НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»
зі спеціальності 172 «Електронні комунікації та радіотехніка»

на тему: « Застосування блокчейн технологій для управління ідентифікацією користувачів та пристроїв»

Виконав:
студент ІІ курсу, групи ЦК-32мп
Ярошінський Дмитро Олександрович _____

Керівник:
Доцент кафедри ТК НН ІТС, к.т.н., с.н.с.,
Міночкін Дмитро Анатолійович _____

Рецензент:
Доцент кафедри ІТТ НН ІТС, к.т.н.,
Суліма Світлана Валеріївна _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Електронні комунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Ярошінському Дмитру Олександровичу

1.Тема дисертації «Застосування блокчейн технологій для управління ідентифікацією користувачів та пристроїв», науковий керівник дисертації Міночкін Дмитро Анатолійович, к.т.н., с.н.с., затверджені наказом по університету від «07» листопада 2024 р. № 4989-с.

2. Термін подання студентом дисертації 10.12.2024 р.

3. Об’єкт дослідження: надання рішення для управління ідентифікацією користувачів та пристроїв з використанням технології блокчейн.

4. Предмет дослідження: методи, алгоритми та технології блокчейн.

5. Перелік завдань, які потрібно розробити:

1. Аналіз та огляд сучасних методів ідентифікації користувачів та пристроїв

2. Аналіз технології блокчейн
3. Використання технології Blockchain для управління ідентифікацією користувачів та пристроїв
4. Розробка стартап-проєкту

5.Орієнтовний перелік ілюстративного матеріалу
Слайд №1 Актуальність роботи
Слайд №2 Сучасні методи ідентифікації
Слайд №3 Архітектура та компоненти Blockchain
Слайд №4 Типи блокчейнів
Слайд №5 Web3 та смарт-контракти
Слайд №6 Засоби для створення додатку
Слайд №7 Запропонований додаток
Слайд №8 Використані Джерела

6. Дата видачі завдання 16 грудня 2023 р

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Розробка, оформлення, узгодження та затвердження технічного завдання на роботу. Аналітичний огляд інформаційних матеріалів. Підбір та опрацювання необхідної науково-технічної літератури.	16.12.2023-15.02.2024	Виконано
2	Вивчення та розбір сучасних методів ідентифікації та аутентифікації	16.02.2024-30.04.2024	Виконано
3	Аналіз технології блокчейн та її аспекти. Розробка демонстраційного додатку з ідентифікацією юзера за допомогою технологій блокчейн; Розробка стартап-проєкту	01.05.2024-31.10.2024	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	01.11.2024-01.12.2024	Виконано
5	Підготовка та оформлення презентації для доповіді	02.12.2024-05.12.2024	Виконано

Студент Дмитро ЯРОШІНСЬКИЙ

Науковий керівник дисертації Дмитро МІНОЧКІН

РЕФЕРАТ

Магістерська дисертація містить 97 сторінок, 23 таблиці, 23 рисунки. Було використано 28 джерел інформації.

Актуальність роботи

Застосування блокчейн-технологій для управління ідентифікацією користувачів та пристроїв є інноваційним підходом, що пропонує у своєму рішенні найвищий рівень безпечночсті, децентралізацію, прозорість та стійкість до несанкціонованих дій. Традиційні методи управління ідентифікацією часто мають слабкі місця, такі як централізовані бази даних, які вразливі до зламів та маніпуляцій. Блокчейн, завдяки своїй децентралізованій природі, дозволяє усунути ці недоліки, створюючи надійні, захищені та масштабовані рішення для ідентифікації.

Для автоматизації процесів ідентифікації використовуються смарт контракти, забезпечуючи гнучкість, інтеграцію з іншими системами та зменшення людського фактора. Цей підхід сприяє створенню нових стандартів безпеки та довіри між користувачами, пристроями та організаціями. Особливо актуальним це стає в умовах стрімкого зростання інтернету речей (IoT) та необхідності безпечної взаємодії мільярдів пристроїв у глобальній мережі.

Очікується, що блокчейн-технології матимуть значний вплив на сучасні системи ідентифікації, забезпечуючи інноваційні способи управління доступом, покращення користувацького досвіду та зниження ризиків, пов’язаних із компрометацією даних.

Метою роботи є дослідження та розробка підходів застосування блокчейн-технологій для управління ідентифікацією користувачів і пристроїв,

що дозволить підвищити безпеку, масштабованість і довіру в сучасних системах.

Об'єкт дослідження - системи управління ідентифікацією користувачів та пристроїв на основі блокчейн-технологій.

Предмет дослідження -методи і технології використання блокчейн для управління ідентифікацією в інформаційних системах.

Методи дослідження. Використання методів критичного аналізу існуючих підходів до ідентифікації, порівняльний аналіз традиційних та блокчейн-орієнтованих систем, а також методи моделювання та симуляції для перевірки ефективності запропонованих рішень.

Отримані результати. Внаслідок досліджень застосування блокчейн-технологій в управлінні ідентифікацією були сформовані рекомендації для розробки децентралізованих систем, які здатні підвищити захищеність даних, зменшити залежність від центральних органів та оптимізувати процес аутентифікації. Запропоновані рішення також демонструють потенціал для автоматизації та інтеграції з іншими системами безпеки.

Галузь застосування. Використання результатів для впровадження блокчейн-технологій у системи управління доступом в різних галузях, таких як фінансовий сектор, здоров'я, телекомунікації, державний сектор та інтернет речей. Отримані висновки сприятимуть розробці сучасних платформ ідентифікації та управління пристроями.

Ключові слова: Блокчейн-технології, ідентифікація користувачів, управління пристроями, децентралізація, безпека даних, смарт-контракти.

ABSTRACT

The master's thesis consists of 97 pages, 23 tables, and 23 figures. 28 sources of information were used

Relevance of the work

The use of blockchain technologies to manage user and device identities is an innovative approach that provides a high level of security, decentralization, transparency, and resistance to unauthorized actions. Traditional identity management methods often have weaknesses, such as centralized databases that are vulnerable to hacking and manipulation. Blockchain, due to its decentralized nature, eliminates these shortcomings, creating reliable, secure, and scalable identity solutions.

The use of smart contracts allows automating identification processes, providing flexibility, integration with other systems, and reducing the human factor. This approach helps to create new standards of security and trust between users, devices, and organizations. This becomes especially relevant in the context of the rapid growth of the Internet of Things (IoT) and the need for secure interaction between billions of devices in the global network.

Blockchain technologies are expected to have a significant impact on modern identification systems, providing innovative ways to manage access, improve user experience, and reduce the risks associated with data compromise.

The aim of the study is to research and develop approaches to the use of blockchain technologies for user and device identification management, which will increase security, scalability and trust in modern systems.

Object of research - user and device identification management systems based on blockchain technologies.

The subject of research is methods and technologies for using blockchain for identity management in information systems.

Research methods. The study uses methods of critical analysis of existing approaches to identification, comparative analysis of traditional and blockchain-oriented systems, as well as modeling and simulation methods to test the effectiveness of the proposed solutions.

Results obtained. As a result of the research on the use of blockchain technologies in identity management, recommendations have been made for the development of decentralized systems that can increase data security, reduce dependence on central authorities, and optimize the authentication process. The proposed solutions also demonstrate the potential for automation and integration with other security systems.

Scope of application. The results of this work can be used to implement blockchain technologies in access control systems in various industries, such as finance, healthcare, telecommunications, public sector, and the Internet of Things. The findings will contribute to the development of modern device identification and management platforms.

Keywords: Blockchain technologies, user identification, device management, decentralization, data security, smart contracts

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

MFA	Multi-factor authentication
POS	Proof-of-Stake
POW	Proof-of-Work
2FA	2 Factor authentication
IMEI	International Mobile Equipment Identity
OTP	One Time Password
MAC	Media Access Control
ID	Identity Document

ВСТУП

Протягом останніх десятиліть зростаюча кількість користувачів мережі Інтернет, мобільних пристроїв та розумних технологій підвищила потребу у забезпеченні безпеки ідентифікації користувачів та пристроїв. Зокрема, традиційні методи автентифікації та авторизації, які широко використовувалися в корпоративних системах, мобільних додатках та інших цифрових середовищах, мають ряд суттєвих вразливостей. Вразливість традиційних підходів проявляється як у центральних серверах для зберігання даних, що стають мішенню для атак, так і у залежності від централізованих контролюючих органів, які можуть обмежувати доступ або зловживати особистими даними.

В умовах таких викликів технологія блокчейну постає як революційне рішення для створення безпечних і децентралізованих систем управління ідентифікацією, що може забезпечити конфіденційність, захист від підробок та прозорість у роботі з персональними даними. Завдяки своїм характеристикам, зокрема незмінності записів і можливості децентралізації, блокчейн дозволяє користувачам зберігати та перевіряти свої дані без посередників, що мінімізує ризики компрометації інформації.

Актуальність дослідження зумовлена необхідністю розробки і використання інноваційного підходу для управління цифровою ідентифікацією, де важливу роль відіграють захищені механізми доступу, децентралізовані сервіси та обмеження доступу до персональних даних для третіх сторін. Блокчейн відкриває двері у світ безпечного зберігання ідентифікаційних даних, пропонуючи розв'язання проблем безпеки та конфіденційності, з якими стикаються як корпоративні мережі, так і приватні користувачі.

Метою даної роботи є дослідження способів інтеграції блокчейн технологій в процеси ідентифікації користувачів та пристроїв, зокрема для забезпечення децентралізації і захисту даних.

РОЗДІЛ 1
АНАЛІЗ ТА ОГЛЯД СУЧАСНИХ МЕТОДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ПРИСТРОЇВ

1.1 Традиційні методи ідентифікації

1.1.1 Традиційні паролі та їх обмеження

Наше життя тісно поєдналося з початком ери інтернету, що кардинально змінило способи комунікації, доступу до інформації та взаємодії з технологіями. З появою цифрових платформ, паролі стали стандартним методом захисту облікових записів користувачів. Вони пропонують простий спосіб автентифікації, оскільки вимагають лише запам’ятовування певної комбінації символів. Але величезним недоліком є багато факторів, один з яких є фактором слабких паролів, створених користувачем. Незважаючи на освідомлення про ризики, слабкі паролі залишаються поширеною проблемою, залишаючи людей та організації вразливими до різноманітних загроз безпеки їх акаунтів та персональних даних. Основною проблемою створення слабких паролів є комбінацією факторів, такі як бажання мати пароль, який легко запам’ятати, використовування цього паролю надалі для великого числа сайтів, недооцінювання ризику кібератак та відсутність навичок створення безпечного, надійного паролю.

