Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Дослідження методів аутентифікації в децентралізованих системах з використанням технології блокчейн»

оцінка « »

Голова ЕК

Лемешко О. В._____

Керівник Сватовський І.І.
(прізвище та ініціали/підпис)

Рецензент Бакуменко Н.С.
(прізвище та ініціали/підпис)

Виконавець студент групи КБ-41
Калинчук С. О.
(прізвище та ініціали/підпис)

Харків 2023

РЕФЕРАТ

Пояснювальна записка містить 41 сторінок, 3 рисунків, 1 таблиць, 7 джерел.

Мета дипломної роботи - дослідження способів аунтентифікації в мережах з використанням технологій блокчейн.

Об’єкт дослідження дипломної роботи є способи аунтентифікації в децентралізованих системах з використанням технологій блокчейн.

Результати проведеної роботи є дослідження галузей в яких використовуються блокчейн технології, розглядання децентралізованих систем аунтентифікації, вимоги до децентралізованих систем аунтентифікації, їх переваги та недоліки, розглядання способів децентралізованої аунтентифікації та порівняння їх між собою.

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний (довідковий) матеріал для розширення рівня професійної.

Ключові слова: BLOCKCHAIN ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА АУНТЕНТИФІКАЦІЯ ПРОТОКОЛ ЦЕНТРАЛІЗОВАНА СИСТЕМА.

.

ABSTRACT

The explanatory note contains 41 pages, 3 figures, 1 tables, 7 sources.

The purpose of the thesis is to study the methods of authentication in networks using blockchain technologies.

The object of research of the thesis is the methods of authentication in decentralized systems using blockchain technologies.

The results of the work are a study of industries that use blockchain technologies, consideration of decentralized authentication systems, requirements for decentralized authentication systems, their advantages and disadvantages, consideration of decentralized authentication methods and their comparison with each other.

The results of the work can be used for educational purposes and as auxiliary (reference) material to expand the level of professional.

Keywords: BLOCKCHAIN DECENTRALIZED SYSTEM AUTHENTICATION PROTOCOL CENTRALIZED SYSTEM.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IoT	–	Internet of Things
DDOS	–	Distributed Denial of Service
DNS	–	Domen Name System
PKI	–	Public Key Infrastructure
DPKI	–	Decentralized Public Key Infrastructure
GDPR	–	General Data Protection Reglament
DID	–	Decentralized Identifier
W3C	–	World Wide Web Consorcium
URI	–	Uniform Resource Identifier
URN	–	Uniform Resource Name

ВСТУП

Технологія розвивається і розширюється в надзвичайно прискореному темпі. Цей процес сприяв появі нових послуг, які знайшли свій шлях у численних аспектах нашого повсякденного життя. Розвиток Інтернету зробив світ дуже взаємопов'язаним, що надало постачальникам послуг можливість досягти величезної клієнтської бази, яка складається з людей з усього. Різні сфери послуг, такі як охорона здоров'я, банківська справа, розваги та багато інших, тепер доступні без необхідності від користувачів залишати свої будинки.

Щоб скористатися послугами, користувачі повинні зареєструватися як клієнти відповідних провайдерів. Під час цього процесу користувач повинен надати деякий тип інформації, яка, в свою чергу, використовується постачальником послуг, щоб забезпечити кращий індивідуально налаштований досвід. У минулому деякі типи інформації навіть не зберігалися ніде, або це було написано на папері, розміщеному в папці в запиленому кабінеті. Проте з технологічним розвитком ці типи даних зберігаються в багатих базах даних з різними полями, що містять широкий спектр особистої інформації. Велика проблема виникає в результаті поєднання вищезгаданих процесів. Чим більше послуг буде доступно, тим більше можливостей користувач може отримати, але вони повинні пройти один і той самий процес реєстрації для кожної послуги окремо, що, в свою чергу, призводить до втрати прозорості наданих ними даних. Іншими словами, споживачі торгують своїми даними, щоб отримати доступ до різних пільг і послуг.

Надання даних по всьому Інтернету означає, що споживачі не можуть відстежувати, які дані вони надають різним службам і для чого вони використовуються. Останнім часом багато питань охоплюють питання кібербезпеки та конфіденційності, що підвищує обізнаність загального населення онлайн-користувачів і призводить до виникнення проблем довіри

між клієнтами та постачальниками послуг. Розрив довіри між споживачами та постачальниками має бути подоланий, а обробка особистої інформації зробила більш керованою.

Перш ніж поглибитися в електронну ідентифікацію, важливо спочатку визначити, що саме означає поняття ідентичності. Французький філософ Пол Рікер визначає ідентичність як поняття, яке пов'язане з двома різними аспектами. Першим з них є Ідем, що є латинським словом для однаковості. Цей аспект ідентичності стосується характеристик, які ніколи не змінюються. Іншими словами, ідентичність – це сукупність ознак, які зберігаються в часі, зберігають сутність. Другий аспект, визначений філософом – це Іпсе, що перекладається з латинського на самостійність. Цей аспект ідентичності пов'язаний з атрибутами та характеристиками, які стійко змінюються протягом усього часу. Тобто, вона складається з особливостей, які роблять когось унікальним серед інших.

Філософські аспекти ідентичності досить складні, а іноді й важкі для розуміння. Існують також інші визначення, пов'язані з терміном ідентичності. Чедвік визначає цифрову ідентичність як набір характеристик або атрибутів, які можуть однозначно ідентифікувати і розрізняти одну сутність від іншої в даному контексті. З цього ми можемо зробити висновок, що ідентичність дозволяє нам краще знати інші об'єкти, з якими ми взаємодіємо. Отримавши це знання, ми можемо легко відокремити добро від поганого, що, в свою чергу, дозволяє нам створити фундамент, на якому ми можемо будувати довіру.

Термін довіра визначається як тверде переконання в істині або здатності кого-небудь або чогось виконати завдання в надійній справі, в конкретному контексті. Довіра є важливим аспектом, і саме «клей» утримує наше суспільство разом.

1 ЕЛЕКТРОННА АУНТЕНТИФІКАЦІЯ

1.1 Електронна аутентифікація в інтернеті

Електронна аутентифікація - це процес перевірки та підтвердження ідентичності користувача з використанням електронних засобів і технологій. Цей метод аутентифікації використовується для забезпечення безпеки та контролю доступу до різних цифрових сервісів, таких як онлайн-банкінг, електронна комерція, електронна пошта та багато інших.

Електронна аутентифікація базується на взаємодії між користувачем та аутентифікаційною системою. Для успішної аутентифікації користувач повинен надати валідні облікові дані, які будуть перевірені аутентифікаційним сервісом. Ці облікові дані можуть включати ім'я користувача, пароль, біометричні дані (такі як відбиток пальця, розпізнавання обличчя), одноразові коди, електронні сертифікати та інші ідентифікатори.[1]

У процесі електронної аутентифікації використовуються різні методи та технології для забезпечення безпеки та надійності. Один з найпоширеніших методів - це парольна аутентифікація. Користувач вводить свій ідентифікаційний пароль, який порівнюється зі збереженим значенням в базі даних. Якщо паролі співпадають, користувачу надається доступ до системи.

Однак паролі мають свої обмеження. Вони можуть бути вкрадені, вгадані або зламані, особливо якщо користувач використовує слабкий пароль.[1] Тому для посилення безпеки використовуються додаткові методи аутентифікації, такі як двофакторна аутентифікація (2FA) або багатофакторна аутентифікація (MFA).

Двофакторна аутентифікація вимагає від користувача надати два різні види облікових даних для підтвердження ідентичності. Наприклад, користувач може ввести свій пароль, а потім отримати одноразовий код на свій мобільний телефон, який потрібно ввести для завершення процесу аутентифікації. Цей підхід забезпечує вищий рівень безпеки, оскільки навіть якщо пароль буде

скомпрометований, зловмисник все ще не зможе отримати доступ без другого фактора.

Багатофакторна аутентифікація розширює підхід 2FA, додавши ще більше факторів перевірки ідентичності. Наприклад, це можуть бути біометричні дані (відбиток пальця, розпізнавання обличчя), фізичні токени або смарт-карти. Комбінація різних факторів забезпечує високий рівень безпеки та захисту від несанкціонованого доступу.

Окрім традиційних методів аутентифікації, електронна аутентифікація також використовує сучасні технології, такі як біометрія. Біометричні дані, такі як відбиток пальця, розпізнавання обличчя або розпізнавання голосу, унікальні для кожної особи і можуть бути використані для точної ідентифікації користувача. Збережені біометричні дані можуть порівнюватися зі скануванням, яке користувач надає під час процесу аутентифікації.

Поміж інших технологій, які використовуються для електронної аутентифікації, варто відзначити такі:

- Електронні сертифікати: Цифрові сертифікати, випущені довіреними організаціями, використовуються для підтвердження автентичності та ідентифікації користувача.
- Технологія блокчейн: Блокчейн може забезпечити безпеку та надійність процесу аутентифікації шляхом розподіленого зберігання даних та перевірки транзакцій.
- Фізичні токени: Фізичні пристрої, такі як USB-ключі або смарт-карти, можуть використовуватися для збереження облікових даних та забезпечення безпеки під час аутентифікації.
- Системи розпізнавання голосу: Інноваційні технології розпізнавання голосу можуть використовуватися для аутентифікації користувачів шляхом перевірки їх унікального голосу.

