Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Аналіз технології блокчейн у сфері кібербезпеки та захисту інформації
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-21-2
Поліщук В.Г.
(прізвище, ініціали)
Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Акулінічев А.А.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Поліщуку В’ячеславу Геннадійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Аналіз технології блокчейн у сфері кібербезпеки та захисту інформації
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2023р.
3. Вихідні дані до роботи: аналітичні дані щодо основних можливостей технології блокчейн та використання технології блокчейн, як засіб для цифрової ідентифікації
4. Перелік питань, що потрібно опрацювати в роботі:
1) Ключові особливості технології блокчейн
2) Можливості використання технології блокчейн
3) Аналіз впровадження технології блокчейн, як засобу для цифрової ідентифікації

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Куля Юлія Едуардівна		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	25.02.2023	Виконано
3	Розробка 1 розділу	05.03.2023	Виконано
4	Розробка 2 розділу	20.03.2023	Виконано
5	Розробка 3 розділу	20.04.2023	Виконано
6	Оформлення кваліфікаційної роботи	15.05.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студент _____ Поліщук В.Г.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Акулінічев А. А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 13 рис., 1 додаток, 23 джерел.

БЛОКЧЕЙН, ДЕЦЕТРАЛІЗАЦІЯ, ТЕХНОЛОГІЇ, ПРИВАТНІСТЬ КРИПТОГРАФІЯ, СМАРТ-КОНТРАКТИ, МАЙНІНГ, ХЕШ-ФУНКЦІЇ, ЦИФРОВИЙ ПІДПИС, ПРИВАТНИЙ КЛЮЧ, ЦИФРОВА ІДЕНТИФІКАЦІЯ, КОНСЕНСУНС, МАСШТАБОВАНІСТЬ, БЕЗПЕКА, НЕЗМІННІСТЬ.

Об'єкт дослідження – процес побудови та використання децентралізованих систем.

Предмет дослідження – методи й засоби побудови блокчейн мереж.

Мета роботи – аналіз шляхів підвищення інформаційної безпеки та досягнення більшої ефективності сучасних систем управління шляхом впровадження блокчейн систем.

Методи досліджень – емпіричний аналіз, формалізація та порівняння.

В нашу інформаційну епоху питання безпеки даних стало одним з найбільш важливих. Здається, що все наше життя стало відслідковуватися через бази даних, а наша конфіденційна інформація стала вразливою.

У роботі проведено дослідження що до блокчейн мереж, принципів функціонування та їх впливу на інформаційну безпеку. Розглянуто їхні переваги та недоліки. Розглянуто як впровадження блокчейн технологій може вплинути на різні сфери діяльності. Особлива увага приділена тому, як блокчейн може змінити методи та засоби цифрової ідентифікації. Також розглянуто яких змін у безпеці можна досягти якщо в майбутньому блокчейн технології змінять поточні системи управління у різноманітних напрямках використання.

ABSTRACT

The report contains: 75 p., 13 figs., 1 application, 23 sources.

BLOCKCHAIN, DECETRALIZATION, TECHNOLOGIES, PRIVACY, CRYPTOGRAPHY, SMART CONTRACTS, MINING, HASH FUNCTIONS, DIGITAL SIGNATURE, PRIVATE KEY, DIGITAL IDENTIFICATION, CONSENSUS, SECURITY, CONSTANCY.

A research object is process of building and using decentralized systems.

The subject of research is methods and means of building blockchain networks.

An aim of work is an analysis of ways to increase information security and achieve greater efficiency of modern management systems through the introduction of blockchain systems.

Methods of researches are empirical analysis, formalization and comparison.

In our information age, the issue of data security has become one of the most important. It seems that our whole lives have been tracked through databases, and our confidential information has become vulnerable.

The research is carried out in the work of blockchain networks, the principles of operation and their impact on information security. Their advantages and disadvantages are considered. Considered how the implementation of blockchain technologies can affect various spheres of activity. Special attention is paid to how blockchain can change the methods and means of digital identification. It is also considered what changes in security can be achieved if in the future blockchain technologies change the current management systems in various areas of use.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AML – anti-money laundering
Dapps – decentralized application
DeFi – decentralized finance
ECC – elliptic curve cryptography
ECDSA – elliptic curve digital signature algorithm
KYC – know your customer
NFT – non-fungible token
PKC – public key cryptography
PoS – proof of stake
Pow – proof of work
SHA-256 – secure hash algorithm
txid – transaction id

ВСТУП

Кібербезпека та захист інформації стали особливо актуальними питаннями у сучасному світі, де технологічний прогрес та все більша інтеграція цифрових технологій у повсякденне життя призводять до підвищення рівня ризику для особистих даних користувачів. Традиційні централізовані системи, хоча і забезпечують певний рівень безпеки, все ж таки не відповідають повністю сучасним вимогам, оскільки вони створюють умови для зловживань, витоку даних та кібератак на один центральний вузол.

Централізація, на відміну від децентралізації, характеризується наявністю одного головного органу або центру управління, який контролює рішення та процеси в системі. Цей підхід має свої переваги, такі як спрощена координація, єдині стандарти та забезпечення порядку. Однак централізація також призводить до зосередження влади, можливості зловживань, залежності від одного пункту відмови та відсутності гнучкості при адаптації до швидко змінюваних умов. Відповідно, існує потреба в альтернативних підходах, які можуть відповісти сучасним вимогам безпеки, прозорості та ефективності, якими володіють децентралізовані системи на основі блокчейну.

Децентралізація в інформаційних системах стала не просто черговим витком технологічної еволюції, вона пропонує кардинально новий підхід, який здатний змінити принципи взаємодії людей. Децентралізація – це процес перерозподілу функцій та повноважень від централізованого управління. Децентралізовані системи передбачають наявність багатьох незалежних учасників, які спільно здійснюють управління процесами. Такий підхід вимагає від учасників спільної дії для дієвої взаємодії без центральної сторони.

Це революційне переосмислення традиційних систем управління привносить величезний потенціал для підвищення ефективності, гнучкості та стійкості до зовнішніх впливів. Оскільки децентралізовані системи відрізняються від класичних централізованих структур, вони забезпечують інноваційні рішення для вирішення сучасних проблем, таких як конфіденційність даних, кібербезпека, прозорість управління та відповідальність.

Одним з найяскравіших прикладів децентралізації є розвиток технології блокчейн, яка дозволяє створювати глобальні, безпечні та непідробні реєстри для зберігання інформації про різні види операцій та активів.

Згідно з принципами децентралізації, блокчейн технологія надає можливість створення мережі, в якій усі учасники мають рівні права та можуть взаємодіяти один з одним без посередників. Вони взаємодіють на основі певних протоколів та консенсусів, які забезпечують згоду учасників щодо дійсності даних та транзакцій.

Блокчейн же, як один з інструментів децентралізації, надає можливість створювати розподілений, але уніфікований запис даних, забезпечуючи високу безпеку та прозорість. Технологія блокчейн є потенційно революційною технологією, оскільки учасники звільняються від необхідності наявності довіри між ними та централізованим регулюючим органом. Створення блокчейн систем має безліч переваг у різних галузях, оскільки вони забезпечують підвищену прозорість і безпеку даних, а також надають можливість створювати автономні та масштабовані рішення для глобальної кооперації між учасниками.

Блокчейн може бути використаний в різних сферах, включаючи фінанси, логістику, охорону здоров'я, громадські послуги, цифрову ідентифікацію та багато інших. Ця технологія дозволяє створювати безпечні та прозорі системи обліку та обміну даними, що може підвищити ефективність та зменшити витрати в цих галузях.

Крім того, використання децентралізованих систем для цифрової ідентифікації сприяє збільшенню довіри між учасниками, оскільки всі дані відкриті та прозорі, але в той же час захищені від несанкціонованого доступу та змін. Таким чином, блокчейн може відігравати ключову роль у розвитку безпечних та децентралізованих інформаційних систем, спрощуючи взаємодію між людьми та організаціями та знижуючи ризики зловживання персональними даними.

На мою думку, у майбутньому можемо очікувати все більше застосувань блокчейну у сфері цифрової ідентифікації, зокрема для надання онлайн-сервісів, доступу до ресурсів та систем, електронного голосування та навіть управління міжнародними паспортами та візами. Це забезпечить безпечніше та ефективніше середовище для взаємодії між людьми та технологіями, яке відповідає вимогам сучасного світу та його швидкому технологічному розвитку.

1 КЛЮЧОВІ ОСОБЛИВОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

1.1 Принципи функціонування блокчейну

Блокчейн – це технологія зберігання та передачі даних в децентралізованій мережі, що базується на послідовному зв'язку блоків. Кожен блок містить унікальний хеш, який відображає весь блок та його вміст, а також хеш попереднього блоку, що підтверджує послідовність блоків та їх зв'язок між собою. Блокчейн забезпечує високу безпеку та надійність даних завдяки використанню криптографічних функцій, які гарантують цілісність та недоступність для зміни або видалення даних, що раніше було записано у блокчейні [1].

Структура блокчейна складається з ланцюжка блоків, кожен з яких представляє собою окрему частину інформації, яка додається до бази даних. Кожен блок має свій унікальний ідентифікатор та інформацію про попередній блок, що формує ланцюг блоків. Інформація в кожному блоку також містить дані про транзакції, дату та час, та інші додаткові дані, що підтверджують правильність блоку. Оскільки блоки пов'язані між собою, записи не можуть бути вилучені, змінені, або відредаговані, так як це призведе до порушення структури блокчейна. Схематично структуру блокчейну зображено на рисунку 1.1.

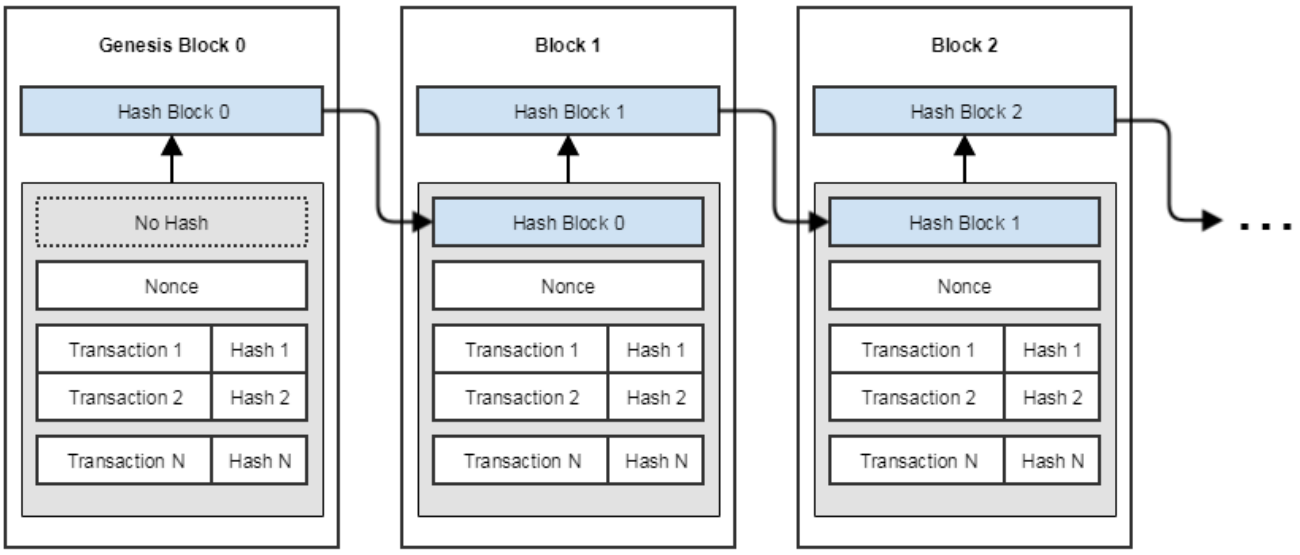


Рисунок 1.1 – Структура блокчейну

Блокчейн працює за принципом децентралізації та консенсусу, тобто він

забезпечує зберігання та передачу даних без посередництва центрального органу, а керування мережею відбувається за рахунок взаємодії всіх її учасників. Коли нові дані готові до додавання в блокчейн, вони транслюються всім учасникам мережі. Кожен учасник може взяти участь у процесі перевірки та підтвердження правильності цих даних, використовуючи свої обчислювальні ресурси та криптографічні алгоритми. Якщо більшість учасників підтверджує правильність даних, вони додаються до нового блоку, який потім підключається до попереднього блоку за допомогою хеш-суми [2].

Щоб перевірити стан блокчейн-мережі особисто, користувач повинен завантажити спеціальне програмне забезпечення. Після установки програми і її запуску на комп'ютері користувача, вона взаємодіє з екземплярами мережі на інших комп'ютерах з метою завантаження або скачування інформації, наприклад інформація про транзакції або блоки. Новий користувач завантажує блок, щоб переконається в тому, що він був створений в рамках правил системи, і передає цю інформацію іншим вузлам мережі. Таким чином виходить екосистема, яка може складатися з сотень, тисяч або десятків тисяч об'єктів, які запускають і синхронізуються з однієї і тієї ж копії бази даних. Такі об’єкти називаються вузли або ноди. Це робить мережу цілодобово доступною.

Цілісність блокчейну підривається якщо записати помилкову інформація про фінансові операції. Так як у розподіленій системі відсутній адміністратор або керівник, який міг би підтримувати роботу мережі. Для того щоб дати гарантію того, що всі учасники будуть діяти чесно, було запропоновано використання алгоритму консенсусу. Алгоритм консенсусу в блокчейні являє собою набір певних математичних правил і функцій, які дозволяють досягти згоди між усіма учасниками і забезпечити працездатність мережі.

Технологія блокчейн може застосовуватися до широкого кола підприємств і може бути використана у різних випадках. Незалежно від контексту, мережа блокчейн буде побудована на певному протоколі, який визначає правила роботи системи. Усі частини системи та учасники мережі повинні дотримуватись цих правил. Алгоритм консенсусу визначає, які заходи необхідно вжити для дотримання цих правил і отримання бажаних результатів. У контексті блокчейну, алгоритм консенсусу відповідає за валідацію транзакцій та блоків [3].

Існує кілька різних технологій консенсусу, які використовуються в блокчейні, кожна з них має свої переваги та недоліки. Найпоширеніші з них.

1) Proof of Work (PoW) – це технологія консенсусу, яка базується на

розрахунку складності задачі. У цій технології, майнери розв'язують складну математичну задачу, щоб здійснити транзакції та отримати винагороду. Проблема цієї технології полягає в тому, що вона вимагає великої кількості обчислень, що збільшує споживання енергії та вартість майнінгу [4].

2) Proof of Stake (PoS) – це алгоритм консенсусу, в якому вирішальним фактором стає кількість монет, які власник має у власному розпорядженні. У цьому алгоритмі власники монет, які утримують їх на своїх гаманцях, мають право на голосування за наступний блок, який буде доданий до блокчейну. Шанс виграти голосування пропорційний кількості монет у власності власника. У випадку успішного голосування власник монет отримує винагороду у вигляді нових монет. Перевагою цієї технології є менше споживання енергії, але вона може призвести до зосередження влади у руках великих власників криптовалюти.

PoW перший алгоритмом консенсусу, який був створений. Він використовується Bitcoin і багатьма іншими криптовалютами. Алгоритм Proof of Work є невід'ємною частиною майнінг процесу. Майнінг PoW включає в себе численні спроби хешування, тому чим більше обчислювальна потужність, тим більше спроб в секунду. Щоб підтвердити блок, суб'єкт даного процесу повинен пожертвувати своєю обчислювальною потужністю, щоб підібрати правильне рішення, встановлене протоколом.

Така робота включає в себе багаторазове хешування даних для отримання числа, нижче певного числового значення. Такий процес називається майнінг. Якщо майнер правильно вгадує рішення блоку, йому надається можливість його сформувати з непідтверджених транзакцій, які були йому відправлені, і таким чином розширити ланцюжок. В результаті своєї роботи, він отримує винагороду, виражену в нативному токені даного блокчейна.

Отже, майнер з високим хешрейтом має більше шансів знайти правильне рішення для наступного блоку. Алгоритм консенсусу PoW гарантує, що майнери зможуть тільки підтверджувати новий блок транзакцій і додавати його в блокчейн, якщо розподілені вузли мережі досягають консенсусу і погоджуються з тим, що хеш блоку, наданий майнером, є підтвердженим Proof of Work, тобто валідований доказом роботи.

Існують також інші моделі, такі як Proof of Stake – підтвердження частки володіння, які не вимагають такої великої обчислювальної потужності і вимагають менше електроенергії, надаючи можливість масштабування для більшої кількості користувачів.

Алгоритм консенсусу Proof of Stake замінює технологію майнінгу PoW механізмом, в якому блоки перевіряються відповідно до часток учасників. Валідатор кожного блоку визначається на основі вкладеної криптовалюти, а не кількістю виділеної обчислювальної потужності. Кожна система PoS може реалізувати алгоритм по різному, але в цілому блокчейн забезпечується псевдовипадковим процесом виборів, який враховує багатство вузла і те, як довго монети заблоковані або знаходяться в частці, поряд з фактором рандомізації [5].

Алгоритми консенсусу мають вирішальне значення для підтримки цілісності і безпеки мережі. Вони забезпечують стан розподілених вузлів, що досягають консенсусу, щодо того, яка версія блокчейна є дійсною. Згода на поточний стан блокчейна, має важливе значення для правильної роботи системи.

Отже, блокчейн – це технологія, яка базується на розподіленій базі даних, в якій записи зберігаються у блоках, які організовані в хронологічному порядку і захищені криптографічними доказами та зв'язані між собою за допомогою хеш-сум.

1.2 Основні принципи транзакцій у блокчейні

Транзакція в блокчейні – це процес збереження даних, що супроводжується передачею криптовалют або іншої інформації між гаманцями. Після створення транзакції в гаманці та її підписання цифровим підписом на основі закритого ключа, транзакція надсилається. Під час перевірки валідаторами блокчейну, які отримують комісійну винагороду, транзакція підтверджується, а комісію за неї сплачує відправник.

Коли транзакція успішно підтверджена, вона включається в блок, а відправити таку ж інформацію двічі неможливо. Після збереження транзакції в блокчейні можна знайти її за допомогою унікального хешу, який часто називають ідентифікатором транзакції або transaction ID (txid). Хеш кожної транзакції є унікальним в межах блокчейну [6].

Кожна транзакція в блокчейні підписується цифровим підписом, створеним за допомогою приватного ключа гаманця. Це забезпечує надійність та безпеку транзакцій у мережі, оскільки тільки власник приватного ключа може підписати транзакцію і здійснити переказ активу.

Крім того, у більшості блокчейнів є механізм підтвердження транзакцій, який використовується для забезпечення безпеки та виключення можливості подвійного витрачання активів. У Bitcoin цей механізм називається «Proof of Work», в Ethereum

– «Proof of Stake», а в інших блокчейнах можуть використовуватись інші механізми. Вся інформація про транзакції у публічному блокчейні є загальнодоступною та прозорою, включаючи адресу відправника та одержувача, переказану суму та інші дані. За допомогою технологій анонімізації основні дані транзакцій можуть бути приховані на деяких блокчейнах. Транзакції можна створювати як у гаманці, підключеному до мережі, так і в автономному режимі з можливістю затримки надсилання.

У блокчейні можуть бути різні види транзакцій. Основні види транзакцій, які зустрічаються у більшості блокчейнів.

1) Переказ коштів: це найпоширеніший вид транзакцій, який використовується для відправки криптовалют між різними адресами у мережі. У таких транзакціях вказується сума, яка буде переведена з однієї адреси на іншу.

2) Створення контракту: цей вид транзакцій використовується для створення нових контрактів, які містять програмний код, який виконується автоматично при виконанні певних умов.

3) Виконання контракту: такі транзакції виконують програмний код, що міститься у контракті. При цьому зазвичай здійснюється переказ криптовалюти або зміна стану контракту.

4) Виконання DApp: такі транзакції використовуються для виконання децентралізованих додатків, які запускаються на блокчейні. У цих транзакціях можуть бути вказані параметри для запуску DApp, такі як адреса контракту, вхідні дані тощо.