Є дуже багато ризиків при використанні слабких паролів, про них поговоримо нижче.

Слабкі паролі відкривають двері для несанкціонованого доступу. Це може різнитися від отримання доступу до особистого акаунту в соціальних мережах, до проникнення в базу даних підприємства, тощо. Потрапивши всередину внутрішнього середовища підприємства, зловмисник може витягти конфіденційну інформацію, видати себе за законного користувача або порушити роботу підприємства.

Захоплення акаунта є прямим наслідком слабкого захисту паролів. Кіберзлочинці, які отримали доступ до одного облікового запису, часто використовують знайдену там інформацію для доступу до інших облікових записів з вищим рівнем доступу до системи, особливо якщо повторно використовується один і той самий пароль. Цей ефект доміно може призвести до широкомасштабної компрометації особистих і професійних цифрових даних.

Один слабкий пароль може призвести до масового витоку даних. Коли зловмисники проникають в один обліковий запис, вони часто можуть переміщатися по всій мережі, отримуючи доступ до величезної кількості конфіденційних даних, від особистої інформації до комерційної таємниці.

Крадіжка особистих даних часто починається з одного скомпрометованого пароля. Зловмисники можуть використовувати викрадені облікові дані, щоб видавати себе за іншу особу, подавати заявки на кредити або займатися шахрайством, і все це під чужим ім'ям.

Слабкі паролі можуть призвести до прямих фінансових втрат. У бізнес-середовищі зламаний обліковий запис може призвести до крадіжки коштів або інтелектуальної власності, що коштуватиме компаніям мільйони. Для приватних осіб крадіжка банківської інформації або кредитних карток може мати негайні та руйнівні фінансові наслідки.

Для менеджерів і власників сайтів слабкі паролі становлять значний ризик. Зловмисники, отримавши доступ, можуть пошкодити сайт, викрасти дані клієнтів або навіть перенаправити трафік на шкідливі сайти, поставивши під загрозу цілісність сайту та репутацію бізнесу.

Шкода, спричинена слабкими паролями, виходить за рамки безпосередніх фінансових втрат. Для бізнесу порушення безпеки може

заплямувати його репутацію, призвести до втрати довіри клієнтів і потенційно непоправної шкоди бренду.

Нарешті, слабкі паролі можуть призвести до юридичних проблем. Порушення даних часто призводить до судових позовів від постраждалих сторін, а компанії можуть бути оштрафовані за нездатність належним чином захистити дані користувачів

1.1.2 Одноразові паролі (OTP)

Що таке одноразовий пароль (OTP)?

Одноразовий пароль (OTP) - це автоматична генерація цифрових або буквено-цифрових рядків символів, який автентифікує користувача для однієї транзакції або сеансу входу в систему[1]. OTP є більш безпечним, ніж статичний пароль, особливо створений користувачем, який може бути слабким і повторно використовуватися в різних облікових записах. OTP можуть замінити традиційну автентифікаційну інформацію для входу або можуть використовуватися на додаток до неї, щоб додати ще один рівень безпеки.

Одноразовий пароль дозволяє уникнути деяких поширених помилок, пов'язаних з безпекою паролів. З OTP IT-адміністраторам та менеджерам з безпеки не потрібно турбуватися про правила складання надійних паролів, тобто: відомі-погані та слабкі паролі, спільне використання облікових даних або повторне використання одного і того ж пароля в різних облікових записах і системах.

Ще однією перевагою одноразових паролів є те, що вони стають недійсними за лічені хвилини - у випадку з TOTP-паролями - або після їх використання - у випадку з HOTP-паролями.[2] Таким чином, одноразові

паролі не дають зловмисникам отримати секретні коди і використовувати їх повторно.

1.1.3 Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація (MFA) – це наче додатковий рівень захисту, який каже: "Пароль – це добре, але цього недостатньо". Цей процес передбачає кілька етапів перевірки особи, щоб забезпечити максимальну безпеку вашого облікового запису.

От уявіть, ви вводите пароль – це перший етап. Але тут вас просять ще ввести код із SMS, відповісти на секретне запитання або навіть скористатися біометрією, наприклад, відбитком пальця. Чому це важливо? Тому що навіть якщо ваш пароль випадково потрапить у чужі руки, без другого (або третього) етапу підтвердження доступ до вашого облікового запису отримати буде практично неможливо.[3]

Багатофакторна аутентифікація зменшує ризики, спричинені людськими помилками, втратою паролів або втраченими пристроями. Завдяки цьому організації можуть впевнено реалізовувати цифрові проєкти. Компанії застосовують цей метод для забезпечення безпеки даних як організації, так і користувачів, що дозволяє безпечно виконувати онлайн-операції та взаємодію.[4]

Також вона підвищує чутливість та швидкість реагування системи захисту. Організації можуть адаптувати багатофакторну аутентифікацію таким чином, щоб вона оперативно інформувала про підозрілі спроби авторизації.

1.1.4 Двофакторна автентифікація (2FA)

Двофакторна автентифікація (2FA) - це особливий тип багатофакторної автентифікації (MFA), який посилює безпеку доступу, вимагаючи

використання двох методів (також званих факторами автентифікації) для підтвердження вашої особи.[6] Ці фактори можуть включати щось, що ви знаєте, наприклад, ім'я користувача та пароль, а також щось, що ви маєте, наприклад, додаток для смартфона, для схвалення запитів на автентифікацію.

Компанії використовують 2FA, щоб захистити особисті та ділові активи своїх співробітників. Це важливо, оскільки не дозволяє кіберзлочинцям викрадати, знищувати або отримувати доступ до ваших внутрішніх записів даних у власних цілях.

Переваги 2FA безмежні. Наприклад, завдяки 2FA користувачам не потрібно носити з собою або завантажувати генератор токенів чи пов'язаний з ним додаток. Більшість веб-сайтів використовують ваш мобільний пристрій для відправки текстів, дзвінків або використовують персоналізовану 2FA для свого бізнесу для підтвердження вашої особи.

Іншою перевагою використання 2FA є відсутність необхідності використовувати апаратний генератор токенів.

Ці типи методів 2FA часто губляться або втрачаються. Однак, завдяки сучасним технологіям, методи 2FA стали більш зручними, ніж будь-коли.

Генератори паролів більш ефективні, ніж традиційні паролі.

Генератори є більш безпечним варіантом, оскільки не існує двох однакових паролів. Введення максимальної кількості паролів не дозволяє кіберзлочинцям зламати систему та отримати доступ до конфіденційних даних. Процес є керованим і зручним для користувача.

Таблиця.1.1

Порівняння традиційних методів ідентифікації

Тип ідентифікації	Приклади	Переваги	Недоліки
Традиційні паролі	Текстові паролі	Простота реалізації, звичність користувачам	Уразливість до зламів, слабкі паролі
Одноразові паролі (OTP)	SMS-коди, код-генератори	Більш високий рівень безпеки, тимчасовість коду	Залежність від додаткових пристроїв або сервісів
Багатофакторна автентифікація (MFA)	Поєднання паролю та OTP або біометрії	Висока безпека, мінімізує ризик компрометації	Складність впровадження, додаткова складність для користувачів
Двофакторна автентифікація (2FA)	Пароль + SMS-код або фізичний токен	Зручність використання, помірний рівень безпеки	Залежність від телефонів або спеціальних пристроїв

1.2 Біометричні методи ідентифікації

1.2.1 Розпізнавання обличчя

Автентифікація за обличчям - це процес, під час якого за допомогою відсканованого фізичного обличчя підтверджується, що особа має доступ до послуги, якою вона користується. Автентифікація за обличчям спирається на власні технології та алгоритми біометричного виявлення пристроїв.

Біометричні алгоритми застосовуються як програмне забезпечення, яке використовує камери пристроїв для цієї мети.[7] Крім того, як додатковий необхідний рівень безпеки часто додається функція розпізнавання рухів, коли користувачеві може бути запропоновано поворушити обличчям, моргнути, кивнути, посміхнутися або зробити будь-який інший рух обличчям під час процесу автентифікації або протягом усього часу доступу до сервісу.

Сама прогресивна система розпізнавання обличчя, яку ми використовуємо у повсякденному житті, існує в пристроях Apple Iphone. Починаючи з Iphone X, який був презентований 3 листопада 2017 року, запропонував нову систему безпеки пристрою – FaceID.[8] Працює він на комбінації інфрачервоного датчика, проєктора точок і спеціального чіпа, щоб забезпечити безпечну автентифікацію. Для початку, телефон сканує обличчя користувача методом проекції 30 000 невидимих точок з використанням інфрачервоної камери.

Рис. 1.1 Зображення людини, зроблене інфрачервоною камерою, яка розблоковує Iphone з FaceID

Метою цього процесу є створення детальної 3D карти обличчя з урахуванням глибини, форми, та унікальних особливостей обличчя. Далі ці дані передаються на спеціальний чип всередині телефону(Secure Enclave), який виконує роль зберігання та обробки біометричних даних.

Кожен раз, коли користувач має підтвердити свою особистість, телефон сканує обличчя користувача та порівнює його з збереженими даними, та в разі співпадіння, розблоковує телефон. Також Face ID використовується майже у всіх додатках, полегшує і прискорює роботу з приватними даними користувача.

