейн-платформи, такі як Ethereum, підтримують смарт-контракти, які є програмними кодами, що автоматизують виконання угод на основі умов, визначених у контракті. Це розширює можливості використання блокчейну на створення децентралізованих додатків (DApps) та автоматизації процесів;
– технологія блокчейн – це децентралізована система збереження та передачі даних, яка базується на концепції ланцюга блоків. Кожен блок у ланцюзі містить криптографічно зв'язані дані, що підтверджують їхню цілісність та послідовність. Ця технологія дозволяє створювати розподілені системи, в яких дані можуть бути збережені та змінені тільки за умови згоди багатьох учасників мережі, а не одного централізованого органу. Блокчейн зазвичай використовується для створення децентралізованих криптовалют, збереження та передачі цифрових активів, а також для реєстрації та підтвердження транзакцій безпекою за допомогою криптографії.

2 ОСНОВНІ ТЕОРЕТИЧНІ МОЖЛИВОСТІ І КОД НАПИСАННЯ BLOCKCHAIN

Механізм роботи технології блокчейн ґрунтується на декількох ключових принципах:

- створення блоків: Учасники мережі збирають нові транзакції в блоки. Кожен блок містить дані про певну кількість транзакцій, час їхнього створення та унікальний ідентифікатор;
- хешування: Після того як блок сформований, він піддається хешуванню. Хеш – це унікальний код, що відображає вміст блоку. Навіть найменша зміна у вмісті блоку призведе до зміни його хешу. У блокчейні використовується шифрування SHA256;
- ланцюг блоків: Кожен блок містить посилання на попередній блок за допомогою свого хешу, утворюючи ланцюг блоків. Це забезпечує послідовність та недоступність даних у блокчейні;
- механізм консенсусу: Учасники мережі повинні домовитися про те, який блок буде доданий до ланцюга. Це досягається за допомогою механізмів консенсусу, таких як "доказ роботи" або "доказ відокремлення", які вимагають від учасників виконання певних завдань для додавання блоків;
- розподілене зберігання даних: Кожен учасник мережі має копію всього блокчейну. Це розподілене зберігання забезпечує безпеку та надійність, оскільки немає одного центрального пункту вразливості;
- децентралізована мережа: Вся мережа блокчейн є децентралізованою, тобто керування та контроль розподілені між всіма учасниками. Це дозволяє уникнути централізованого контролю та забезпечити безпеку та стійкість мережі.

Загалом, ці принципи створюють надійний та ефективний механізм для зберігання, передачі та підтвердження даних у блокчейні.

2.1 Код написання блокчейну

Перше, що нам потрібно зробити – це визначитися зі структурою блоку. Ми повинні включити всі необхідні елементи. Наприклад: індекс, відмітка, дані, хеш та хеш попереднього блоку.

Ланцюжок блоків виглядає як на рис. 2.1.

Рисунок 2.1 – Схема блокчейну

На зображенні ми можемо спостерігати "genesis-блок" і наступні блоки, які ґрунтуються на хеші попереднього блоку. Якщо придивитися уважніше, можна побачити, наприклад, "індекс", який показує, який це блок за ліком, починаючи з першого. Далі "timestamp" – цей рядок вказує час, коли цей блок був створений. Потім рядок "data", який містить конкретні дані для цього блоку. Наступним за списком йде два рядки хешування, де перший містить хеш самого блоку, що відповідає за його вміст, а під ним – хеш попереднього блоку, з яким пов'язаний хеш наступного блоку. Зміна хеша попереднього блоку призведе до зміни хеша наступного блоку. Ось приклад коду на мові JavaScript, який використовується для написання блоків у блокчейні:

```
var generateNextBlock = (blockData) => {
```

var previousBlock = getLatestBlock(); – Цей виклик функції витягує останній блок у блокчейні.

var nextIndex = previousBlock.index + 1; – Цій змінній присвоюється значення індексу попереднього блоку плюс одиниця, що вказує позицію нового блоку в блокчейне.

var nextTimestamp = new Date().getTime() / 1000; – Ця змінна відображає поточний час у секундах з моменту появи Unix (1 січня 1970 року).

var nextHash = calculateHash(nextIndex, previousBlock.hash, nextTimestamp, blockData); – Цей виклик функції обчислює хеш для нового блоку, використовуючи його Індекс, хеш попереднього блоку, мітку часу та дані блоку.

return new Block(nextIndex, previousBlock.hash, nextTimestamp, blockData, nextHash); – Це створює новий блок із обчисленим індексом, хешем попереднього блоку, міткою часу, даними блоку та новим хешем і повертає його.

};

Наступним кроком буде розгляд хешування блока. Ось код, як може виглядати функція хешування:

```
var calculateHash = (index, previousHash, timestamp, data) => {
    return CryptoJS.SHA256(index + previousHash + timestamp + data).toString(); – При цьому використовується бібліотека CryptoJS для обчислення хешу SHA256 при об'єднанні індексу блоку, хешу попереднього блоку, часової мітки і даних блоку. Потім результат перетворюється на рядок.
);
```

Далі нам потрібно буде десь зберігати наш ланцюг блоків. У пам'яті використовується масив JavaScript для зберігання блокчейну. Перший блок у ланцюзі завжди є "генезис-блок", який має такий код:

```
var getGenesisBlock = () => {
```

return new Block(0, “0”, 1465154705, “my genesis block!”, “816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7”); }; – При цьому створюється новий блок з наступними параметрами.
var blockchain = [getGenesisBlock()]; – Викликає функцію get Genesis Block для створення генезис-блоку і додає його в масив блокчейна.