5) Внесення змін до блокчейну: цей вид транзакцій використовується для внесення змін до самого блокчейну, наприклад, зміна протоколу або параметрів мережі.

6) Перевірка статусу транзакції: цей вид транзакцій використовується для отримання інформації про статус вже відправленої транзакції, наприклад, чи вона була успішно відправлена та підтверджена в мережі.

У кожному блокчейні можуть бути свої особливості та додаткові типи транзакцій.

Схема транзакція складається зі входу, суми переданого активу та виходу. Входи – це активи, які були отримані у вхідних платежах та наразі наявні в гаманці, і вони передаються у транзакції. При створенні транзакції відправник створює вихідний платіж на потрібну суму, який називається виходом. Виходи однієї транзакції потім використовуються новим власником як входи нових транзакцій.

Транзакція може бути змінена або перенаправлена тільки до того, як вона буде підтверджена в мережі. Після додавання транзакції в блок, вона залишається в блокчейні назавжди і зберігається на всіх повних вузлах мережі. Для зміни будь-якої транзакції, яка вже зберігається в блокчейні, доведеться перебудувати всі блоки, які були створені після запису цієї транзакції [7].

Залежно від блокчейну, можуть бути різні обмеження на кількість входів і виходів в одній транзакції. Також може бути встановлена комісія за транзакцію, яка сплачується в криптовалюті і призначена мережевим вузлам, які перевіряють транзакцію та додають її в блокчейн. У процесі транзакції можуть виникати різні помилки або проблеми. Наприклад, може статися так, що відправник передав занадто малу комісію за транзакцію, і через це її не обробили протягом деякого часу. При створенні транзакції, важливо правильно встановити комісію, яка визначається витратами на обробку транзакції мережею. Занадто низька комісія може призвести до того, що транзакція не буде оброблена, а занадто висока може призвести до зайвих витрат.

Загалом, транзакції в блокчейні є важливим елементом функціонування цієї технології. Вони дозволяють передавати активи та іншу інформацію між учасниками мережі без посередництва централізованих інституцій, а також забезпечують безпеку та стійкість блокчейну. Однак, при роботі з транзакціями необхідно дотримуватися певних правил та використовувати належні засоби захисту, щоб уникнути втрати активів чи інших проблем.

Крім зберігання і передачі криптоактивів, транзакції можуть містити іншу корисну інформацію, таку як текстові повідомлення, дані про товари чи послуги, що купуються або продаються, та інші дані, які можуть зберігатися в блокчейні. Крім того, у деяких блокчейнів є можливість створювати розумні контракти, що дозволяють автоматизувати виконання угод і забезпечують безпеку операцій за допомогою технології криптографічних підписів.

Отримувачі транзакцій у блокчейні можуть перевірити автентичність отриманої інформації, а відправники можуть бути впевнені, що їхні операції будуть збережені в мережі блокчейну назавжди. Крім того, транзакції у блокчейні є прозорими та загальнодоступними, що забезпечує високий рівень безпеки та контролю.

Багато блокчейн-систем дозволяють створювати програми, які можуть автоматично генерувати транзакції, що робить їх використання більш зручним та ефективним. Крім того, транзакції можна здійснювати не лише з криптовалютами,

а й з будь-якими іншими активами, такими як нерухомість, права на інтелектуальну власність, цінні папери та інші.

Усі транзакції у блокчейні є незворотними, тобто після їх підтвердження і запису в блокчейн, неможливо відмінити операцію. Тому важливо бути обережним при відправці транзакцій і перевіряти всю інформацію, що вводиться перед її підтвердженням. Загалом, транзакції у блокчейні є важливою складовою технології, яка дозволяє безпечно та ефективно здійснювати різноманітні операції, забезпечуючи високий рівень автентичності, прозорості та безпеки.

1.3 Забезпечення безпеки технології блокчейн

Безпека є одним з ключових аспектів технології блокчейн, оскільки вона забезпечує надійність системи і захист від можливих атак. Оскільки блокчейн мережа є розподіленою і децентралізованою, вона має покращену стійкість до кібератак та має високу надійність.

Блокчейни використовують різні механізми безпеки, такі як передові криптографічні методи, математичні моделі поведінки та прийняття рішень. Найважливішими функціями для забезпечення безпеки блокчейну є концепції консенсусу та незмінності. Консенсус забезпечує здатність вузлів у мережі узгоджувати справжній стан мережі та достовірність транзакцій, і його досягнення залежить від алгоритмів консенсусу. Незмінність дозволяє блокчейну уникнути змін у підтверджених транзакціях, що забезпечує цілісність даних та записаних транзакцій. Поєднання цих функцій є основою безпеки даних у блокчейні, яке забезпечує дотримання системних правил та узгодження всіх сторін з поточним станом мережі. Кожен новий блок перевіряється перед його додаванням до блокчейну, що забезпечує цілісність та безпеку даних у блокчейн технології [8].

Блокчейни в значній мірі покладаються на криптографію для забезпечення безпеки даних. Однією з надзвичайно важливих криптографічних функцій у цьому контексті є хешування. Хешування – це процес, при якому алгоритм, відомий як хеш-функція, отримує вхідні дані будь-якого розміру і повертає певний висновок, що містить значення фіксованої довжини.

Незалежно від розміру вхідних даних, вихід завжди має однакову довжину. Якщо вхід зміниться, результат буде зовсім іншим. Однак, якщо вхідні дані не змінюються, отриманий хеш завжди однаковий, незалежно від того, як часто виконувалася хеш-функція. Наприклад, якшо алгоритмом SHA-256, який

використовується у біткойні, захешувати дві майже однакові фрази змінивши тільки регістр першої літери, то в результаті буде отримано зовсім різні результати. Приклад такого хешування показано на рисунку 1.2.

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Рисунок 1.2 – Приклад хешу за алгоритмом SHA-256

У блокчейнах хеші використовуються як унікальний ідентифікатор кожного блоку даних. Кожен блок містить хеш попереднього блоку, тому їх можна зв'язати в один ланцюжок. Крім того, хеш кожного блоку залежить від даних, що містяться в цьому блоку, що означає, що будь-яка зміна даних у блоку призведе до зміни його хешу. Таким чином, хеш-ідентифікатори кожного блоку базуються на даних, які він містить, та хеші попередніх блоків, що дозволяє забезпечити надійність та незмінність всього блокчейну [9].

Окрім захисту та запису транзакцій у регістри, криптографія також відіграє роль у захисті гаманців, що використовуються для зберігання криптовалют. Відкритий та приватний парні ключі, що дозволяють користувачам отримувати та надсилати платежі, створюються за допомогою асиметричного шифрування. Відкриті ключі використовуються для генерації цифрових підписів транзакцій, що дозволяє аутентифікувати право власності. Природа асиметричної криптографії не дозволяє нікому, крім власника приватного ключа, отримати доступ до коштів, що зберігаються в гаманці, тому ці кошти зберігаються в безпеці, доки власник не вирішить їх витратити.

На додаток до криптографії, відносно нова концепція, відома як криптоекономіка, також відіграє важливу роль у підтримці безпеки мереж блокчейнів. Це пов’язано з областю досліджень, відомою як теорія ігор, яка математично моделює раціональне прийняття рішень учасниками різних ситуацій із заздалегідь визначеними правилами та винагородами. Хоча традиційна теорія ігор може бути широко використана у багатьох випадках, криптоекономіка спеціально моделює та описує поведінку вузлів у розподілених системах блокчейнів.

Криптоекономіка – це відносно нова галузь, яка поєднує в собі елементи

економіки та криптографії. Вона вивчає економічні аспекти блокчейнів та криптовалют, включаючи механізми, за допомогою яких вони функціонують, взаємодіють та стимулюють різні поведінки учасників мережі. Криптоекономіка досліджує як економічні теорії, так і технічні аспекти, пов'язані з розподіленою системою, зокрема проблеми безпеки, масштабування та гарантії виконання угод.

Криптоекономіка допомагає зрозуміти, які інструменти, правила та механізми застосовуються в блокчейнах для досягнення певних економічних цілей, таких як забезпечення безпеки та захисту від зловживань, збільшення ефективності та масштабування мережі, створення нових бізнес-моделей та стимулювання різних поведінок учасників мережі. Безпека криптоекономіки базується на уявленні, що блокчейн-системи дають більше стимулів діяти чесним вузлам, ніж зловмисній або помилковій поведінці. Алгоритм консенсусу Proof of Work, що використовується у видобутку біткойнів, є гарним прикладом такої структури стимулювання.

Коли була створена структура видобутку біткойнів, вона була спеціально розроблена як дорогий та ресурсомісткий процес. Через свою складність та вимоги до обчислень, PoW вимагає значних витрат грошей та часу, незалежно від того, де і як знаходиться майнінговий вузол. Отже, така структура є сильним стримуючим фактором для зловмисної діяльності та значним стимулом для чесного видобутку корисних копалин. Нечесні або неефективні вузли швидко будуть виключені з мережі, тоді як чесні та ефективні майнери можуть отримати значну винагороду за кожен блок [10].

Підтримка балансу між ризиками та перевагами забезпечує також захист від можливих атак, які можуть підірвати консенсус, передаючи більшість хешрейту мережі блокчейн групі або організації. Ця атака, відома як атака 51%, може мати надзвичайно руйнівні наслідки. За рахунок конкуренції майнінгу Proof of Work та розміру мережі біткойна, ймовірність успіху зловмисника, який здійснює атаку, дуже мала.

Атака 51% є однією з найбільш серйозних загроз для блокчейн-мереж. Ця атака полягає в тому, що хакери намагаються здійснити контроль над більшістю мережевої потужності, або хешрейту, мережі, що дає їм змогу змінювати транзакції і поділитися на дві різні гілки блокчейну, що призводить до подвійного витрачання та інших атак.

В основі цієї атаки лежить концепція більшості. Якщо зловмисник може здійснити контроль над більшістю мережевої потужності, він може домінувати

процесом прийняття рішень в мережі, включаючи зміну блоків, відкидання транзакцій і навіть подвійне витрачання.

Однак для успішної атаки 51% потрібна велика кількість обчислювальної потужності, і вона стає набагато складнішою з ростом розміру мережі. Більшість блокчейн-мереж зараз використовують механізми консенсусу, які унеможливлюють такий тип атаки, або мають високий поріг для виконання. Такі механізми консенсусу, як Proof of Work, Proof of Stake та інші, допомагають захистити блокчейн-мережі від атак 51%.

Витрати на обчислювальну потужність, необхідну для досягнення 51% контролю над величезною блокчейн мережею, буде астрономічною, що забезпечить негайне стримування таких великих інвестицій для відносно невеликої потенційної винагороди. Поки вартість створення більшості шкідливих вузлів залишається непомірно високою, а для чесної діяльності існують кращі стимули, система зможе процвітати без значних збоїв. Однак, невеликі блокчейн мережі, безумовно схильні до більшості атак, тому що загальна швидкість хешування цих систем значно нижче, ніж у біткоїна.

Отже, блокчейн технології мають потенціал вирішувати проблеми безпеки в цифрових транзакціях та забезпечувати високий рівень захисту даних. Завдяки своїй децентралізованій структурі та криптографічним методам захисту, блокчейн може захистити транзакції від змін та фальсифікації даних.

Оскільки використання технології блокчейн продовжує розвиватися, системи безпеки також змінюються. Наприклад, приватні блокчейни, які зараз розробляються для комерційних підприємств, в більшій мірі покладаються на безпеку за допомогою контролю доступу, ніж на механізми теорії ігор, які необхідні для безпеки більшості публічних блокчейнів.

1.4 Використання криптографії в блокчейні

Криптографія є ключовим елементом у блокчейн технології, оскільки вона забезпечує безпеку та конфіденційність даних, які зберігаються в мережі. Одним з основних криптографічних методів, які використовуються у блокчейні, є хеш-функції. Хеш-функція є математичною функцією, яка приймає довільний вхідний рядок і перетворює його на фіксований рядок фіксованої довжини. Цей вихідний рядок, який називається хешем, використовується для ідентифікації даних в мережі.

Інший криптографічний метод, що використовується у блокчейні – це цифровий підпис. Цифровий підпис – це електронний еквівалент підпису в реальному світі, який забезпечує перевірку автентичності даних. Для створення цифрового підпису використовується закритий ключ, який відомий тільки власнику [11].

Асиметрична криптографія або криптографія з відкритим ключем Public Key Cryptography (PKC) використовує як закритий, так і відкритий ключ, на відміну від симетричної криптографії, де використовується тільки один ключ. Використання пари ключів PKC надає унікальні можливості, що дозволяють вирішувати проблеми, які є властивими іншим криптографічним методам. Цей вид криптографії є важливим компонентом сучасної комп'ютерної безпеки.

У схемі PKC відкритий ключ використовується відправником для шифрування інформації, в той час як закритий ключ використовується одержувачем для розшифровки. Оскільки два ключа відрізняються один від одного, відкритий ключ може безпечно використовуватися спільно, не ставлячи під загрозу приватну безпеку. Кожна пара асиметричних ключів унікальна, гарантуючи, що повідомлення зашифроване з використанням відкритого ключа, може бути прочитано тільки тією людиною, яка володіє відповідним закритим ключем. Принцип роботи шифрування показано на рисунку 1.3.

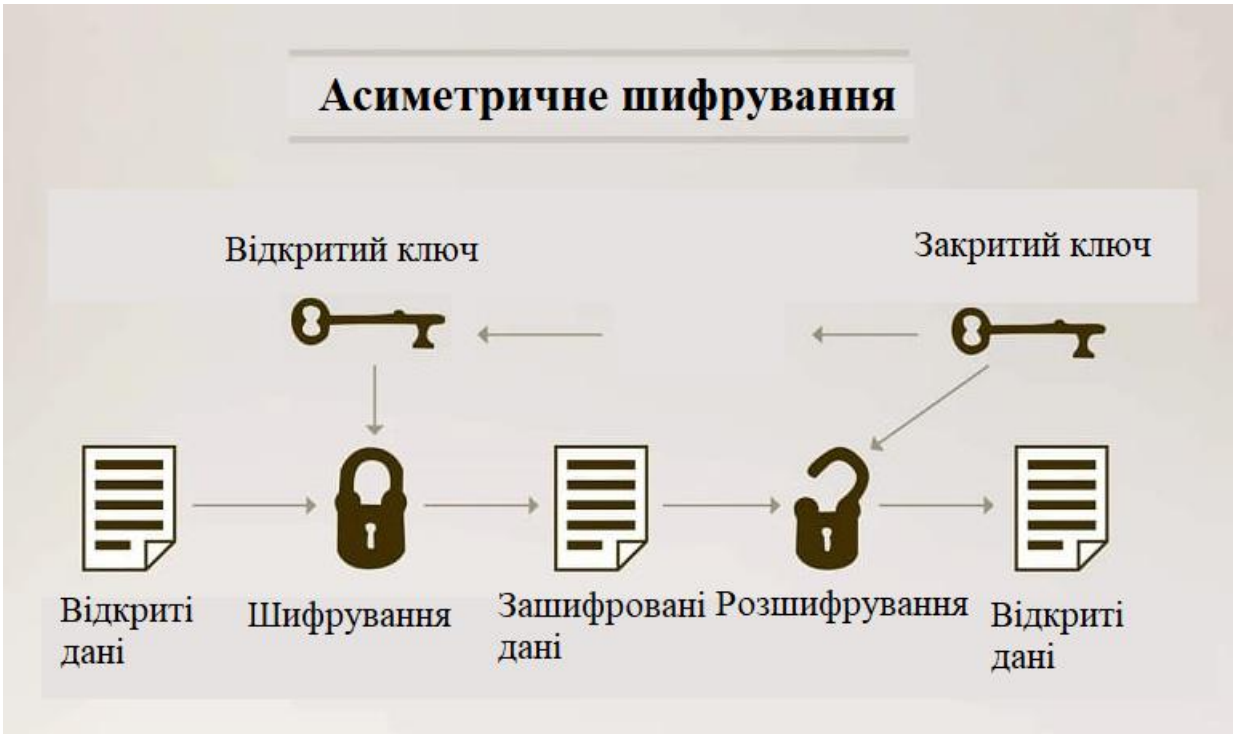


Рисунок 1.3 – Принцип роботи асиметричного шифрування

Оскільки алгоритми асиметричного шифрування використовують пари ключів, які математично пов'язані, то довжина цих ключів значно більша, ніж у симетричній криптографії. Зазвичай ця довжина становить від 1024 до 2048 бітів, що робить надзвичайно складним обчислення закритого ключа за його відкритим аналогом. Один з найбільш поширених алгоритмів асиметричного шифрування, що використовується сьогодні, це RSA. У схемі RSA ключі генеруються за допомогою модуля, який виходить за рахунок множення двох чисел, часто двох великих простих чисел. Зазвичай, модуль генерує два ключі: відкритий ключ, який може бути загальнодоступним, і закритий ключ, який повинен зберігатися в таємниці.

Криптографія з відкритим ключем вирішує одну з давніх проблем симетричних алгоритмів, яка полягає в передачі ключа, який використовується як для шифрування, так і для дешифрування. Відправлення цього ключа по небезпечному з'єднанню є ризикованим і може бути розкритим третім особам, які зможуть потім прочитати будь-які повідомлення, зашифровані за допомогою даного ключа. Хоча й існують криптографічні методи, наприклад такі як протокол обміну ключами Діффі-Хеллмана для вирішення цієї проблеми, вони уразливі для атак. У криптографії з відкритим ключем, навпаки. Ключ, використовуваний для шифрування, може безпечно передаватися по будь-якому з'єднанню. В результаті чого, асиметричні алгоритми забезпечують більш високий рівень захисту в порівнянні з симетричними [12].

Незважаючи на те, що РКС може бути використана для підвищення безпеки даних та перевірки цілісності повідомлень, вона має деякі недоліки. Ці алгоритми можуть бути дуже повільними, особливо коли вони мають шифрувати або розшифровувати великі обсяги даних. Крім того, цей тип криптографії є залежним від того, що закритий ключ буде залишатися секретним. Якщо ж закритий ключ стане відомим третій стороні, то всі дані, які були зашифровані відповідним відкритим ключем, стануть доступні. Крім того, користувачі можуть втратити свої закриті ключі і в цьому випадку вони не зможуть отримати доступ до своїх зашифрованих даних.

Підходи криптографії з відкритим ключем широко використовуються в сучасних комп'ютерних системах для забезпечення безпеки конфіденційної інформації. Наприклад, вони можуть застосовуватися для зашифрування електронної пошти з метою забезпечення конфіденційності вмісту. Також системи РКС можуть використовуватися як засіб забезпечення безпечного середовища для електронного голосування, що дозволяє виборцям брати участь у виборах зі своїх

домашніх комп'ютерів. Незважаючи на ці переваги, важливо враховувати обмеження асиметричної криптографії, зокрема її повільну роботу з великими обсягами даних і залежність від збереження секретного ключа.

РКС також застосовується в блокчейн технології та криптовалютах. При створенні нового криптовалютного гаманця генерується пара ключів – відкритий та закритий ключ. Відкритий ключ використовується для генерації публічної адреси, яка може безпечно передаватись іншим. Закритий ключ використовується для створення цифрових підписів та перевірки транзакцій і повинен зберігатись в таємниці. Після того, як транзакція була підтверджена валідацією хеша, що міститься в цифровому підписі, вона може бути додана в реєстр блокчейн. Система перевірки цифрового підпису гарантує, що лише власник криптовалютного гаманця зі своїм закритим ключем може здійснювати операції з коштами.

Асиметричні шифри, які застосовуються в блокчейнах та криптовалютах, мають певні відмінності від тих, що використовуються для забезпечення комп'ютерної безпеки. Наприклад, ECDSA (elliptic curve digital signature algorithm) – це спеціальний шифр, який використовують Bitcoin і Ethereum для перевірки транзакцій. Цей алгоритм шифрування ґрунтується на еліптичних кривих, що забезпечує більшу швидкість та ефективність в порівнянні з іншими асиметричними шифрами.