1.2.2 Відбитки пальців та райдужна оболонка ока

Відбитки пальців є одним із найстаріших і найпоширеніших біометричних методів. Ця технологія базується на унікальності кожного відбитка пальця, що робить їх ідеальним способом автентифікації. Відбитки пальців важко підробити, і їх важко забути, на відміну від паролів. Використання відбитків пальців у смартфонах і інших пристроях стало звичайною практикою.[9] Наприклад, технологія Touch ID від Apple дозволяє користувачам швидко розблоковувати пристрій і підтверджувати платежі за допомогою відбитка пальця. Однак незважаючи на свою ефективність, система не є абсолютно безпечною, оскільки існують методи для обходу біометричних захистів, включаючи використання копій відбитків пальців.

Райдужна оболонка ока — ще один потужний біометричний метод, який базується на унікальних малюнках у райдужній оболонці. Це досить новий метод у порівнянні з відбитками пальців, але він має високий рівень точності та надійності.[10] Апаратні засоби для сканування райдужної оболонки зазвичай використовуються в системах високої безпеки, таких як у військових або державних установах. Процес ідентифікації відбувається за допомогою

спеціальних камер, які захоплюють зображення райдужки ока. Цей метод має переваги у порівнянні з відбитками пальців, адже райдужна оболонка менше піддається змінам з віком і не так легко підробляється.

1.2.3 Голосова ідентифікація

Голосова ідентифікація є сучасним біометричним методом, який використовує унікальні характеристики голосу людини для підтвердження її особи. Цей метод стає все більш популярним завдяки розвитку технологій обробки звуку та штучного інтелекту.[11] Він дозволяє зручно та швидко ідентифікувати користувачів, використовуючи лише їхній голос.

Процес голосової ідентифікації зазвичай включає кілька етапів: запис голосу, аналіз голосових характеристик (такі як висота, тембр, швидкість мовлення та інші параметри) та порівняння отриманих даних з уже зареєстрованими зразками в базі даних. Важливо зазначити, що голосова ідентифікація може бути реалізована в режимі реального часу, що робить її зручною для використання в багатьох сферах, таких як банківські послуги, телефони та інші системи доступу.

Переваги голосової ідентифікації включають зручність використання та можливість безконтактного доступу. Користувачі можуть підтверджувати свою особу, просто промовивши фразу, що значно спрощує процес входу до систем. Проте, незважаючи на свою зручність, цей метод має і певні недоліки. Наприклад, голос може бути зміненим через хворобу, стрес або навіть під впливом навколишнього середовища, що може ускладнити ідентифікацію. Крім того, голосова ідентифікація піддається атакам, таким як відтворення записів голосу або використання технологій синтезу мови.

1.2.4 Біометрія поведінки

Поведінкова біометрія аналізує цифрову фізичну та когнітивну поведінку користувача, щоб відрізнити діяльність кіберзлочинців від законних клієнтів, виявити шахрайство та крадіжку особистих даних. Справжні клієнти та шахраї взаємодіють з цифровими платформами по-різному. Якщо ви вводите інформацію по одній клавіші за раз, то злочинці частіше копіюють і вставляють дані у форму. Очевидно, що все набагато складніше, але основний висновок полягає в тому, що ми можемо використовувати поведінкові дані, щоб зрозуміти шахрайську діяльність.[12]

Поведінкова біометрія використовує машинне навчання для аналізу шаблонів людської активності та виявлення того, чи дійсно хтось є тим, за кого себе видає, коли взаємодіє в Інтернеті, і чи керує цією активністю людина, чи це частина автоматизованої атаки.

Ключова перевага поведінкової біометрії полягає в тому, що вона працює пасивно у фоновому режимі веб- або мобільного сеансу користувача, відстежуючи тисячі параметрів, таких як те, як людина тримає телефон, як вона прокручує або перемикається між полями, тим самим мінімізуючи перешкоди в користуванні.

Як окреме рішення або як частина багаторівневого плану боротьби з шахрайством, поведінкова біометрія дає надзвичайні результати і викриває найсучасніші шахрайські атаки.

Таблиця.1.2

Порівняння біометричних методів ідентифікації

Тип ідентифікації	Приклади	Переваги	Недоліки
Розпізнавання обличчя	Face ID, системи розпізнавання	Зручність, швидкість	Чутливість до умов освітлення, питання конфіденційності
Відбитки пальців та райдужка ока	Сканери відбитків, ретинальні сканери	Висока точність, унікальність	Вартість обладнання, можливі фізичні пошкодження
Голосова ідентифікація	Розпізнавання голосу	Безконтактність, доступність	Чутливість до шуму, можливість імітації голосу
Біометрія поведінки	Аналіз клавіатурного почерку, ходьби	Постійний моніторинг, складність підробки	Складність впровадження, потреба в великій кількості даних

1.3 Криптографічна ідентифікація

Криптографічна ідентичність відіграє вирішальну роль в автентифікації, де вона підтверджує особу користувача або пристрою. У типовому сценарії, наприклад, при вході на захищений веб-сайт, криптографічні методи підтверджують автентичність веб-сайту і гарантують, що ваші облікові дані для входу надійно передаються у вигляді зашифрованих даних, захищаючи їх

від перехоплення або підробки.[13] Крім того, ці методи часто включають двофакторну автентифікацію, коли користувач надає додатковий доказ, наприклад, одноразовий код, надісланий на телефон, що ще більше посилює безпеку. Такий багаторівневий підхід гарантує, що навіть якщо облікові дані для входу скомпрометовані, несанкціонований доступ все одно можна запобігти, захищаючи конфіденційну інформацію користувача.

Цифрові підписи є важливим інструментом, який використовується для забезпечення цілісності та автентичності цифрового документа або повідомлення. Вони створюються за допомогою закритого ключа відправника, який функціонує як унікальний криптографічний підпис, а потім додається до документа або повідомлення.[14] Цей підпис може перевірити будь-хто, хто має доступ до відкритого ключа відправника, тим самим підтверджуючи, що повідомлення не було змінено з моменту його підписання. Крім того, цифровий підпис забезпечує неможливість відмови від нього, тобто відправник не може заперечити автентичність підписаного документа або повідомлення, що ще більше підвищує довіру та безпеку в цифровому спілкуванні.

1.4 Ідентифікація пристроїв

1.4.1 MAC – адреса

MAC-адреса (Media Access Control address) — це унікальний ідентифікатор, який присвоюється кожному мережевому інтерфейсу пристрою на рівні апаратного забезпечення. Вона є 48-бітовою адресою, яка зазвичай записується у вигляді шести пар шістнадцяткових чисел, розділених двокрапками (наприклад, 05:7J:3F:6D:2M:5P) [15].

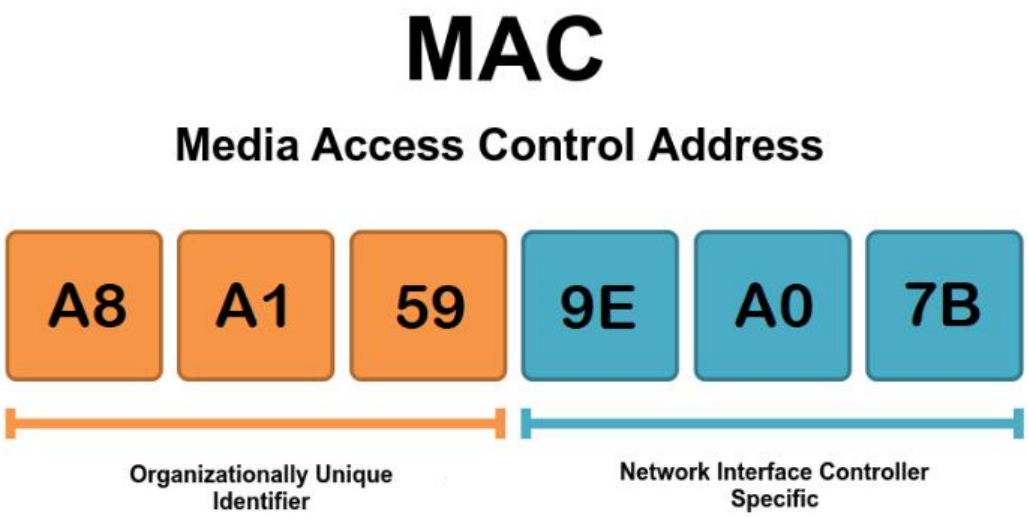

Рис. 1.2 Розшифровка адреси MAC

Основними аспектами MAC-адрес є унікальність і незмінність: MAC-адреса присвоюється виробником обладнання, що забезпечує унікальність кожного пристрою в межах локальної мережі. Вона зберігається на мережевій карті (NIC) пристрою і не змінюється за замовчуванням, хоча деякі пристрої дозволяють користувачам тимчасово її змінити. Перші три октети (перші 24 біти) позначають виробника пристрою, це частина називається Organizationally Unique Identifier (OUI). Останні три октети (останні 24 біти) використовуються для унікального ідентифікаційного номера, присвоєного пристрою виробником.

Роль у локальних мережах: MAC-адреса використовується для передачі даних на рівні каналу передачі даних у локальних мережах (LAN), таких як Ethernet. Наприклад, коли комп'ютер надсилає пакет даних в локальній мережі, він використовує MAC-адресу для того, щоб ідентифікувати конкретний пристрій-одержувач.

Безпека та контроль доступу: Оскільки MAC-адреса є унікальною, її часто використовують для контролю доступу в мережах. Адміністратори мережі можуть дозволяти або блокувати доступ до мережі на основі MAC-адреси. Однак, через можливість "підробки" або спуфінгу MAC-адреси, цей метод захисту не є абсолютним.

Одним із варіантів є метом MAC фільтрація - багато маршрутизаторів підтримують MAC-фільтрацію, що дозволяє обмежити доступ до мережі для певних пристроїв. Це пропонує додатковий рівень безпечності, але через можливість зміни MAC-адрес цей метод також має обмежену ефективність.

1.4.2 IMEI та серійні номери

IMEI (International Mobile Equipment Identity) та серійні номери — це унікальні ідентифікатори, які допомагають визначити конкретний пристрій у мережі або на рівні виробника. Вони використовуються переважно для ідентифікації мобільних пристроїв, забезпечення безпеки, та управління обладнанням.[16]

IMEI – це 15-значний номер, який присвоюється кожному мобільному пристрою, що підтримує GSM, UMTS, або LTE-мережі. Він є унікальним для кожного пристрою і не залежить від мобільного оператора чи SIM-карти.