У будь-який момент часу нам потрібно мати можливість перевірити, чи є блок або ланцюг блоків прийнятними з точки зору цілісності. Це особливо важливо, коли ми отримуємо нові блоки від інших вузлів і повинні вирішити, приймати їх чи ні. Ось як може виглядати код перевірки:

```
var isValidNewBlock = (newBlock, previousBlock) =>{
    if (previousBlock.index +1 !== newBlock.index) {
        console.log(‘invalid index’);
        return false; – Це гарантує, що індекс нового блоку буде рівно на одиницю більше, ніж індекс попереднього блоку. Якщо ця умова не виконується, програма реєструє "недійсний індекс" і повертає значення false.
    } else if (previousBlock.hash !== newBlock.previousHash) {
        console.log(‘invalid previoushash’) {
        return false; – Це гарантує, що попереднє хеш-поле нового блоку збігається з хеш-полем попереднього блоку. Якщо ця умова не виконується, програма реєструє "невірний попередній хеш" і повертає значення false.
    } else if (calculateHashForBlock(newBlock) !== newBlock.hash) {
        console.log(‘invalid hash: ‘+ calculateHashForBlock(newBlock) + ‘’+newBlock.hash); – Це гарантує, що хеш нового блоку буде правильно обчислений на основі його вмісту. Якщо обчислений хеш не відповідає хеш-полю нового блоку, він реєструє "недійсний хеш:" + обчислити хеш для блоку(newBlock) + "" + newBlock.хеш і повертає значення false.
        return false;
    }
```

```
    return true;
};
```

Коли у вас вже є ланцюг, що складається з декількох блоків, і виникає конфлікт між вузлами, коли у двох блоків попередній хеш однаковий, вам потрібно вибрати ланцюг з більшою кількістю блоків. Ось приклад того, як можна порівнювати довжину ланцюгів:

```
var replaceChain = (newBlocks) => {
    if (isValidChain(newBlocks) && newBlock.length > blockchain.length) {
    console.log('Received blockchain is valid. Replacing current blockchain with received blockchain'); – реєструє повідомлення про те, що новий блокчейн дійсний і замінить поточний.
    blockchain = newBlocks; – Замінює поточний блокчейн новим блокчейном.
    broadcast(responseLatestMsg()); – Це передає повідомлення іншим вузлам, ймовірно, інформуючи їх про новий стан блокчейна. Передбачається, що це повідомлення генерується функцією response Latest Msg.
    } else {
        console.log('Received blockchain invalid'); – Реєструє повідомлення, яке вказує на те, що новий блокчейн недійсний і не замінить поточний.
    }
};
```

2.2 Вузли зв'язку

Вузли в блокчейні відіграють важливу роль у підтримці мережі, забезпечуючи її децентралізацію та безпеку. Ще їх називають нодами. Основне завдання вузлів – підтверджувати законність кожної наступної партії мережевих транзакцій, відомих як блоки. Крім того, кожен вузол має свій унікальний ідентифікатор у мережі, що допомагає відрізнити один вузол від іншого.

Функції вузлів:

- зберігання копії blockchain: кожна нода в мережі blockchain зберігає повну копію blockchain, що означає, що вузли містять інформацію про всі блоки та транзакції, які коли-небудь відбувалися в мережі;
- підтвердження транзакцій: Ноди перевіряють транзакції, які вони отримують від інших вузлів. Це включає перевірку підписів, балансів та інших правил протоколу blockchain. Після успішної перевірки нода може передати транзакцію іншим вузлам;
- участь у консенсусі: Ноди можуть брати участь у процесі досягнення консенсусу щодо нових блоків. Залежно від конкретного механізму консенсусу (наприклад, Proof of Work, Proof of Stake тощо), ноди можуть обчислювати хеші блоків, голосувати за правильність блоків або виконувати інші дії, спрямовані на підтвердження нових блоків;
- поширення інформації: Ноди передають інформацію про нові блоках і транзакціях по мережі блокчейна. Це допомагає забезпечити оновлення блокчейна на всіх вузлах мережі і підтримує його актуальним;
- підтримка безпеки мережі: колективна участь нод в мережі забезпечує безпеку блокчейна. Наприклад, в системах Proof of Work Майнер (спеціальні ноди) використовують обчислювальну потужність для захисту мережі від атак;

– управління конфліктами: Ноди можуть допомогти у вирішенні конфліктів і невідповідностей в мережі. Наприклад, якщо дві ноди вносять суперечливі зміни в блокчейн, механізм консенсусу допомагає визначити правильну версію блокчейна.

Наступним кроком буде розгляд класифікації вузлів, які можна зустріти в мережі:

– повні вузли (Full nodes) – це найважливіший тип узлів в мережі блокчейну, оскільки вони містять повну копію блокчейну. Ці узли зберігають копію кожної транзакції та блоку у мережі, що дозволяє їм незалежно перевіряти повну історію блокчейну. Вони працюють в одноранговій мережі, що дозволяє їм взаємодіяти з іншими вузлами, щоб забезпечити актуальність та точність блокчейну. Зазвичай такими вузлами керують ентузіасти криптовалют або ж творці блокчейну, які потребують високого рівня безпеки та контролю над своїми блокчейн-транзакціями;
– легкі вузли (Light nodes) – це спрощена форма повних вузлів, які не містять у собі всю історію блокчейну, а лише окремі її частини. Наприклад, інформація щодо конкретної транзакції або окремого блоку. Вони були створені для здійснення операцій на слабкопотужних пристроях, таких як телефони або планшети. Ці вузли ефективніші порівняно з повними вузлами, але менш безпечні і постійно потребують обміну інформацією з повними вузлами;
– майнерські вузли (Miner nodes) – ці вузли відповідають за перевірку транзакцій та додавання нових блоків до ланцюжка. Вони виконують складні обчислення для вирішення математичних задач, що дозволяє їм створювати нові блоки і отримувати винагороду у вигляді криптовалюти. Проте для цього потрібне спеціальне обладнання та програмне забезпечення для виконання обчислень. Зазвичай ними керують великі майнінгові пули або приватні особи з достатніми ресурсами.

Порівняння звичайних нодів і Майнінг нодів представлено на рис. 2.2.