Алгоритм ECDSA, що використовує еліптичну криву та кінцеве поле, дозволяє створювати підписи для даних, аутентичність яких може бути перевірена третіми сторонами. У випадку з Bitcoin, такими даними є транзакції передачі права власності. Криптографія, яка лежить в основі схем цифрових підписів криптовалют, дозволяє здійснювати верифікацію транзакцій між двома сторонами в децентралізованій мережі. ECC (Elliptic Curve Cryptography) має значну перевагу перед шифруванням за методом RSA, оскільки розмір ключа, який використовується для ECC, набагато менше, ніж для RSA, при цьому ECC забезпечує такий же рівень безпеки. Один з головних недоліків ECC полягає в тому, що він відносно складний для реалізації та вимагає багато ресурсів для обчислень. Хоча RSA використовується набагато ширше в Інтернеті, ECC є більш ефективною формою RSA, що і служить причиною її використання в блокчейн технологіях.

Технологія в основі Bitcoin переосмислює концепцію права власності. У традиційному сенсі володіти чим-небудь. Зазвичай ця концепція значить або зберігати фізично чи юридично цей об'єкт особисто, або передати на відповідальне зберігання довіреної структурі, наприклад банку.

У випадку з Bitcoin все інакше. Самі біткоіни не зберігаються ні центрально, ні локально, жодна структура не виступає в ролі їх кастодіана. Біткоіни існують як записи в блокчейні, копії якого розподіляються мережею пов'язаних комп'ютерів. Володіти біткоіном означає мати можливість передавати контроль над ним іншому користувачеві, створюючи запис передачі в блокчейні. Доступ до пари ключів ECDSA, відкритого і закритого, і надає таку можливість [13].

ECDSA має окремі процедури для підпису і для верифікації. Кожна процедура – це алгоритм, що складається з декількох арифметичних операцій. Алгоритм підпису використовує закритий ключ, алгоритм верифікації – відкритий ключ.

Отже можна виділити основні переваги використання криптографічних методів у блокчейн технологіях.

1) Конфіденційність і безпека. Криптографічні методи забезпечують конфіденційність і безпеку обміну даними між учасниками блокчейн мережі. Транзакції зашифровані за допомогою асиметричної криптографії, що дозволяє забезпечити конфіденційність даних та захист від несанкціонованого доступу.

2) Аутентифікація. Криптографічні методи дозволяють відслідковувати всі транзакції та перевіряти їх автентичність. Це допомагає запобігати шахрайству та іншим видам атак.

3) Недоступність до змін. За допомогою криптографічних методів можна забезпечити недоступність до змін даних у блокчейні. Кожен блок містить хеш попереднього блоку, що робить майже неможливим зміну вже записаних транзакцій.

4) Децентралізація. Використання криптографічних методів дозволяє забезпечити децентралізацію та незалежність від централізованих організацій, що забезпечує більшу надійність та безпеку блокчейн мережі.

5) Прозорість. Криптографічні методи дозволяють забезпечити відкритість та прозорість даних у блокчейн мережі. Усі транзакції є відкритими та доступними для перегляду всіма учасниками мережі, що забезпечує більшу прозорість та відповідальність.

Серед недоліків можна виділити наступні.

1) Обмеження складності. Криптографічні алгоритми, особливо асиметричні алгоритми, можуть бути досить повільними, коли вони працюють з великими обсягами даних. Це може знизити продуктивність мережі блокчейн, особливо якщо багато користувачів проводять транзакції одночасно.

2) Необхідність безпечного зберігання ключів. Для захисту даних в блокчейні використовуються криптографічні ключі. Але якщо закритий ключ був випадково переданий або розкритий, безпеку всіх повідомлень, які були зашифровані за допомогою відповідного відкритого ключа, буде поставлена під загрозу. Користувачі також можуть випадково втратити свої закриті ключі, і в цьому випадку вони не зможуть отримати доступ до зашифрованих даних [14].

3) Використання неефективних криптографічних методів. Якщо криптографічний метод недостатньо ефективний, то це може спричинити вразливості в мережі блокчейн. Такі проблеми можуть виникнути, якщо користувачі вирішать використовувати застарілі або менш безпечні методи шифрування, щоб заощадити ресурси.

Отже, криптографія з відкритим ключем грає важливу роль в захисті сучасних цифрових систем, від комп'ютерної безпеки до перевірки криптовалютних транзакцій. Використовуючи парні відкриті і закриті ключі, алгоритми асиметричної криптографії вирішують фундаментальні проблеми безпеки, представлені симетричними шифрами. Незважаючи на те, що РКС використовується вже протягом багатьох років, регулярно розробляються нові програми та застосування, зокрема в області блокчейнів та криптовалют.

1.5 Проблема масштабування в технологіїі блокчейн

Масштабованість блокчейну – це його здатність збільшувати кількість оброблюваних транзакцій з плином часу, щоб відповідати зростаючому попиту. У комп'ютерних системах масштабування можна досягти через покращення продуктивності обладнання, або через оптимізацію програмного забезпечення. У блокчейні масштабування вимагає більш складних рішень, оскільки необхідно забезпечити не тільки швидкість, але й безпеку, децентралізацію та інші ключові властивості.

Хоча протоколи, наприклад біткоїн, мають багато переваг, масштабованість не входить до їх числа. Запуск біткоїн-ноди відносно недорогий і можливий навіть на технічно слабких пристроях. Однак, оскільки тисячі вузлів повинні знати про діяльність один одного, існують певні обмеження щодо їх пропускної здатності. Блокчейн обмежує кількість транзакцій, які можуть бути оброблені, щоб уникнути зростання розміру бази даних до неприйнятних розмірів. Це обмеження пов'язано з обмеженою пропускною здатністю вузлів, які повинні знати про діяльність інших

вузлів. Якщо база даних швидко стає занадто великою, вузли не зможуть ефективно взаємодіяти між собою. Крім того, якщо блоки стають занадто великими, їх не можна швидко повторно передати по мережі, що може призвести до затримок у підтвердженні транзакцій та збільшення їх вартості [15].

Ця проблема створює складну ситуацію з обмеженими можливостями вирішення. Коли мережа перевантажена транзакціями, користувачам доводиться платити високі комісії, щоб їх транзакції були оброблені вчасно. У зв'язку з цим масштабованість розглядається як щось, що має бути досягнуто на оффчейн рівні, тоді як на базовому рівні блокчейну безпеку та децентралізацію необхідно максимально зберігати.

Оффчейн – це транзакції, що відбуваються за певною мережею блокчейну, про які можна пізніше повідомити або згрупувати разом, перш ніж відправити їх в основну мережу. Оффчейн-масштабування відноситься до методів, які дозволяють виконувати транзакції без збільшення кількості блоків в блокчейні. Протоколи, які підключаються до блокчейну, дають можливість користувачам відправляти та отримувати кошти без транзакцій, які з'являються у головній мережі. Одним з найвідоміших рішень в цьому напрямку є сайдчейн. Використання оффчейн-технологій може допомогти у покращенні швидкості транзакцій та зниженні комісій, але також може вимагати додаткових механізмів безпеки для забезпечення захисту від шахрайства та інших атак.

Сайдчейном називається побічний ланцюжок, який являє собою окремий блокчейн. Однак це не автономна платформа, так як вона має деяку прив'язку до основного блокчейну. Основна мережа і сайдчейн є функціонально сумісними, це означає, що активи можуть вільно переміщатися з одної мережі в іншу. Сайдчейн здатний на те, що ,наприклад, біткоїн мережа зробити не може [16].

Оффчейн-рішення використовуються для поліпшення ефективності мережі та розширення функціональності за допомогою додаткових технологій та протоколів. Такі рішення можуть включати в себе різні підходи, такі як використання розподілених систем для обробки транзакцій, покращення процесу маршрутизації транзакцій в мережі, використання технологій рівня 2, таких як Lightning Network, для швидкої обробки транзакцій між вузлами без необхідності підтвердження кожної транзакції на основному блокчейні, та інші підходи, що дозволяють зменшити навантаження на головний блокчейн.

Оффчейн рішення можуть допомогти розв'язати проблеми масштабованості та швидкодії мережі блокчейну, що є важливими факторами для подальшого

розвитку цієї технології та її застосування у реальному світі.

Для досягнення масштабованості блокчейну також використовуються інші підходи. Наприклад, одним із способів є зменшення розміру транзакцій шляхом використання компресії даних. Крім того, можна використовувати різні алгоритми підтвердження транзакцій, такі як Proof of Stake, які не потребують великих обчислювальних ресурсів, що зменшує навантаження на мережу. Також можливість горизонтального масштабування, коли розподілені бази даних можуть бути розділені на декілька серверів, що дозволяє обробляти більшу кількість транзакцій.

Незважаючи на те, що оффчейн-рішення можуть допомогти поліпшити масштабованість та швидкодію мережі блокчейну, важливо пам'ятати про збереження безпеки та децентралізації. Такі рішення можуть зменшувати навантаження на головний блокчейн, але вони не повинні впливати на безпеку та надійність мережі.

Таким чином можна виділити основні переваги використання оффчейн рішень.

1) Підвищена швидкість транзакцій. Оффчейн рішення дозволяють виконувати більше транзакцій на одиницю часу, оскільки не всі транзакції повинні бути записані безпосередньо на блокчейні.

2) Зменшення комісій. Оскільки оффчейн рішення дозволяють виконувати більше транзакцій без збільшення розміру блокчейну, комісії за перекази можуть бути менші.

3) Покращена масштабованість. Оффчейн рішення дозволяють блокчейнам бути більш масштабованими, оскільки більше транзакцій може бути оброблено за один раз.

4) Більш висока приватність. Оскільки не всі транзакції записуються безпосередньо на блокчейні, більше даних може бути збережено приватно.

5) Нові можливості. Оффчейн рішення дозволяють розробникам створювати нові додатки та розширювати функціонал блокчейнів.

Однак, використання оффчейн рішень має також деякі недоліки.

1) Потенційний ризик безпеки, особливо при використанні рішень, що не повністю децентралізовані.

2) Вимога до додаткових ресурсів та обладнання для підтримки та обробки оффчейн транзакцій.

3) Необхідність розробки та підтримки додаткових протоколів та

технологій для роботи з оффчейн транзакціями.

Блокчейн – це система, яка ретельно вирішує компроміси між безпекою, швидкістю та масштабованістю. Наприклад, біткоїн – це один з найбільш безпечних та децентралізованих блокчейнів, але він має обмежену пропускну здатність. Транзакції у блокчейні біткоїна можуть бути швидшими, ніж традиційні, проте вони все ще є відносно повільними порівняно з іншими блокчейн-системами. Блоки генеруються кожні 10 хвилин, а комісійні збори можуть значно зростати при перевантаженні мережі. Однак оффчейн-рішення, такі як сайдчейн, можуть допомогти поліпшити швидкодію та масштабованість блокчейну, дозволяючи виконувати більше транзакцій за менший час та зменшуючи навантаження на головний блокчейн. Сайдчейни дозволяють користувачам виконувати багато транзакцій у внутрішній мережі, а потім підтверджувати їх у головній мережі блокчейну, зменшуючи кількість транзакцій, які потрібно зберігати в головній мережі блокчейну.

Мережі сайдчейнів можуть використовувати різні правила та механізми консенсусу, і не обов'язково використовувати Proof of Work алгоритм. Вони можуть бути налаштовані з будь-якою кількістю параметрів, в залежності від потреб користувачів та розробників. Сайдчейни також можуть мати доступ до оновлень, яких немає в головному ланцюжку, і можуть генерувати більші блоки, що дозволяє збільшити швидкість обробки транзакцій.

Сайдчейни можуть працювати автономно і не впливати на роботу основної мережі у разі критичних помилок. Це дозволяє використовувати їх для тестування нових функцій та проведення експериментів, що інакше потребували б підтримки більшості учасників мережі. Зростання популярності сайдчейнів пов'язано з бажанням користувачів уникнути недоліків транзакцій в основному блокчейні. Однак, з метою збереження децентралізації мережі, необхідно збалансувати її зростання, створивши обмеження на зростання блокчейна, щоб нові вузли могли легко приєднуватися. Якщо користувачі будуть задоволені компромісами мережі, то сайдчейни можуть стати важливим кроком у напрямку ефективного масштабування.

Ще одним із можливих методів масштабування блокчейну є шардінг. Шардінг – це метод горизонтального масштабування, який використовується для покращення пропускної здатності блокчейн мережі шляхом розділення бази даних на більш дрібні фрагменти – шарди. Кожен шард містить лише певну частину даних з блокчейну, замість того, щоб зберігати всю базу даних на кожному вузлі мережі.

Цей метод дозволяє розподілити обробку транзакцій між більшою кількістю вузлів, знижуючи завантаження на кожен вузол і збільшуючи пропускну здатність мережі. Крім того, шардінг дозволяє збільшити кількість транзакцій, які можуть бути оброблені в мережі блокчейну за певний період часу. Однією з переваг шардування мережі є спрощення та доступність запуску ноди. Оскільки дані мережі розподіляються між шардами, вже не потрібно зберігати всю історію блокчейну на валідаторах. Замість цього валідатор повинен зберігати лише підтвердження цілісності даних.

Однією з основних переваг шардінгу є збільшення масштабуваності блокчейну. За допомогою шардінгу можна зменшити навантаження на головний блокчейн та забезпечити більшу кількість транзакцій на одиницю часу. Крім того, використання шардінгу дозволяє зменшити витрати на обробку даних, оскільки частини даних можуть зберігатися на менш потужних серверах.

Однак, шардінг також має свої недоліки. Зокрема, він може призвести до зменшення безпеки мережі, оскільки кожен шард працює незалежно і може стати мішенню для атак, якщо не будуть вжиті відповідні заходи захисту. Крім того, реалізація шардінгу може бути складною технічною задачею, оскільки потрібно добре продумати алгоритми розділення бази даних і забезпечити правильну взаємодію між шардами.

Таким чином, шардінг є одним із можливих методів масштабування блокчейну, який може допомогти покращити пропускну здатність мережі та збільшити кількість оброблюваних транзакцій. Однак, його впровадження потребує ретельного планування та забезпечення безпеки мережі.

Технологія блокчейн продовжує зростати та розвиватись. Завдяки новим технологіям та підходам, таким як шардінг, оффчейн рішення та різні протоколи консенсусу, можливо підвищити пропускну здатність мережі та знизити комісійні збори. Однак, при цьому необхідно забезпечити децентралізацію та безпеку мережі, щоб уникнути можливості злочинних дій. Крім того, важливо знайти баланс між пропускною здатністю та децентралізацією, щоб забезпечити ефективність та стабільність мережі. Остаточний успіх масштабування блокчейну залежить від того, наскільки успішно вдасться розв'язати ці технічні та організаційні виклики.

1.6 Архітектура приватних блокчейнів

Приватний блокчейн – це контрольована компаніями або організаціями мережа, до якої мають доступ тільки певні учасники. Це означає, що довіра відбувається лише між учасниками мережі. Приватний блокчейн часто використовується в бізнесі, коли необхідно забезпечити конфіденційність та контроль над мережею. Такі блокчейни не є глобальними і не доступні для перевірки ззовні. В таких блокчейнах процес створення блоків є централізованим і контролюється однією організацією. Інші користувачі можуть мати доступ лише для перегляду інформації, але їм не надається право на проведення операцій, ведення аудиту або управління додатками, які залежать від довірених вузлів [17].

Основні переваги приватних блокчейнів полягають в їх гнучкості та контрольованості. Деякі з основних переваг таких блокчейнів включають наступне.

1) Приватність і конфіденційність. Всі дані, що зберігаються в приватних блокчейнах, захищені від зовнішнього доступу та зберігаються в приватних мережах, що забезпечує високий рівень конфіденційності та приватності.

2) Швидкість та масштабованість. Приватні блокчейни зазвичай працюють швидше та забезпечують більшу пропускну здатність порівняно з публічними блокчейнами, оскільки вони не мають тієї самої кількості вузлів для підтримки.

3) Гнучкість. Приватні блокчейни можуть бути налаштовані та настроєні під конкретні потреби бізнесу та дозволяють змінювати правила та параметри залежно від потреб.

4) Керованість. Оскільки приватні блокчейни керуються централізованою організацією, керівники можуть легко визначати правила та параметри для всіх учасників мережі.

5) Ефективність. Приватні блокчейни можуть допомогти зменшити бюрократію та оптимізувати бізнес-процеси, що може призвести до економії часу та коштів.

6) Безпека. Приватні блокчейни мають більш високий рівень безпеки, оскільки доступ до них обмежений та керується лише довіреними вузлами.

Приватні блокчейни відрізняються від загальнодоступних публічних блокчейнів тим, що вони встановлюють свої власні правила, які визначають, хто має доступ до перегляду операцій та передачі даних в ланцюжок. У приватних блокчейнах не має децентралізації, тому що існує чітка ієрархія контролю. Однак,

вони є розподіленими, тому що кілька вузлів підтримують копії ланцюжка на своїх пристроях. На відміну від публічних блокчейнів, приватні мережі дозволяють контролювати доступ до даних, що забезпечує більш високий рівень безпеки. Також, вони можуть бути більш ефективними, оскільки вони не потребують великої кількості обчислювальних ресурсів для роботи. Концепція приватного блокчейну показано на рисунку 1.4.

Рисунок 1.4 – Концепція приватного блокчейну

Приватний блокчейн працює за принципом розподіленої бази даних, яка забезпечує безпеку і надійність зберігання і передачі даних між вузлами мережі. У приватному блокчейні транзакції підтверджуються відповідними дозволами та перевірками здійснюваними контролюючими організаціями або учасниками мережі залежно від визначених правил.

Для забезпечення цілісності та безпеки блокчейну, приватні блокчейни використовують різні протоколи консенсусу, щоб упевнитися, що всі вузли мережі

погоджуються з тим, що стається в мережі та що блоки додані до ланцюжка правильним чином.

Оскільки приватний блокчейн є контрольованим однією або кількома організаціями, то можливо використовувати більш прості технології, порівняно з загальнодоступними публічними блокчейнами. Наприклад, можна використовувати менш потужні алгоритми консенсусу, які дозволяють більш швидко проводити транзакції та зберігати інформацію на пристроях вузлів мережі з меншою потужністю обчислень.

Приватний блокчейн може бути створений без використання алгоритму консенсусу, замість цього може бути використаний алгоритм заздалегідь призначених валідаторів. Ці валідатори є вузлами, що відповідають за валідацію транзакцій, і набір вузлів, що підписують кожен блок. В разі зловживання учасниками, їх можна легко виявити і видалити з мережі, оскільки особистість кожного учасника відома, а управління мережею знаходиться в одних руках. Завдяки такому типу управління блокчейном, діяльність учасників може бути координованою досить просто. І хоча приватні блокчейни можуть не використовувати доказ роботи, цей протокол все одно може бути підключений для підвищення безпеки, спрощення аудиту та, як результат, посилення контролю над системою для кінцевих користувачів.

Окрім описаних вже переваг, приватні блокчейни мають інші можливості, які роблять їх більш гнучкими і придатними для застосування в різних галузях.

1) Можливість створення корпоративних рішень. Приватні блокчейни можуть бути використані для створення корпоративних рішень, що дозволяє компаніям забезпечити більш ефективний обмін даними між різними підрозділами та установами. Використання приватного блокчейну може допомогти зменшити затримки в обробці даних, знизити вартість транзакцій і забезпечити більшу прозорість управління.

2) Підвищення рівня конфіденційності. Приватні блокчейни забезпечують більш високий рівень конфіденційності, оскільки учасники мережі можуть контролювати доступ до даних, які знаходяться на блокчейні. Це особливо важливо для компаній, що працюють з конфіденційною інформацією, такою як медичні записи, фінансові та особисті дані.

3) Розширення функціональності блокчейнів. Приватні блокчейни можуть бути додатково налаштовані та розширені для різних функцій, наприклад, для використання у програмних додатках та розробці інтелектуальних контрактів.