Електронна аутентифікація має велике значення у сучасному цифровому світі, де безпека та конфіденційність даних стають все більш важливими. Вона дозволяє забезпечити авторизований доступ до різних сервісів та захистити

користувачів від шахрайства та несанкціонованого доступу. З розвитком нових технологій та інновацій у цій галузі, електронна аутентифікація продовжуватиме змінюватися та вдосконалюватися, забезпечуючи надійний та безпечний цифровий досвід для користувачів. [1]

1.2 Проблеми електронної аутентифікації та ідентифікації та способи їх вирішення

Проблеми електронної аутентифікації та ідентифікації є важливими аспектами в цифровому світі. Ці проблеми включають забезпечення безпеки, захист конфіденційності, управління ідентичністю та зручність використання. У цілях безпеки та ефективності більше сітем використовують багатофакторну аутентифікацію, біометрію та блокчейн-технологію.

Одна з основних проблем електронної аутентифікації - це позитивна ідентифікація особи. Користувачі повинні бути впевнені в тому, що їх ідентичність валідна та несанкціоновані особи не можуть отримати доступ до їх облікових записів. У таких випадках, багатофакторна аутентифікація використовує два або більше факторів для підтвердження ідентичності, наприклад, пароль разом з одноразовим кодом, який надсилається на мобільний пристрій. Це підвищує рівень безпеки, оскільки необхідно зламати не лише один, але кілька факторів для отримання доступу.

Друга проблема - це збереження конфіденційності облікових даних. Користувачі повинні бути впевнені, що їх особисті дані залишаються приватними та недоступними для третіх осіб. Використання шифрування та захисту даних є важливими компонентами у забезпеченні конфіденційності. Також, управління доступом може бути застосовано для обмеження прав доступу до облікових даних, дозволяючи лише авторизованим особам отримувати доступ. [2]

Третя проблема - це управління ідентичністю в мережі. З великою кількістю сервісів та платформ, на які ми реєструємося, у нас часто виникає проблема запам'ятовування багатьох паролів та користувальницьких імен.

Рішенням може бути використання систем управління ідентичністю, які дозволяють користувачам мати єдиний ідентифікатор та пароль для доступу до різних сервісів. Такі системи можуть використовувати цифрові сертифікати для підтвердження ідентичності та забезпечення безпеки.

Четверта проблема - це зручність використання. Користувачі вимагають зручних та легких у використанні методів аутентифікації. У цьому контексті біометричні технології, такі як сканер відбитків пальців, розпізнавання обличчя або сканер сетчатки ока, стають все більш популярними. Вони дозволяють швидко та зручно підтверджувати ідентичність без необхідності запам'ятовування паролів. [2]

Способи вирішення цих проблем включають використання багатофакторної аутентифікації, вдосконалення шифрування та захисту даних, розвиток систем управління ідентичністю, використання біометричних технологій та впровадження блокчейн-технології. Крім того, важливо проводити постійну оцінку та аудит безпекових заходів для забезпечення відповідності змінюючимся загрозам та вимогам безпеки.

Загалом, електронна аутентифікація ідентифікація є складним завданням, яке вимагає комплексного підходу та постійного вдосконалення. Розвиток нових технологій та інновацій у цій галузі допоможе забезпечити більшу безпеку, конфіденційність та зручність для користувачів у цифровому середовищі. [1]

2 ОГЛЯД ТЕХНОЛОГІЇ BLOCKCHAIN

2.1 Загальна характеристика blockchain технології

Blockchain (ланцюжок блоків) є революційною технологією, що забезпечує безпеку, надійність та прозорість в області обміну даними і здійснення транзакцій. Його основним принципом є створення послідовного ланцюжка блоків, що містять криптографічно захищені записи транзакцій. Кожен блок містить хеш-функцію попереднього блоку, що забезпечує неперевершеність послідовності блоків.

Однією з ключових характеристик blockchain є його децентралізованість. Він працює на основі мережі вузлів, де кожен вузол має копію всієї ланки блоків. [3] Це означає, що немає центрального органу чи посередника, що контролює систему. Замість цього, учасники мережі спільно підтверджують та підтримують консенсус щодо валідності та правильності транзакцій, що забезпечує надійність та відсутність можливості зміни чи фальсифікації даних.

Іншою важливою характеристикою blockchain є безпека. Кожна транзакція, що вноситься до блоку, підписується цифровим підписом, що забезпечує її автентичність та непереборність. Крім того, цифрові записи блокчейну зберігаються на всіх вузлах мережі, що робить їх важкими до вторгнення або знищення. [3] Також, блокчейн використовує криптографію для шифрування даних, що забезпечує конфіденційність та приватність інформації.

Ще одна важлива характеристика блокчейну - прозорість. Кожен вузол мережі може переглядати записи транзакцій, що зроблені у блоках. Це дозволяє створювати довіру між учасниками мережі, оскільки всі можуть бачити та перевіряти операції. Прозорість також дозволяє виявляти шахрайства, помилки та недоліки в системі.

Blockchain має широкий спектр застосувань у різних галузях. Він може бути використаний для безпечного обміну криптовалют, таких як Bitcoin та Ethereum. Також, блокчейн може бути застосований у фінансовому секторі для

здійснення міжбанківських транзакцій, в системах управління ланцюгами постачання, у сфері охорони здоров'я для зберігання медичних записів та обміну даними, у сфері нерухомості для ведення реєстру власності та багато інших.

Щоб вирішити проблеми масштабованості та швидкодії, деякі блокчейн-платформи, наприклад, Ethereum, використовують механізми розумних контрактів. Розумні контракти є програмними кодами, які автоматизують виконання угод між сторонами без посередництва. Вони дозволяють створювати та виконувати умови транзакцій автоматично, що спрощує та прискорює процеси. [4]

Надалі, розвиток технології блокчейн може включати в себе вдосконалення протоколів консенсусу, покращення шкалування мережі, впровадження приватності даних та розширення областей застосування. Застосування блокчейну в різних секторах діяльності продовжуватиме зростати, що створюватиме нові можливості для ефективного та безпечного обміну даними та транзакціями.

Загалом, блокчейн технологія є інноваційним рішенням, що забезпечує децентралізацію, безпеку, прозорість та ефективність в області обміну даними. Вона відкриває нові перспективи для покращення економічних, соціальних та технологічних процесів у різних галузях та сприяє створенню інноваційних рішень, що прискорюють розвиток суспільства. [3]

2.2 Структура технології blockchain

Технологія блокчейн є складною системою, що базується на децентралізованій структурі та забезпечує безпечний обмін даними та транзакцій між учасниками мережі. Структура блокчейну включає різні компоненти та процеси, що співпрацюють для забезпечення функціональності та надійності системи. Нижче наведено загальну характеристику структури технології блокчейн.

1) Блоки:

Блок є основною одиницею даних у блокчейні. Він містить інформацію про транзакції, такі як дані, час виконання, хеш попереднього блоку та інші метадані. Блоки зв'язані послідовним чином, утворюючи ланцюжок блоків. Кожен блок містить унікальний ідентифікатор (хеш), який створюється на основі даних блоку.

2) Хеш-функції:

Хеш-функції використовуються для перетворення даних блоку в унікальний хеш-код. Хеш-код є строковим значенням фіксованої довжини, що ідентифікує блок. Будь-яка зміна в даних блоку автоматично змінює хеш-код. Це дозволяє виявляти будь-які спроби зміни даних в блоках та забезпечує надійність технології блокчейн.

3) Розподілена мережа:

Блокчейн є розподіленою мережею, що складається з вузлів (комп'ютерів), що співпрацюють між собою. Кожен вузол мережі має повну копію блокчейну. Це дозволяє всім учасникам мережі бачити та перевіряти транзакції. Вузли співпрацюють за допомогою протоколу консенсусу, щоб досягти згоди про поточний стан блокчейну.

4) Протокол консенсусу:

Протокол консенсусу визначає правила, за якими вузли мережі досягають згоди про правильний стан блокчейну. Найпоширенішим протоколом консенсусу є Proof of Work (PoW), в якому вузли виконують складні обчислювальні завдання для підтвердження транзакцій та створення нових блоків. Існують також інші протоколи консенсусу, такі як Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та інші.

5) Публічний ключ і приватний ключ:

Учасники мережі блокчейн мають криптографічні ключі - публічний та приватний ключі. Публічний ключ використовується для ідентифікації користувача та отримання транзакцій, а приватний ключ забезпечує підписання та автентифікацію транзакцій. Це забезпечує безпеку та конфіденційність в мережі блокчейн.

6) Смарт-контракти:

Смарт-контракти - це програми, що забезпечують автоматичне виконання угод на блокчейні. Вони зберігаються в мережі і виконуються після виконання певних умов. Смарт-контракти дозволяють автоматизувати та спростити процеси, такі як переказ активів, виконання угод та інші.

7) Конфіденційність та безпека:

Блокчейн забезпечує високий рівень безпеки та конфіденційності. За допомогою криптографічних методів, дані блокчейну захищені від несанкціонованого доступу та маніпуляцій. Кожна транзакція підписується приватним ключем, що забезпечує її автентифікацію та неперевершеність.

8) Нестримність:

Одним з ключових аспектів блокчейн є його нестерпність. Коли транзакція включена в блок та підтверджена консенсусом мережі, вона стає нестерпною і не може бути видалена або змінена без згоди більшості учасників мережі. Це забезпечує надійність та неперервність транзакцій.