Рисунок 2.2 – Порівняння звичайних нодів і Майнінг нодів

У деякому роді користувач повинен контролювати ноди. Це робиться за допомогою створення свого http-сервера. Ось приклад коду:

```
const http = require('http');
const express = require('express');
const bodyParser = require('body-parser');
const app = express();
```

app.use(bodyParser.json()); – Це проміжне програмне забезпечення аналізує тіла запитів JSON, полегшуючи обробку даних JSON у запитах POST.

```
function getBlockchain() {
```

return [{ /* дані блоку 1 */ }, { /* дані блоку 2 */ }, { /* дані блоку 3 */ }];
} – Ця функція повертає макет блокчейну, що складається з трьох блоків із заповнювачами даних. У реальному додатку це дозволило б отримати поточний стан блокчейна.

function addBlock(data) {
return { /* дані нового блоку */};
} – Ця функція приймає дані та повертає новий блок із заповнювачами даних. У реальному додатку це створило б новий блок, додало б його в блокчейн і повернуло б новий блок.

app.get('/blocks', (req, res) => {
    const blockchain = getBlockchain();
    res.json(blockchain);
}); – Кінцева точка для отримання поточного стану блокчейна.
Вона викликає getBlockchain () і відправляє блокчейн у вигляді відповіді у форматі JSON.

app.post('/addBlock', (req, res) => {
    const data = req.body.data;
    const newBlock = addBlock(data);
    res.json({message: "Новий блок додано", block: newBlock});
}); – Кінцева точка для додавання нового блоку в блокчейн.
Вона зчитує дані з тіла запиту, викликає AddBlock (дані) і відправляє відповідь у форматі JSON з повідомленням і новим блоком.

const port = 3000;
const server = http.createServer(app);
server.listen(port, () => {
    console.log(`Сервер запущено на порті ${port}`);

```
});
```

Тут використовуються МОК-функції: get Blockchain() і adBlock(data) для отримання блокчейна і додавання нового блоку в ланцюжок.

3 ЗАСТОСУВАННЯ BLOCKCHAIN У РІЗНИХ ГАЛУЗЯХ

У цьому розділі ми розглянемо застосування блокчейну в різних сферах життя людини.

3.1 Фінансова сфера

Найголовнішою перевагою, з мого погляду, блокчейна над фіатними операціями у фінансовій сфері буде те, що він допоможе заощадити багато грошей, знизивши витрати на міжінституціональні перекази коштів. Це означає, що комісійні виплати будуть мінімізовані. З цього випливає наступний плюс – анонімність. Адже при відправленні грошей, наприклад, з України в США, до вашої транзакції будуть додані 3-4 комісії, а кілька фінансових організацій будуть відстежувати та аналізувати вашу транзакцію. Таким чином, не може йтися про конфіденційність.

Ось, в яких випадках може використовуватися блокчейн технології:

Ринки капіталів

– емісія
– продаж та торгівля
– кліринг та розрахунок
– послуги та інфраструктура післяторгового обслуговування
– обслуговування активів
– кастодія

Управління активами

– запуск фонду
– управління списком акціонерів
– трансферне агентство в управлінні активами
– адміністрування фонду

Платежі та перекази

– внутрішні роздрібні платежі
– внутрішні оптові та цінні папери
– міжнародні перекази
– токенізована валюта, стейблкоїни та криптовалюти

Банківські послуги та кредитування

– прогнозування кредитів та кредитний рейтинг
– синдикація кредитів, підписання та видача
– забезпечення активів

Торгове фінансування

– акредитиви та коносаменти
– фінансові структури

Страхування

– обробка та виплата заявок на страхування
– параметризовані контракти
– страхові ринки

Впровадження блокчейна в медицину і створення єдиної мережі може виглядати так, як на рисунку 3.1.

Рисунок 3.1 - Впровадження технології блокчейн у різні сфери життя людини

На графіку можна помітити, що технологія блокчейн найбільше використовується у фінансовій сфері, особливо з огляду на торгівлю криптовалютами, яка зараз активно розвивається на біржах. Однак створені консорціуми компаній, які спільно тестують цю технологію. Наприклад, консорціум з 15 компаній, до якого увійшли BNP Paribas, Shell plc. та інші, заснували ще одну компанію під назвою komgo SA, яка розробляє платформу на основі блокчейн 2.0 для фінансової торгівлі різними товарами.

3.2 Медицина

Сучасна система охорони здоров'я часто має недостатньо ефективні механізми обміну медичною інформацією. Пацієнтам часто доводиться самостійно доставляти свої медичні записи в нові медичні заклади або знову проходити медичні обстеження. Це не лише незручно, але й може призвести до неправильного лікування через недостатню інформацію про медичну історію. Однією з ключових проблем є фрагментація інформації про пацієнтів, яка може зберігатися в різних базах даних різних медичних закладів. Завдяки технології блокчейн з'являються нові можливості для зберігання та управління медичними даними, що стає основою для багатьох сучасних розробок в галузі охорони здоров'я.

Наприклад, можна створити єдину мережу, що об'єднає лікарів, документи, направлення та результати, які будуть зберігатися у хмарі, де у кожного пацієнта буде свій електронний підпис, а також підключити до цієї мережі інститути, які надають нам медичні послуги, лікарні чи клініки.

Впровадження блокчейна в медицину і створення єдиної мережі може виглядати так, як на рисунку 3.2.