Це дозволяє компаніям створювати більш складні та інноваційні продукти, які використовують технології блокчейну.

4) Забезпечення відповідності та регулювання. Приватні блокчейни дозволяють компаніям забезпечити відповідність законодавчим та регуляторним вимогам, оскільки вони можуть контролювати доступ до інформації та забезпечити рівень прозорості, що відповідає потребам регуляторів та законодавців.

Хоча приватні блокчейни і мають низку переваг для деяких організацій, однак їх застосування може бути обмеженим. На відміну від публічних блокчейнів, де кожен може стати вузлом мережі та здійснювати транзакції, у приватних блокчейнах доступ можуть мати тільки певні вузли або користувачі, що дозволяє організації зберігати контроль над мережею.

Приватні блокчейни можуть також бути менш безпечними, порівняно з публічними блокчейнами, оскільки вони контролюються однією організацією. Якщо зловмисники зможуть проникнути в систему, то вони можуть отримати повний контроль над мережею, що може призвести до викрадення даних, порушення конфіденційності або навіть до зупинки роботи всієї мережі.

Крім того, використання приватних блокчейнів може призвести до збільшення витрат на управління мережею, оскільки забезпечення безпеки, забезпечення відповідності правовим нормам та навіть підтримка програмного забезпечення може вимагати значних витрат. Також варто враховувати, що приватні блокчейни можуть бути менш ефективними за певних умов порівняно з публічними блокчейнами, оскільки вони можуть бути менш децентралізованими та залежити від ієрархічної структури управління.

Можна виділити основні недоліки приватних блокчейнів.

1) Централізація. Приватні блокчейни зазвичай мають одну контрольну точку, що призводить до того, що всі дані знаходяться в руках небагатьох людей або організацій. Це може стати проблемою в разі зловживання правами адміністратора або в разі порушення безпеки.

2) Масштабованість. Приватні блокчейни зазвичай мають обмежену масштабованість, що може стати проблемою при збільшенні обсягу транзакцій та додаванні нових учасників в мережу.

3) Інтероперабельність. Приватні блокчейни зазвичай мають власні правила та протоколи, що може ускладнити взаємодію з іншими блокчейнами або системами.

4) Відсутність децентралізації. Приватні блокчейни зазвичай мають

обмежену кількість учасників та не гарантують повну децентралізацію мережі, що може стати проблемою при зменшенні кількості вузлів, які підтримують мережу.

5) Витрати на створення. Створення приватного блокчейну може бути витратним процесом, оскільки він вимагає високих витрат на розробку та налаштування інфраструктури.

Таким чином, деякі особливості приватних блокчейнів можуть бути одразу і перевагами і недоліками залежно від ситуації та конкретного використання. Наприклад, можлива централізованість управління приватним блокчейном може забезпечувати швидкість та ефективність, але в той же час порушувати принципи безпеки та децентралізації.

Також, приватні блокчейни можуть виявитися менш відкритими та прозорими, що може створювати проблеми з взаємодією з іншими мережами, або забезпечення відкритості відносно транзакцій та дій певних учасників мережі.

Ще одним важливим фактором є можлива проблема сумісності та міграції до інших мереж. Приватний блокчейн може бути створений для рішення конкретних завдань, проте у випадку потреби в масштабуванні та розширенні можливостей використання, можуть виникати проблеми з перенесенням даних на інші мережі або додатки.

Отже, важливо ретельно розглядати переваги та недоліки приватних блокчейнів в контексті конкретних вимог та потреб користувачів. Тільки тоді можна зробити вірний вибір між приватним та публічним блокчейнами, залежно від потреб та мети використання.

Приватні блокчейни надають багато переваг для компаній, оскільки вони дозволяють використовувати технології блокчейн для внутрішнього використання, зберігаючи при цьому приватні дані. Ці технології можуть замінити багато централізованих компаній, що існують сьогодні. Приватні блокчейни можуть бути основою для інновацій у послугах, які використовують регістри або системи фінансового обліку.

Однак, необхідно звернути увагу на те, що використання приватних блокчейнів може мати певні недоліки. Наприклад, ці мережі є менш децентралізованими порівняно з публічними блокчейнами, оскільки їх контролює певна організація або група компаній. Крім того, може бути складно досягти повної безпеки в приватному блокчейні, оскільки інформація може бути доступна лише для обраних користувачів, що робить її вразливою до внутрішньої кіберзлочинності. Приватні мережі завдяки своїй конфігурації є найбільш

підходящими для компаній, коли юридична особа хоче скористатися перевагами технології блокчейн, не роблячи свою мережу доступною для інших.

1.7 Архітектура публічних блокчейнів

Публічні блокчейни – це відкриті децентралізовані мережі, що забезпечують можливість здійснювати транзакції безпосередньо між учасниками без посередницьких послуг. У публічних блокчейнах, будь-який учасник може створювати, перевіряти та записувати транзакції в ланцюжок блоків, що забезпечує децентралізовану перевірку операцій та гарантує їх безпеку.

Публічні блокчейни є відкритими системами, до яких має доступ будь-який користувач, кожен з яких може виконувати транзакції. При цьому, щоб забезпечити безпеку операцій, вони використовують криптографічні механізми верифікації, такі як PoW або PoS. Такі механізми забезпечують безпеку, яка не може бути зламана навіть в разі наявності зловмисника, який має доступ до мережі [18].

Однією з основних особливостей публічних блокчейнів є їх децентралізація. У таких мережах немає центрального органу управління, а керування мережею відбувається через співпрацю між вузлами, що дозволяє забезпечити безпеку операцій і уникнути зловживань.

Оскільки публічні блокчейни є відкритими та загальнодоступними, то кожен може перевірити будь-яку транзакцію, яка була проведена в мережі. Це робить їх ідеальним інструментом для тих, хто шукає безпеку та прозорість при здійсненні фінансових операцій, відправці повідомлень, управлінні даними та інших цифрових активів.

Завдяки своїй відкритості та безцензурності, публічні блокчейни стають все популярнішим інструментом для зберігання та обміну різноманітних цифрових активів, включаючи криптовалюти, токени та інші цифрові ресурси.

Конроль публічним блокчейном здійснюється спільнотою членів мережі, що включає розробників, користувачів, постачальників послуг та майнерів. Кожен, хто бажає, може приєднатися до мережі та виконувати роль у досягненні консенсусу, за що отримує винагороду. Приклад концепції публічного блокчейну показано на рисунку 1.5.

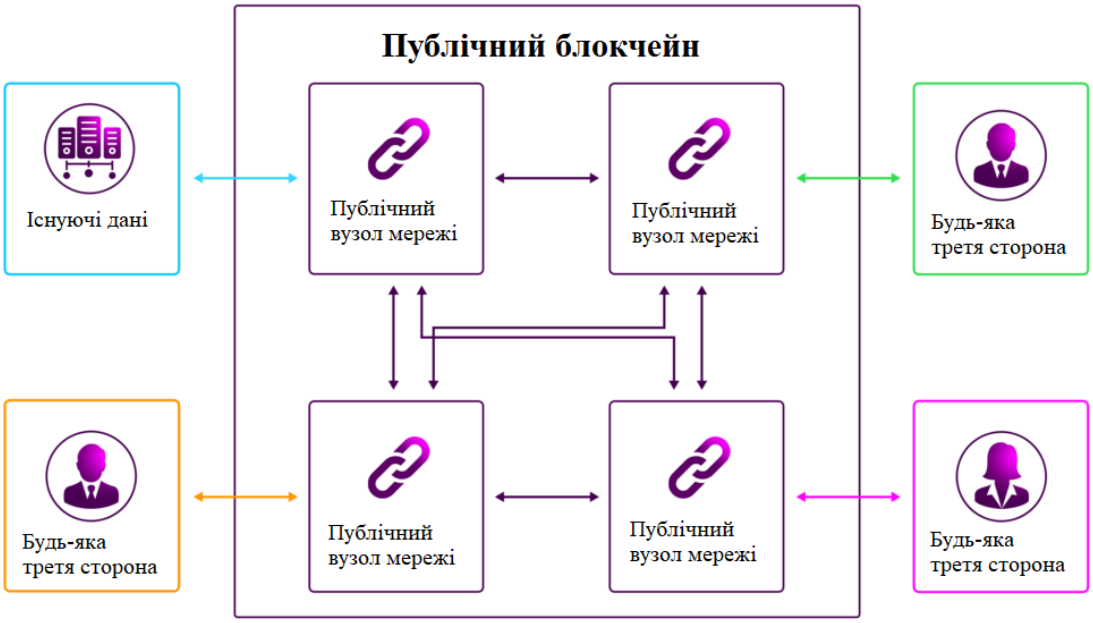


Рисунок 1.5 – Концепція публічного блокчейну

Основними перевагами публічних блокчейнів є.

1) Децентралізація. У публічному блокчейні немає централізованого органу керування, тому ніхто не має можливості контролювати або маніпулювати даними в ланцюжку блоків. Кожен вузол мережі має рівні права і може перевірити будь-яку транзакцію в мережі.

2) Прозорість. Публічні блокчейни забезпечують високий рівень прозорості, оскільки кожна транзакція є відкритою та доступною для перегляду всіма користувачами мережі. Це дає можливість відстежувати перекази коштів та перевіряти легітимність транзакцій.

3) Безпека. Публічні блокчейни захищені криптографічними методами, що забезпечує високий рівень безпеки транзакцій та збереження даних у мережі.

4) Відкритість. Публічні блокчейни відкриті для всіх, хто бажає приєднатися до мережі, незалежно від їхньої географічної розташування, національності або статусу. Це дозволяє користувачам з різних країн обмінюватися даними та активами без перешкод.

5) Інновації. Публічні блокчейни надають можливість розробляти нові додатки та сервіси, які можуть змінити традиційні способи функціонування різних галузей, включаючи фінансову сферу, медицину, логістику та інші. Це відкриває широкі можливості для інновацій та розвитку нових ринків.

Ефективність мережі досягається завдяки оновленням протоколів, які

запобігають шкідливим змінам. Ось чому система дозволяє створювати децентралізовані програми з мінімальними витратами на обслуговування. Такі блокчейни надають спосіб захисту користувачів проти несанкціонованого доступу до їх особистих даних та цифрових ідентифікаторів. Завдяки технології розподіленого реєстру, усі учасники мережі забезпечують перевірку транзакцій та даних ідентифікації, що допомагає підтримувати безпеку і цілісність інформації. В результаті, користувачі можуть бути впевнені в автентичності та надійності своїх цифрових ідентифікаторів. Також такі блокчейни надають спосіб захисту користувачів програм, обмежуючи можливості розробників. У програмах на публічному блокчейні розробник не може сам по собі змінювати код або дані.

Публічні блокчейни володіють мережевими ефектами. Користувачі одного додатка, створеного на основі публічного блокчейну, часто стають першими користувачами інших додатків на тій же платформі, оскільки вони дізнаються про них через взаємодію між програмами. Наприклад, мобільний гаманець, розроблений на основі публічного блокчейну, може інтегрувати функціонал для співпраці з іншими децентралізованими додатками на тому ж блокчейні, що в результаті значно розширює потенційну базу користувачів.

Незважаючи на свої переваги, публічні блокчейни також мають свої недоліки. При збільшенні кількості користувачів та транзакцій у мережі, зростає розмір блоків та складність їх обробки, що може призводити до зниження продуктивності та збільшення часу обробки транзакцій. Ця проблема відома як проблема масштабування блокчейну.

Для вирішення цієї проблеми розробники блокчейну пропонують різні рішення, такі як збільшення розміру блоків, використання сайдчейнів або впровадження шарування, що дозволяє проводити мікротранзакції поза основною мережею, тим самим зменшуючи навантаження на неї.

Такі рішення сприяють підвищенню швидкості транзакцій, зниженню комісій і підвищенню загальної продуктивності мережі. Однак, вони також можуть мати побічні ефекти, такі як збільшення енергоспоживання, зниження ступеня децентралізації або погіршення безпеки.

Для успішного масштабування блокчейну потрібно ретельно виважувати всі аспекти і налагоджувати параметри мережі таким чином, щоб забезпечити оптимальний баланс між продуктивністю, децентралізацією та безпекою.

Отже, таким чином можна виділити основні недоліки публічних блокчейнів.

1) Проблема масштабування. Чим більше користувачів та транзакцій, тим

більше навантаження на мережу, що може призвести до зниження продуктивності та збільшення часу обробки транзакцій.

2) Витрати на енергію. Висока енергоспоживання деяких публічних блокчейнів, особливо тих, що використовують механізм консенсусу Proof of Work, створює питання екологічності та економічної ефективності.

3) Відсутність приватності. Всі транзакції в публічних блокчейнів є прозорими та відкритими для всіх користувачів мережі, що може порушувати приватність користувачів.

4) Зберігання даних. У публічних блокчейнів усі вузли зберігають повну копію всіх транзакцій, що створює вимоги до зберігання та передачі великих обсягів даних, а також ставить під загрозу децентралізацію, оскільки малі вузли можуть не мати достатніх ресурсів для зберігання всієї інформації.

5) Збільшення комісій. Під час пікового навантаження на мережу, комісії за транзакції можуть зростати, що зменшує доступність та ефективність блокчейнів для масового використання.

Враховуючи наведені вище особливості та недоліки публічних блокчейнів, можна зробити деякі висновки щодо їхнього потенціалу та обмежень у сучасному світі.

Попри проблеми масштабування, витрати на енергію та інші обмеження, публічні блокчейни продовжують забезпечувати децентралізовані та безпечні рішення для широкого спектру застосувань, зокрема фінансових операцій, цифрової ідентифікації, голосування та іншого.

Завдяки своїй відкритості та прозорості, публічні блокчейни можуть сприяти розвитку інноваційних екосистем, залученню різноманітних стейкхолдерів та створенню нових відкритих ринків. Водночас, необхідність забезпечення конфіденційності даних та приватності користувачів може стати важливою проблемою для публічних блокчейнів, яка вимагає розробки та впровадження додаткових механізмів захисту.

Для подолання обмежень публічних блокчейнів та підвищення їхньої ефективності та надійності, спільнота розробників активно працює над масштабувальними рішеннями, альтернативними механізмами консенсусу та підвищенням приватності. У майбутньому публічні блокчейни можуть стати ще більш зручними, безпечними та доступними інструментами для широкого застосування в різних галузях.

2 МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Технологія блокчейн є однією з найбільш революційних технологій нашого часу. Вона може бути застосована в різних галузях і принести значний внесок у покращення функціонування різних систем. Завдяки своїм особливостям, таким як децентралізація, безпека та надійність, блокчейн відкриває нові можливості в багатьох сферах, включаючи фінанси, логістику, медицину, нерухомість, інтелектуальну власність та інші. Більш того, децентралізовану мережу можна налаштувати як прозору базу даних, видиму всім учасникам. У цьому сенсі технологія блокчейн надає можливість створювати розподілений, але і в той же час уніфікований запис даних, що сприяє зменшенню шахрайства, забезпеченню прозорості та автоматизації процесів.

Таким чином, блокчейн може відігравати важливу роль у створенні нових бізнес-моделей, спрощенні бюрократії та поліпшенні доступу до ресурсів та послуг для користувачів по всьому світу. Завдяки своїй гнучкості, блокчейн забезпечує адаптацію до специфічних потреб різних індустрій, що дозволяє йому відповідати викликам сучасного світу та стати ефективним інструментом у руках фахівців різних напрямків.

2.1 Використання блокчейну в державному управлінні

Використання блокчейн технологій у державному управлінні може забезпечити більш ефективну і прозору роботу органів влади, зменшення ризику корупції та покращення послуг для громадян. Незважаючи на те, що дана технологія має безліч потенційних переваг в управлінні, у державних органів є кілька основних причин розглянути можливість використання блокчейну. До них можна віднести посилення децентралізації, цілісність і прозорість усіх даних, а також підвищення ефективності та зниження експлуатаційних витрат.

Системи, які використовують блокчейн, забезпечують високу незмінність даних, а структуру мережі можна налаштувати таким чином, щоб дозволити доступ до інформації лише в деяких випадках і дозволяти вносити зміни тільки уповноваженим сторонам. Різні керівні органи можуть діяти як валідатори, які беруть участь у процесі розподілу та валідації. Це суттєво зменшує можливість підробки даних та шахрайства [19].

В залежності від налаштувань системи неурядові організації, університети та громадяни можуть виступати в якості вузлів, що призведе до ще більш високого ступеня децентралізації. Крім того, ці механізми перевірки можуть запобігати іншим поширеним типам помилок пов'язаних з введенням даних, наприклад блок даних в якому відсутня фундаментальна інформація, буде відхилений розподіленою мережею вузлів.

Також блокчейн може відіграти значну роль у виборчому процесі, оскільки справедливі та відкриті вибори є важливою складовою демократії, а високий рівень незмінності даних в блокчейн мережі робить його чудовим рішенням для запобігання підробки голосів. Проте, додаткова безпека це не єдина перевага цієї технології – за допомогою блокчейну можливо забезпечити безпечне онлайн-голосування.

Блокчейн може бути використаний для зберігання та захисту всіх державних записів, забезпечуючи складнішу маніпуляцію та більшу прозорість щодо доступу до цієї інформації. У даний час більшість урядових даних зберігається на централізованих серверах, що контролюються органами влади або невеликою групою людей, що спрощує різні види маніпуляцій з їх боку. Використання блокчейну забезпечує децентралізацію влади шляхом розподілення процесу перевірки та зберігання даних.

З цієї причини блокчейни можуть використовуватися в якості прозорої бази даних, яка зменшує потребу в довірі між державними органами і цивільними особами. Децентралізовані блокчейни можуть забезпечити постійний доступ до всієї документації співробітників правоохоронних органів, що в свою чергу полегшує роботу контролюючих органів над розкриттям корупційних правопорушень чи зловживань владою, тим самим скорочуючи або усуваючи необхідність в посередниках пов'язаних з обміном даних і фінансових транзакцій. Подібна інфраструктура органів державної влади може значно ускладнити урядовцям процес заплутування незаконної фінансової діяльності спрямовуючи кошти через ряд непрозорих приватних організацій.

Ще однією причиною використання блокчейн-технологій в державному управлінні є можливість знизити витрати на експлуатацію завдяки підвищенню продуктивності державних органів. Оскільки держава фінансується за рахунок громадян, ефективне використання бюджетних коштів є ключовим фактором. Системи, засновані на блокчейні та смарт-контрактах, можуть автоматизувати завдання та робочі процеси, що дозволить скоротити час та витрати на весь процес

обміну документами.

Незважаючи на те, що скорочення витрат на адміністративні послуги є надзвичайно практичним, це також може допомогти зміцнити довіру з боку громадян. Поліпшення ефективності та зниження витрат призведе до підвищення рейтингу керівних органів, а за рахунок скорочення операційних витрат уряд зможе вкладати більше коштів на розвиток інших державних галузей, таких як освіта, безпека і охорона здоров'я.

Збір податків – ще один процес, який можна оптимізувати за допомогою цієї технології. Реєстри, засновані на блокчейнах, можуть забезпечити простий обмін грошей між сторонами відповідно до чітко визначених умов. Це може призвести до різкого зменшення адміністративних витрат, пов’язаних зі збором та розподілом податкових коштів. Наприклад, зберігаючи всі платіжні записи та обробляючи декларації на приватних блокчейнах, органи збору податків можуть забезпечити підвищену безпеку для захисту окремих платників податків від шахрайства або крадіжки особистих даних.

Хоча блокчейн можна використовувати для підвищення цілісності, прозорості та ефективності циркуляції даних, існують певні обмеження, пов'язані з використанням цієї технології в адміністративному секторі.

1) Мережа блокчейн може бути спроектована для більш гнучкої роботи, дозволяючи зміну раніше записаних даних, але це, в свою чергу, вимагає схвалення з боку більшості перевіряючих вузлів, що може спричинити проблеми, пов’язані з децентралізацією системи та призвести до деяких розбіжностей між учасниками.