Структура технології блокчейн є основою її функціонування та надійності. Вона поєднує блоки, хеш-функції, розподілену мережу, протоколи консенсусу, криптографічні ключі, смарт-контракти та інші компоненти, щоб забезпечити безпеку, неперервність та децентралізацію в обміні даними та виконанні транзакцій. [3]

Коли вузол знаходить варіант, який задовольняє умову, він розсилає отриманий блок іншим підключеним вузлам для перевірки. Якщо блок не містить помилок, він вважається доданим до ланцюжка, і наступний блок повинен містити його геш. На рисунку 2.1 зображена структура блока.

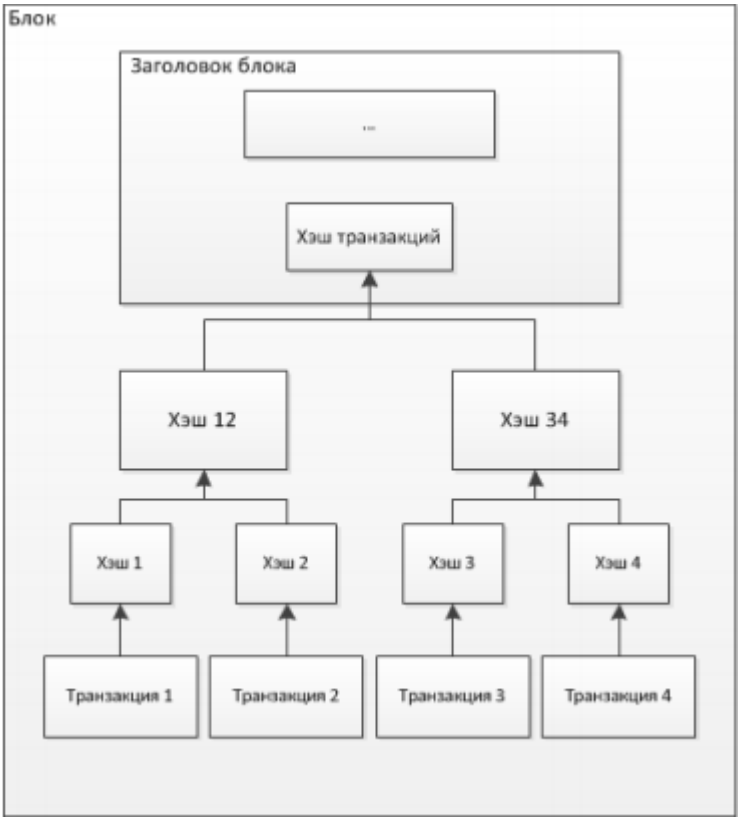

Рисунок 2.1 – Структура геш-дерева

Блоки утворюються одночасно багатьма "Майнерами" і відправляються в мережу для включення до розподіленої бази блоків. Часто виникають ситуації, коли декілька нових блоків у різних частинах мережі вважають один і той же попереднім блоком, що призводить до гілкування ланцюжка блоків. Інформацію про нові блоки можна обмежити свідомо або випадково (наприклад, в рамках локальної мережі). В такому випадку можуть розвиватися паралельні гілки. [4]

Кожен новий блок може містити як однакові, так і різні транзакції порівняно з іншими блоками. Транзакції, що були включені тільки до відхиленої гілки (включаючи виплату винагороди), втрачають свій статус

підтверджених. Якщо це транзакція з переказом біткоїнів, вона буде поставлена в чергу і пізніше включена до наступного блоку. Транзакції виплати винагороди за створення блоків не повторюються в інших гілках, що означає, що "зайві" біткоїни, виплачені за формування блоків, не отримують додаткових підтверджень і не використовуються. Таким чином, ланцюжок блоків містить історію володіння, яку можна перевірити, наприклад, на спеціалізованих веб-сайтах.

Blockchain утворює розподілену базу даних, яка постійно зростає і складається з ланцюжка блоків, що містять інформацію про всі транзакції. Копії бази даних або її частини зберігаються на багатьох комп'ютерах і синхронізуються згідно з встановленими правилами побудови блокчейну. Інформація в блоках не шифрується і доступна у відкритому вигляді, але захищена від змін завдяки криптографічним хешам. [4]

База даних блокчейну зберігає інформацію про всі транзакції у незашифрованому вигляді, але ці дані підписуються за допомогою асиметричного шифрування. Для запобігання подвійного витрачання тієї ж суми використовуються мітки часу, які реалізовані шляхом формування ланцюжка спеціальних блоків. Кожен блок містить геш попереднього блоку і свій порядковий номер. Кожен новий блок підтверджує транзакції, містить підтвердження всіх попередніх блоків і додає додаткове підтвердження для транзакцій у всьому ланцюжку. Редагування інформації вже існуючого блоку є практично неможливим, оскільки вимагало б бути зміненими всі наступні блоки. Це робить успішну атаку подвійного витрачання (double-spending) практично неможливою. [3]

2.3 Використання blockchain технології

Blockchain - це технологія, яка може бути застосована в різних сферах життя. Один з найвідоміших прикладів застосування блокчейн - це Bitcoin. Bitcoin є електронною валютою, концепт якої був представлений в 2009 році Сатоші Накамото, і він базується на принципах блокчейн-технології, описаних у самоопублікованому документі Сатоші Накамото.

Bitcoin використовує криптографічні принципи для створення унікальних, непідробних та ділених маркерів валюти. Користувачі зберігають свої криптографічні ключі, що відповідають їхнім грошам, локально на своєму комп'ютері і здійснюють транзакції безпосередньо один з одним через децентралізовану мережу піринговых вузлів. Валідність грошових переказів перевіряється шляхом консенсусу учасників мережі. Кожна фізична монета в системі має свій унікальний криптографічний ключ.

Блокчейн - це технологія, яка може мати широкі застосування в різних сферах життя. Один з найвідоміших прикладів використання блокчейн - це Bitcoin. Bitcoin є електронною валютою, яку було запропоновано Сатоші Накамото в 2008 році і представлено в 2009 році. Основою Bitcoin є концепція блокчейн-технології, яка описана в самостійно опублікованому документі Сатоші Накамото. [3]

Bitcoin використовує криптографічні принципи для створення унікальних, непідробних та ділених маркерів валюти. Кожен користувач зберігає свої криптографічні ключі, які відповідають їхнім грошам, на своєму локальному комп'ютері. Транзакції відбуваються безпосередньо між користувачами через децентралізовану мережу піринговых вузлів. Валідність грошових переказів перевіряється шляхом досягнення консенсусу серед учасників мережі. Кожна фізична монета в системі має свій унікальний криптографічний ключ.

Під час здійснення транзакції користувач додає відкритий ключ отримувача до монети та підписує її своїм особистим приватним ключем. Це запобігає можливості подвійного витрачання однієї монети. Всі транзакції поширюються серед інших учасників мережі, а повний список транзакцій зберігається у розподіленій базі даних блокчейну. Під час кожної нової транзакції ключі перевіряються за списком попередніх транзакцій. Іншими словами, Bitcoin ґрунтується на реєстрації переміщення грошових коштів за допомогою асиметричного шифрування. [4]

Blockchain технологія має широкий спектр застосувань у реальному житті, які відкривають нові можливості для покращення ефективності, безпеки та довіри в різних галузях. Нижче описані деякі з них:

– Фінансові послуги:

  Blockchain може використовуватися для забезпечення безпечних та швидких транзакцій у фінансовій сфері. Наприклад, міжнародні грошові перекази можуть бути значно прискорені та здешевлені, оскільки блокчейн дозволяє пряму передачу коштів без посередництва банків. Крім того, використання смарт-контрактів дозволяє автоматичне виконання угод та відрахування платежів, що спрощує процеси фінансового обліку та мінімізує ризики.

– Логістика та поставки:

  Blockchain може полегшити відстеження та перевірку походження товарів у ланцюжку поставок. За допомогою блокчейну можна створити недоступну для змін децентралізовану базу даних, в якій фіксуються всі етапи переміщення товарів від постачальника до кінцевого споживача. Це дозволяє підтвердити автентичність товару, перевірити його якість та виявити можливі порушення.

– Голосування та демократія:

  Blockchain може забезпечити прозорість та безпеку у процесі голосування. Запис голосів на блокчейні дозволяє уникнути підробки або втрати голосів, а також забезпечує можливість перевірки результатів голосування всіма зацікавленими сторонами. Це може підвищити довіру до виборчих процесів та зробити їх більш прозорими.

– Інтелектуальна власність:

  Blockchain може використовуватися для захисту прав інтелектуальної власності, наприклад, авторських прав, патентів та товарних знаків. Запис даних про створення або винайдення на блокчейні забезпечує недвозначність та непорушність інформації, а також може слугувати доказом в разі судових суперечок.

– Спостереження за походженням продуктів:

  Blockchain може допомогти споживачам перевірити походження та якість продуктів. Запис інформації про виробника, дату виготовлення, склад та інші характеристики на блокчейні дозволяє стежити за всіма етапами виробництва та постачання продукту, що забезпечує додаткову довіру споживача до якості товару.

– Енергетика:

  Blockchain може сприяти впровадженню розумних енергетичних систем та підтримувати енергетичний обмін між різними учасниками мережі. Запис та автоматичне виконання угод про купівлю-продаж енергії на блокчейні дозволяє оптимізувати розподіл та використання енергії, що сприяє більш стабільній та стійкій енергетичній системі.