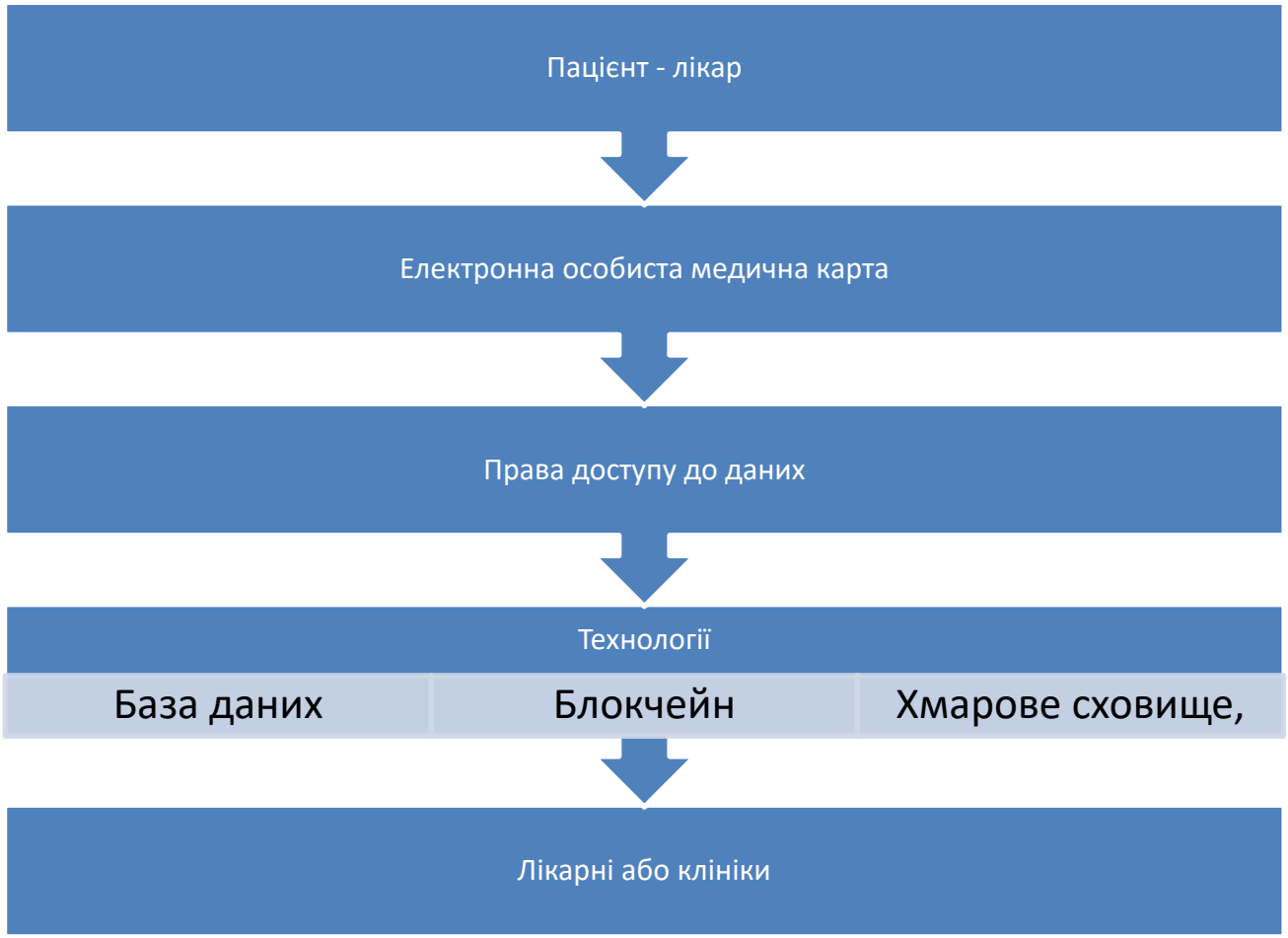

Рисунок 3.2 - Управління медичними даними в блокчейні.

Крок 1: Початкові дані та аналізи створюються під час взаємодії пацієнта і лікаря, який направляє на аналізи або обстеження. Дані містять медичну історію, поточні проблеми та іншу медичну інформацію.

Крок 2: Електронна медична карта містить усі документи, історію, аналізи та інше, зібране на кроці 1.

Крок 3: Тут створюється захист цих даних, оскільки їх власником є безпосередньо пацієнт. Сторони, які бажають отримати доступ до цієї інформації, повинні отримати дозвіл від особи, яка ними володіє.

Кроки 4, 5, 6: Цей етап є ключовим для системи, оскільки дані поміщаються в базу даних та хмарове сховище, де блокчейн забезпечує захист даних.

Крок 7: На цьому етапі використовуються ці дані лікарнями або іншими установами, куди конкретний пацієнт звертається. І незалежно від того, де

знаходиться пацієнт, вся інформація знаходиться в його телефоні, і він може нею скористатися в будь-який момент.

Якщо проаналізувати, які технології блокчейн можуть бути задіяні, то отримаємо приблизно таке:

Приватні блокчейни:

– електронна медична картка
– медична історія та документи

Блокчейн 2.0 – "etheruim blockchain":

– дані про пацієнта
– аналізи

Консорціумні блокчейни:

– медичні дані

Доказ принадності:

– медичні дані

Ця система дозволить підвищити захист та спростити бюрократію, щоб пацієнти могли отримувати медичну допомогу швидше та якісніше. Їм не доведеться носити з собою купу аналізів та свою історію хвороб, оскільки все буде в хмарі та легко доступне. Звісно, впровадження цієї системи залежить від бажання суспільства та влади.

3.3 Оборонна сфера

Впровадження технології блокчейн в оборонну сферу могло б принести ряд плюсів:

- безпека даних: Блокчейн забезпечує високий рівень безпеки завдяки своїй децентралізованій структурі та криптографічним методам. Це може бути особливо важливим в оборонній сфері, де конфіденційність та цілісність даних відіграють вирішальну роль.
- відстежуваність і прозорість: завдяки нередактіруемой природі блокчейна, операції і транзакції можуть бути легко відслідковані і верифіковані. Це може допомогти у виявленні будь-яких несанкціонованих дій або змін у системі.
- покращене управління логістикою: Блокчейн може бути використаний для поліпшення управління логістикою і ланцюгами поставок в оборонній сфері. Це допомагає знизити ризики втрати вантажів, поліпшити прозорість і ефективність процесів. Можна використати приклад літака F-16, який входить до озброєння США та складається з тисяч запчастин і деталей. В цьому випадку загальна логістична система буде саме тим, що потрібно для полегшення управління ланцюгами постачання.
- боротьба з корупцією: технологія блокчейн може допомогти в боротьбі з корупцією, оскільки всі операції будуть надійно захищені від маніпуляцій і фальсифікацій. Це підвищує довіру і прозорість в оборонній сфері.
- покращена автоматизація і ефективність: Блокчейн може скоротити необхідність в проміжних учасників і спростити процеси завдяки використанню смарт-контрактів. Це може призвести до підвищення автоматизації та ефективності в оборонній сфері.
- захист від кібератак: оскільки дані зберігаються в децентралізованій мережі, блокчейн може надати додатковий рівень захисту від

кібератак і хакерських атак. Цілком можливо використовувати блокчейн у військовій сфері у всіх напрямках – від "випуску озброєння" до запобігання видаленню інформації, що неможливо в разі звичайних баз даних. Крім того, блокчейн може підтримувати механізми управління та контролю за допомогою багатосторонньої аутентифікації. Якщо кілька сторін мають права на керівництво та вони повинні досягти консенсусу перед прийняттям певних заходів, то система буде краще захищена від помилок.