2) Конфіденційність інформації також є одним з ключових елементів у цій галузі, оскільки всі записи, додані до блокчейну, будуть доступні, і це може суперечити існуючому процесу обробки особистих даних, як приклад можна навести таку процедуру, як зняття судимості. У країнах, які визнають право людини на реабілітацію, незмінність даних може суперечити чинному законодавству. Можливим рішенням цієї проблеми може бути використання функції спалювання даних.

Хоча деякі переваги все ще є гіпотетичними, багато країн вже проводять різні експерименти. Ось кілька прикладів реального використання блокчейн-технологій у державному управлінні.

1) У 2008 році Естонія запустила проєкт, який передбачав створення електронної системи державного управління з використанням блокчейн-технологій. За допомогою цієї системи громадяни можуть отримувати доступ до

своїх особистих даних, а також здійснювати онлайн-оплату податків та отримувати різні державні послуги.

2) У 2018 році уряд Індії запустив проєкт IndiaChain, який передбачає створення блокчейн-інфраструктури для покращення роботи державних установ та забезпечення більш ефективного і безпечного обміну даними.

3) У 2016 році уряд Китаю оголосив про створення «National Blockchain and Distributed Accounting Technology Standardization Technical Committee», який має на меті розробити стандарти для використання блокчейн-технологій у державному секторі.

4) У 2019 році уряд США запустив програму «Blockchain for Grant Payments», яка передбачає використання блокчейн-технологій для забезпечення більш ефективного та безпечного виділення грантів.

5) У 2017 році уряд Данії запустив проєкт, який передбачає використання блокчейн-технологій для забезпечення безпечного зберігання медичних даних громадян та їх ефективного обміну між різними медичними закладами.

Отже можна зробити висновок, що блокчейн технології можуть змінити підхід до державного управління та привести до більш ефективного та прозорого управління. Вони дозволяють розподілити процес перевірки та зберігання даних ефективно, що зменшує ризики маніпуляцій та зловживань з боку урядовців. Також, вони можуть допомогти забезпечити постійний доступ до документації, що полегшує роботу контролюючих органів та зменшує необхідність у посередниках при обміні даними та фінансових транзакціях.

На реальних прикладах використань у різних країнах було показано, що застосування блокчейн технологій може покращити якість державних послуг та зробити їх доступнішими для громадян. Крім того, такі технології можуть знизити експлуатаційні витрати, що є важливим фактором для держав, що покладаються на бюджетні кошти.

2.2 Інноваційні можливості блокчейну в галузі розробки ігор

В останні роки ігрова індустрія зазнала значного росту та розвитку, стаючи однією з найбільш прибуткових та популярних галузей на світовому рівні. Завдяки технологічному прогресу, геймери отримують все більше можливостей для занурення у віртуальний світ, а розробники ігор постійно шукають нові способи залучення користувачів та розширення своїх продуктів. В цьому контексті

блокчейн технологія відкриває нові інноваційні можливості для галузі розробки ігор, які можуть вплинути на досвід гравців та принести значні переваги для розробників.

У цьому розділі буде розглянуто інноваційні можливості блокчейну в галузі розробки ігор, зокрема його вплив на внутрішню економіку гри, управління віртуальними товари та послугами, забезпечення безпеки та прозорості гри, а також використання розумних контрактів для автоматизації процесів та розробки децентралізованих ігрових платформ.

Сучасні онлайн-ігри переважно працюють за централізованою моделлю, що означає зберігання всіх даних на сервері, повний контроль над яким належить розробникам. Інформація, що зберігається на серверах, включає облікові записи та історію ігрових подій та предметів, таких як колекційні предмети, предмети персонажів або віртуальні монети, що отримують гравці.

Ця модель має кілька недоліків, зокрема, велика залежність від розробників, які можуть впливати на гру та її економіку, забороняти гравцям торгувати віртуальними предметами та контролювати доступ до гри. Використання технології блокчейн може змінити цю модель, забезпечивши більшу децентралізацію та владу для гравців. За допомогою блокчейну можливо створити віртуальну економіку, де предмети гри можуть бути унікальними, не залежними від розробників та можуть бути продані за реальні гроші [20].

Крім того, за допомогою смарт-контрактів можна розробити правила торгівлі та взаємодії гравців в грі, які виконуються автоматично та безперервно, забезпечуючи безпеку та прозорість. Також, блокчейн дозволяє створювати більш складні та відкриті ігрові світи, що можуть залучити більше гравців та забезпечити нові можливості для інтерактивної гри та взаємодії між гравцями.

В ситуації, коли база даних контролюється певною компанією, гравці не мають реального права власності на свої аккаунти та віртуальні предмети. Більше того, централізовані сервери мають наступний ряд недоліків та вразливостей.

1) Різноманітні збої, що виникають через технічні складнощі або перевантаження серверів.

2) Вторгнення хакерів, які можуть красти особисті дані гравців та їх ігрові ресурси.

3) Можливість припинення роботи серверів гри, що призводить до втрати доступу до аккаунтів та віртуального майна.

4) Необґрунтовані блокування аккаунтів гравців або неправомірні санкції.

5) Брак прозорості в ігрових механіках, що може призвести до недовіри гравців до розробників та адміністрації гри.

6) Маніпуляції з ігровою економікою з боку розробників або адміністраторів, що можуть порушувати справедливість і баланс гри для користувачів.

Технологія блокчейн може зменшити або навіть усунути більшість зазначених проблем. Використовуючи розподілену базу даних, система на основі блокчейну може перевіряти та захищати різні види цифрової інформації, включаючи ігрові історії, віртуальні предмети та токенізовані активи. Основна мета полягає у тому, щоб зменшити контроль ігрових компаній та передати владу гравцям. В результаті, кожен гравець зможе володіти своїм аккаунтом та цифровими активами, а користувачі матимуть можливість обмінювати ці активи за своїм бажанням.

Зазвичай, кожен актив представлений у вигляді унікального токена NFT (non-fungible token). Ці активи можуть включати ігрові карти, ексклюзивні скіни, зброю, персонажів тощо. Незалежно від виду активу, всі вони можуть бути пов'язані з конкретним токеном на блокчейні, сумісним з децентралізованою мережею. Це дозволяє гравцям забезпечувати власність, обмін та використання своїх активів без обмежень та залежності від ігрових компаній.

Ці переваги блокчейну створюють нові можливості та горизонти для ігрової індустрії. Розробники можуть створювати ігри з відкритим кодом і децентралізованою економікою, забезпечуючи гравцям більшу свободу дій та гнучкість. Відкритий код дозволяє створювати спільноти навколо ігор, які зможуть активно впливати на розвиток та покращення ігрового досвіду.

Крім того, застосування блокчейну сприяє створенню міжігрових екосистем, де гравці можуть використовувати свої активи в різних іграх, а також співпрацювати з іншими гравцями у межах децентралізованого ринку. Це може стимулювати інноваційність та конкуренцію серед розробників, адже вони повинні пропонувати унікальні та цікаві ігрові сценарії, щоб привернути увагу гравців.

Ігрові компанії володіють правом контролю над шансами отримання рідкісних предметів та керують економікою своїх ігор. Вони також можуть обмежувати обіг ігрових предметів, роблячи їх непридатними для обміну. Ігри, засновані на блокчейні, дозволяють розвиток децентралізованих торгових платформ. Такий підхід усуває потребу в довірі між гравцями та гарантує захист від цензури. Гравці мають можливість вільно купувати, продавати та обмінювати

свої ігрові активи.

Блокчейн і смарт-контракти сприяють зниженню комісійних відрахувань та прискоренню транзакцій. Це дає змогу обробляти значну кількість платежів, що стосуються не лише угод між гравцями, а й між гравцями та розробниками.

Завдяки цьому, ігрова індустрія може стати більш гнучкою та демократичною, де гравці отримують більше контролю над своїми активами, а розробники зможуть налаштовувати ігрові механіки відповідно до потреб спільноти гравців. Такі зміни сприятимуть створенню нових ігрових досвідів, а також забезпечать стійкість ігрової екосистеми в цілому.

Коли гра розміщена на централізованому сервері, розробники мають можливість покинути проект або припинити існування гри в будь-який момент. Застосування блокчейн-технології дозволяє гравцям продовжувати грати, навіть якщо розробники зупиняють підтримку проекту. Залежно від реалізації, блокчейн може надати змогу створенню децентралізованих, прозорих серверів з відкритим вихідним кодом. У таких ситуаціях, гру можна модифікувати тільки за умови, що більшість учасників мережі підтримує такі зміни.

Крім того, децентралізований характер блокчейну забезпечує захист від втручання хакерів і шахраїв, оскільки система не має спільних вразливих точок. Доти, поки блокчейн продовжує працювати, гра залишається активною.

Такий підхід сприяє створенню стійких ігрових екосистем, де влада розподіляється між гравцями та розробниками, а не зосереджена в руках однієї компанії. Це також може стимулювати спільноту гравців до розвитку та модифікації ігор, а також сприяти підтримці та розвитку ігор незалежно від оригінальних розробників.

Таким чином можна виділити основні аспекти впровадження блокчейну в ігровій індустрії.

1) Віртуальна економіка і криптовалюти. Впровадження блокчейну в ігрову індустрію може значно вплинути на віртуальні економічні системи в іграх. Зокрема, застосування криптовалют може полегшити транзакції між гравцями, спростити внутрішні покупки та обмін віртуальними товарами і послугами. Крім того, криптовалюти можуть забезпечити більшу фінансову безпеку, знижуючи ризик шахрайства та крадіжки аккаунтів.

2) Власність та управління віртуальними активами. За допомогою блокчейну, гравці зможуть володіти та керувати своїми віртуальними активами, такими як предмети, зброя, персонажі або навіть віртуальні ділянки землі, на

децентралізованій платформі. Це означає, що власність над активами буде безпосередньо належати гравцям, а не розробникам ігор. Таке рішення може сприяти розвитку вторинного ринку віртуальних товарів, сприяти рівній конкуренції та стимулювати ріст економіки в іграх.

3) Безпека та прозорість. Блокчейн може забезпечити більш безпечне та прозоре середовище для гравців та розробників. Завдяки технології розподіленого реєстру, маніпуляції з ігровими даними стануть практично неможливими. Це може зменшити ризик шахрайства, нечесної конкуренції та інших негативних явищ у іграх.

4) Розумні контракти та автоматизація. Застосування розумних контрактів в ігровій індустрії може автоматизувати ряд процесів, таких як розподіл прибутків, управління правами та проведення транзакцій. Це може сприяти ефективності та забезпечити більш справедливе та прозоре функціонування ігор.

5) Крос-геймінг та міжігрова співпраця. Блокчейн може сприяти розвитку крос-геймінгу та міжігрової співпраці, дозволяючи гравцям використовувати свої віртуальні активи та досягнення в різних іграх на одній платформі. Це може стимулювати розвиток нових ігрових екосистем, партнерств та спільнот, забезпечуючи більш згуртоване та інтегроване ігрове середовище.

6) Відкритість для розробників та інновацій. Відкриті блокчейн-платформи можуть сприяти інноваціям в ігровій індустрії, надаючи розробникам доступ до інструментів, ресурсів та спільноти, необхідних для створення нових ігор та додатків. Це може прискорити розвиток ігрової індустрії та створити нові можливості для гравців, розробників та інших зацікавлених сторін.

У цілому, впровадження блокчейну в галузі розробки ігор може принести ряд переваг, що стосуються безпеки, ефективності, інновацій та віртуальної економіки. Застосування цієї технології може відкрити нові горизонти для гравців та розробників, сприяючи розвитку ігрової індустрії та пошуку нових способів взаємодії та розваги.

Однак, слід враховувати, що використання блокчейну в іграх також має певні недоліки. Наприклад, він може призвести до збільшення витрат на розробку ігор, оскільки розробники повинні враховувати більш складні аспекти децентралізованої архітектури. Також, швидкодія транзакцій в блокчейні може бути недостатньою для деяких ігрових ситуацій, що вимагають миттєвої взаємодії.

Хоча блокчейн технологія може принести численні переваги для ігрової індустрії, таких як децентралізація, безпека та забезпечення власності гравців на їх

ігрові активи, варто також звернути увагу на можливі негативні аспекти та виклики, пов'язані з її впровадженням.

Крім того, існують ще деякі недоліки використання блокчейну в іграх.

1) Масштабованість. Багато блокчейнів можуть зіткнутися з проблемами масштабованості, що обмежують кількість транзакцій, які можуть бути оброблені за одиницю часу. Це може стати проблемою в іграх з великою кількістю гравців або ігрових операцій.

2) Комісії. Транзакції в блокчейні часто супроводжуються комісіями, які можуть рости залежно від завантаженості мережі. Для ігрових платформ це може стати перешкодою, оскільки гравці можуть не бажати сплачувати додаткові кошти за кожну ігрову транзакцію.

3) Комплексність розробки. Розробка ігор на блокчейні може бути складнішою порівняно з традиційними методами. Розробники повинні вивчити нові інструменти та платформи, а також забезпечити безпеку та прозорість смарт-контрактів.

4) Енергетична ефективність. Деякі блокчейни, зокрема ті, що використовують механізм консенсусу Proof of Work, можуть вимагати значних обсягів енергії для підтримки мережі. Це може привести до підвищення енергетичних витрат та впливу на навколишнє середовище.

5) Юридичні аспекти. Регулювання криптовалют та блокчейн-технологій може суттєво відрізнятися в різних країнах. Ігрові компанії повинні розуміти та дотримуватися місцевих законодавчих вимог, які можуть стосуватися використання блокчейну в їхніх іграх.

Враховуючи ці недоліки, розробники та компанії, що працюють над іграми на основі блокчейну, повинні ретельно виважувати всі переваги та недоліки перед впровадженням даної технології у свої проекти. Важливо розуміти, що для деяких ігрових жанрів та аудиторій, блокчейн може принести значні переваги, в той час як для інших, традиційні підходи до розробки ігор можуть бути ефективнішими.

Для прискорення швидкодії транзакцій та зменшення комісій, може бути розглянуте використання «Layer 2» рішень, які допомагають підвищити ефективність блокчейн-мереж. Також можуть бути вивчені альтернативні консенсусні механізми, які є більш екологічно сталими та енергоефективними.

Також, важливо пам'ятати, що блокчейн є ще молодою технологією, яка продовжує розвиватися та вдосконалюватися. З появою нових блокчейн-платформ, протоколів та рішень, ігрова індустрія може відкрити для себе ще більше

можливостей для створення захоплюючих, безпечних та інтерактивних ігрових досвідів.

З урахуванням вищезазначеного, блокчейн має значний потенціал для ігрової індустрії, пропонуючи нові можливості щодо власності, обміну та застосування цифрових активів. Розробники та гравці мають можливість експериментувати з новими концепціями та бізнес-моделями, які можуть призвести до революції в ігровій галузі.

Такі інновації можуть стимулювати зростання віртуальних світів та соціальних платформ, на яких гравці будуть мати можливість спілкуватися, торгувати та здійснювати спільні проекти. Завдяки блокчейну, гравці зможуть створювати цінність в іграх та відчувати реальну користь від своїх віртуальних активів.

Однак, щоб ці переваги стали реальністю, ігрові компанії та розробники повинні співпрацювати зі спільнотами гравців та дотримуватися стандартів блокчейн-технологій. Це може включати у себе роботу над оптимізацією швидкодії транзакцій, забезпечення безпеки даних та розвиток інфраструктури для підтримки масштабованості блокчейн-додатків.

У майбутньому, блокчейн може стати основою для нового покоління ігор, які дозволять гравцям отримувати неперевершений ігровий досвід та більше контролю над своїми віртуальними активами. Це може сприяти розвитку глобальної ігрової екосистеми, де гравці, розробники та інвестори спільно працюють над створенням нових світів та ігрових можливостей.

2.3 Інновації в банківській галузі за допомогою блокчейну

Блокчейн-технологія продовжує революціонізувати багато індустрій, і банківська галузь не є винятком. Впровадження блокчейну в сфері фінансів відкриває нові можливості та інноваційні рішення для вирішення традиційних проблем банківської системи, таких як швидкість операцій, вартість послуг, безпека та прозорість транзакцій. У цьому розділі буде розглянуто, як блокчейн може змінити підхід до банківських послуг та прискорити розвиток інновацій в галузі.

У сучасному світі банківські установи відіграють роль посередників у глобальній економіці, контролюючи та налагоджуючи всі аспекти фінансової системи через власні внутрішні обліки. Через те, що ці дані не є відкритими для

громадського доступу, вони створюють невпевненість щодо надійності банків та їх здебільшого застарілої інфраструктури. Технологія блокчейн має потенціал трансформувати не тільки світові фондові ринки, але й саму банківську індустрію, замінюючи посередників стабільною, безмежною та прозорою системою, до якої кожна особа зможе легко отримати доступ.

Ця революційна технологія може допомогти банкам вирішити наболілі проблеми, такі як складність міжбанківських розрахунків, прозорість операцій, надійність та безпеку даних клієнтів. Блокчейн також сприятиме розвитку децентралізованих фінансових сервісів та сприяє створенню нових інноваційних фінансових продуктів та бізнес-моделей. Однак, для досягнення цих переваг, необхідно адаптуватися до нових технологій, розробляти відповідні стандарти та регулятивні акти, а також забезпечувати підтримку та співпрацю між всіма учасниками ринку.

Однією з ключових переваг блокчейну в банківській галузі є покращення в міжбанківських розрахунках. Традиційно, ці процеси можуть займати кілька днів через комплексність системи та необхідність підтвердження операцій третіми сторонами. Блокчейн може спростити цей процес, забезпечуючи миттєве та безпечне проведення транзакцій без участі посередників. Це знижує витрати на операції та забезпечує більшу прозорість для клієнтів.

Технологія блокчейн може зменшити час очікування для транзакцій, зробити їх економічнішими, спрощувати доступ до капіталу, підвищувати захист даних та гарантувати виконання зобов'язань у транзакціях за допомогою смарт-контрактів. Внаслідок інноваційних особливостей блокчейн-технології, способи взаємодії нових блоків з транзакціями між собою можуть відкрити можливості для створення цілком нових типів фінансових послуг.

Завдяки блокчейну міжнародні платежі можуть стати швидшими та менш витратними. Зараз міжнародні транзакції потребують участі ряду посередників, які забезпечують переказ коштів від одного банку до іншого. Це може займати кілька днів і вимагати високих комісій. За допомогою блокчейну можна об'єднати різні валютні коридори в єдину мережу, що сприяє миттєвим та економічним транзакціям [21].

Ще одним напрямком інновацій є використання смарт-контрактів у банківській діяльності. Смарт-контракти автоматично виконуються при настанні певних умов, визначених сторонами. Це може застосовуватися в різних сферах, таких як виплата кредитів, страхові виплати, управління активами та інші. Завдяки

автоматизації процесів, смарт-контракти допомагають скоротити витрати на адміністрування та забезпечують більшу надійність та прозорість.

Технологія блокчейн може перетворити сферу кредитування, яка досі була монополізована банками та іншими кредитними компаніями. Такі установи зазвичай пропонують позики під високі відсотки та обмежують доступ до капіталу на основі кредитних рейтингів, що робить процес позичання тривалим та дорогим. Однак, банки є важливими учасниками економіки, які забезпечують необхідні кредитні кошти для придбання дорогих товарів.

Технологія блокчейн може змінити цю систему, дозволяючи людям безпосередньо отримувати та надавати позики один одному, обходячи традиційні кредитні установи. Децентралізована природа блокчейну дозволяє створювати смарт-контракти, які забезпечують автоматизовану обробку кредитних операцій, а також забезпечують відсутність посередників, що зменшує витрати на процес кредитування та ризик невиконання платежів. Більше того, забезпечення транзакцій в блокчейні може бути забезпечено за допомогою криптографії, що забезпечує безпеку та конфіденційність усіх операцій. В результаті, блокчейн технологія може стати інструментом для створення більш ефективної системи кредитування.