– Медицина:

  Blockchain може бути використаний для безпечного збереження та обміну медичних даних пацієнтів. За допомогою блокчейну можна забезпечити конфіденційність та цілісність медичних записів, а також дати пацієнтам контроль над своїми даними та можливість поділитися ними з медичними спеціалістами за потреби.

– Смарт-контракти:

  Blockchain дозволяє використовувати смарт-контракти - програми, які автоматично виконують умови, записані в них. Це може бути застосовано в різних галузях, включаючи страхування, нерухомість, ліцензування та багато інших. Смарт-контракти дозволяють ефективно та безпечно укладати угоди між сторонами, уникати конфліктів та забезпечувати автоматичні платежі.

Це лише кілька прикладів використання blockchain технології у реальному житті. За допомогою блокчейну можна досягти більшої безпеки, прозорості, ефективності та довіри в різних сферах діяльності. З ростом інтересу до цієї технології ймовірно, з'являться нові, неймовірні застосування,

які змінять наше сприйняття багатьох процесів і покращать якість нашого життя. [4]

2.4 Можливості та переваги децентралізованих систем щодо забезпечення механізмів захисту

Децентралізація відноситься до процесу розподілу влади, фінансів або зусиль без втручання централізованого керівного органу. В багатьох компаніях вже давно використовуються децентралізовані системи управління. Однак управління фінансами дійсно стало можливим тільки з появою технології блокчейн.

Децентралізація в блокчейні означає, що в системі відсутній централізований сервер, а всі майнери та учасники мережі є рівноправними. Розробники не контролюють операції в блокчейні, а підтвердження транзакцій здійснюється самими користувачами мережі. Технологія передбачає розподіл обчислювальних потужностей і даних по всьому світу, а інформація повторюється кілька разів для запобігання втраті, а також система має високу стійкість до DDOS-атак.

Децентралізована система забезпечує високий рівень безпеки транзакцій і зберігання коштів. Оскільки інформація про всю історію транзакцій зберігається у кожного з користувачів, то таку систему неможливо обдурити або знищити. Кожна транзакція підтверджується кількома незалежними вузлами (нодами), що унеможливлює підміну даних або підкуп перевіряючих.

У порівнянні з локальними системами, що використовуються у банківських установах, обмін коштів через децентралізовану систему займає набагато менше часу, дозволяючи здійснювати велику кількість транзакцій у декілька секунд. Це можливо завдяки тому, що в blockchain обчислювальні потужності розподілені по всій земній кулі, а велика кількість учасників мережі забезпечує високу швидкість обробки.

Важливою перевагою децентралізованих систем електронних валют є відсутність зовнішнього регулювання. Наприклад, у випадку незаконних дій сервера, правоохоронні органи можуть конфіскувати обладнання та розробки

власника. Але у випадку децентралізованих криптовалют, неможливо вилучити технологію або обчислювальні потужності, оскільки вони належать великій кількості людей, а сама технологія доступна громадськості. Якщо хоч один учасник мережі зберігає копію технології, вона може бути відновлена. Незалежність криптовалют від влади та регулюючих органів також запобігає політичним маніпуляціям їх вартістю. Тому курс криптовалюти відображає чесний попит і пропозицію на неї. [4]

Функціонування централізованих систем безпосередньо залежить від органу, який забезпечує їх роботу і контролює їх. Так одна людина або незначна група людей можуть приймати рішення, які неминуче вплинуть на всіх учасників без попереднього узгодження з ними. При децентралізації мережі такий процес неможливий, так як кожен вузол зв'язку є рівноправним учасником мережі.

Незважаючи на переваги централізованого управління, яке забезпечує ефективне розподілення ресурсів та прийняття відповідальних рішень, такі системи також стикаються з ризиком шахрайства. У порівнянні з цим, децентралізація дозволяє мінімізувати такі ризики, оскільки виключає можливість впливу на керівництво через підкуп.

Прикладом різниці між централізованим та децентралізованим управлінням є криптовалютні біржі. Децентралізовані біржі, засновані на технології блокчейн, дають користувачам повний контроль над їх коштами, тоді як централізовані біржі дозволяють тільки обмінювати, купувати та продавати криптознаки на їх серверах, при цьому приватні ключі гаманців часто зберігаються на сервері біржі у зашифрованому вигляді. [4]

У випадку централізованого розподілу фіатних грошей, у користувача є лише паперові гроші, а основні активи зберігаються у державних установах. У децентралізованих електронних валютах власник повністю контролює свої активи, а доступ до них та здійснення транзакцій здійснюється за допомогою секретного ключа. У разі централізованих фіатних валют, наприклад, гроші на

банківському рахунку, управління коштами також знаходиться в руках фінансової установи, яка має право блокувати та знімати кошти. [4]

Таким чином, децентралізовані системи дозволяють уникнути проблем, пов'язаних з централізованим управлінням, таким як шахрайство та контроль над активами користувачів. Вони надають більшу автономію та контроль користувачам, а також зменшують можливість зовнішнього втручання в операції з коштами. [3]

Децентралізовані системи мають значний потенціал у забезпеченні механізмів захисту в різних сферах діяльності. Вони змінюють традиційний підхід до безпеки, переносячи фокус з централізованих організацій на розподілені мережі та алгоритми консенсусу. Опишемо основні можливості та переваги децентралізованих систем у забезпеченні механізмів захисту.

– Надійність та стійкість до збоїв:

  Децентралізовані системи є більш стійкими до внутрішніх збоїв та атак. Замість одного центрального вузла, інформація розподіляється по всій мережі, що ускладнює заволодіння контролем над системою атакуючих. Навіть якщо деякі вузли виявляться несправними або поступають зловмисними спробами, решта мережі все ще продовжує працювати, забезпечуючи безперебійну роботу системи.

– Конфіденційність та приватність:

  Децентралізовані системи забезпечують більшу конфіденційність та приватність, оскільки кожен користувач має повний контроль над своїми особистими даними. Відомості не зберігаються в централізованих сховищах, що підвищує рівень захисту від несанкціонованого доступу та зловживання даними третіми особами. Деякі блокчейн-платформи навіть використовують шифрування для додаткового захисту приватності користувачів.

– Недоступність до змін: Одна з ключових переваг блокчейн-технології полягає в недоступності до змін інформації, яка була занесена до блоку. Кожен блок містить хеш попереднього блоку, що робить зміну даних у

блоках практично неможливою без зміни хешу всієї попередньої ланки блоків. Це забезпечує надійну систему збереження даних та унеможливлює їхню підробку або видалення.

– Перевірка автентичності:

  Блокчейн технологія дозволяє перевірити автентичність даних, що в ній зберігаються. Кожна транзакція або запис в блокчейні має унікальний цифровий підпис, який може бути перевірений всіма вузлами мережі. Це гарантує, що дані не змінені та є достовірними, а також дозволяє встановити історію транзакцій.

– Прозорість:

  Децентралізовані системи можуть бути прозорими, оскільки кожен учасник мережі має доступ до всіх записів, що зберігаються в блокчейні. Це дозволяє забезпечити більшу відкритість та впевненість в трансакціях, оскільки будь-яка недоречна або шкідлива діяльність буде виявлена та вирішена шляхом консенсусу всієї мережі.

– Швидкість та ефективність:

  Хоча децентралізовані системи можуть бути менш ефективними з точки зору швидкості операцій порівняно з централізованими системами, розробники активно працюють над вдосконаленням технології. Впровадження шарів або масштабованих рішень дозволяє забезпечити більшу швидкість та продуктивність мережі, що робить її придатною для реалізації різноманітних завдань.

– Відсутність посередників:

  Децентралізовані системи дозволяють уникнути використання посередників або посередницьких послуг, що допомагає знизити витрати та ризики шахрайства. Користувачі можуть взаємодіяти один з одним безпосередньо через блокчейн, що сприяє ефективнішому та безпечному обміну цінностями.

Всі ці можливості та переваги децентралізованих систем дозволяють їм ефективно застосовуватись у різних галузях життя. Наприклад, вони можуть

бути використані для безпечної передачі цифрових активів, обміну криптовалют, створення електронних голосувань, ведення медичних записів, управління ланцюгами постачання, підтвердження автентичності товарів або документів, створення смарт-контрактів та багато іншого. [4]

Застосування блокчейн-технології у реальному житті вже спостерігається в таких галузях, як фінанси, логістика, охорона здоров'я, громадські послуги, енергетика та багато іншого. Завдяки своїм перевагам у забезпеченні механізмів захисту, децентралізовані системи надають нові можливості для створення безпечного та надійного цифрового середовища у різних сферах життя.

2.5 Механізми аутентифікації з використанням blockchain технології

Blockchain технологія надає унікальні можливості для реалізації механізмів аутентифікації та ідентифікації з високим рівнем безпеки. Нижче наведено докладний опис деяких з таких механізмів:

Публічний ключ/приватний ключ: Одним з найпоширеніших механізмів аутентифікації в blockchain є використання криптографічних ключів - публічних та приватних ключів. Кожен користувач має унікальний набір ключів. Публічний ключ використовується для ідентифікації користувача, а приватний ключ застосовується для підтвердження автентичності і підпису транзакцій.