Рис. 1.3 Наліпка з IMEI кодом пристрою

Структура IMEI:

Перші 8 цифр — це Type Allocation Code (TAC), який вказує на модель пристрою і виробника. Наступні 6 цифр — це серійний номер пристрою.

Остання цифра — це контрольна сума для перевірки правильності IMEI. IMEI допомагає операторам ідентифікувати та відстежувати пристрої, підключені до їх мережі. Наприклад, якщо телефон загублено або вкрадено, оператор може заблокувати IMEI, щоб пристрій не підключався до мобільних мереж. IMEI широко використовується для безпеки. Оператори та виробники можуть блокувати пристрої, які використовуються для шахрайства або нелегальної діяльності, шляхом додавання їх IMEI до чорного списку.

Серійні номери

Це унікальний номер, який присвоюється кожному пристрою або компоненту під час виробництва. Серійні номери дозволяють ідентифікувати конкретний екземпляр продукту, а не лише модель[17]. Серійні номери використовуються для відстеження продуктів під час виробництва,

гарантійного обслуговування, та підтримки. Вони допомагають виробникам та сервісним центрам визначити історію обслуговування, технічні характеристики, а також перевіряти справжність пристроїв, що важливо для боротьби з підробками. Серійні номери не дозволяють відстежити пристрій в мережі, але вони важливі для технічної підтримки, ремонту та захисту від шахрайства.

Різницею між IMEI та серійними номерами - IMEI є універсальним стандартом для мобільних пристроїв і використовується мобільними операторами для ідентифікації в мережі. Серійний номер є унікальним номером конкретного пристрою, який виробник використовує для власного обліку і управління, зокрема для технічного обслуговування. Обидва ідентифікатори забезпечують додаткову безпеку та контроль, але використовуються в різних цілях і на різних рівнях.

1.4.3 SIM-карти

SIM-карта (Subscriber Identity Module) — це знімний чіп, який вставляється в мобільний телефон або інший пристрій і зберігає інформацію про абонента мобільної мережі. Головна функція SIM-карти полягає у збереженні унікального ідентифікатора користувача, який дозволяє оператору мобільного зв’язку ідентифікувати абонента і надавати доступ до мережі.[18]

Основні функції SIM-карт:

Ідентифікація абонента: Зберігає унікальний номер IMSI (International Mobile Subscriber Identity), який оператори використовують для автентифікації та авторизації користувача.

Зберігання даних: Зберігає контактні дані, повідомлення та іншу важливу інформацію, хоча обсяг цих даних обмежений.

Безпека: SIM-карта захищена ПІН-кодом (PIN), що дозволяє уникнути несанкціонованого доступу, і може містити інформацію для захищених транзакцій.

1.4.4 IP адреса та User-Agent

IP-адреси та User-Agent є важливими ідентифікаторами, які допомагають розпізнавати пристрої та програмне забезпечення, що взаємодіють з мережею або веб-сайтами.

IP-адреса (Internet Protocol address) — це унікальний числовий код, який використовується для ідентифікації кожного пристрою, що підключений до мережі Інтернет. Вона забезпечує можливість обміну даними між пристроями в мережі. Розрізняють два основних типи IP-адрес: IPv4, що базується на 32-бітній системі, та IPv6, створений на основі 128-бітної архітектури для подолання обмежень попередньої версії.

IPv4: Класична версія, що складається з 32 біт і виглядає як чотири групи чисел, перечислених крапками (для прикладу - 172.189.19.5). Однак обмежена кількість комбінацій (приблизно 4,3 мільярда) спричинила потребу в новішій версії.

IPv6: Сучасніша версія, що складається зі 128 біт і дозволяє мати неймовірно велику кількість унікальних адрес[19]. IPv6 записується як вісім груп шістнадцяткових чисел, розділених двокрапками (наприклад, 2004:0xy3:47k5:0000:0000:918j:0956:1488).

Призначення IP-адрес - вказання на унікальний пристрій у мережі, що дозволяє маршрутизаторам направляти інформацію між пристроями. За IP-адресою можна визначити приблизне місце розташування користувача, хоча точність залежить від провайдера та налаштувань мережі. IP-адреси дозволяють фільтрувати доступ до ресурсів, встановлювати брандмауери та відстежувати підозрілу активність.

User-Agent

User-Agent — це рядок, який відправляє браузер або інший клієнт (наприклад, мобільний додаток) під час HTTP-запиту на сервер. Він містить інформацію про вид пристрою,систему встановлену на пристрої, версію браузера і так далі[20].

Компоненти User-Agent:

Назва та версія браузера: Вказує, яким браузером користується користувач, наприклад, "Mozilla/5.0".

Операційна система: Ідентифікує операційну систему, як-от "Windows NT 10.0" або "iPhone; CPU iPhone OS 14_0".

Тип пристрою: Може містити інформацію про тип пристрою, наприклад, "Mobile" для мобільних пристроїв або "Tablet" для планшетів.

Призначення User-Agent:

Адаптація контенту: На основі User-Agent сервер може надавати спеціалізований контент, оптимізований для конкретного браузера або пристрою.

Аналітика та статистика: User-Agent дозволяє збирати дані про типи пристроїв і браузерів, які використовують користувачі, для аналітики та покращення продукту.

Захист і безпека: User-Agent може використовуватись для виявлення аномалій або підозрілої активності, що важливо для захисту веб-додатків.

Таблиця.1.3

Порівняння інших методів ідентифікації

Тип ідентифікації	Приклади	Переваги	Недоліки
MAC-адреса	Унікальні апаратні ідентифікатори	Унікальність пристрою	Легкість підміни (спуфінгу)
IMEI та серійні номери	Номери пристроїв	Унікальність, вбудовані на рівні обладнання	Вразливість до фізичних атак або заміни
SIM-карти	GSM ідентифікатори	Унікальність, зв'язок із користувачем	Залежність від мобільного оператора
IP-адреса та User-Agent	IP-логування, дані браузера	Легкість отримання	Нестабільність IP, можливість спуфінгу

Висновки

У першому розділі було розглянуто сучасні методи ідентифікації користувачів та пристроїв, які відіграють ключову роль у забезпеченні безпеки та захисту даних у цифровому середовищі. Було проаналізовано традиційні та новітні підходи до аутентифікації, починаючи від класичних паролів до багатофакторної аутентифікації (MFA) та біометричних методів. Кожен із цих методів має свої переваги та обмеження.

Зокрема, **традиційні паролі**, хоча й залишаються найпоширенішим методом аутентифікації, поступово втрачають свою ефективність через обмеження у безпеці, що зумовлено ризиками злому та складністю запам'ятовування. Натомість одноразові паролі (OTP), а також багатофакторна

(MFA) та двофакторна (2FA) аутентифікація забезпечують додатковий рівень безпеки, знижуючи вразливість систем до несанкціонованого доступу.

Біометричні методи, такі як розпізнавання обличчя, відбитки пальців та голосова ідентифікація, через зручність стають все більш популярними та особливо, високому рівню захисту. Проте, вони також мають технічні та етичні виклики, пов'язані із забезпеченням конфіденційності та точності розпізнавання.

Крім того, було розглянуто криптографічні методи, що забезпечують надійне шифрування ідентифікаційних даних, та методи ідентифікації пристроїв, включаючи MAC-адреси, IMEI, серійні номери, SIM-карти, IP-адреси та User-Agent. Ці методи дозволяють ідентифікувати пристрої в мережі та контролювати доступ до ресурсів на основі унікальних характеристик.

Загалом, комплексний підхід до ідентифікації користувачів і пристроїв, що включає поєднання різних методів, є необхідним для забезпечення безпеки сучасних інформаційних систем. Подальший розвиток цих технологій сприятиме зменшенню ризиків уразливостей та підвищенню рівня захисту даних у цифровому середовищі.

РОЗДІЛ 2
АНАЛІЗ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Вступ до блокчейн технологій

Історія виникнення блокчейну

Блокчейн технологія виникла у 2008 році як основа для криптовалюти Bitcoin, яку представив анонімний творець під псевдонімом Сатоші Накамото. Основною метою створення Bitcoin було забезпечення децентралізованої електронної платіжної системи, яка не потребувала б центрального фінансового посередника, такого як банк або уряд. Перший блок в ланцюжку, відомий як "генезис-блок", був видобутий у січні 2009 року, започаткувавши таким чином нову еру у фінансових технологіях.[21]

Відтоді блокчейн технологія розвивалася та адаптувалася до різних сфер застосування. Спочатку вона була тісно пов'язана з криптовалютами, проте з часом її потенціал визнали у сферах управління даними, контрактами, ідентифікації та багатьох інших. У 2015 році з'явилася платформа Ethereum, яка ввела поняття смарт-контрактів, дозволяючи програмувати автоматизовані угоди та розширюючи можливості блокчейну далеко за межі фінансових транзакцій.

Сьогодні блокчейн технологія застосовується у різноманітних галузях, включаючи логістику, охорону здоров'я, державне управління та управління ідентифікацією. Її здатність забезпечувати прозорість, незмінність та децентралізацію робить її привабливою для вирішення складних задач, пов'язаних з безпекою та управлінням даними.

Основні поняття та принципи роботи

Блокчейн є розподіленою базою даних, що складається з поєднаних послідовним методом блоків, у якому кожен блок налічує набір транзакцій. Основні поняття та принципи роботи блокчейну включають:

Блок: Основна одиниця зберігання даних у блокчейні. Кожен блок містить кілька ключових елементів:

Дані транзакцій: Інформація про проведені операції.

Хеш попереднього блоку: Унікальний ідентифікатор попереднього блоку, що забезпечує зв'язок між блоками.

Хеш поточного блоку: Унікальний ідентифікатор поточного блоку, створений за допомогою криптографічного алгоритму.

Nonce: Число, яке використовується у процесі добування (майнінгу) блоку для досягнення певних умов хешу.