Технологія блокчейн надає можливість будь-якій особі у світі бути частинкою нової кредитної екосистеми, яка є інтегральною складовою децентралізованих фінансів, відомих як DeFi (Decentralized Finance). Ця кредитна екосистема DeFi базується на фінансових додатках, розроблених на платформі блокчейн, що сприяє створенню доступної фінансової системи. Головна мета полягає у розробці відкритої, безкоштовної та прозорої екосистеми фінансових послуг, доступної для всіх і функціонуючої незалежно від урядового втручання. Користувачі матимуть повний контроль над своїми активами і зможуть взаємодіяти з цією екосистемою через децентралізовані однорангові додатки, відомі як dapps (decentralized application). Однорангове кредитування на основі блокчейну дозволяє кожному вільно позичати та надавати кошти за допомогою простих, безпечних та економічно вигідних методів без будь-яких обмежень.

DeFi включає в себе різноманітні сервіси, такі як кредитування, страхування, інвестиційні платформи та стабільні монети, які можуть забезпечити більшу фінансову свободу. Схематичне зображення екосистеми DeFi представлено на рисунку 2.1.

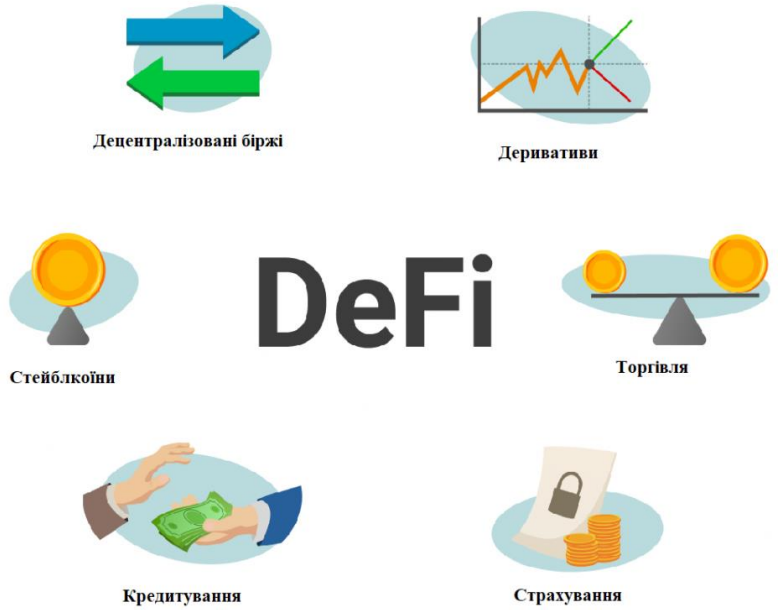


Рисунок 2.1 – Екосистема DeFi

Більшість наявних та потенційних застосунків у сфері децентралізованого фінансування передбачають розробку та використання смарт-контрактів. Замість традиційного договору, який використовує юридичну мову для встановлення умов між сторонами, смарт-контракт базується на комп'ютерному коді. Оскільки усі умови викладені у вигляді коду, смарт-контракти мають властивість самостійного виконання. Це забезпечує надійне виконання та автоматизацію великої кількості бізнес-процесів, які наразі потребують ручного управління.

Також важливим аспектом є забезпечення безпеки та захисту даних клієнтіів у банківській галузі. Блокчейн може допомогти у вирішенні цієї проблеми, оскільки він забезпечує високий рівень шифрування та надійності для зберігання та обміну даними. Зокрема, технологія розподіленого реєстру може зменшити ризики втрати чи крадіжки інформації, а також захистити клієнтів від шахрайства.

Блокчейн також може вплинути на екосистеми ідентифікації клієнтів KYC (Know Your Customer) та боротьбу з відмиванням грошей AML (Anti-Money Laundering). Блокчейн може спростити процеси KYC та AML, завдяки зберіганню перевіреної інформації про клієнтів в розподіленому реєстрі, що забезпечує швидкий доступ до даних для банків та регуляторів. Це не тільки знижує витрати на здійснення таких процедур, але й забезпечує відповідність законодавчим вимогам.

Впровадження блокчейну в банківській галузі може також стимулювати розвиток нових бізнес-моделей та продуктів, спрямованих на задоволення потреб

сучасних клієнтів. Наприклад, можуть з'явитися нові форми мікрокредитування, краудфандингу, платіжних систем або інвестиційних платформ, які більше відповідають потребам клієнтів, надають більше можливостей для заробітку та зменшують витрати на операції.

Отже, підсумовуючи усе це, можна виділити такі переваги використання блокчейну у банківській індустрії.

1) Зниження витрат. Блокчейн може скоротити витрати на операції та обробку даних, завдяки автоматизації та відсутності потреби в посередниках.

2) Швидкість транзакцій. Блокчейн забезпечує більш швидкі транзакції, порівняно з традиційними банківськими системами.

3) Безпека даних. Розподілена структура блокчейну робить його важким для хакерів та забезпечує кращий захист даних.

4) Відкритість та прозорість. Блокчейн дозволяє створювати відкриті та прозорі системи, які забезпечують довіру між сторонами.

5) Смарт-контракти. Автоматичне виконання умов смарт-контрактів може полегшити та прискорити бізнес-процеси.

6) Децентралізовані фінансові сервіси DeFi. Блокчейн сприяє розвитку DeFi, що відкриває нові можливості та інноваційні фінансові послуги.

7) Доступність та інклюзивність. Блокчейн може полегшити доступ до фінансових послуг для непредставлених та недостатньо представлених населення груп, сприяючи фінансовій інклюзивності.

8) Міжнародні платежі. Блокчейн спрощує міжнародні платежі, знижуючи витрати та забезпечуючи швидкість переказів.

9) Регуляторний звіт та відповідність. Блокчейн може полегшити виконання регуляторних вимог та поліпшити процеси звітності для банків.

Попри очевидні переваги блокчейну в банківській індустрії, потрібно також розглянути деякі недоліки та перешкоди, які можуть виникнути під час впровадження цієї технології. Розуміння цих проблем допоможе банківським і фінансовим установам краще оцінити вартість та можливості реалізації блокчейн-технологій у своїх операціях. Деякі недоліки та перешкоди, які можуть уповільнити впровадження впровадження блокчейну.

1) Технічні виклики. Блокчейн все ще знаходиться на ранніх етапах розвитку, і деякі технічні проблеми, такі як масштабованість, швидкість транзакцій та затримки, потребують подальших удосконалень.

2) Регуляторні питання. Відсутність чіткого регулювання та стандартів

для блокчейну може змусити банки бути обережними в його впровадженні. Регулятори по всьому світу активно працюють над формулюванням рекомендацій та правил щодо використання блокчейну в банківському секторі.

3) Прийняття та інтеграція. Оскільки блокчейн змінює традиційні бізнес-моделі, банкам може бути важко прийняти нові технології, що вимагає реорганізації внутрішніх процесів та інтеграції з існуючими системами.

4) Проблеми з приватністю. Блокчейн може забезпечити високий рівень прозорості, однак він може порушувати питання приватності клієнтів та даних, які мають бути вирішені.

5) Енергетична ефективність. Деякі блокчейн-платформи, такі як Bitcoin, споживають значні кількості енергії для своєї роботи, що може створювати проблеми з екологією та енергетичною ефективністю.

6) Консенсус та управління. Визначення оптимального механізму консенсусу та управління для блокчейну в банківській індустрії є викликом, оскільки банки зазвичай займаються важливими фінансовими операціями і потребують високого рівня безпеки та надійності. Знайти механізм, який гарантує достатній рівень децентралізації без втрати продуктивності та ефективності, є суттєвим аспектом.

7) Міжнародна співпраця. Для успішного застосування блокчейну на міжнародному рівні, банки та фінансові установи повинні співпрацювати з іншими країнами та регуляторами, що може бути складним процесом через різні законодавства та стандарти.

8) Суперечливість та невизначеність. Оскільки блокчейн є порівняно новою технологією, деякі компанії та особи можуть бути схильні до сприйняття технології як неперевіреної та суперечливої, що може сповільнити її впровадження.

Ураховуючи ці недоліки та перешкоди, банківська індустрія повинна зосередитись на розвитку рішень та політик, які відповідають потребам галузі та допомагають подолати ці виклики. Впровадження блокчейну у банківську сферу може потребувати часу, але у довгостроковій перспективі це може принести значні переваги для фінансової інфраструктури та клієнтів по всьому світу.

Підсумовуючи, інновації в банківській галузі за допомогою блокчейну відкривають нові можливості для розвитку сектора, покращення якості та доступності фінансових послуг. Однак, необхідновраховувати, що успішне впровадження блокчейну в банківську сферу потребує співпраці між різними сторонами: банками, регуляторами, розробниками технологій та клієнтами.

Важливо розробляти та впроваджувати відповідні стандарти, нормативні акти та принципи безпеки, щоб забезпечити стабільність, надійність та довіру до нових технологій та інновацій.

Також слід враховувати технічні обмеження блокчейну, такі як проблеми зі швидкістю транзакцій або масштабуванням. Вирішення цих проблем може потребувати додаткових досліджень та розробок в області блокчейн-технологій, а також створення нових підходів та архітектурних рішень.

Окрім того, успішна інтеграція блокчейну в банківській галузі потребує зміни у ставленні та підходах до роботи. Зокрема, може бути необхідно підготувати та перекваліфікувати співробітників банків, щоб вони могли ефективно працювати з новими технологіями та інструментами. Також може знадобитися додаткова робота з підвищення обізнаності клієнтів про переваги та можливості, які надає блокчейн.

Враховуючи всі вищезазначені аспекти, можна сказати, що блокчейн має великий потенціал для інновацій в банківській галузі. Проте успіх цього процесу залежить від здатності всіх учасників ринку адаптуватися до нових технологій.

2.4 Застосування технології блокчейн в медичній галузі

Застосування технології блокчейн в медичній галузі відкриває нові можливості для поліпшення якості та ефективності медичного обслуговування, а також забезпечення безпеки та конфіденційності даних пацієнтів. Використання блокчейну може привести до оптимізації процесів, зменшення витрат та покращення доступності медичних послуг для всіх користувачів.

Одним із ключових напрямків застосування блокчейну в медичній галузі є створення єдиної, безпечної та конфіденційної системи обміну медичною інформацією між різними учасниками охорони здоров'я, такими як лікарі, клініки, лабораторії та страхові компанії. Блокчейн може забезпечити надійне зберігання електронних медичних записів та гарантувати їхню автентичність, що сприятиме забезпеченню якості медичної допомоги та вчасного доступу до важливої інформації про пацієнта.

Функції блокчейну, які дозволяють йому бути використаним в якості захищеного журналу фінансових операцій, також можуть бути використані для зберігання медичної інформації. Оскільки більшість блокчейн-мереж створюються як розподілені системи, які використовують криптографічні методи для запису та захисту даних, зламати або змінити будь-яку інформацію без згоди всіх учасників

мережі буде надзвичайно складно. Таким чином, незмінність даних стає ключовою перевагою для створення надійної бази медичних записів пацієнтів. Схематично побудову блокчейну, як базу даних медичної картки показано на рисунку 2.2.

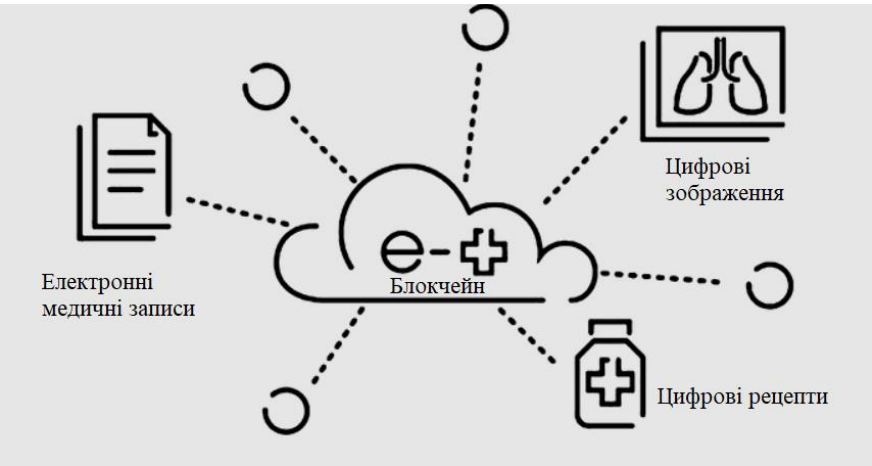


Рисунок 2.2 – База даних медичної картки

Використання блокчейну у медичній сфері може сприяти створенню спільних баз даних для наукових досліджень та клінічних випробувань, що значно підвищить ефективність розробки нових ліків та методів лікування. Забезпечивши безпечний обмін медичними даними між дослідниками та медичними установами, блокчейн може зробити процес затвердження нових лікарських засобів швидшим та більш надійним.

Додатково, однорангова архітектура, яка використовується в блокчейн-мережах, дозволяє синхронізацію медичних записів пацієнтів між різними комп'ютерами в режимі реального часу під час їх оновлення. Відповідно, кожен вузол має власну копію всієї мережі блокчейну, яка регулярно синхронізується з іншими вузлами, що гарантує актуальність та достовірність даних. Таким чином, децентралізація та обмін даними стають ключовими елементами.

Ступінь децентралізації блокчейн-мереж може варіюватися залежно від розташування вузлів та використовуваної архітектури. У сфері охорони здоров'я блокчейни зазвичай розробляються як приватні мережі, на відміну від публічних. У той час як публічні блокчейни відкриті для участі будь-кого, приватні мережі потребують дозволу та контролюються меншою кількістю вузлів, що забезпечує більшу безпеку та контроль над конфіденційністю даних.

Крім того, блокчейн може сприяти розвитку телемедицини та віддалених медичних консультацій, що забезпечить пацієнтам можливість отримувати

консультації та допомогу від спеціалістів, незалежно від їх географічного розташування. Смарт-контракти можуть автоматизувати процеси виставлення рахунків, оплати та звітності, забезпечуючи прозорість та ефективність взаємодії між пацієнтами та медичними працівниками.

Це також може сприяти розвитку віддалених моніторингових систем, які дозволяють медичним працівникам стежити за станом здоров'я пацієнтів на відстані і отримувати вчасні повідомлення про будь-які зміни, що вимагають втручання. Все це допоможе забезпечити більш індивідуальний та ефективний підхід до охорони здоров'я, зменшуючи навантаження на медичних працівників та поліпшуючи якість допомоги пацієнтам.

Застосування блокчейну може відіграти ключову роль у моніторингу та контролі якості ліків, а також в боротьбі з контрафактними медикаментами. Завдяки цій технології, можна відстежувати весь ланцюжок постачання фармацевтичних препаратів – від виробника, через дистриб'юторів, аж до аптек і кінцевих споживачів. Це дозволяє гарантувати якість та безпеку медикаментів, сприяючи запобіганню продажу контрафактних препаратів.

Така система відстеження також може полегшити виявлення та розслідування випадків контрафакції, сприяючи швидкому відновленню легітимності ланцюжка постачання. Зокрема, блокчейн може допомогти у боротьбі зі злочинними схемами, що забезпечують незаконний обіг фармацевтичних препаратів, такими як перепродаж рецептурних ліків або просочення контрафактної продукції на ринок.

Крім того, застосування блокчейну в ланцюжку постачання ліків може сприяти підвищенню ефективності та зменшенню витрат для фармацевтичних компаній, аптек та споживачів завдяки автоматизації процесів обміну даними, контролю якості та оплати за продукцію.

Використання блокчейн технології в медичній сфері може принести значні переваги, які відображаються в ряді ключових аспектів. Зокрема, блокчейн може вдосконалити безпеку даних, сприяти співпраці між учасниками та оптимізувати адміністративні процеси. Нижче наведений перелік деяких переваг, використання блокчейн технологій у цій сфері.

1) Забезпечення конфіденційності та безпеки медичних даних. Блокчейн допомагає зберігати медичні дані безпечно та захищено за допомогою криптографічних методів, що забезпечує конфіденційність інформації пацієнтів.

2) Єдина база медичних записів. Блокчейн може сприяти створенню

єдиної бази медичних записів, яка дасть можливість лікарям, клінікам та іншим учасникам охорони здоров'я легко обмінюватися важливою інформацією про пацієнтів.

3) Забезпечення безпеки ланцюжка постачання ліків. Блокчейн дозволяє відстежувати весь ланцюжок постачання медикаментів від виробника до кінцевого споживача, забезпечуючи якість та безпеку препаратів та запобігаючи контрафакції.

4) Розвиток телемедицини. Блокчейн може підтримувати віддалені медичні консультації, що надає можливість пацієнтам отримувати консультації та допомогу від спеціалістів, незалежно від їх географічного розташування.

5) Автоматизація процесів оплати та звітності. Смарт-контракти на базі блокчейну можуть автоматизувати процеси виставлення рахунків, оплати та звітності, забезпечуючи прозорість та ефективність взаємодії між пацієнтами та медичними працівниками.

6) Відслідковування та звітність досліджень. Блокчейн може сприяти реєстрації та зберіганню результатів медичних досліджень.

7) Забезпечення незмінності даних. Блокчейн гарантує незмінність медичних записів, що забезпечує достовірність інформації та унеможливлює зміну або знищення даних без відповідного дозволу.

8) Спрощення координації між учасниками медичної індустрії. Блокчейн сприяє співпраці між різними учасниками медичної галузі, такими як лікарі, аптеки, страхові компанії та регулятори, спрощуючи обмін даними та координацію.

9) Відкритість та прозорість. Блокчейн допомагає забезпечити відкритість та прозорість медичних записів, дозволяючи пацієнтам контролювати власні дані та давати згоду на їх передачу відповідним особам.

10) Зниження адміністративних витрат. Завдяки автоматизації процесів та зменшенню потреби в ручному введенні даних, блокчейн може знизити адміністративні витрати та підвищити ефективність роботи медичних установ.

11) Відстеження та контроль за доступом до медичної інформації. Блокчейн дозволяє відстежувати, хто та коли мав доступ до медичних записів, забезпечуючи контроль та підвищуючи відповідальність учасників медичної галузі.

Отже, блокчейн технології можуть принести значні переваги для медичної індустрії, поліпшуючи безпеку, прозорість, ефективність та доступність медичної інформації та послуг.

Однак, незважаючи на численні переваги та можливості, що відкриває блокчейн для медичної галузі, є ряд викликів та обмежень, що пов'язані з впровадженням цієї технології. До таких викликів належать питання приватності та захисту даних, а також необхідність встановлення єдиних стандартів інтероперабельності між різними системами та учасниками. Крім того, потрібно забезпечити належний рівень освіти та підготовки медичних фахівців для ефективного використання блокчейн-технологій у своїй роботі.

Серед основних викликів та обмежень, які можуть заважати швидкому та ефективному впровадженню технології блокчейн, можна виділити настуупні.

1) Приватність та захист даних. Забезпечення конфіденційності та безпеки медичної інформації є критично важливим. Відповідність законодавству з охорони даних є обов'язковою, і будь-яка технологія, що впроваджується в медичній сфері, повинна гарантувати дотримання цих норм.

2) Єдині стандарти інтероперабельності. Щоб впровадити блокчейн на масштабі галузі, необхідно розробити та прийняти єдині стандарти для обміну даними між різними системами та учасниками. Це вимагає співпраці та координації між різними зацікавленими сторонами, що може зайняти значний час.

3) Освіта та підготовка медичних фахівців. Для успішного впровадження блокчейн-технологій у медичній сфері, медичні працівники повинні бути освічені та навчені відповідно. Це може вимагати значних зусиль у навчанні та перепідготовці персоналу, а також забезпечення доступу до необхідних ресурсів.

4) Технічні та інфраструктурні обмеження. Впровадження блокчейну може зіткнутися з технічними та інфраструктурними обмеженнями, такими як недостатня швидкість опрацювання транзакцій, масштабованість системи, а також високі витрати на створення та підтримку інфраструктури. Ці обмеження можуть уповільнити широке впровадження технології, а також створити перешкоди для менших медичних закладів з обмеженими ресурсами.