- Цифровий підпис: За допомогою приватного ключа користувач може створювати цифровий підпис для підтвердження автентичності та непорушеності даних. Цей підпис може бути перевірений за допомогою відповідного публічного ключа, що дозволяє іншим користувачам перевірити автентичність підпису та переконатися, що дані не були змінені. [3]
- Багатофакторна аутентифікація: Blockchain може бути використаний для реалізації багатофакторної аутентифікації, де кілька факторів використовуються для підтвердження ідентичності користувача. Наприклад, окрім приватного ключа, можуть бути використані

біометричні дані, паролі, токени або інші фактори для забезпечення високого рівня безпеки. [3]

- Самоврядування: Blockchain може дозволити користувачам самостійно керувати своїми ідентифікаційними даними і надавати доступ до них. Замість централізованих організацій, користувачі можуть контролювати свою ідентичність та надавати доступ до неї за допомогою смарт-контрактів, що забезпечує більшу приватність та контроль.
- Децентралізовані ідентифікаційні системи: Blockchain може бути використаний для створення децентралізованих ідентифікаційних систем, де інформація про користувачів зберігається в розподілених блоках. Це дозволяє кожному користувачеві мати унікальну ідентичність, яка не залежить від централізованих організацій і забезпечує більшу безпеку та незалежність. [3]
- Захист від DDOS-атак: Завдяки своїй розподіленій природі, blockchain може бути більш стійким до DDOS-атак, оскільки він не має єдиного центру, який можна зупинити. Кожен вузол в мережі має свою копію блокчейну, що дозволяє системі продовжувати працювати навіть при атаках на окремі вузли. [3]

Ці механізми аутентифікації та ідентифікації на основі blockchain технології дозволяють забезпечити високий рівень безпеки, автентичності та незалежності у цифрових транзакціях та обміні даними. Вони розширюють можливості традиційних систем і надають нові перспективи для захисту особистих інформаційних ресурсів та забезпечення безпеки користувачів.

Відкритий blockchain перетворює централізований корінь довіри на децентралізовану модель, де кожен може використовувати цей корінь довіри. Технологія blockchain замінює реліантність на математичну надійність. Замість того, щоб покладатися на централізований орган, такий як консорціум або уряд, як корінь довіри, використовується алгоритм, який працює на багатьох машинах та розповсюджується в децентралізованій мережі. Мережа Bitcoin є

прикладом, де така модель була успішно впроваджена і функціонує без помилок вже впродовж восьми років.

Всі blockchain мають загальну криптографічну структуру:

– Кожна транзакція в blockchain підписана автором, що дозволяє підтвердити автентичність та непорушеність даних.
– Кожна транзакція, окремо або в складі блоків, зв'язана з попередніми за допомогою цифрового хешу. Це створює послідовність блоків, де зміна будь-якого блоку автоматично впливає на всі наступні блоки, що робить маніпулювання минулими операціями дуже складним.
– Підтверджені транзакції реплікуються на всіх машинах у мережі за допомогою консенсусного алгоритму. Це забезпечує однакову копію блокчейну на кожній машині та запобігає змінам даних без згоди більшості учасників. [4]

У результаті отримується незмінна криптографічна книга записів, яка робить практично неможливим зміну попередніх операцій або зловмисний контроль над майбутніми.

Blockchain ідеально підходить для реєстру самообслуговування на основі відкритих ключів, оскільки кожна транзакція в blockchain має цифровий підпис, який вимагає закритий ключ. Тому використання blockchain для зберігання асоційованого відкритого ключа або іншого криптографічного ключа, з яким пов'язана правовласність, є логічним кроком в перехід від централізованої інфраструктури управління публічними ключами (PKI) до децентралізованої PKI (DPKI).

Основні характеристики PKI реалізовані в інфраструктурі blockchain:

– Механізм сертифікації атрибутів, що характеризують користувача, і пов'язані з його публічним ключем.
– Механізм відклику наданих сертифікатів.
– Можливість контролю доступу до атрибутів.

Користувач, який володіє парою відкритий-закритий ключ, створює та контролює смарт-контракт, який містить атрибути, такі як ім'я, вік,

ідентифікаційний код і т. д. Список атрибутів може варіюватися за бажанням користувача. [4]Інші учасники взаємодії мають можливість підтвердити достовірність представлених атрибутів, підписавши відповідні сертифікати або запитати підписані сертифікати. Модель взаємодії в системі ідентифікації зображена на рисунку 2.2.

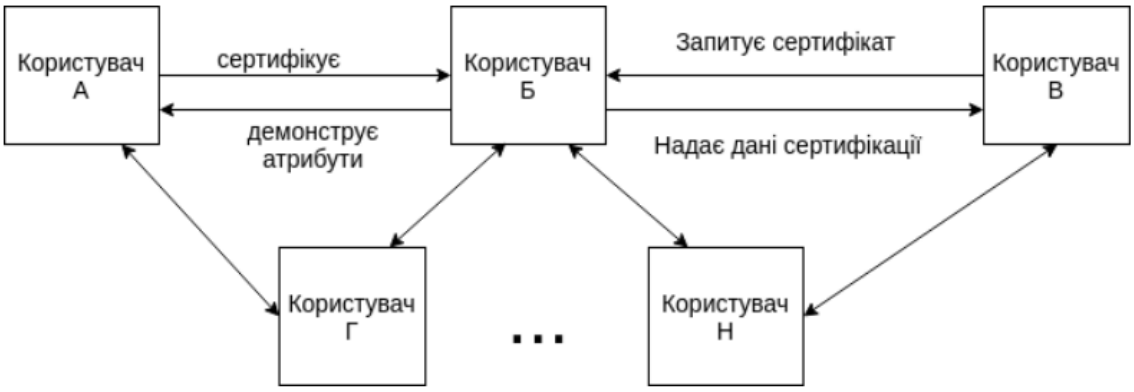

Рисунок 2.2 – Модель взаємодії користувачів

Blockchain PKI використовує blockchain сертифікати, які містять публічний ключ, метадані та дані, які підлягають сертифікації. Щоб підтвердити валідність blockchain сертифікату, верифікатор перевіряє, чи сертифікат присутній у сховищі підписаних сертифікатів користувача і чи він не знаходиться серед відкликаних сертифікатів цього користувача.

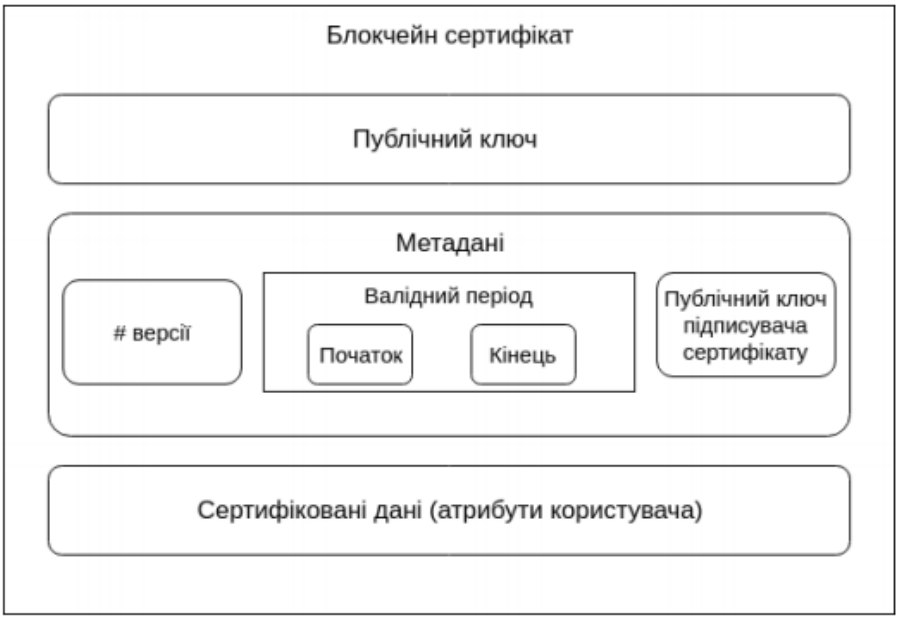

Рисунок 2.3 – Blockchain сертифікат

Система, яка базується на Ethereum blockchain та використовує розумні контракти, дозволяє користувачам керувати своєю ідентичністю та атрибутами ідентичності інших осіб відповідно до моделі Web-of-Trust. Смарт-контракт зосереджений навколо кожного користувача, який публікує свої атрибути, підписи та відкликані сертифікати на blockchain для демонстрації своєї ідентичності. Кожен користувач асоціюється з Ethereum-адресою, що виступає як його відкритий ключ і контролюється приватним ключем. Мова Solidity використовується для написання контрактів і підтримує структури даних, такі як struct. Хоча сама сутність (користувач) не визначена як структура даних в контракті, вона обумовлена реалізацією Ethereum. Кожна транзакція Ethereum має власника, який є 20-байтною адресою, і для проведення валідної транзакції вона повинна бути підписана приватним ключем, пов'язаним з адресою власника. [3]

Таким чином, Ethereum-адреса виступає хорошим ідентифікатором особи або користувача системи. Структури Attribute, Certificate і Revocation мають поле з адресою користувача. У випадку Certificate, це поле визначає підписувача сертифікату, а у випадку Revocation (відклику сертифікатів) поле користувача існує за замовчуванням, оскільки тільки користувач, який надав сертифікат, може його відкликати. Щоб бути універсальним, система самостійної ідентичності на blockchain має діяти як глобальна соціальна утиліта, доступна для всіх власників ідентифікаторів, емітентів та верифікаторів, схоже на роботу Інтернету, WEB або системи доменних імен.