Ланцюжок блоків: Послідовність блоків, з'єднаних між собою хешами. Кожен новий блок посилається на попередній, створюючи незмінний запис усіх транзакцій.

Децентралізація: Блокчейн не залежить від центрального адміністративного органу. Копії блокчейну зберігаються на багатьох вузлах (комп'ютерах) у мережі, що забезпечує його стійкість до збоїв та атак.

Консенсусний механізм: Процедура, за якою всі учасники мережі погоджуються з поточним станом блокчейну. Основні механізми консенсусу включають:

Proof of Work (PoW) примушує учасників вирішувати складні обчислювальні задачі для підтвердження транзакцій та додавання нових блоків.

Proof of Stake (PoS) пропонує створення нових блоів на основі балансу власних монет учасника, що зменшує енергоспоживання порівняно з PoW.

Інші алгоритми, наприклад, **Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT)** тощо, які мають свої специфічні особливості та переваги.

Криптографія: Використовується для забезпечення безпеки даних у блокчейні. Кожен блок пов'язаний з попереднім за допомогою хеш-функції, що робить зміну будь-якого блоку без виявлення майже неможливою.

Незмінність: Після додавання блоку до блокчейну його дані не можуть бути змінені або видалені без зміни всіх наступних блоків, що практично робить блокчейн незмінним.

Прозорість: Усі операції, що зберігаються в блокчейні, відкриті для перегляду всім учасникам мережі, що сприяє підвищенню рівня довіри та забезпечує максимальну відкритість процесів.

2.2 Архітектура та компоненти блокчейну

Структура блоку

Отже, блокчейн формується з блоків, і кожен блок – це як сторінка в книзі, де записуються всі транзакції. Давайте розберемо, що саме знаходиться в одному блоці:

Дані транзакцій: Це, по суті, записи про всі операції, які відбулися. Наприклад, у криптовалютах це можуть бути перекази біткоїнів між користувачами.

Хеш попереднього блоку: Уявіть, що кожен блок має свій унікальний код, який називається хешем. Хеш попереднього блоку додається до нового блоку, щоб вони були пов’язані між собою. Це як посилання на попередню сторінку в книзі[22].

Хеш поточного блоку: Це свій власний унікальний код для цього блоку, який створюється за допомогою спеціального алгоритму. Він забезпечує цілісність даних у блоці.

Nonce: Це просто число, яке майнери використовують для того, щоб знайти правильний хеш. Процес пошуку цього числа називається майнінгом і він потрібен для підтвердження блоків.

Мережеві моделі

Блокчейн працює в мережі, яка складається з багатьох комп'ютерів, або вузлів. Є декілька типів мережевих моделей, які використовуються в блокчейні:

Розподілена мережа: У цій моделі кожен вузол має копію всього блокчейну. Це підвищує рівень надійності і стійкості до збоїв, бо немає єдиного центру, який може відмовити.

Пірингові протоколи: Тут кожен вузол підключається до декількох інших вузлів, створюючи мережу "пірінгу". Це дозволяє ефективно поширювати інформацію між усіма учасниками.

Механізми консенсусу

Консенсусний механізм – це спосіб, за яким всі учасники мережі погоджуються з тим, які блоки додавати до ланцюга. Є кілька різних методів консенсусу:

Proof of Work (PoW): Це найвідоміший механізм, який використовує, наприклад, Bitcoin. У PoW майнери змагаються, щоб розв'язати складну математичну задачу. Той, хто першим знайде рішення, отримує право додати новий блок і отримати винагороду. Цей процес потребує багато обчислювальної потужності та енергії.

Proof of Stake (PoS): Цей метод менш енерговитратний. Тут право створювати нові блоки залежить від кількості монет, які володіє учасник. Чим більше монет – тим більше шансів стати валідатором блоку. Це робить PoS більш екологічно дружнім варіантом.

Як це все працює разом

Уявіть собі блокчейн як дуже безпечну та прозору книгу записів, де кожен новий запис пов'язаний з попереднім. Коли хтось хоче додати новий блок, мережа використовує один з механізмів консенсусу, щоб переконатися, що цей блок є дійсним і відповідає правилам мережі. Потім блок додається до ланцюга, і всі вузли оновлюють свої копії блокчейну.

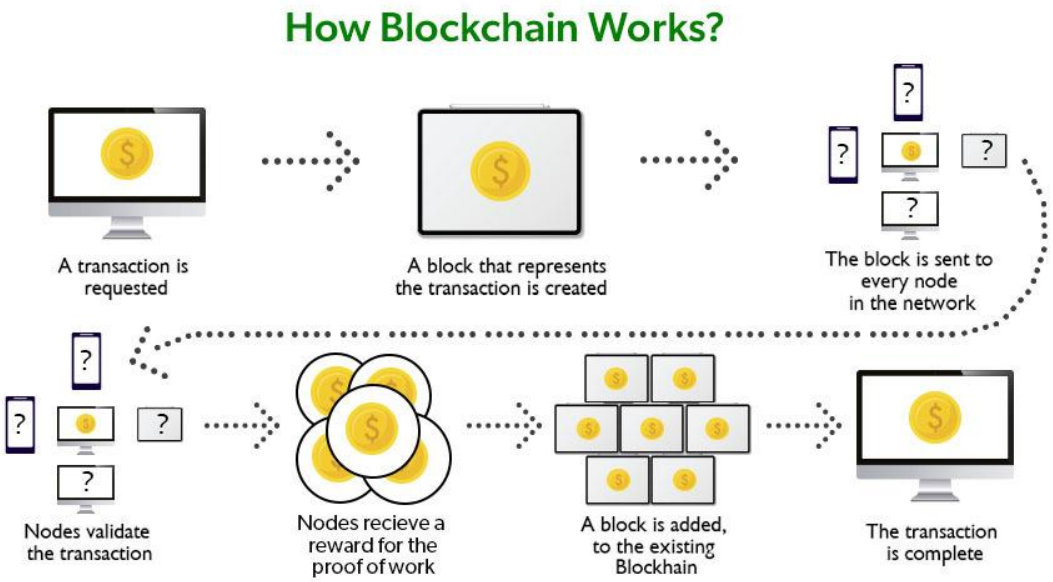

Рис. 2.1 Схема роботи технології блокчейн

Завдяки криптографії та механізмам консенсусу змінити інформацію в блокчейні практично неможливо без контролю над більшістю мережі. Всі транзакції відкриті і можуть бути перевірені будь-яким учасником мережі.

Відсутність єдиної точки контролю робить блокчейн стійким до збоїв і атак.

2.3 Типи блокчейнів та їх характеристика

Коли ми говоримо про блокчейн, важливо розуміти, що існують різні його типи, кожен з яких має свої унікальні особливості та підходить для

певних завдань. Найпоширенішими є **публічні**, **приватні** та **консорціумні** блокчейни, а також гібридні та спеціалізовані варіанти.

Публічний блокчейн є найвідомішим типом, до якого належать такі криптовалюти, як Bitcoin та Ethereum. Основною характеристикою публічного блокчейну є відкритий доступ: кожен охочий може долучитися до мережі, брати участь у перевірці транзакцій і додавати нові блоки до блокчейну.

Це забезпечує високу ступінь децентралізації, оскільки немає централізованого контролю, а всі користувачі рівноправні між собою. Прозорість також є важливою рисою публічних блокчейнів – всі транзакції доступні для перегляду кожному користувачу мережі. Однак ця відкритість призводить до певних недоліків, таких як низька швидкість транзакцій через складні механізми консенсусу та високе енергоспоживання, особливо при використанні Proof of Work (PoW)[23].

Приватний блокчейн створюється для обмеженого кола учасників, наприклад, в межах однієї компанії або групи організацій. Основна відмінність приватного блокчейну полягає в обмеженому доступі: лише запрошені учасники можуть долучатися до мережі та брати участь у верифікації транзакцій. Це забезпечує більший контроль над мережею і підвищує конфіденційність даних, оскільки транзакції можуть бути приховані від зовнішніх спостерігачів. Приватні блокчейни зазвичай управляються однією організацією або групою організацій, що дозволяє досягати вищої швидкості транзакцій та ефективності. Однак менша ступінь децентралізації може знижувати рівень безпеки, і мережа стає залежною від довіри до центрального органу управління.

Консорціумний блокчейн представляє собою гібрид між публічним та приватним блокчейнами, де мережею управляє група організацій замість однієї. Це означає, що лише довірені організації можуть бути учасниками

мережі, що забезпечує баланс між децентралізацією та контролем. Консорціумні блокчейни дозволяють спільно керувати мережею та приймати рішення щодо її розвитку, що покращує масштабованість і швидкість транзакцій завдяки обмеженій кількості учасників. Однак для успішного функціонування консорціумного блокчейну необхідний високий рівень співпраці та довіри між учасниками, а також може бути менш прозорим порівняно з публічними блокчейнами.

Гібридні блокчейни поєднують елементи як публічних, так і приватних блокчейнів, що дозволяє організаціям контролювати доступ до певних частин мережі, залишаючи інші частини відкритими для громадськості. Це надає гнучкість у налаштуванні доступу та управління даними, дозволяючи використовувати переваги обох типів блокчейнів. Однак гібридні блокчейни мають складнішу архітектуру та управління, що може вимагати більше ресурсів для підтримки та забезпечення безпеки.

Окрім основних типів, існують також спеціалізовані блокчейни, розроблені для конкретних задач, такі як управління ідентифікацією користувачів та пристроїв. Наприклад, платформа Sovrin орієнтована на цифрову ідентичність, дозволяючи користувачам контролювати свої власні ідентифікаційні дані. Спеціалізовані блокчейни оптимізовані для виконання конкретних завдань, що підвищує їх ефективність, але одночасно обмежує універсальність використання, оскільки вони призначені для вузького кола завдань і залежать від підтримки та розвитку конкретними організаціями або спільнотами.