5) Регуляторні вимоги та затвердження. У медичній сфері існують суворі регуляторні вимоги, і будь-яке нове впровадження технології повинне пройти ряд затверджень від різних регуляторних органів. Це може зайняти значний час та ресурси, і процес може бути складним та бюрократичним.

6) Відсутність готовності до змін. Зміна парадигми роботи та впровадження нових технологій може викликати опір серед деяких медичних працівників та зацікавлених сторін. Це може стати перешкодою для широкого прийняття блокчейну в медичній галузі, якщо не буде належної підтримки та

просвіти щодо переваг технології.

7) Захист інтелектуальної власності. Питання захисту інтелектуальної власності, такі як патенти, авторські права та комерційні таємниці, можуть стати проблематичними в контексті блокчейну. Визначення правил та процедур для захисту інтелектуальної власності, а також вирішення спорів, може бути важкою задачею в децентралізованому середовищі.

Ураховуючи ці виклики та обмеження, важливо працювати над подоланням перешкод, щоб забезпечити успішне впровадження блокчейн-технологій у медичній сфері. Це вимагає співпраці між усіма зацікавленими сторонами, включаючи уряди, регуляторні органи, медичні заклади, медичних працівників, технологічних компаній та пацієнтів. Разом вони повинні вирішувати ці проблеми через спільну роботу над стандартами, нормами, освітою, технічними рішеннями та інноваціями.

Незважаючи на виклики, пов'язані з впровадженням технології блокчейну в медичній галузі, потенціал її використання є вражаючим, а успішна інтеграція може привести до значних поліпшень у якості медичного обслуговування та загальному рівні життя людей на глобальному рівні.

Використання блокчейну може революціонізувати ряд аспектів медичної індустрії, включаючи обмін медичною інформацією, контроль ліків, телемедицину, а також захист конфіденційності пацієнтів. Все це сприятиме створенню більш ефективної та безпечної системи охорони здоров'я, яка буде працювати на благо пацієнтів та медичних працівників.

У висновку, хоча впровадження блокчейну в медичну галузь має певні перешкоди та недоліки, його можливості не можна недооцінювати. Згодом, з досвідом і науковими розробками, ця технологія може відіграти значну роль у формуванні майбутнього охорони здоров'я та покращенні якості життя людей по всьому світу.

3 АНАЛІЗ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН, ЯК ЗАСОБУ ДЛЯ ЦИФРОВОЇ ІДЕНТИФФІКАЦІЇ

3.1 Вплив блокчейн технологій на цифрову ідентифікацію

Технологія блокчейн, може бути використана для створення безпечної та ефективної системи цифрової ідентифікації. Однією з головних переваг технології блокчейн є її децентралізований характер. Блокчейн забезпечує збереження та обмін даними між користувачами, які можуть перевіряти автентичність інформації без посередництва третіх осіб. Це дозволяє знизити вартість проведення транзакцій та забезпечує високий рівень безпеки.

Однією з головних проблем традиційної ідентифікації є збереження та обробка персональних даних. Технологія блокчейн може розв'язати цю проблему, оскільки вона забезпечує збереження даних у розподіленому реєстрі, що не може бути змінено або видалено без попереднього погодження всіх учасників мережі. Це забезпечує надійний захист даних та їхню безпеку, а також унеможливлює несанкціонований доступ до них.

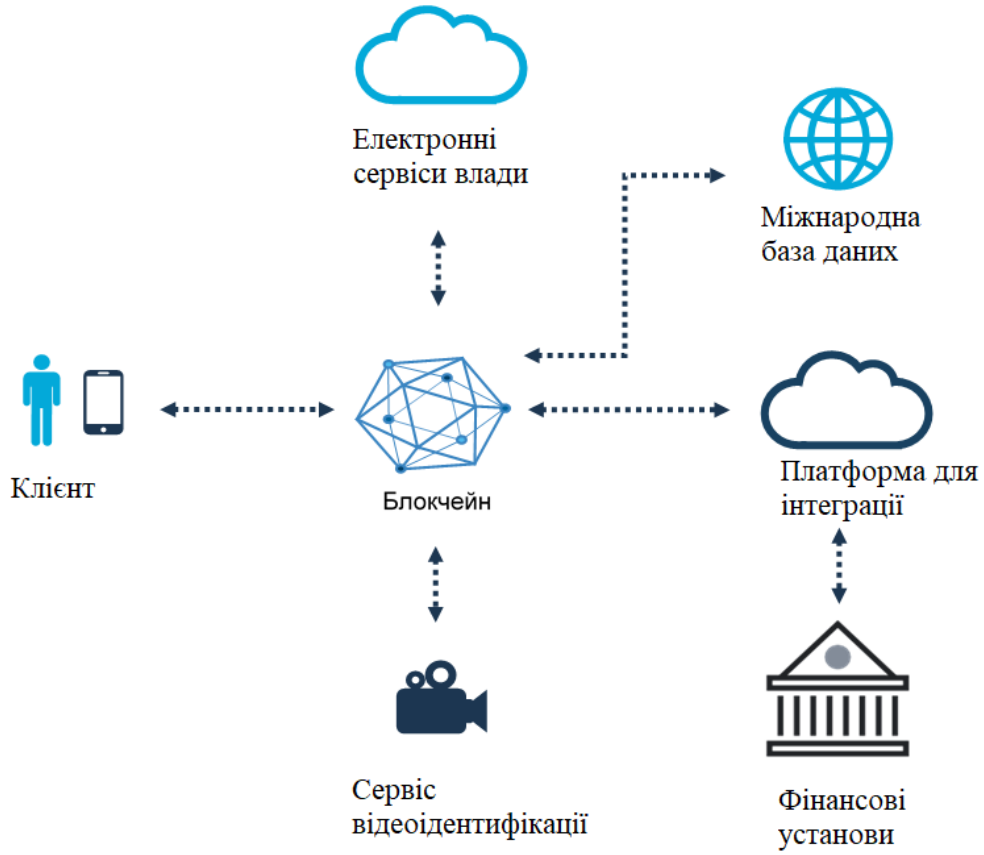
Управління цифровою ідентифікацією та перевірка документів є одним з найбільш перспективних напрямків використання технології блокчейн. Це обумовлено тим, що у минулому мільйони людей по всьому світу стали жертвами витоків персональних даних. У зв'язку з цим, на сьогодні існує нагальна потреба у більш безпечних методах зберігання, передачі та перевірки особистої інформації. Блокчейн технології є відповідним рішенням для вирішення цієї проблеми, оскільки вони забезпечують надійний захист даних та їх безпеку, що робить їх відмінним варіантом порівняно з централізованими базами даних. Тому використання технології блокчейн у системах управління цифровою ідентифікацією та перевірки документів має великий потенціал і є важливим кроком до більш безпечного світу [22].

Коли файли записуються в блокчейн, їх достовірність гарантується за допомогою мережі вузлів, які підтримують систему. Це означає, що кожен запис в блокчейн підтверджується користувачами, що гарантує достовірність інформації.

В такій системі вузли можуть виконувати роль органів влади чи державних установ, що затверджують цифрову документацію, де кожен вузол має право голосувати і підтверджувати правильність даних. Це забезпечує ще більшу

достовірність інформації, оскільки файли в кінцевому підсумку можуть бути використані так само, як і офіційні документи, але з вищим рівнем безпеки.

Система цифрової ідентифікації, заснована на блокчейні, дозволяє аутентифікувати цифрові дані без необхідності прямого обміну інформацією між сторонами. Для цього застосовуються криптографічні методи, такі як хеш-функції або цифрові підписи. Будь-який документ може бути перетворений в хеш, який містить всю інформацію, що використовувалась для його створення, виступаючи в ролі цифрового відбитка пальця. Урядові установи та інші довірені організації можуть надавати послугу створення цифрових підписів для надання документу юридичної сили. Така система є відповідним рішенням для підвищення безпеки зберігання, передачі та перевірки особистої інформації, що є особливо актуальним у сучасному світі, де мільярди людей щороку стикаються з витоком їх персональних даних. Приклад представлення блокчейну, як платформи для цифрової трансформації представлено на рисунку 3.1.



33

Рисунок 3.1 – Блокчейн, як платформа цифрової трансформації

Одним із можливих сценаріїв використання технології блокчейн як засобу

цифрової ідентифікації може бути передача документу в уповноважений орган для створення унікального цифрового відбитку. Наступним етапом є створення цифрового підпису, який гарантує дійсність хешу, який виступає в якості офіційного документа фізичної особи. Такий підхід дозволяє забезпечити високий рівень безпеки та достовірності інформації, знижуючи ризик її втрати або зловживання. Крім того, цей процес можуть здійснювати не лише урядові установи, але й інші довірені організації, що дозволяє підвищити ефективність та швидкість роботи системи [23].

Впровадження блокчейн-технологій для цифрової ідентифікації може принести ряд переваг, які стосуються безпеки, прозорості та контролю над особистими даними. Ось деякі з них.

1) Безпека. Блокчейн забезпечує високий рівень безпеки завдяки криптографічним методам та децентралізованій структурі. Це зменшує ризик злому, втрати або крадіжки ідентифікаційних даних, оскільки вони зберігаються на багатьох комп'ютерах у мережі, а не на одному централізованому сервері.

2) Прозорість та верифікація. Блокчейн забезпечує прозорість та незмінність інформації, що дозволяє легко відстежувати та перевіряти історію даних ідентифікації. Це сприяє відновленню довіри між учасниками та забезпечує високий рівень впевненості в автентичності інформації.

3) Самостійний контроль над даними. Застосування блокчейн для цифрової ідентифікації надає користувачам можливість контролювати та управляти своїми даними, відкриваючи доступ тільки тим сторонам, яким дозволяють. Це сприяє збереженню приватності та дозволяє користувачам самостійно вирішувати, з ким і коли ділитися своєю ідентифікаційною інформацією.

4) Зменшення шахрайства та крадіжки ідентичності. Блокчейн може значно зменшити ризик шахрайства та крадіжки ідентичності, оскільки дані неможливо змінити або видалити без відповідного дозволу. Це утруднює фальсифікацію документів та ідентифікаційних даних, що може призвести до зниження кількості випадків шахрайства та злочинів, пов'язаних з крадіжкою ідентичності.

5) Зниження бюрократії та витрат. Використання блокчейн-технологій для цифрової ідентифікації може спростити процеси та зменшити витрати на документообіг, оскільки потреба в фізичних документах та посередниках зменшується. Це також може пришвидшити процеси верифікації та забезпечити

більш ефективну взаємодію між учасниками.

6) Крос-країнна ідентифікація. Блокчейн-технології можуть полегшити крос-країнну ідентифікацію, спрощуючи процеси перевірки для людей, які переміщуються між країнами або працюють за кордоном. Це може відкрити нові можливості для міжнародної співпраці та обміну ресурсами.

7) Доступність. Блокчейн-технології можуть допомогти забезпечити цифрову ідентифікацію для людей, які не мають доступу до традиційних форм ідентифікації, таких як паспорти або посвідчення особи. Це може забезпечити включення та доступ до важливих послуг, таких як банківські послуги, охорона здоров'я та освіта, для найбільш вразливих верств населення.

8) Інтеграція з іншими технологіями. Блокчейн може бути інтегрований з іншими технологіями, такими як IoT, штучний інтелект або біометрія, для створення ще більш надійних та ефективних систем цифрової ідентифікації.

9) Забезпечення прав та зобов'язань. Використання блокчейн-технології для цифрової ідентифікації може сприяти встановленню та дотриманню прав та зобов'язань у різних сферах, таких як робота, оподаткування та соціальні послуги. Це може полегшити взаємодію між урядовими органами, приватним сектором та громадянами, а також забезпечити більш точні дані для прийняття рішень.

10) Запобігання централізації влади. Блокчейн децентралізує управління ідентифікаційними даними, розподіляючи відповідальність між учасниками мережі. Це може допомогти запобігти надмірній централізації влади та зменшити ризик зловживань або цензури.

11) Збереження історії транзакцій. Блокчейн може зберігати історію транзакцій, пов'язаних з цифровою ідентифікацією, створюючи аудиторський слід та забезпечуючи відповідальність учасників. Це може допомогти забезпечити прозорість та довіру між сторонами, що взаємодіють у різних контекстах.

12) Екологічна стійкість. Використання блокчейн-технологій для цифрової ідентифікації може зменшити споживання паперу та інших матеріалів, пов'язаних з традиційними формами ідентифікації. Це може сприяти сталому розвитку та зменшити негативний вплив на довкілля.

У цілому, блокчейн-технології можуть значно покращити системи цифрової ідентифікації, пропонуючи більш безпечні, прозорі та ефективні рішення для управління особистими даними. Ці переваги можуть сприяти більш швидкому та надійному обміну інформацією, забезпечити кращий захист приватності та сприяти встановленню довіри між учасниками мережі.

Однак, слід враховувати, що для успішного впровадження блокчейн-технологій в системи цифрової ідентифікації потрібно подолати ряд викликів. До них можуть належати питання щодо масштабування, приватності, стандартів та регулювання. Вирішення цих викликів може вимагати співпраці між різними зацікавленими сторонами, включаючи уряди, приватний сектор, академічну спільноту та громадян.

Також, для забезпечення успішного впровадження блокчейн-технологій у системи цифрової ідентифікації важливо забезпечити належний рівень освіти та підготовки користувачів та фахівців, що працюють у цій сфері. Розвиток навичок та розуміння роботи блокчейн-технологій може сприяти більш широкому їх прийняттю та використанню.

У подальшому, блокчейн може стати ключовим інструментом для цифрової ідентифікації та може мати значний вплив на різні сфери життя, включаючи фінанси, охорону здоров'я, освіту та багато інших. Проте, це можливо лише за умови, що потенційні виклики та обмеження будуть враховані та подолані на всіх етапах розвитку та впровадження технології.

Модна виділити такі потенційні недоліки та перешкоди впровадження блокчейн технології, як засобу цифрової ідентифікації.

1) Існує можливість атаки 51%, що більш вірогідно для менших блокчейн мереж. Такий вид атаки може змінити порядок записів у блокчейні, реорганізуючи його. Ця проблема особливо стосується публічних блокчейнів, де кожен може долучатися до процесу перевірки та валідації блоків. У свою чергу, приватні блокчейн мережі можуть зменшити ймовірність таких атак, оскільки тільки довірені особи виступатимуть в якості валідаторів. Проте це може призвести до більш централізованої та менш демократичної моделі.

2) Системи також залишаються уразливими для різних видів шахрайства, зокрема синтетичного розкрадання персональних даних. Синтетична ідентифікація передбачає створення нової особистості на основі реальної інформації з різних джерел. Оскільки кожен фрагмент інформації є достовірним, системи можуть визнати створені шахраями ідентифікатори як справжні. Це є популярним видом атаки, що використовується злочинцями при здійсненні шахрайських операцій з кредитними картами. Для вирішення цієї проблеми можна використовувати цифрові підписи, щоб комбінація документів не приймалася як підтвердження в мережі блокчейн. Наприклад, державні установи можуть надавати цифрові підписи для кожного окремого документа, а також загальний цифровий підпис для всіх

даних, що зареєстровані на одну особу.

3) Відсутність регуляторного фреймворку. Блокчейн технологія все ще розвивається, тому не завжди існують чіткі правила та регуляторні вимоги до використання цієї технології в сфері цифрової ідентифікації.

Отже, впровадження технології блокчейн як засобу для цифрової ідентифікації має значний потенціал для покращення безпеки та ефективності процесу ідентифікації. Однак, перед її впровадженням слід ретельно розглянути всі переваги та недоліки, та забезпечити надійний захист конфіденційності та приватності даних користувачів.

Незважаючи на обмеження та недоліки, технологія блокчейн має значний потенціал у зміні способу перевірки, зберігання та обміну цифровими даними. Хоча багато компаній та стартапів вже вивчають цю можливість, їм ще потрібно довго працювати, щоб вдосконалити цю інновацію. Проте, на мою думку, у найближчі роки ми побачимо значну кількість послуг, пов'язаних з управлінням цифровою ідентифікацією, де блокчейн виконуватиме ключову роль.

3.2 Технічна реалізація

Було створено програму яка демонструє як блокчейн може бути використанний для цифрової ідентифікації.

Організація може створити масштабовану мережу блокчейну, у якій кожен користувач буде мати свою власну пару приватного та публічного ключів. Приватний ключ буде зберігатися тільки у користувача, а публічний ключ буде відкритим для перевірки цифрового підпису. Це забезпечує безпеку та автентичність даних користувача.

Цей приклад може слугувати базою для розробки більш широкого застосунку цифрової ідентифікації. У випадку використання організацією на більших масштабах, система цифрової ідентифікації буде розширена та оптимізована для забезпечення ефективної роботи у мережі блокчейну.

У випадку великої мережі блокчейну, інформація про користувачів може бути розподілена між різними блоками у ланцюгу. Це сприяє прозорості та відстежуваності змін у даних користувачів, а також зменшує можливість централізованого контролю чи зловживання інформацією.

Щоб забезпечити приватність даних користувачів, можна використати технології шифрування для зберігання даних у блоках. Таким чином, лише

користувачі з відповідними приватними ключами зможуть розшифровувати та отримувати доступ до своєї особистої інформації.

Для підтримки децентралізації, у мережі блокчейну можуть бути використані вузли, які відповідають за перевірку та зберігання блоків. Участь різних сторін у процесі валідації та збереження даних допомагає підвищити безпеку системи та зменшити ризик зловживання або атаки.

Оскільки мережа блокчейну використовує консенсусний алгоритм для визначення правильної версії ланцюжка блоків, це забезпечує додатковий рівень захисту від зловживань. Відтак, потенційні зловмисники зіткнуться з важким завданням переконати більшість учасників мережі в прийнятті неправильної версії ланцюжка блоків.

У масштабній системі цифрової ідентифікації різні організації та сторони можуть використовувати та надавати послуги на основі цієї ідентифікації. Наприклад, банки, урядові органи, медичні заклади та інші установи можуть перевіряти користувачів, що претендують на доступ до їхніх послуг, на основі цифрових підписів та публічних ключів. Це сприяє зменшенню шахрайства, забезпечує автентичність даних користувачів і полегшує процеси перевірки.

Використання блокчейну для цифрової ідентифікації може також полегшити міжнародну співпрацю, оскільки система ідентифікації буде заснована на загальноприйнятих стандартах та технологіях. У такому випадку, уряди, корпорації та громадяни з різних країн зможуть співпрацювати та обмінюватися інформацією ефективніше та безпечніше.

Цей код демонструє використання технології блокчейн для створення системи цифрової ідентифікації. Він складається з наступних компонентів.

1) Клас User: представляє користувача системи ідентифікації. Він містить основні дані користувача, такі як ім'я, прізвище, ідентифікаційний номер та рік народження.

2) Метод register: створює хеш особистої інформації користувача, а потім підписує цей хеш за допомогою особистого ключа користувача.

3) Метод sign_data: використовується для підпису даних за допомогою особистого ключа користувача.

4) Клас Block: представляє блок у блокчейні, що містить дані користувача, попередній хеш та хеш блоку.

5) Клас Blockchain: представляє послідовність блоків, що містять інформацію про користувачів. Він також включає методи для додавання блоків та

перевірки валідності блокчейну.

6) Функція generate_keys: генерує пару ключів для кожного користувача, особистий та загальнодоступний.

7) Функція verify_signature: перевіряє підпис користувача, використовуючи його загальнодоступний ключ.

8) Функція verify_all_signatures: перевіряє всі підписи у блокчейні, переконуючись, що вони валідні.

Після створення класів та функцій, код генерує ключі для трьох користувачів, реєструє їх в системі і додає їх до блокчейну. Потім він перевіряє валідність блокчейну та виводить інформацію про кожен блок у ньому.

Загалом, цей код слугує як приклад того, як технологія блокчейн може бути використана для створення системи цифрової ідентифікації. Використання блокчейну забезпечує надійність та безпеку даних, а також забезпечує відстежуваність та прозорість історії змін. Цифрові підписи, засновані на криптографічних парах ключів, забезпечують автентичність даних користувача та підтверджують їх ідентичність.