Системи Інтернету, Web та DNS ґрунтуються на відкритих протоколах і стандартах, використовують відкрите програмне забезпечення і мають відкрите управління. Це означає, що вони не належать жодній окремій компанії або федерації, і кожен має можливість використовувати їх і вносити поліпшення. Система самостійної ідентичності, заснована на публічному blockchain, повинна працювати так само, щоб забезпечити ідентичність для всіх. Вона не може бути заснована на власних технологіях або контролюватися однією компанією або консорціумом. Іронія деяких запропонованих рішень

ідентифікації на blockchain полягає в тому, що вони намагаються використовувати унікальні властивості blockchain - можливість взаємодії конкуруючих сторін з одним універсальним джерелом правди - для створення рішень, що контролюються однією компанією або консорціумом. Однак самоврядна ідентичність означає, що ідентичність завжди перебуває під контролем власника, і її не можна відібрати. Власник ідентичності стає провайдером своєї власної ідентичності завдяки відкритому ключу на публічному blockchain. Самоврядна ідентичність дає власнику повний контроль над тим, що стосується його ідентичності, але не означає, що він контролює всі аспекти своєї ідентичності. Власники ідентичності все ще взаємодіють з іншими емітентами перевірених претензій для встановлення довіри до своєї ідентичності. Кожен громадський blockchain був розроблений з певною метою.

Bitcoin був створений з метою створення глобальної криптовалюти. У 2008 році Сатоші Накамото опублікував документ, в якому описав унікальну модель стимулювання роботи для децентралізованої мережі криптовалюти. Результати говорять самі за себе: це один з найбільших розподілених обчислювальних проектів у світі, який працює впродовж восьми років без порушення основного блоку. Він також налічує тисячі розробників і стартапів у своїй спільноті, а його криптовалюта генерує нові блоки щодня. [3]

Ethereum, з іншого боку, був створений з метою створення глобального комп'ютера для смарт-контрактів і децентралізованих додатків (dapps). Віталік Бутерін запропонував його у кінці 2013 року з метою вирішення проблеми відсутності мови сценаріїв в Bitcoin. З того часу Ethereum став спільнотою з більш ніж 30 000 розробників і сприяв створенню Enterprise Ethereum Alliance - глобального консорціуму, який розробляє приватні версії публічної мережі для використання у підприємствах.

2 СИСТЕМИ ДЕЦЕНТРАЛІЗОВАНІЇ АУТЕНТИФІКАЦІЇ

3.1 Системи децентралізованої аутентифікації

Системи децентралізованої аутентифікації (Decentralized Identity Systems) представляють собою інноваційний підхід до управління ідентичністю та автентифікацією, який базується на блокчейн-технології та забезпечує користувачам контроль над своїми особистими даними та цифровою ідентичністю. У традиційних системах ідентифікації, основаних на централізованому підході, користувачі залежать від центральних постачальників ідентифікації, таких як урядові органи чи комерційні компанії, для перевірки своєї особи та отримання доступу до різних ресурсів. Однак, такі системи стикаються з рядом проблем, таких як недостатня безпека, вразливість до кібератак, централізоване зберігання та контроль над особистими даними. Системи децентралізованої аутентифікації пропонують альтернативний підхід, що розв'язує ці проблеми та надає користувачам більший контроль та конфіденційність щодо їхньої ідентичності та особистих даних. [5]

Структура систем децентралізованої аутентифікації базується на концепції децентралізованих ідентифікаторів (Decentralized Identifiers - DIDs) та верифікованих претензій (Verifiable Claims). Децентралізований ідентифікатор - це унікальний цифровий ідентифікатор, який прив'язаний до конкретної особи чи сутності і забезпечує їм контроль над своєю ідентичністю. Кожен користувач може створити свій власний DID, який складається з унікального коду, що ідентифікує їх у мережі блокчейн, а також криптографічних ключів, що забезпечують безпеку та автентифікацію. [5]

Для підтвердження своєї ідентичності та отримання доступу до різних ресурсів, користувачі можуть отримувати верифіковані претензії. Верифікована претензія - це цифрове підтвердження певного факту чи вимоги, видане відповідною стороною або довіреною установою. Наприклад, це може бути підтвердження про вік, місце проживання, професійні кваліфікації тощо. Ці

претензії можуть бути випущені на основі децентралізованого ідентифікатора користувача та підписані відповідними цифровими ключами. Вони можуть бути перевірені іншими сторонами за допомогою публічних ключів, що дозволяє підтвердити достовірність претензій та впевнитись у ідентичності користувача. [5]

Однією з ключових переваг систем децентралізованої аутентифікації є контроль користувача над своїми особистими даними. Користувачі мають можливість зберігати свої дані в зашифрованому вигляді на своєму персональному пристрої чи в обліковому записі, контролюючи, кому та коли надавати доступ до цих даних. Вони можуть вибирати, які атрибути своєї ідентичності розкривати в різних контекстах, що забезпечує більшу приватність та захист від небажаної розкриття особистої інформації.

Ще одною перевагою є більша безпека систем децентралізованої аутентифікації. Завдяки використанню криптографічних методів та блокчейн-технології, системи децентралізованої аутентифікації забезпечують міцну автентифікацію та захист від шахрайства та підробки. Цифрові підписи та шифрування дозволяють перевіряти ідентичність та цілісність даних, що забезпечує надійність системи. [6]

Крім того, системи децентралізованої аутентифікації сприяють більшій прозорості та недискримінації. Завдяки використанню верифікованих претензій та децентралізованих ідентифікаторів, можливо забезпечити об'єктивне підтвердження певних вимог та фактів без прив'язки до конкретної особи чи організації. Це дозволяє уникнути дискримінації та встановити справедливі правила доступу до ресурсів.

Системи децентралізованої аутентифікації мають широкий спектр застосувань у різних сферах життя. Вони можуть бути використані в електронній комерції, банківській сфері, охороні здоров'я, освіті, громадській адміністрації та багатьох інших галузях. Наприклад, у сфері електронної комерції системи децентралізованої аутентифікації можуть забезпечувати безпечну автентифікацію користувачів та запобігати шахрайству з

банківськими картками. У сфері охорони здоров'я, ці системи можуть забезпечувати безпечний обмін медичною інформацією та контроль доступу до особистих медичних даних. [6]

Узагалі, системи децентралізованої аутентифікації відкривають нові можливості для покращення безпеки, приватності та ефективності процесів ідентифікації та автентифікації. Вони дозволяють зберігати та керувати цифровою ідентичністю користувача без залучення посередників, забезпечуючи більший контроль та приватність. Застосування децентралізованих систем аутентифікації має потенціал перетворити спосіб, яким ми управляємо своєю ідентичністю та взаємодіємо в цифровому світі, роблячи його більш безпечним, прозорим та гнучким. [6]

3.2 Вимоги до систем децентралізованої аутентифікації

Системи децентралізованої аутентифікації стають все більш важливими в цифровому світі, оскільки вони дозволяють забезпечити безпеку та приватність при взаємодії користувачів з різними сервісами та платформами. Проектування та реалізація систем децентралізованої аутентифікації вимагає врахування ряду важливих вимог, які забезпечують їх ефективність та надійність. Деякі з цих вимог описані нижче:

- Безпека: Головною вимогою до систем децентралізованої аутентифікації є забезпечення високого рівня безпеки. Система повинна бути стійкою до різних видів атак, таких як перехоплення, підробка або викрадення ідентифікаційних даних. Вона повинна використовувати потужні криптографічні алгоритми для шифрування та підпису даних, а також механізми перевірки цілісності та аутентичності.
- Приватність: Вимога до приватності полягає у забезпеченні захисту конфіденційної інформації користувачів. Система повинна дозволяти користувачам контролювати доступ до своїх особистих даних та встановлювати, які дані вони хочуть розкривати при аутентифікації. Крім того, система повинна забезпечувати анонімність користувачів,

уникати прямого зв'язку між їхніми особистими даними та їхньою цифровою ідентичністю.

- Масштабованість: Система децентралізованої аутентифікації повинна бути масштабованою, щоб забезпечити безперебійну роботу при великій кількості користувачів та великому обсязі транзакцій. Вона повинна бути здатною обробляти велику кількість запитів та підтримувати високу швидкість обробки, щоб забезпечити плавну та ефективну автентифікацію користувачів.
- Відкритість: Вимога до відкритості полягає у доступності та гнучкості системи. Система повинна бути відкритою для інтеграції з різними сервісами та платформами. Вона повинна підтримувати стандартизовані протоколи та інтерфейси, що дозволяють взаємодіяти з іншими системами аутентифікації та ідентифікації.
- Впевненість: Система децентралізованої аутентифікації повинна забезпечувати впевненість у валідності ідентичності користувача. Вона повинна мати механізми перевірки та підтвердження достовірності інформації, представленої користувачем при аутентифікації. Це може включати використання біометричних даних, мультифакторної аутентифікації або перевірку інформації через зовнішні джерела.
- Гнучкість: Вимога до гнучкості полягає у забезпеченні різноманітних методів аутентифікації та ідентифікації. Система повинна підтримувати різні види аутентифікаційних факторів, таких як паролі, біометричні дані, криптографічні ключі тощо. Користувачі повинні мати можливість вибирати найбільш зручний та безпечний спосіб аутентифікації для своїх потреб.
- Взаємодія з існуючими системами: Система децентралізованої аутентифікації повинна бути здатною взаємодіяти з існуючими системами автентифікації та ідентифікації. Вона повинна бути сумісною зі стандартними протоколами та протоколами відкритого ключа, що

використовуються в інших системах, щоб забезпечити сумісність та взаємодію з ними.