– інновації в галузі військових технологій: впровадження блокчейна може стимулювати інновації в оборонній сфері, від розробки більш безпечних систем зв'язку до поліпшення систем управління зброєю і автономних технологій.

Ці переваги підкреслюють потенціал технології блокчейн для поліпшення безпеки, ефективності та прозорості в оборонній сфері.

Так, багато розвинених країн і регіонів в даний час впроваджують технологію блокчейн в оборонну промисловість, щоб підвищити ефективність. Наприклад, Міністерство оборони США уклало угоду на 9,5 мільйонів доларів з компанією з блокчейном SIMBA Chain для розгортання платформи для обміну повідомленнями та виконання.

3.4 Торгівля

Також як і в інших сферах життєдіяльності, блокчейн застосуємо в торгівлі чим-завгодно. Наприклад, сфера нерухомості, продаж картин, роздрібна торгівля та ін.

3.4.1 Сфера нерухомості

Переваги блокчейн-технологій в продажі нерухомості полягають у забезпеченні прозорості, безпеки та ефективності у всьому процесі транзакції. Блокчейн може забезпечити безпеку та невід'ємність даних, що дозволить уникнути шахрайства та будь-яких змін договорів без дозволу всіх учасників. Крім того, він може забезпечити відстеження історії власності, що допоможе у вирішенні спорів та уникненні земельних конфліктів. Також блокчейн може зменшити витрати на операційні послуги та прискорити процес укладення угод завдяки автоматизації багатьох процесів. Також, завдяки смарт-контрактам забудовники зможуть швидше та зручніше продавати квартири, оскільки будь-хто, будучи в будь-якому місці, зможе переглянути документи на квартиру, а також фото або відео. Люди зможуть підписувати документи та угоди онлайн в системі, що прискорить цей процес. Крім того, послуги нотаріуса також можуть бути переведені в онлайн-режим, де він зможе підтвердити належність квартири до певної сторони. І завдяки властивостям смарт-контрактів ані забудовник, ані покупець не зможуть обманути один одного, і кожен отримає своє.

Наприклад, у 2019 році місцевий будівельний гігант в Бразилії залучив до співпраці місцевий стартап Growth Tech, завдяки якому був реалізований проект під назвою Notary Ledger. Цей проект дозволяє відстежувати та запитувати нотаріальні послуги у цифровому форматі. Даний проект був заснований на технологіях від компанії IBM Blockchain. Цей проект допоміг

забудовнику продати всі квартири приблизно за 20 хвилин. У майбутньому вони планують використовувати цю систему для видачі свідоцтв про народження, смерть і т. д. Документ із цим підписом також буде дійсним і матиме такі ж строки, як і документ, підписаний особисто в офісі, оскільки у їхньому випадку за угодою слідкував цілий консорціум нотаріусів. Ці операції матимуть більшу прозорість і безпеку, що скоротить кількість шахрайських угод і зменшити строки надання послуг.

3.4.2 Роздрібна торгівля

В останні кілька років блокчейн набирає обертів серед роздрібних організацій, урядових організацій і політиків, що призвело до того, що багато теоретичні приклади використання блокчейна в роздрібній торгівлі були реалізовані на практиці.

Наприклад, мережа Walmart Канада використовувала блокчейн, щоб вирішити, мабуть, найбільш поширену та постійну проблему, пов'язану з логістикою та транспортуванням – управлінням величезною кількістю накладних та платежів у мережі перевізників вантажів. Щорічно Walmart Канада доставляє понад 500 000 вантажів до розподільних центрів, розкиданих по всій країні, та покладається на 70 сторонніх перевізників вантажів для доставки цих товарів.

Організація руху величезної кількості продуктів є надзвичайною логістичною викликом. Кожному з тисяч місячних відправлень потрібно, щоб працівники вручну збирали та вводили понад 200 пунктів даних у кожну накладну. Величезна кількість ручної роботи, необхідної для переміщення товарів, неодмінно призводить до розбіжностей даних та затримок у реконсиліації. В результаті більше 70% накладних містили розбіжності в даних. Ці недоліки ланцюжка постачання в основному випливали з несумісності корпоративних систем, які використовували Walmart та ці 70 перевізників вантажів.

Для вирішення цих проблем Walmart Канада об'єднала зусилля з DLT Labs, розробником рішень блокчейн для підприємств. Після майже двох років строгого пілотного тестування дозволений блокчейн, відомий як DL Freight, був запущений у 2021 році. DL Freight тепер служить як єдине джерело правди для всіх учасників мережі, де на кожному етапі процесу всі дані незмінно записані в блокчейні. Після впровадження DL Freight лише 1% накладних були спірними, що в 70 разів менше, ніж до впровадження.

Далі компанія Carrefour, яка приєдналася до IBM Food Trust у 2018 році та постійно розширює перелік товарів, які відстежуються за допомогою блокчейну. У 2019 році Carrefour розпочав використання блокчейну для відстеження 20 видів продуктів, включаючи курку, яйця, молоко, сир та інші основні продукти. Завдяки QR-коду, прикріпленому до кожного продукту, клієнти можуть отримати докладну інформацію про його походження, включаючи ім'я виробника, дату збору врожаю, місце культивування та інші дані. У тому ж році Carrefour повідомив, що продукти, відстежувані за допомогою блокчейну, відзначаються помітно збільшеними обсягами продажів.