Розуміння різних типів блокчейнів є важливим кроком у виборі найкращого рішення для управління ідентифікацією користувачів та пристроїв. Кожен тип блокчейну має свої сильні та слабкі сторони, і вибір залежить від конкретних вимог та цілей проєкту. Публічні блокчейни

забезпечують високу прозорість та безпеку, але можуть бути менш ефективними для корпоративних потреб. Приватні та консорціумні блокчейни пропонують більший контроль та швидкість, але вимагають довіри між учасниками. Гібридні та спеціалізовані блокчейни надають додаткову гнучкість та оптимізацію для специфічних завдань, таких як управління ідентифікацією.

2.4 Смарт контракти та їх роль

Смарт-контракти стали справжнім проривом у світі блокчейн технологій, і їх роль у управлінні ідентифікацією не можна недооцінювати. Але що ж таке смарт-контракти і як вони допомагають у цьому процесі?

Смарт-контракти можна уявити як автоматизовані угоди, які виконуються самі собою, коли виконуються певні умови. Вони працюють на блокчейні, що забезпечує їх високий рівень безпеки. Уявіть, що вам потрібно підтвердити ідентичність користувача або пристрою – смарт-контракт може зробити це автоматично, без потреби втручання людини[24].

Однією з основних переваг смарт-контрактів є їхня можливість автоматично виконувати процеси перевірки особи та надання доступу. Наприклад, коли користувач намагається отримати доступ до певного ресурсу, смарт-контракт може автоматично перевірити його ідентифікаційні дані та вирішити, чи надати доступ. Це робить процес швидшим та зменшує ризик помилок або зловживань.

Крім того, смарт-контракти забезпечують високий рівень безпеки. Оскільки вони працюють на блокчейні, всі умови контракту є прозорими і доступними для перевірки всіма учасниками мережі. Це означає, що ніхто не може змінити умови контракту після його створення, що забезпечує довіру між сторонами.

Ще одна важлива особливість смарт-контрактів – їхня здатність взаємодії з посторонніми блокчейн-додатками. Наприклад, смарт-контракт для управління ідентифікацією може інтегруватися з іншими системами, такими як бази даних користувачів або системи управління доступом, створюючи єдину, безпечну екосистему для управління ідентичністю.

Використання смарт-контрактів у управлінні ідентифікацією також сприяє мінімізації витрат і підвищенню ефективності. Автоматизація процесів означає меншу потребу в ручній роботі та менше можливостей для помилок. Крім того, зменшується залежність від посередників, що також може знизити витрати.

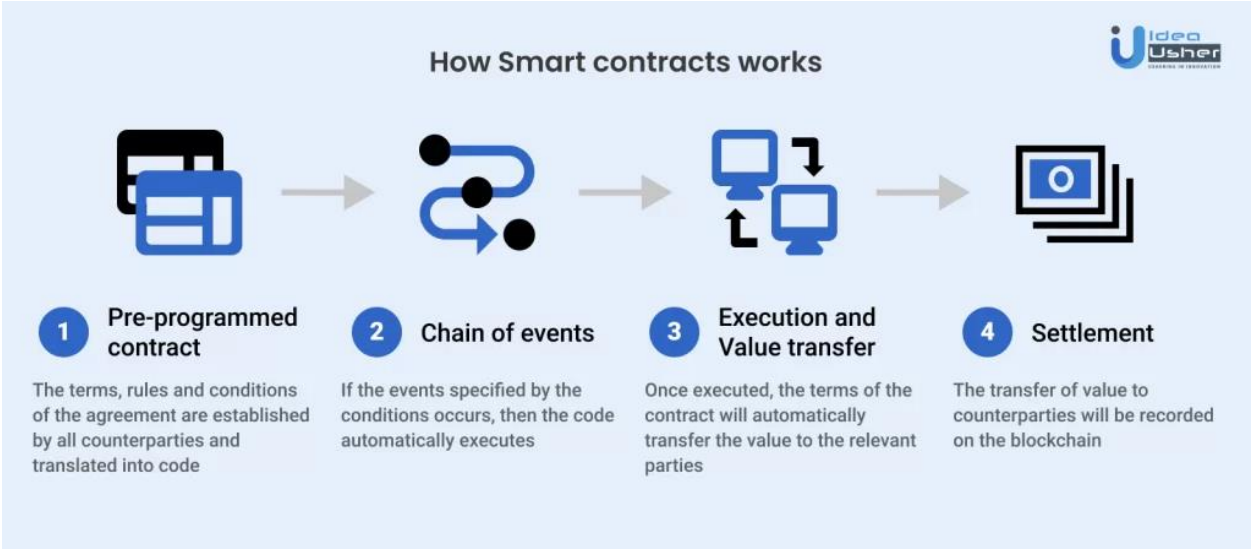

Рис. 2.2 Приклад роботи смарт-контрактів

Наприклад, у системах децентралізованої ідентифікації, таких як ті, що пропонуються платформою uPort або Microsoft Identity Overlay Network, смарт-контракти відіграють ключову роль у забезпеченні безпеки над ідентифікаційними даними користувачів. Вони дозволяють користувачам самостійно керувати своїми даними, визначати, хто має доступ до них, і автоматично контролювати ці процеси без потреби в центральному органі.

Смарт-контракти також відкривають нові можливості для інновацій у сфері управління ідентифікацією. Наприклад, вони можуть у створенні комплексних систем автентифікації, які адаптуються до змінних умов або ризиків. Такі системи можуть автоматично змінювати рівень безпеки або вимоги до ідентифікації в залежності від контексту, забезпечуючи більш гнучкий та ефективний підхід до управління ідентичністю.

2.5 Приватність та захист даних у блокчейні

Однією з найважливіших переваг блокчейн технології є її здатність забезпечувати високий рівень приватності та захисту даних. У традиційних централізованих системах управління ідентифікацією дані користувачів зберігаються на центральних серверах, що робить їх вразливими до атак, витоків інформації та зловживань. Блокчейн, навпаки, розподіляє ці дані по всій мережі, що значно підвищує їхню безпеку.

Приватність у блокчейні досягається за рахунок використання складних криптографічних методів. Кожен користувач має свій унікальний криптографічний ключ, який використовується для підпису транзакцій та доступу до їхніх даних. Це означає, що навіть якщо хтось отримує доступ до блокчейну, він не зможе легко ідентифікувати конкретного користувача без знання його приватного ключа[25].

Крім того, блокчейн дозволяє застосовувати різні методи анонімізації даних. Наприклад, використання псевдонімів дозволяє зберігати ідентифікаційні дані користувачів прихованими від загального доступу, забезпечуючи при цьому можливість підтвердження їхньої автентичності. Такі технології, як zero-knowledge proofs, дозволяють доводити достовірність

певних даних без розкриття самих даних, що додатково підвищує рівень приватності.

Захист даних у блокчейні також забезпечується завдяки його децентралізації. Оскільки копії блокчейну зберігаються на багатьох вузлах мережі, немає єдиного місця, яке можна було б атакувати або зламати, щоб отримати доступ до всіх даних. Навіть якщо декілька вузлів будуть скомпрометовані, решта мережі залишаться захищеними, що робить блокчейн надзвичайно стійким до різних видів кіберзагроз.

Важливо також зазначити, що блокчейн може відповідати сучасним регуляторним вимогам захисту даних, наприклад «Загальний регламент про захист даних (GDPR)» в Європейському Союзі. Наприклад, хоча блокчейн за своєю природою є незмінним, існують рішення, які дозволяють управляти особистими даними таким чином, щоб забезпечити їхню відповідність праву на забуття. Це досягається шляхом зберігання особистих даних за межами блокчейну або використання механізмів шифрування, які дозволяють контролювати доступ до цих даних.

Крім криптографічних методів, блокчейн забезпечує додатковий рівень безпеки через використання консенсусних механізмів. Наприклад, у системах з Proof of Work (PoW) або Proof of Stake (PoS) транзакції підтверджуються багатьма учасниками мережі, що ускладнює можливість фальсифікації або маніпулювання даними. Це особливо важливо у контексті управління ідентифікацією, де точність і достовірність даних є критично важливими.

Також варто відзначити, що блокчейн підтримує прозорість процесів управління ідентифікацією. Кожен користувач може самостійно перевірити свої дані та транзакції, що підвищує рівень довіри до системи. Проте при цьому забезпечується конфіденційність завдяки анонімізації та шифруванню даних.

2.6 Інтеграція блокчейну з існуючими системами управління ідентифікацією

Інтеграція блокчейн-технологій з традиційними системами управління ідентифікацією є важливим кроком для переходу до більш децентралізованих та безпечних рішень. Цей процес включає поєднання переваг централізованих систем, таких як LDAP або Active Directory, з децентралізованими можливостями блокчейну, що дозволяє покращити безпеку, прозорість та контроль над ідентифікаційними даними [26].

Роль Web3 у інтеграції блокчейну

Web3, або децентралізована веб-інфраструктура, є важливою складовою сучасних блокчейн-рішень. Вона забезпечує основу для створення децентралізованих додатків (dApps), які можуть ефективно інтегруватися з існуючими системами управління ідентифікацією. Web3 дозволяє користувачам взаємодіяти з блокчейном через браузери або спеціальні додатки, використовуючи криптографічні ключі для аутентифікації та авторизації[27].

Наприклад, за допомогою Web3 можна створювати інтерфейси, які дозволяють користувачам легко підключати свої ідентифікаційні дані до блокчейну, забезпечуючи при цьому зручний доступ до централізованих та децентралізованих сервісів. Це сприяє плавному переходу від традиційних систем до нових, більш безпечних та прозорих блокчейн-рішень.

Технічні аспекти інтеграції

Для інтеграції блокчейну з традиційними системами управління ідентифікацією часто використовуються API (Application Programming Interface) та шлюзи, які дозволяють обмінюватися даними між централізованою системою та блокчейн-мережею. Web3 забезпечує

інструменти та бібліотеки, такі як Web3.js, які спрощують процес взаємодії між фронтендом додатків та блокчейном.

Крім того, важливо враховувати сумісність протоколів та форматів даних. Для цього можуть використовуватися адаптери або транслятори, які перетворюють дані з одного формату в інший без втрати інформації. Наприклад, дані з Active Directory можуть бути конвертовані у формат, придатний для запису в блокчейн, забезпечуючи консистентність та актуальність інформації.