Далі наведено приклад роботи коду, на рисунках 3.2 та 3.3 показано генезис-блок та блок №1. Програма відображає інформацію про кожен блок та підтвердження валідності блоку.

```
Blockchain is valid:  True
Block 0:
Data: Genesis Block
Hash: b4c8f5b9531df178c740df27e9dde1666873b3ff409c3fff61309e6ea1e03382
Previous Hash: 0
Genesis Block (no signature)
```

Рисунок 3.2 – Генезис-блок

```
Block 1:
Data: 98e583c46e6b034741f150105320a7edf63bb88ac44a30c25014b02009db37d1
Hash: b8c5c61ce387a6a47f1d12b1e44d01a666e1315b389ba6566da54db83009b614
Previous Hash: b4c8f5b9531df178c740df27e9dde1666873b3ff409c3fff61309e6ea1e03382
Signature valid: True
```

Рисунок 3.3 – Блок №1

Далі наведено перелік з поясненнями того, що саме означає отримана інформація.

1) «Blockchain is valid: True» – це підтвердження, що блокчейн є валідним та не містить помилок або змін. Якщо було б «False», це означало б, що щось змінено або зламано в ланцюжку блоків.

2) «Block 0» – це перший блок, так званий генезис-блок, який є стартовим блоком в будь-якому блокчейні.

3) «Data: Genesis Block» – це дані, які містяться в генезис-блоку. В цьому випадку, дані просто позначають, що це генезис-блок.

4) «Hash:b4c8f5b9531df178c74….f61309e6ea1e03382» – це унікальний хеш генезис-блоку, який генерується на основі даних цього блоку.

5) «Previous Hash: 0» – хеш попереднього блоку. Оскільки генезис-блок є першим блоком, його попередній хеш відсутній, тому значення дорівнює 0.

6) «Genesis Block (no signature)» – це вказівка на те, що у генезис-блоку немає підпису, оскільки він є стартовим блоком.

7) «Block 1» - це другий блок в ланцюжку блоків.

8) «Data: 98e583c46e6b034741….ac44a30c25014b02009db37d1» – це дані, які містяться в блоку №1. В даному випадку, це хеш публічного ключа користувача, який може представляти цифрову ідентифікацію.

9) «Hash: b8c5c61ce387a6a47f1d1….9ba6566da54db83009b614» – це унікальний хеш блоку №1, який генерується на основі даних цього блоку та попереднього хешу.

10) «Previous Hash: b4c8f5b9531df178c7…09c3fff61309e6ea1e03382» – це хеш попереднього блоку (генезис-блоку) у ланцюжку. Це важливий компонент, який забезпечує послідовність та взаємозв'язок між блоками.

11) «Signature valid: True» – це підтвердження, що підпис даних у блоку №1 є дійсним. Це означає, що дані були підписані приватним ключем користувача, а підпис може бути перевірений за допомогою публічного ключа користувача. Якщо було б «False», це означало б, що підпис не може бути перевірений або дані були змінені.

Далі у блоках 2 та 3 все подібно до блоку 1. Вони також використовують хеш попереднього блоку для забезпечення зв'язку між ними та послідовності блоків у ланцюжку. Кожен з цих блоків містить інформацію про користувача та підпис, згенерований за допомогою приватного ключа відповідного користувача. Блоки 2 та 3 показано на рисунку 3.4.

```
Block 2:
Data: e380ab156f2d3f0a0b8d662fcc31106edad36fee18d9e0bf0fd0000f348a9c08
Hash: 08c882df9888a24fd37b3228d39285d36ccaf304ed3d9d34490c4d19f5da18af
Previous Hash: b8c5c61ce387a6a47f1d12b1e44d01a666e1315b389ba6566da54db83009b614
Signature valid: True

Block 3:
Data: ba27149ebadc23084721619d19f095b8a029bc02d471aa15d3ab44e3a8302088
Hash: 2ec955106a6cc74c3e14f12b3dd60d050ad79603001d44ee07eedc9f7c502f7e
Previous Hash: 08c882df9888a24fd37b3228d39285d36ccaf304ed3d9d34490c4d19f5da18af
Signature valid: True

All signatures in the blockchain are valid.
```

Рисунок 3.4 – Інформація про блоки 2 та 3

При виведенні інформації про блоки 2 та 3 ми можемо побачити, що.

1) «Data» містить хешовану інформацію про користувача, яка є унікальною для кожного користувача.

2) «Hash» є унікальним хешем, що відображає дані блоку та хеш попереднього блоку.

3) «Previous Hash» містить хеш попереднього блоку, що забезпечує послідовність та взаємозв'язок між блоками.

4) «Signature valid: True» підтверджує, що підпис даних у блоках 2 та 3 є дійсним. Це означає, що дані були підписані приватним ключем відповідного користувача, а підпис може бути перевірений за допомогою публічного ключа користувача.

Таким чином, блоки 2 та 3 також демонструють, як інформація про різних користувачів може бути збережена та перевірена в системі цифрової ідентифікації на основі блокчейну.

«All signatures in the blockchain are valid.», означає, що підписи всіх блоків у ланцюжку блокчейна були успішно перевірені та є дійсними.

Це важливо для довіри до системи цифрової ідентифікації, оскільки воно підтверджує, що дані користувачів не були змінені або підроблені після того, як вони були записані в блокчейн. Кожен підпис є унікальним та пов'язаним з публічним ключем відповідного користувача, що дозволяє перевірити автентичність даних у кожному блоку.

У цьому прикладі, оскільки всі підписи в блокчейні є дійсними, можна стверджувати, що система ідентифікації працює вірно та захищена від спроби підробки або зміни даних користувачів.

Таким чином, вся інформація про користувача є підтвердженою за допомогою його приватного ключа. У подальшому, у кожній програмі, яка інтегрує цю систему цифрової ідентифікації, користувач зможе за допомогою свого приватного ключа підтвердити свою ідентичність.

Це надає значні переваги в безпеці та зручності, оскільки користувачі не повинні передавати чутливу інформацію, таку як паролі або персональні дані, кожен раз, коли їм потрібно авторизуватися або підтвердити свою особистість. Замість цього, вони можуть просто використовувати свій приватний ключ для підпису даних, які можуть бути перевірені за допомогою відповідного публічного ключа. Це полегшує інтеграцію цієї системи ідентифікації в різноманітні додатки та сервіси, дозволяючи користувачам легко підтверджувати свою ідентичність без ризику витоку або крадіжки чутливої інформації.

На завершення, приклад, наведений у коді, є початковим кроком для реалізації потенціалу блокчейну в сфері цифрової ідентифікації. Розвиток та впровадження таких систем можуть внести значний вклад у підвищення безпеки, прозорості та ефективності управління особистою інформацією в різних відносинах, включаючи фінансові послуги, охорону здоров’я, освіту та урядові послуги.

Далі для прикладу було навмисно змінено дані в одному з блоків, щоб змусити код видавати False та показати, що блокчейн не є валідним. Це порушить послідовність хешів та підписів, які забезпечують правильність блокчейна. На рисунку 3.5 показано рядок коду який змінює один із блоків.

```
blockchain.chain[1].data = ("New Data", None)
print("Blockchain is valid:", blockchain.validate_blockchain())
```

Рисунок 3.5 – Зміна інформації у блоці

Цей рядок змінює дані в блоку з індексом 1 у ланцюгу блокчейна (blockchain.chain[1]) на нові дані, які ми називаємо «New Data». Зміна даних вже доданого блоку може порушити валідність блокчейна. («New Data», None) – це кортеж, який містить два значення: рядок «New Data» та «None». Замість коректних

даних, які містилися в блоку, було встановлюємо нові дані, що вказують на те, що блок було змінено або пошкоджено.

Після виконання цього рядку, валідність блокчейна буде порушена, оскільки хеші блоків і підписи користувачів більше не будуть послідовно пов'язані. Зміна даних в блокчейні може призвести до того, що функція validate_blockchain() поверне False, вказуючи на те, що блокчейн не є валідним. Результат перевірки показано на рисунку 3.6.

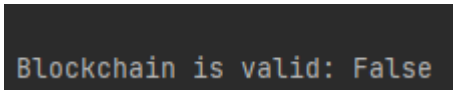


Рисунок 3.6 – Результат перевірки функції validate_blockchain()

У великому та захищеному блокчейні змінити дані вже доданих блоків майже неможливо через декілька причин.

1) Консенсус. Блокчейни, особливо в публічних мережах, функціонують на основі консенсусу між учасниками мережі. Це означає, що будь-яка зміна в існуючому блоку повинна бути погоджена більшістю учасників мережі. Зміни без консенсусу будуть відхилені мережею.

2) Криптографічна безпека. Кожен блок містить хеш попереднього блоку, що створює послідовність блоків, які взаємно залежні. Зміна даних в одному блоку призведе до зміни його хешу, що зіпсує послідовність блоків. Зловмисник повинен змінити хеші всіх наступних блоків, що є непрактичним через високу складність криптографічних хеш-функцій.

3) Розподілена мережа. Блокчейн є розподіленою мережею, що означає, що копії ланцюга блоків зберігаються на багатьох комп'ютерах учасників мережі. Щоб змінити дані в блокчейні, зловмисник повинен одночасно змінити дані на більшості цих копій, що є майже неможливим завданням.

4) Енергетичні витрати. У випадку блокчейнів з доказом роботи Proof of Work, як Bitcoin, зміна існуючих блоків вимагає від зловмисника витратити величезні кількості обчислювальної потужності та енергії. Це робить такі атаки дуже дорогими та непрактичними.

Таким чином, завдяки комбінації криптографічної безпеки, консенсусу, розподіленої структури мережі та енергетичних витрат, великі та захищені блокчейни забезпечують високий рівень безпеки. Ці фактори ускладнюють спроби змінити дані в існуючих блоках і захищають блокчейн від атак.

Ця властивість блокчейну, що надає надійність та стабільність, робить його привабливим для застосувань у цифровій ідентифікації, фінансах, логістиці та багатьох інших сферах. Відповідно, усі учасники мережі можуть довіряти незмінності даних та здійснювати безпечні транзакції або обмін інформацією.

Використання блокчейну як засобу цифрової ідентифікації має ряд переваг, які випливають з його розподіленої, безпечної та незмінної природи. Розглянутий код слугує яскравим прикладом, який демонструє можливості такого підходу. Основні переваги включають.

1) Безпека. Блокчейн забезпечує високий рівень безпеки завдяки криптографічному підпису, який пов'язує дані користувача з його приватним ключем. Це гарантує, що лише власник приватного ключа може підтвердити свою ідентичність.

2) Незмінність. Блокчейн відрізняється незмінністю даних, що забезпечує надійність та прозорість всіх записів. Це робить спроби підробки чи зміни існуючих записів майже неможливими.

3) Контроль користувача. Блокчейн дозволяє користувачам контролювати свою цифрову ідентичність та відповідні дані. Вони можуть самостійно вирішувати, з ким ділитися своєю інформацією, забезпечуючи приватність та згоду на обробку даних.

4) Децентралізація. Розподілена структура блокчейну зменшує залежність від централізованих організацій та посилює довіру до системи цифрової ідентифікації.

5) Спрощення доступу. Блокчейн може спростити процес верифікації ідентичності для різних сервісів та платформ. Користувачам потрібно лише один раз зареєструвати свою ідентичність, після чого її можна буде використовувати для доступу до різних сервісів, що підтримують блокчейн-ідентифікацію.

6) Міжнародна сумісність. Блокчейн-технологія не має географічних обмежень, що дозволяє їй функціонувати на міжнародному рівні. Це сприяє створенню глобальних стандартів цифрової ідентифікації.

З рахуванням всіх цих переваг, використання блокчейну як засобу цифрової ідентифікації має великий потенціал для забезпечення надійної, безпечної та прозорої системи ідентифікації в різних сферах суспільства. Розробка та впровадження таких систем може сприяти вирішенню проблем, пов'язаних з кібербезпекою, приватністю даних та довірою до онлайн-сервісів.

ВИСНОВКИ

В кваліфікаційній роботі розглянуто процес підвищення інформаційної безпеки та досягнення більшої ефективності сучасних систем управління шляхом впровадження блокчейн систем та розроблено програму яка демонструє як блокчейн технології можуть змінити цифрову ідентифікацію.

З цією метою, було проаналізовано потенціал технології блокчейну в підвищенні безпеки, прозорості, відповідальності та ефективності. Як блокчейн поліпшує конфіденційність, водночас усуваючи необхідність довіри, а також формує цінний інтернет-ресурс, що дозволяє користувачам здійснювати необмежену кількість транзакцій, а учасникам отримувати справедливу винагороду.

Завдяки відсутності необхідності довіри та високовартісної безпеки, блокчейн може підвищити ефективність. Таким чином, технологія блокчейн створює можливості для розподілених, але одночасно узгоджених записів даних. Це сприяє покращенню продуктивності та безпеки різних секторів і організацій.

Показано, якою важливою на сьогоднішній день є децентралізація, яка забезпечує зменшення залежності від одного контрольного органу та дозволяє розподіляти владу між учасниками мережі. Блокчейн втілює цю ідею децентралізації, створюючи структуру, що виключає можливість маніпуляції та централізованого контролю.

Ця децентралізована структура дозволяє покращити безпеку, забезпечити прозорість та створює умови для підзвітності кожного учасника мережі. Відкриваючи нові можливості, децентралізація може сприяти розвитку підприємництва, інновацій та співпраці між різними галузями.

Отже, децентралізація, як одна з ключових характеристик технології блокчейн, відіграє важливу роль у сучасному світі. Вона може стати інструментом для підсилення захисту інформації, забезпечуючи ефективність та безпеку різних секторів і сприяючи сталому розвитку суспільства.

Усі транзакції у блокчейні є незворотними, тобто після їх підтвердження і запису в блокчейн, неможливо відмінити операцію. Тому важливо бути обережним при відправці транзакцій і перевіряти всю інформацію, що вводиться перед її підтвердженням. Загалом, транзакції у блокчейні є важливою складовою технології, яка дозволяє безпечно та ефективно здійснювати різноманітні операції,

забезпечуючи високий рівень автентичності, прозорості та безпеки.

Отже, блокчейн технології мають потенціал вирішувати проблеми безпеки в цифрових транзакціях та забезпечувати високий рівень захисту даних. Завдяки своїй децентралізованій структурі та криптографічним методам захисту, блокчейн може захистити транзакції від змін та фальсифікації даних.

Оскільки використання технології блокчейн продовжує розвиватися, системи безпеки також змінюються. Наприклад, приватні блокчейни, які зараз розробляються для комерційних підприємств, в більшій мірі покладаються на безпеку за допомогою контролю доступу, ніж на механізми теорії ігор, які необхідні для безпеки більшості публічних блокчейнів.

Блокчейн може бути використаний в різних сферах, включаючи фінанси, логістику, охорону здоров'я, громадські послуги, цифрову ідентифікацію та багато інших. Ця технологія дозволяє створювати безпечні та прозорі системи обліку та обміну даними, що може підвищити ефективність та зменшити витрати в цих галузях.

Представлено аналіз можливості використання технології блокчейн для цифрової ідентифікації. Незважаючи на недоліки та обмеження, технологія блокчейн має великий потенціал для зміни способу перевірки, зберігання та обміну цифровими даними. Багато компаній та стартапів вже вивчають цю можливість, проте вони ще повинні пройти довгий шлях у вдосконаленні даної інновації. У майбутньому, блокчейн вірогідно відіграє ключову роль в розробці та підтримці систем цифрової ідентифікації.

Впровадження технології блокчейн як засобу для цифрової ідентифікації має значний потенціал для покращення безпеки та ефективності процесу ідентифікації. Однак, перед її впровадженням слід ретельно розглянути всі переваги та недоліки, та забезпечити надійний захист конфіденційності та приватності даних користувачів.

У розробленій програмі практично показано використання блокчейну як засобу цифрової ідентифікації та що ця технологія має великий потенціал для забезпечення надійної, безпечної та прозорої системи ідентифікації в різних сферах суспільства. Розробка та впровадження таких систем може сприяти вирішенню проблем, пов'язаних з кібербезпекою, приватністю даних та довірою до онлайн-сервісів.

Окремі результати роботи доповідалися на міжнародних наукових конференціях [1, 7, 22].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Поліщук В. Г. Визначення та особливості технології блокчейн у сучасному світі / В. Г. Поліщук // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 52-53.

2. What is a node in a cryptocurrency network [Електронний ресурс]. – 2019. – Режим доступа до ресурсу: https://marketbusinessnews.com/financial-glossary/node-cryptocurrency-network/.

3. Blockchain Fundamentals [Електронний ресурс]. – Режим доступа до ресурсу: https://blockgeeks.com/guides/blockchain-fundamentals/.

4. Finney H. Reusable Proofs of Work [Електронний ресурс]. – Режим доступа до ресурсу: https://nakamotoinstitute.org/finney/rpow/index.html.

5. Proof of Stake (PoS) Cryptocurrency [Електронний ресурс]. – Режим доступа до ресурсу: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

6. Bitcoin Energy Consumption Index [Електронний ресурс]. – Режим доступа до ресурсу: https://digiconomist.net/bitcoin-energy-consumption.

7. Поліщук В. Г. Блокчейн як засіб забезпечення безпеки в цифровому світі / В. Г. Поліщук // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 54-55.

8. Standard Transactions [Електронний ресурс]. – Режим доступа до ресурсу: https://bitcoin.org/en/developer-guide#standard-transactions.

9. Proof of Work vs. Proof of Stake: Basic Mining Guide [Електронний ресурс]. – Режим доступа до ресурсу: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

10. What Is a Hash? Hash Functions and Cryptocurrency Mining [Електронний ресурс]. – 2023. – Режим доступа до ресурсу: https://www.investopedia.com/terms/h/hash.asp

11. Поповський В. В. Основи криптографічного захисту інформації в телекомунікаційних системах. Навчальний посібник. Частина 1 / В. В. Поповський, А. В. Персіков. – Харків: СМИТ, 2010. – 352 с.

12. Specification for the Advanced Encryption Standard [Електронний ресурс]. – 2001. – Режим доступа до ресурсу: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.

13. How Secure is Blockchain Technology? [Електронний ресурс]. – Режим доступа до ресурсу: https://builtin.com/blockchain/blockchain-security.

14. Back A. Hashcash [Електронний ресурс]. – 2002. – Режим доступа до ресурсу: http://www.hashcash.org/papers/hashcash.pdf.

15. Blockchain Cryptography Explained [Електронний ресурс]. – Режим доступа до ресурсу: https://101blockchains.com/blockchain-cryptography/.

16. What is Sidechains [Електронний ресурс]. – Режим доступа до ресурсу: https://hackernoon.com/what-are-sidechains-1c45ea2daf3.

17. Private, Public, and Consortium Blockchains - What's the Difference? [Електронний ресурс]. – Режим доступа до ресурсу: https://academy.binance.com/en/articles/private-public-and-consortium-blockchains-whats-the-difference

18. Public Vs Private Blockchain [Електронний ресурс]. – 2021. – Режим доступа до ресурсу: https://101blockchains.com/public-vs-private-blockchain/.

19. Blockchain in Government and the Public Sector [Електронний ресурс]. – 2020. – Режим доступа до ресурсу: https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

20. Decentralized Applications (dApps) [Електронний ресурс]. – Режим доступа до ресурсу: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp.

21. A Beginner's Guide to Decentralized Finance (DeFi) [Електронний ресурс]. – Режим доступа до ресурсу: https://academy.binance.com/en/articles/private-public-and-consortium-blockchains-whats-the-difference

22. Поліщук В. Г. Блокчейн, як засіб для цифрової ідентифікації у сучасному світі / В. Г. Поліщук // Харків, ХНУРЕ, Матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті». Том 4. – 2023. – С. 56-57.

23. Blockchain Use Cases: Digital Identity [Електронний ресурс]. – 2019. – Режим доступа до ресурсу: https://academy.binance.com/en/articles/blockchain-use-cases-digital-identity