У 2021 році Carrefour розширила використання блокчейну в роздрібній торгівлі, впровадивши відстеження своїх ексклюзивних текстильних товарів. А в 2022 році стала першим роздрібним торговцем, який використовував блокчейн для відстеження власних органічних продуктів під брендом. Тепер увесь асортимент продуктів Carrefour Bio відстежується за допомогою блокчейну, що дозволяє споживачам з більшою впевненістю приймати рішення про покупку.

Цей процес влаштований так:

- фермери, скануючи QR-код, додають продукт в базу, реєструючи його, додаючи його тим самим в загальну блокчейн систему цієї компанії.
- далі на фабриці перевіряють вагу і якість товару і знову ж через QR-код, додають звіт про товар в систему.
- далі логістична компанія перевозить продукти до продавця.
- продавець перевіряє товар, скануючи QR-код і додає звіт про товар в систему.
- покупець через хмару, де зберігається вся інформація про товар, може прийшовши в магазин відсканувати QR-код і дізнатися хто, як, коли і в якій якості привіз цей товар.

З погляду бізнесу, використання Carrefour блокчейну дає йому перевагу перед конкурентами, оскільки це значно підвищує довіру клієнтів. Як зазначив керівник проекту блокчейну Carrefour, такі ініціативи створюють "хало-ефект", що забезпечує високу ймовірність того, що клієнти, які довіряють Carrefour одному типу продукту, будуть також довіряти йому й іншим.

3.4.3 Мистецтво

Блокчейн-технології або додатки в музиці, кіно або театрі можуть зробити прорив у цих сферах. Наприклад, візьмемо NFT, які стали популярними у 2020 році. Звичайно, це не найкращий приклад, оскільки ці картинки не представляли нічого значущого, але все ж. Це був перший крок до впровадження блокчейн-технологій в галузь мистецтва.

Під час COVID-19 основний заробіток індустрії мистецтва був через інтернет, що трохи змінило уявлення людей, особливо артистів.

Впровадження блокчейн-технологій в цю сферу дозволить скоротити кількість посередників між артистом і його аудиторією, що в подальшому дозволить артисту контролювати своє творіння і безпосередньо спілкуватися з аудиторією.

Також блокчейн-технології допоможуть артистам зберігати право власності на свої продукти і тим самим скоротити кількість піратського контенту в мережі.

Можна виділити ще кілька інших переваг впровадження технології блокчейн:

- сильний удар по монополіям в індустрії: Блокчейн дає можливість дрібним
- підприємцям-художникам покінчити з домінуванням великих аукціонних будинків і художніх галерей.
- анонімність створювача: блокчейн використовує публічні дані, при цьому створювач може залишитися непоміченим.
- підтвердження власності: у випадку втрати, поломки або видалення, право власності завжди залишиться за створювачем. Тому що в мережі блокчейн неможливо нічого змінити.
- підтвердження якості файлів: Блокчейн підтверджує створення оригінальних або високоякісних зображень у роботах.

– операції з криптовалютами: Суттєво прискориться продаж та покупка, при цьому банківські комісії зникнуть.
– загроза шахрайства: За рахунок використання смарт-контрактів зменшиться кількість обманутих і шахраїв на ринку мистецтва.
– оцифровка галерей: Фізичні простори втратять свою значимість на користь децентралізованого і автономного онлайн-ринку, який буде функціонувати завдяки інтелектуальним контактам.

Наприклад, застосунок Open Music Initiative, де створювачі продають свої продукти напряму. Ця платформа не прибуткова, вона просто дозволяє створювачам контролювати продажі своїх продуктів. Вони можуть переглянути кількість програвань їх музики і де вона була програна.

Блокчейн-сервіси з'явилися на ринку продажу квитків, щоб зменшити рівень шахрайства і спекуляцій. Смарт-квитки дозволяють створювати унікальні реєстри авторизованих покупців, щоб відповідальні за захід особи могли відстежувати та блокувати перепродаж квитків.

3.5 Переваги

У цьому розділі ми розглянемо переваги блокчейна. Наприклад, можна виділити такі переваги:

- надійність даних: Блокчейн забезпечує високий рівень надійності даних за рахунок криптографічного хешування та розподіленого збереження. Це робить його важким для змінення або фальсифікації даних.
- децентралізація: Блокчейн не має центрального пункту вразливості, оскільки кожен учасник мережі має копію блокчейну. Це ускладнює атаки типу "одна точка вразливості" і забезпечує більшу стійкість до кіберзлочинності.
- прозорість та імутабельність: Дані, збережені у блокчейні, доступні для перевірки та перевірки всіма учасниками мережі. Це забезпечує прозорість та довіру до даних. Крім того, імутабельність дозволяє відстежувати всі зміни, зроблені з даними, що робить їх непіддаємими модифікаціям.
- шифрування даних: Деякі блокчейн-платформи дозволяють шифрувати дані, що забезпечує додатковий рівень безпеки для конфіденційних інформаційних активів.

3.6 Обмеження

У цьому розділі ми розглянемо обмеження блокчейна. Наприклад, можна виділити такі обмеження:

– масштабування: Сучасна архітектура блокчейну ґрунтується на технології розподілених книг, що передбачає, щоб усі вузли в мережі підтверджували кожну транзакцію. Хоча це ефективний спосіб забезпечення безпеки та запобігання шахрайству, він також створює вузьке місце в системі. Чим більше вузлів додається в мережу, тим повільніше стає час обробки транзакцій. Це відбувається тому, що кожен вузол повинен підтвердити кожну транзакцію, що створює великий мережевий трафік і сповільнює роботу системи.
– ще однією проблемою поточної архітектури блокчейну є обмежена кількість транзакцій, які можуть бути оброблені за секунду. Наприклад, Bitcoin може обробляти лише 7 транзакцій на секунду, а Ethereum – 15 транзакцій на секунду. Це далеко від тисяч транзакцій на секунду, що обробляються традиційними платіжними системами, такими як Visa та Mastercard.
– вартість: Розгортання та підтримка блокчейн мереж може бути дорогою, особливо для приватних або корпоративних рішень, де необхідно створити та утримувати власні вузли.
– приватність: Хоча дані в блокчейні захищені криптографією, сама структура ланцюжка може розкривати деяку інформацію про транзакції, що порушує конфіденційність. Так, концепція блокчейну має свої недоліки, які можуть бути використані хакерами для успішних атак. Хакери можуть експлуатувати ці недоліки, щоб виконати різні види атак і завдати шкоди системі.
– легалітет: Багато країн ще не регулюють технологію блокчейн, що може створювати правову невизначеність для бізнесів та користувачів.