Виклики та рішення

Одним із основних викликів при інтеграції блокчейну з існуючими системами є питання масштабованості. Блокчейн-мережі, особливо публічні, можуть мати обмежену пропускну здатність, що ускладнює обробку великої кількості транзакцій, характерних для великих організацій. Web3 дозволяє використовувати гібридні архітектури, де критичні дані зберігаються на блокчейні, а менш важливі – у централізованих системах, забезпечуючи баланс між безпекою та ефективністю.

Іншим викликом є питання сумісності протоколів та форматів даних. Для подолання цього можна використовувати стандартизацію даних та розробку уніфікованих API, що дозволяють різним системам взаємодіяти без необхідності кардинальних змін у їхній архітектурі.

Приклади успішної інтеграції

Проєкти, такі як IBM Hyperledger та Microsoft Azure Active Directory, демонструють успішну інтеграцію блокчейн-технологій з існуючими системами управління ідентифікацією. Hyperledger пропонує інструменти для створення приватних блокчейн-мереж, які можуть бути легко інтегровані з корпоративними системами управління ідентифікацією через API та шлюзи.

Це дозволяє організаціям використовувати переваги блокчейну, зберігаючи при цьому існуючу інфраструктуру.

Microsoft Azure Active Directory підтримує інтеграцію з блокчейн-технологіями через різні API та шлюзи, що дозволяє підприємствам використовувати децентралізовані механізми управління ідентифікацією разом з централізованими сервісами, забезпечуючи більшу гнучкість та безпеку.

Гібридні архітектури

Гібридні архітектури є перспективним напрямком інтеграції блокчейну з існуючими системами управління ідентифікацією. У таких архітектурах блокчейн використовується для зберігання критичних даних та забезпечення їхньої незмінності та безпеки, тоді як централізовані системи продовжують обробляти менш чутливі дані та виконувати повсякденні операції. Web3 забезпечує необхідні інструменти для створення таких гібридних систем, дозволяючи ефективно поєднувати переваги обох підходів.

2.7. Стандарти та протоколи управління ідентифікацією в блокчейні

У сфері управління ідентифікацією на блокчейні існує низка стандартів та протоколів, які сприяють забезпеченню сумісності, безпеки та ефективності систем. Ці стандарти визначають, як ідентифікаційні дані створюються, зберігаються, обмінюються та верифікуються у децентралізованих середовищах.

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) є однією з основних технологій для децентралізованої ідентифікації. Вони дозволяють користувачам створювати унікальні, незмінні ідентифікатори, які не залежать від централізованих

організацій. DIDs забезпечують більший контроль користувачів над їхніми особистими даними та дозволяють безпечно обмінюватися ідентифікаційною інформацією між різними сервісами [28].

Verifiable Credentials

Verifiable Credentials (VCs) – це стандартизований спосіб надання та перевірки ідентифікаційних даних. Вони дозволяють створювати довірені цифрові сертифікати, які можуть бути легко перевірені іншими сторонами без необхідності звертатися до первинного джерела даних. Стандарт W3C для Verifiable Credentials забезпечує сумісність між різними системами та платформами, що полегшує інтеграцію блокчейн-рішень у існуючі інфраструктури.

OAuth та OpenID Connect у контексті блокчейну

OAuth та OpenID Connect – це популярні протоколи для аутентифікації та авторизації, які можуть бути адаптовані для роботи з блокчейн-середовищами. Вони дозволяють користувачам надавати доступ до своїх даних без розкриття паролів, використовуючи криптографічні ключі та токени доступу. Це забезпечує безпечний та ефективний спосіб управління доступом у децентралізованих системах.

Interoperability Standards

Сумісність між різними блокчейн-платформами є ключовим аспектом для створення єдиної екосистеми управління ідентифікацією. Стандартизація протоколів обміну даними та взаємодії між різними блокчейнами дозволяє створювати інтегровані рішення, які працюють незалежно від конкретної платформи. Це сприяє більш широкому прийняттю блокчейн-технологій у сфері управління ідентифікацією та забезпечує їхню масштабованість.

2.8. Правові та регуляторні аспекти використання блокчейну для управління ідентифікацією

Використання блокчейн-технологій для управління ідентифікацією користувачів та пристроїв приносить значні переваги, такі як підвищена безпека, прозорість та децентралізація. Однак разом із цими перевагами виникають і численні правові та регуляторні виклики, які необхідно враховувати для успішного впровадження таких систем.

Відповідність законодавству про захист даних

Одним із ключових аспектів є відповідність систем управління ідентифікацією на базі блокчейну чинним законодавчим вимогам щодо захисту персональних даних. Наприклад, Загальний регламент про захист даних (GDPR) в Європейському Союзі вводить жорсткі вимоги до збору, обробки та зберігання персональних даних, забезпечуючи високий рівень конфіденційності та безпеки. Блокчейн, за своєю природою, є незмінним та децентралізованим, що може ускладнити дотримання таких вимог, як право на видалення даних (право на забуття)[25].

Для забезпечення відповідності GDPR та подібним регуляціям, розробники систем управління ідентифікацією можуть використовувати такі підходи:

Зберігання персональних даних поза блокчейном: Блокчейн може використовуватися для зберігання лише хешів або посилань на дані, що зберігаються в централізованих або розподілених базах даних.

Використання шифрування: Персональні дані можуть бути зашифровані перед записом у блокчейн, що забезпечує їхню конфіденційність.

Механізми контролю доступу: Впровадження смарт-контрактів для управління доступом до даних дозволяє користувачам самостійно контролювати, хто має доступ до їхніх ідентифікаційних даних.

Юридичний статус смарт-контрактів

Смарт-контракти, які активно використовуються у системах управління ідентифікацією на блокчейні, також підлягають юридичному регулюванню. У багатьох країнах законодавство ще не повністю визначило статус смарт-контрактів, що створює певні невизначеності щодо їхньої законності та можливостей правового захисту.

Для вирішення цих питань важливо:

Уточнювати юридичний статус: Вивчати місцеве законодавство щодо смарт-контрактів та враховувати його при розробці блокчейн-рішень.

Використовувати юридично перевірені шаблони: Розробка смарт-контрактів на основі юридично перевірених стандартів може допомогти забезпечити їхню відповідність законодавству.

Співпрацювати з юристами: Залучення юридичних експертів на ранніх етапах розробки систем управління ідентифікацією допоможе уникнути потенційних правових ризиків.

Регуляторні вимоги до децентралізованих систем

Децентралізовані системи управління ідентифікацією на блокчейні часто стикаються з регуляторними вимогами, що передбачають наявність центрального контролю або відповідальних осіб за обробку даних. Оскільки блокчейн-технології прагнуть усунути необхідність у центральних посередниках, це може створювати труднощі при дотриманні таких вимог.

Можливі шляхи вирішення:

Використання гібридних моделей: Поєднання децентралізованих блокчейн-рішень з централізованими елементами може допомогти відповідати регуляторним вимогам.

Розробка нових нормативів: Співпраця з регуляторами для створення нормативної бази, яка враховує особливості блокчейн-технологій.

Підвищення прозорості: Забезпечення високого рівня прозорості процесів управління ідентифікацією може сприяти довірі з боку регуляторів.

Захист інтелектуальної власності

Інтеграція блокчейну у системи управління ідентифікацією також потребує врахування питань захисту інтелектуальної власності. Наприклад, алгоритми консенсусу, смарт-контракти та інші компоненти блокчейн-систем можуть бути об'єктами патентування або авторського права.

Важливо:

Захищати власні розробки: Подавати патенти або реєструвати авторські права на інноваційні рішення, що використовуються у системах управління ідентифікацією.

Дотримуватися ліцензійних угод: Використовувати відкриті стандарти та ліцензії, що дозволяють інтеграцію з іншими системами без порушення прав інтелектуальної власності.

Уважно вивчати ліцензійні умови: Перед впровадженням сторонніх рішень переконатися, що їх ліцензійні умови відповідають вимогам вашої системи.

Кібербезпека та відповідальність

Використання блокчейн-технологій для управління ідентифікацією вимагає суворого дотримання стандартів кібербезпеки. Регулятори можуть вимагати впровадження певних заходів безпеки, а також визначення відповідальності за можливі порушення.

Основні аспекти:

Впровадження стандартів безпеки: Використання міжнародних стандартів кібербезпеки, таких як ISO/IEC 27001, для захисту даних.

Визначення відповідальності: Чітке визначення відповідальності за управління та захист ідентифікаційних даних у рамках блокчейн-систем.

Регулярні аудити та перевірки: Проведення регулярних аудиторських перевірок безпеки систем управління ідентифікацією на блокчейні для виявлення та усунення потенційних загроз.

Висновки

У другому розділі магістерської роботи було детально розглянуто блокчейн технології та їхнє застосування в управлінні ідентифікацією користувачів та пристроїв. Починаючи з основних понять та історії виникнення блокчейну, було показано, як ця технологія еволюціонувала від створення криптовалют до широкого спектру застосувань у різних галузях, включаючи безпеку та управління даними.

Архітектура та компоненти блокчейну були проаналізовані з акцентом на структурі блоків, механізмах консенсусу та криптографічних методах, що забезпечують безпеку та незмінність даних. Огляд різних типів блокчейнів – публічних, приватних, консорціумних, гібридних та спеціалізованих – дозволив зрозуміти їхні специфічні характеристики та переваги у контексті управління ідентифікацією.

Особлива увага була приділена смарт-контрактам, які відіграють ключову роль у автоматизації процесів аутентифікації та авторизації, забезпечуючи високу безпеку та ефективність систем управління ідентифікацією. Розглянуті методи приватності та захисту даних демонструють, як блокчейн може забезпечувати конфіденційність

користувачів, водночас відповідаючи вимогам сучасних регуляторних стандартів, таких як GDPR.

Інтеграція блокчейну з існуючими системами управління ідентифікацією показала можливості поєднання централізованих та децентралізованих підходів, використовуючи інструменти Web3 та гібридні архітектури для досягнення оптимальної сумісності та масштабованості. Стандарти та протоколи управління ідентифікацією, такі як Decentralized Identifiers (DIDs) та Verifiable Credentials, були розглянуті як ключові елементи, що забезпечують сумісність та ефективну взаємодію між різними блокчейн-платформами.