Враховуючи ці вимоги, системи децентралізованої аутентифікації можуть забезпечувати високий рівень безпеки, приватності та зручності для користувачів. Вони дозволяють забезпечити автентифікацію без посередництва централізованих організацій та зберігати контроль над особистими даними. Децентралізовані системи аутентифікації стають основою для розвитку безпеки в цифровому світі та відкривають нові можливості для захисту інформації та приватності користувачів. [5]

3.3 Приклади систем децентралізованої аунтефікації

На сьогоднішній день існує кілька прикладів систем децентралізованої аутентифікації, які надають користувачам контроль над їхніми ідентичністю. Деякі з них включають:

- Sovrin: Sovrin є відкритою, глобальною системою ідентичності, побудованою на технології blockchain. Вона дозволяє користувачам контролювати свою цифрову ідентичність і надавати доступ до своїх ідентифікаційних даних за потреби. Sovrin базується на принципі децентралізованих ідентифікаторів і публічного ключа, що дозволяє власникам ідентичності бути самими собою провайдерами своєї ідентичності.
- uPort: uPort є системою децентралізованої ідентичності на базі Ethereum. Вона дозволяє користувачам створювати і керувати своїми цифровими ідентичностями, включаючи особисті дані та сертифікати. Користувачі можуть самостійно вирішувати, які дані ідентичності розкриваються третім сторонам і які права доступу надаються.
- Blockstack: Blockstack - це платформа, яка дозволяє створювати децентралізовані додатки з власною системою ідентифікації. Користувачі можуть створювати і керувати своїми цифровими ідентичностями за допомогою приватних ключів, що зберігаються на

їхньому пристрої. Це дає їм повний контроль над своїми особистими даними і доступом до додатків на платформі.

– SelfKey: SelfKey - це система децентралізованої ідентичності, яка дозволяє користувачам контролювати свої особисті дані та ідентичність. Вона використовує технологію блокчейн, щоб забезпечити безпеку та приватність ідентифікаційних даних. Користувачі можуть самостійно вирішувати, кому надавати доступ до своїх даних та яку інформацію розкривати. [6]

Ці приклади систем децентралізованої аутентифікації демонструють різноманітність підходів до забезпечення користувачам контролю над їхньою ідентичністю та приватністю. Кожна з цих систем використовує різні технології та протоколи, але спільною метою є створення децентралізованих рішень, які надають користувачам більшу свободу та безпеку щодо їхньої ідентичності. [6]

3.3.1 uPort

uPort - це система децентралізованої ідентифікації та управління цифровою ідентичністю, побудована на основі технології блокчейн. Вона надає користувачам контроль над їхніми особистими даними та забезпечує безпеку, приватність і надійність при взаємодії в цифровому середовищі. Розроблена командою ConsenSys, uPort використовує блокчейн Ethereum для забезпечення впевненості в достовірності даних та автентифікації користувачів. [5]

Основна мета uPort - замінити традиційні централізовані системи ідентифікації, які контролюються окремими організаціями, на децентралізовану та самоуправляючу систему. Вона дозволяє користувачам створювати та керувати своєю цифровою ідентичністю, що дає їм повний контроль над їхніми особистими даними. Завдяки використанню блокчейн, дані користувачів захищені криптографічними механізмами, що гарантує безпеку і недоступність для сторонніх. [5]

Структура uPort базується на технології самоідентифікації, де користувачі самі контролюють свою ідентичність та особисті дані. У системі uPort кожен користувач має свій унікальний цифровий ідентифікатор, відомий як

"ідентифікатор DID" (Decentralized Identifier). Цей ідентифікатор забезпечує унікальність та перевірку ідентичності користувача. [5]

Крім того, у системі uPort використовуються "атестації" (атестаційні записи), які дозволяють користувачам підтверджувати свою особисту інформацію, таку як ім'я, адреса, вік, сертифікати тощо. Атестації засновані на криптографічних підписах та дозволяють підтвердити валідність та непередбачуваність даних. Користувачі можуть збирати атестації від різних джерел, таких як урядові органи, банки, освітні заклади тощо, що додає до їхньої цифрової ідентичності більшу достовірність та довіру.

Для забезпечення безпеки, система uPort використовує криптографічні протоколи, такі як публічні та приватні ключі, щоб забезпечити автентифікацію та підтвердження ідентичності користувачів. Кожен користувач має свій приватний ключ, який використовується для підпису атестацій та транзакцій, а його публічний ключ використовується для перевірки підпису та доступу до інформації. [5]

Однією з ключових переваг uPort є забезпечення приватності користувачів. Завдяки децентралізованій природі системи, користувачі контролюють, яку інформацію вони розкривають та кому вони надають доступ. Вони можуть встановлювати рівні доступу для різних сторін та сервісів, що забезпечує захист особистих даних.

Крім того, uPort дозволяє користувачам взаємодіяти з різними додатками та сервісами, використовуючи одну цифрову ідентичність. Користувачі можуть автентифікуватися та передавати атестації від своєї цифрової ідентичності до різних додатків, що спрощує процес реєстрації та взаємодії з платформами. [5]

Загалом, uPort надає користувачам контроль, безпеку та приватність при управлінні їхньою цифровою ідентичністю. Вона пропонує новий підхід до ідентифікації, де користувачі мають повний контроль над своїми даними та можуть взаємодіяти з різними сервісами без необхідності розкривати особисту інформацію. Застосування uPort може знайти в сферах, таких як фінанси,

медицина, урядові послуги та багато інших, де захист особистих даних та надійність ідентифікації є важливими. [5]

3.2.2 Sovrin

Sovrin - це відкрита та децентралізована платформа для цифрової ідентичності, яка надає людям контроль над своїми особистими даними та дозволяє їм безпечно та приватно обмінюватися інформацією з різними організаціями та сервісами. Створена на базі технології blockchain, Sovrin пропонує новий підхід до ідентифікації, забезпечуючи гнучкість, безпеку та захист особистих даних. [6]

Одна з основних переваг Sovrin полягає у тому, що вона дозволяє кожній особі володіти своєю цифровою ідентичністю та контролювати доступ до своїх даних. Користувачі мають можливість створювати та управляти своїми цифровими ідентифікаторами, які можуть бути перевірені та використовувані різними організаціями. Це дає людям більшу прозорість та контроль над своїми особистими даними, уникаючи централізованих баз даних, які можуть бути зламані або зловживані.

Архітектура Sovrin базується на розподіленій головній книзі (DLT), використовуючи технологію блокчейну. Кожен учасник мережі має свою власну "комірку пам'яті" або "гаманець", де зберігається його ідентифікатор та атрибути. Комірки пам'яті підтримуються взаємодією з розподіленою головною книгою, що забезпечує високу надійність та безпеку даних. [6]

Один з ключових елементів Sovrin - це децентралізована система видачі атрибутів, яка дозволяє користувачам отримувати валідні атрибути (наприклад, документи про освіту, дозволи, сертифікати тощо) від відповідних випускників атрибутів. Це означає, що користувач може пред'явити свої атрибути для перевірки без потреби розкривати повну інформацію про себе. Наприклад, при зверненні до роботодавця, користувач може надати докази про свою освіту без необхідності розкривати інші особисті дані. [6]

Ще однією важливою особливістю Sovrin є підтримка "нульового знання" (zero-knowledge), що дозволяє перевіряти достовірність ідентифікаційних

атрибутів без розкриття конкретної інформації. Це забезпечує високу приватність та захист особистих даних. Наприклад, при перевірці віку, користувач може підтвердити, що йому більше 18 років, не розкриваючи свою точну дату народження. [7]

Sovrin також надає гнучкість в створенні різних типів ідентифікаторів та взаємодії з різними блокчейнами та системами ідентифікації. Вона підтримує використання стандартних протоколів та API, що дозволяє легко інтегрувати її з існуючими системами та сервісами.

У сфері застосування Sovrin може бути використана в багатьох галузях, включаючи фінансові послуги, медицину, урядові послуги, логістику, торгівлю та багато інших. Наприклад, в банківській сфері, Sovrin може допомогти встановити безпечні канали комунікації між різними фінансовими установами та клієнтами, забезпечуючи високий рівень ідентифікації та автентифікації. [7]

Також Sovrin може бути використана в урядових системах для забезпечення безпечного та прозорого взаємодії з громадянами. Наприклад, видача паспортів або інших документів може бути зручнішою та безпечнішою завдяки використанню цифрових ідентифікаторів Sovrin. [7]

Основні переваги Sovrin включають:

- Приватність та захист даних: Sovrin дозволяє користувачам контролювати доступ до своїх особистих даних та надає механізми шифрування та анонімізації інформації.
- Гнучкість: Sovrin підтримує різні типи ідентифікаторів та протоколи, що дозволяє легко інтегрувати її з різними системами та сервісами.
- Децентралізація: Sovrin базується на технології блокчейн, що забезпечує розподілену та безпечну збереження даних без централізованого управління.
- Взаємодія та обмін даними: Sovrin дозволяє безпечно обмінюватися інформацією з різними організаціями та сервісами, забезпечуючи надійність та достовірність даних.