– енергозалежність: Деякі консенсусні механізми, такі як Proof-of-Work, вимагають великих кількостей енергії для майнінгу, що може призводити до екологічних проблем.

Хоча блокчейн має свої обмеження, його переваги у забезпеченні безпеки даних в багатьох випадках важливіше за них, особливо в умовах, де довіра та надійність є критичними.

3.7 Атаки на систему блокчейн

Безумовно, жодна технологія не може бути на 100% захищеною, і блокчейн не є винятком. Атаки на розподілені бази даних відрізняються способом взлому: метою є механізм консенсусу, що дозволяє змінювати інформацію, яка вноситься в реєстр.

Ось кілька прикладів хакерських атак на системи блокчейн:

– атака 51% – це найбільш поширена загроза для мережі блокчейн. Назва атаки – аналогія з контрольним пакетом акцій у бізнес-сфері. Проблема полягає в протоколі Proof-of-Work, який використовують такі проекти, як Bitcoin, Litecoin, Monero та інші: атака полягає в узгодженому дії більшості власників всього підключеного обчислювального обладнання. Такі умови дозволяють хакеру здійснити атаку подвійного витрачання, під час якої він може витратити більшу суму, ніж має в своєму гаманці. У результаті відбувається захоплення блокчейну, і всі кошти учасників переходять у власність хакерів. У великих мережах ймовірність проведення такої атаки в декілька разів нижче через велику кількість учасників і високоцінне обладнання. У серпні 2016 року блокчейни Ethereum, Krypton і Shift стали жертвами атаки 51%. За допомогою подвійного витрачання були вкрадені мільйони монет. Після нападу розробники посилили захист мереж, наприклад, в Krypton збільшили кількість підтверджень, необхідних для здійснення транзакції, до тисячі.

– атака Eclipse, відома також як атака затемнення, є особливим типом кібератаки, коли хакер створює штучну область біля одного вузла для контролю над його діями. Зловмисник перенаправляє вихідні та вхідні дані з цільового вузла на свої власні, відокремлюючи обманутого користувача від реальної мережі. Ізоляція цільового вузла дозволяє підтверджувати неправомірні транзакції від його імені та відрізати його від обміну даними з сусідніми вузлами – хакеру не

потрібно взламувати мережу в цілому, він обмежується невеликим набором вузлів. Для блокування вузла використовується ботнет або фантомна мережа для заповнення вузла IP-адресами для синхронізації при наступному підключенні. Наслідками атаки затемнення зазвичай є атаки подвійного витрачання, про які вже було сказано вище, а також порушення живлення майнера, коли взломлений користувач витрачає електроенергію та час на вирішення завдань штучних блоків, які не існують у реальній мережі блокчейна.

– атака Сивілли – це найпоширеніший тип атак на P2P-мережі (мережі з однорівневою архітектурою з рівними учасниками). Цей метод отримав свою назву на честь відомого випадку, коли жінка страждала від дисоціативного розладу особистості: вузол у блокчейні також набуває декількох сутностей. Для проведення атаки зловмисники об'єднуються та контролюють значну кількість вузлів у мережі. Після виконаних маніпуляцій та захоплення необхідної кількості вузлів хакери намагаються вивести мережу з ладу, керуючи валідними та створюючи невалідні транзакції. Вперше атаку Сивілли описав експерт з Microsoft Джон Доссі, на думку якого мережа не може відрізняти фізичне обладнання. Були зроблені спроби створення та впровадження механізмів для розпізнавання та ідентифікації ПК, але безрезультатно. Збиток від такої атаки може мати різноманітні наслідки – від накрутки рейтингу до фальсифікації голосів. У випадку успіху зловмисник може відключити взламаних користувачів від мережі, здійснити атаку 51% та двоїстого витрачання, а також переглядати потік усіх проведених транзакцій завдяки спеціальним програмам.
– DDoS-атаки, що також називаються атаками відмови у обслуговуванні, базуються на відправці великої кількості ідентичних запитів. У Bitcoin існує вбудований захист від таких випадків. Наприклад, розмір блоків і скриптів у мережі обмежений, що

ускладнює можливість засмічення пулів пам'яті вузлів. Крім того, кількість підписів для перевірки та запитів на перевірку багатоключів також обмежена. Клієнти блокчейна блокують транзакції вузлів з підозрілою активністю. У одному з останніх оновлень Bitcoin Satoshi була впроваджена функція для реєстрації нетипових транзакцій вагою понад 100 кілобайт. Окрім адресата перевіряється гаманець і валідність адресата.

Авжеж, існує багато різних способів обману або взлому, проте всі вони досить складні для втілення і потребують все більше підготовки, оскільки технології блокчейн не стоять на місці і постійно вдосконалюються кожен день.

3.8 **Рекомендації щодо використання blockchain для безпеки даних**

Ось деякі рекомендації щодо використання технології блокчейн для забезпечення безпеки даних:

- оцінка потреб: Перш ніж впроваджувати блокчейн, важливо ретельно проаналізувати потреби вашої компанії та визначити, чи відповідає блокчейн цим потребам. Використання блокчейну має сенс там, де потрібна децентралізована система збереження даних та відстеження їхньої історії.
- вибір підходящої платформи: Виберіть блокчейн-платформу, яка найкращим чином відповідає вашим потребам та вимогам проекту. Це може бути публічний, приватний чи консорціальний блокчейн, залежно від рівня конфіденційності та контролю, який ви шукаєте.
- забезпечення безпеки ключів доступу: Важливо дотримуватися найвищих стандартів безпеки для збереження і управління приватними ключами доступу до блокчейн-гаманця або облікового запису. Ці ключі є важливими для забезпечення доступу до цифрових активів.
- шифрування даних: Використовуйте шифрування для захисту конфіденційних даних перед їхнім збереженням у блокчейні. Це додасть додатковий рівень безпеки та захистить ваші дані від несанкціонованого доступу.
- аудит та відповідність: Підтримуйте ретельний аудит та відстеження всіх транзакцій у вашій блокчейн-мережі. Це допоможе виявити будь-які аномальні дії та забезпечити відповідність з правовими вимогами.
- навчання та підготовка персоналу: Проведіть навчання для вашого персоналу щодо безпеки та використання блокчейн-технології. Це допоможе забезпечити правильне розуміння та ефективне використання цієї технології.

– постійне оновлення безпекових заходів: Слід постійно оновлювати свої заходи безпеки, оскільки кіберзагрози постійно еволюціонують. Використовуйте нові техніки та заходи, щоб захистити свої дані від потенційних загроз.

Враховуючи ці рекомендації, ви зможете максимально забезпечити безпеку даних у своїй блокчейн-мережі.

3.9 Заключення

В заключенні хотілося б відзначити, що блокчейн – це дуже нова і не досліджена технологія, якій ще дуже довго потрібно проявити себе, щоб вона могла підірвати усталену систему. Основними проблемами для впровадження будуть набагато більші електропотребування, яке в деяких країнах відіграє важливу роль. Далі по списку – високі витрати на розробку технології та її підтримку. Ще однією проблемою може стати те, що ця технологія умовно безкоштовна. Тому що в патентному бюро США понад 1 тисяча патентів на розподілені реєстри, отже компанії не дарма патентують свої винаходи, щоб у майбутньому отримати з них прибуток. Далі можна згадати про анонімність. Так, з одного боку, ця система анонімна для інститутів, які не мають стосунку до цієї системи, але, наприклад, спецслужби чи держава, у якої є законний доступ до всіх даних, наприклад, банку, вони можуть легко дізнатися, як, куди і скільки ви переказали грошей, саме через те, що система блокчейн дуже прозора.

ВИСНОВКИ

Технологія блокчейн привертає дедалі більше уваги в багатьох галузях завдяки своїм унікальним властивостям, серед яких найбільш значущими є забезпечення безпеки та цілісності даних. Блокчейн – це розподілена база даних, де всі транзакції зберігаються у вигляді блоків, які з'єднані між собою криптографічними засобами. Ця структура дозволяє створити прозору та децентралізовану систему, яка має високий рівень захисту від змін та підробок.

ПЕРЕЛІК ПОСИЛАНЬ

1. Prihodko P. Flare: An Approach to Routing in Lightning Network. електрон. версия. 2016. Дата оновлення: 07.2016. URL : https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf (дата звернення: 15.04.2024)

2. Mamoshina P. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. електрон. версия. 2017. Дата оновлення: 02.2017. URL : https://bitfury.com/content/downloads/11_9_17_bitfury_insilico_research_paper.pdf (дата звернення 16.04.2024)

3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. електрон. версия. 2009. Дата оновлення: 2009. URL : https://bitcoin.org/bitcoin.pdf (дата звернення: 17.04.2024)

4. Andreas M. Antonopoulos. Mastering Bitcoin. 2010. Дата оновлення: 12.2014. URL : https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf (дата звернення: 18.04.2024)

5. Pradeep A. What are Blockchain nodes? 2024. Дата оновлення: 10.04.2024. URL : https://www.blockchain-council.org/blockchain/blockchain-nodes/ (дата звернення: 19.04.2024)

6. Consensys.io. Blockchain in Financial Service. електрон. версия. 2024. URL : https://consensys.io/blockchain-use-cases/finance#capitalmarkets (дата звернення: 20.04.2024)

7. Blockchain Technology Market Size & Trends. 2023. електрон. версия. Дата оновлення: 2023. URL : https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market (дата звернення: 21.04.2024)

8. Блокчейн 3. 2023. електрон. версия. Дата оновлення: 13.10.2023. URL : https://learn.bybit.com/ru/glossary/definition-blockchain-3.0 (дата звернення: 22.04.2024)

9. Ющенко Н. Розвиток блокчейн-технологій в Україні та світі. 2018. електрон. версия. Дата оновлення: 2018. URL : https://economyandsociety.in.ua/journals/19_ukr/40.pdf (дата звернення: 23.04.2024)

10. Конах Ю. Правові аспекти застосування систем на основі технології блокчейн. Магістерська робота. 2018. електрон. версия. Дата оновлення: 2018. URL : https://core.ac.uk/download/pdf/323529564.pdf (дата звернення: 24.04.2024)

11. Костенко О. Блокчейн і метавсесвіт: правові аспекти. 2022. електрон. версия. Дата оновлення: 09.2022. URL : http://lsej.org.ua/9_2022/123.pdf (дата звернення: 25.04.2024)

Декларація

академічної доброчесності

здобувача ступеня вищої освіти ЗНУ

Я, Власенко Дмитро Максимович

студент __4__ курсу, _____ заочної_____ форми навчання, математичного факультету, спеціальності 121 Комп'ютерні науки, адреса електронної пошти _____dmitriy.vol.vlasenko@gmail.com_____, –

підтверджую, що написана мною кваліфікаційна робота магістра на тему «ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ТА ЦИФРОВИХ ТРАНЗАКЦІЙ» відповідає вимогам академічної доброчесності та не містить порушень, що визначені у ст. 42 Закону України «Про освіту», зі змістом яких ознайомлений/ознайомлена;

– заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії;

– згоден/згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності у будь-який спосіб, у тому числі за допомогою інтернет-системи, а також на архівування моєї роботи в базі даних цієї системи.

Студент

30.05.2024		Власенко Д.М.
(дата)	(підпис)	(прізвище, ініціали)

Науковий керівник

(дата)	(підпис)	(прізвище, ініціали)