– Підтримка стандартів: Sovrin використовує відкриті та стандартизовані протоколи, що дозволяє легко інтегрувати її з існуючими системами та технологіями. [7]

У висновок можна сказати, Sovrin - це потужна та інноваційна платформа для цифрової ідентичності, яка дозволяє людям контролювати свої дані та безпечно взаємодіяти з різними організаціями та сервісами. Вона використовує технологію блокчейн та надає гнучкість, приватність та захист особистих даних. Sovrin має потенціал вплинути на багато галузей, де цифрова ідентичність є важливою, і сприяти побудові безпечних та довіреної цифрової інфраструктури. [7]

3.3 Порівняльна характеристика uPort та Sovrin

uPort і Sovrin - це дві розроблені системи децентралізованої ідентичності, які мають за мету забезпечити користувачам контроль над своїми персональними даними та приватністю в онлайн-середовищі. Вони працюють на базі технології блокчейн, проте вони мають певні відмінності у своєму підході та функціоналі.

Одна з ключових відмінностей між uPort і Sovrin полягає в архітектурному підході. uPort базується на Ethereum блокчейні, що дозволяє створювати децентралізовані ідентифікаційні реєстри та контролювати доступ до персональних даних. Користувачі можуть створювати та керувати своїми цифровими ідентифікаторами (DID) та самостійно визначати, яку інформацію вони хочуть розкрити.

З іншого боку, Sovrin використовує розподілену технологію реєстру, відому як Ledger of Digital Identity (DLedger). Ця технологія забезпечує безпечний обмін ідентифікаційною інформацією та персональними даними. Sovrin заснований на ідеї децентралізованої системи ідентифікації, де власники ідентичності контролюють свої дані, а цифрові ідентифікатори (DID) створюються для безпечного ідентифікування у цифровому просторі.

Обидва рішення дозволяють користувачам зберігати свої персональні дані в зашифрованому вигляді та керувати доступом до них. Вони надають засоби для підтвердження ідентичності та підпису цифрових транзакцій, що дозволяє впевнено використовувати ці системи в різних сферах, включаючи фінансові послуги, медицину, освіту та багато іншого.

Однією з переваг uPort є його відкритий характер та зручний інтерфейс. Він дозволяє розробникам створювати додатки, які можуть використовувати ідентифікаційні дані з uPort, щоб забезпечити безпечну та автентичну взаємодію з користувачами. uPort також підтримує стандарти для децентралізованої ідентифікації, такі як OpenID Connect та W3C Verifiable Credentials, що робить його сумісним з іншими системами та протоколами.

Sovrin також має свої переваги. Одна з них - це його масштабованість. Система Sovrin може обробляти великі обсяги транзакцій та ідентифікаційних запитів, що робить його придатним для використання в масштабних проектах та організаціях. Крім того, Sovrin надає можливість встановлювати довірені взаємозв'язки між суб'єктами ідентичності, що дозволяє забезпечити впевнену ідентифікацію та обмін даними в децентралізованому середовищі.

Водночас, якщо говорити про недоліки, uPort потребує підключення до мережі Ethereum для своєї роботи, що може вплинути на швидкість та витрати обробки транзакцій. У Sovrin також є виклик забезпечити широку прийнятність інфраструктури та стандартів відкритої ідентичності.

У підсумку, як uPort, так і Sovrin представляють цінні рішення для децентралізованої ідентичності. Обидва вони працюють на базі технології блокчейн і дозволяють користувачам контролювати свої дані та ідентичність. Вибір між ними залежатиме від конкретних потреб та вимог проекту. uPort підходить для швидкої інтеграції з додатками та розробкою зручного інтерфейсу, тоді як Sovrin має перевагу масштабованості та можливості налагодження довіреного взаємозв'язку. В остаточному підсумку, обидва ці рішення працюють на досягнення спільної мети - забезпечення безпеки,

приватності та контролю користувача над їхньою ідентичністю в цифровому світі.

У таблиці 3.1 вказано узагальнені результати оцінки кожної системи залежно від кожного закону ідентичності.

Ці закони допомагають оцінити схеми управління ідентифікацією і визначити їх сильні та слабкі сторони з точки зору контролю користувача, конфіденційності, безпеки та досвіду користувачів.

Таблиця 3.1 – Порівняння систем децентралізованої ідентифікації

Закон	uPort	Sovrin
Контроль та згода з боку користувача	Користувач контролює створення і розкриття uPortID і може довести право власності на uPortID без центрального органу. Але атрибути, що зберігаються в реєстрі, можуть пропускати інформацію.	За проектом користувачі можуть вибрати, які ідентифікатори використовуються і які атрибути виявляються. Мережа довіри яка може бути посилена репутаційною системою, допомагає захистити користувачів від обману.
Мінімальне розкриття інформації для обмеженого використання	Користувачам не потрібно розкривати особисті дані для створення ідентифікаторів uPort для рахунків з низьким значенням.	Підтримка анонімних облікових даних на основі доказів з нульовим знанням дозволяє користувачам ділитися своєю інформацією “найменш вірогідна ідентичність у кількох контекстах "
Обґрунтовані сторони	Структура JSON атрибутів у реєстрі є видимим для всіх, що може пропускати інформацію до чесного зловмисника - навіть якщо це зашифровано.	Атрибути доступні лише для тих, кого вибирає користувач, і агентствам, яким доручено діяти від їхнього імені.

Закон	uPort	Sovrin
Спрямована ідентичність	Підтримує односпрямоване спільне використання ідентифікаторів між сторонами, але не заважає об'єктам взаємодіяти з ідентифікаторами поза мережою, наприклад, на веб-сайтах	Підтримуються універсальні ідентифікатори.
Розробка плюралізму операторів і технологій	Типи атрибутів, які створюють провайдери ідентичності третьої сторони, використовують конкретний формат даних, який зберігається в реєстрі.	Очікується створення ринку посередників (агентств) між користувачами та мережею «Соврін». Можуть бути інтерфейси з іншими системами ідентичності.
Інтеграція з людиною	Надає мобільний додаток. Функція відновлення соціальних криптографічних ключів присутня. Незрозумілість у використанні та розумінні користувачів. Вплив на конфіденційність uPort.	Реалізація була націлена на теперішню технологію, а не на досвід користувачів. Незрозумілість у використанні та розуміння конфіденційності користувачами.
Постійний досвід у різних контекстах	Взаємодія з користувачем, керування мобільним додатком. Послідовно впроваджується сканування QR-коду для всіх застосувань.	Не присутній. Це сильно залежатиме від ринку реалізацій клієнтів мобільних пристроїв мережі Соврін.

Таблиця 3.1 – Порівняння систем децентралізованої ідентифікації

ВИСНОВКИ

Справді, цифрова ідентичність є постійно розвиваючимся полем, і управління технологіями ідентифікації клієнтів та ідентичності клієнтів стає ще більш важливим для бізнесу. Гнучка, масштабована та орієнтована на клієнта стратегія управління ідентифікацією є необхідною для забезпечення споживачів інноваційними та новими механізмами автентифікації і створення значущого досвіду.

Технологія Blockchain та розподілені книги (DLT) дійсно мають величезний потенціал у сфері цифрової ідентичності. Їх децентралізована природа та можливість досягнення консенсусу забезпечують безпеку, надійність та прозорість. Використання блокчейну може спростити та підвищити ефективність фінансових операцій, внутрішніх взаєморозрахунків та мікроплатежів між фізичними особами.

Цифрові ідентифікатори (DID) на базі блокчейну відіграють революційну роль у понятті ідентичності в Інтернеті. Вони надають власникам повний контроль над своєю ідентичністю та конфіденційністю і дають можливість створювати та перевіряти ідентифікатори за допомогою цифрових підписів. Застосування загальнодоступного блокчейну для DID дозволяє перевіряти облікові дані та забезпечувати докази власності відкритого ключа.

Стандартизація технології DID вже почала рухатися вперед, що сприятиме подальшому розвитку і впровадженню цих систем. Наприклад, World Wide Web Consortium активно працює над стандартами для децентралізованої ідентифікації.

Загалом, цифрова ідентичність та технології ідентифікації продовжують розвиватися, пропонуючи нові можливості для бізнесу та споживачів. Управління ідентичністю стає ключовим фактором у створенні безпечних та інноваційних цифрових сервісів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Decentralized Identity Management System for Self-Soverign Identity, Ангелов А, Мілков М, Соренсен М, 2018, Aalborg University Copenhagen 2-4 с
2. Blockchain Technology Overview NISTIR 8202, Яга Д, Мілл П, Робі Н, Скарфон К, 2018
3. The Advantages and Disadvantages of the Blockchain Technology, Голосова Ю, Романовс А, 2018, 1-4 с
4. A First Look at Identity Management Schemes on the Blockchain, Дюнфі П, Петіколас Ф, 2018
5. uPort: A Platform for Self-Sovereign Identity, Люндкіст К, Хек Р, Торстенссон Дж, Міттон З, Сена М, 2017
6. Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, Віндлі Ф, Рід Д, 2018 16-23 с
7. Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, Віндлі Ф, Рід Д, 2018 16-23 с