Правові та регуляторні аспекти використання блокчейну для управління ідентифікацією висвітлили необхідність відповідності законодавчим вимогам, забезпечення захисту інтелектуальної власності та впровадження заходів кібербезпеки. Це підкреслює важливість тісної співпраці з юридичними експертами та регуляторами для успішного впровадження блокчейн-рішень у сфері управління ідентифікацією.

Загалом, розділ 2 підтвердив, що блокчейн технології мають значний потенціал для покращення систем управління ідентифікацією користувачів та пристроїв завдяки своїм унікальним властивостям, зокрема децентралізації, незмінності інформації, підвищеній безпеці та прозорості. Водночас, успішне впровадження таких рішень вимагає врахування технічних, стандартних та правових аспектів, що забезпечить їхню ефективність та відповідність сучасним вимогам.

РОЗДІЛ 3
ЗАСТОСУВАННЯ БЛОКЧЕЙН ТЕХНОЛОГІЇ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ТА ПРИСТРОЇВ

3.1 Теоретичні відомості

У цьому підпункті буде розглянуто ключові інструменти та технології, які буде використано для розробки та розгортання додатку для ідентифікації користувачів та пристроїв, зокрема Truffle, Solidity, Ganache, MetaMask, Web3.js, Create React App**.**

Truffle

Truffle — це фреймворк для розробки смарт-контрактів, який спрощує весь життєвий цикл розробки блокчейн-додатків. Він надає потужні інструменти для компіляції, розгортання, тестування та налагодження смарт-контрактів.

Основні компоненти Truffle:

Компіляція контрактів: Автоматичне перетворення Solidity-коду в байт-код, який виконується в Ethereum Virtual Machine (EVM).

Міграції: Сценарії для розгортання контрактів на блокчейні, що дозволяють керувати різними версіями та оновленнями.

Тестування: Можливість писати тести для смарт-контрактів на JavaScript або TypeScript з інтеграцією популярних бібліотек для тестування (наприклад, Mocha).

Консоль: Інтерактивне середовище для взаємодії з розгорнутими контрактами.

Truffle значно полегшує процес розробки, дозволяючи зосередитися на логіці контрактів та інтеграції з фронтендом.

Solidity — це мова програмування, спеціально розроблена для створення смарт-контрактів, які виконуються на блокчейні Ethereum. Основні особливості Solidity:

Синтаксис, схожий на JavaScript, C++ або Python, що робить її зрозумілою для розробників з досвідом у цих мовах.

Статична типізація: Змінні мають визначений тип, що дозволяє уникати помилок на етапі компіляції.

Управління пам’яттю: Solidity використовує storage, memory та calldata для ефективного управління даними.

Події: Смарт-контракти можуть викликати події, які слухаються додатками поза блокчейном.

Ganache — це локальний блокчейн-симулятор, який дозволяє розробникам тестувати та налагоджувати свої смарт-контракти в середовищі, максимально наближеному до реального. Основними перевагами Ganache є швидке тестування без необхідності підключення до публічних мереж, підтримка декількох облікових записів з початковими балансами та детальний лог транзакцій, що дозволяє відслідковувати кожен крок виконання контракту.

Ganache ідеально підходить для тестування інтеграції між смарт-контрактами та веб-додатками.

MetaMask — це розширення для браузерів на базі рушія Chromium, яке виконує роль Ethereum-гаманця. Воно забезпечує зручну взаємодію з блокчейн-додатками безпосередньо через браузер. Основна функція MetaMask — це підписання транзакцій: користувач отримує сповіщення і підтверджує операції, які ініціюються додатками. Крім цього, MetaMask дозволяє управляти кількома гаманцями, кожен із яких може бути пов’язаний як із основною мережею Ethereum, так і з локальними або тестовими блокчейнами, наприклад, через Ganache.

Web3.js — це JavaScript-бібліотека, яка надає інструменти для взаємодії з Ethereum-блокчейном. Вона використовується для виконання таких завдань, як підключення до смарт-контрактів, відправлення транзакцій та отримання даних із блокчейна. У вашому проєкті Web3.js використовується для роботи з контрактом Auth. З її допомогою можна підключатися до контракту та викликати його функції. Це дозволяє легко інтегрувати функціонал блокчейна у додатки, забезпечуючи доступ до даних та функцій смарт-контрактів.

Create React App — це офіційний інструмент, розроблений командою React, який спрощує процес створення нових проєктів на основі бібліотеки React. Він автоматично налаштовує всі необхідні конфігурації, такі як Webpack та Babel, що дозволяє розробникам зосередитися на написанні коду без витрат часу на складні налаштування середовища. Для демонстрації цього додатку був використаний конкретно він.

3.2 Підготовка до запуску додатку

Для компіляції та запуску нам знадобиться встановити досить багато програм, які потрібно налаштувати перед тим як приступити до презентації роботи програми.

Першим етапом буде завантаження середовища для запуску (IDE). Можна вибрати або Visual Studio Code, або Remix Project. Вони підтримують потрібні нам мови програмування.

Далі нам треба завантажити та встановити Node Package Manager — це керувальник пакетів для мови програмування JavaScript.

Далі у середовищі, де ми запускаємо програму, треба відкрити консоль і прописати команду:

npm i

Команда **npm i** (або **npm install**) виконує встановлення залежностей на основі наведеного файлу **package.json**

Ось що буде встановлено:

@emotion/react та **@emotion/styled**: Для стилізації компонентів.

@mui/пакети: Компоненти Material-UI для створення сучасного UI.

react, react-dom: Бібліотека React і DOM-рендеринг.

react-router-dom: Для управління маршрутизацією в додатку.

react-scripts: Сценарії, які підтримують інструменти CRA (Create React App).

truffle: Інструмент для управління та тестування смарт-контрактів.

web3: Бібліотека для взаємодії з блокчейном Ethereum.

Далі встановлені залежності завантажуються у папку **node_modules**.

Також створюється файл **package-lock.json**, який фіксує точні версії встановлених пакетів для забезпечення стабільності збірки.

Далі ми завантажуємо додаток Ganache з офіційного сайту та встановлюємо:

https://archive.trufflesuite.com/ganache/

Далі при відкритті натискаємо кнопку “QUICKSTART”. Ця кнопка автоматично створює локальну мережу з існуючого шаблону.

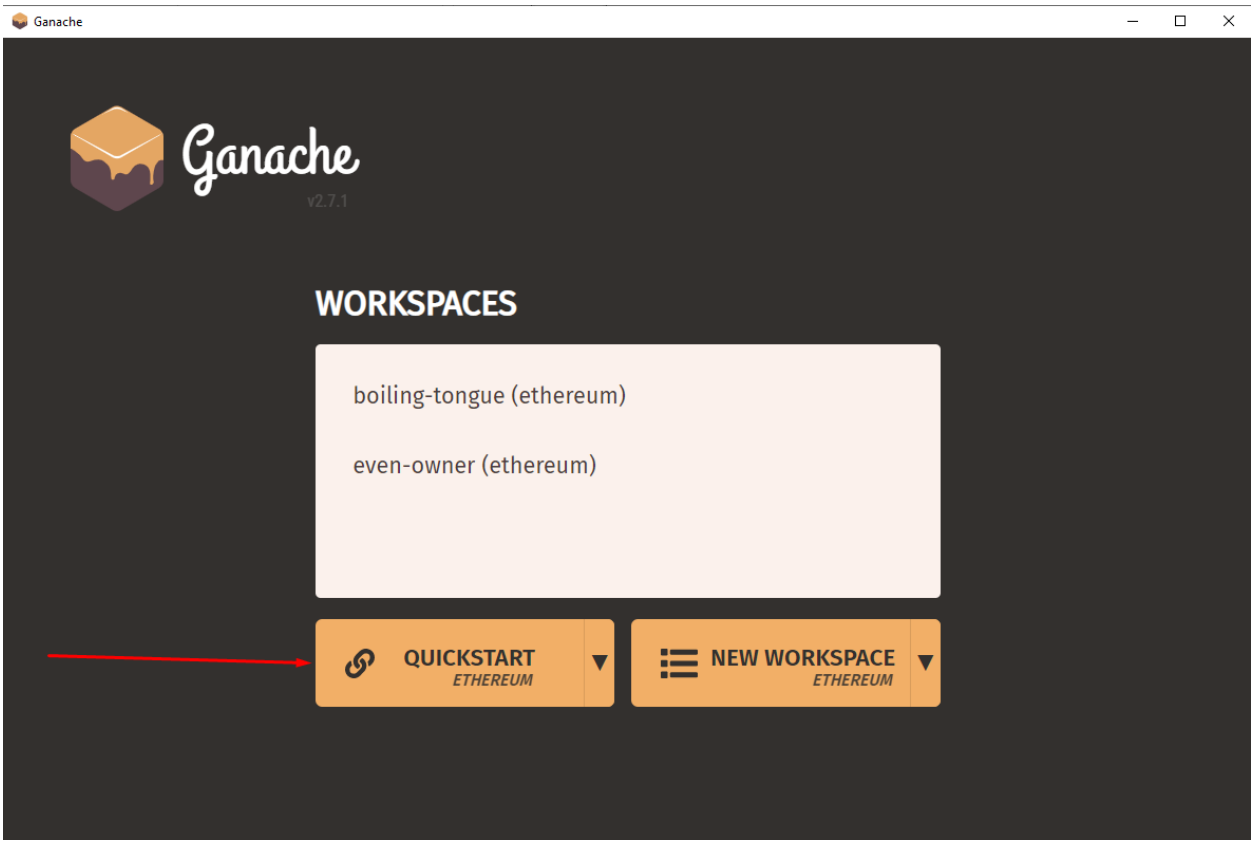

Рис 3.1 Початковий екран додатку Ganache

Далі переходимо в налаштування, натиснувши на шестерню зверху справа у вікні – вона веде до налаштувань програми.

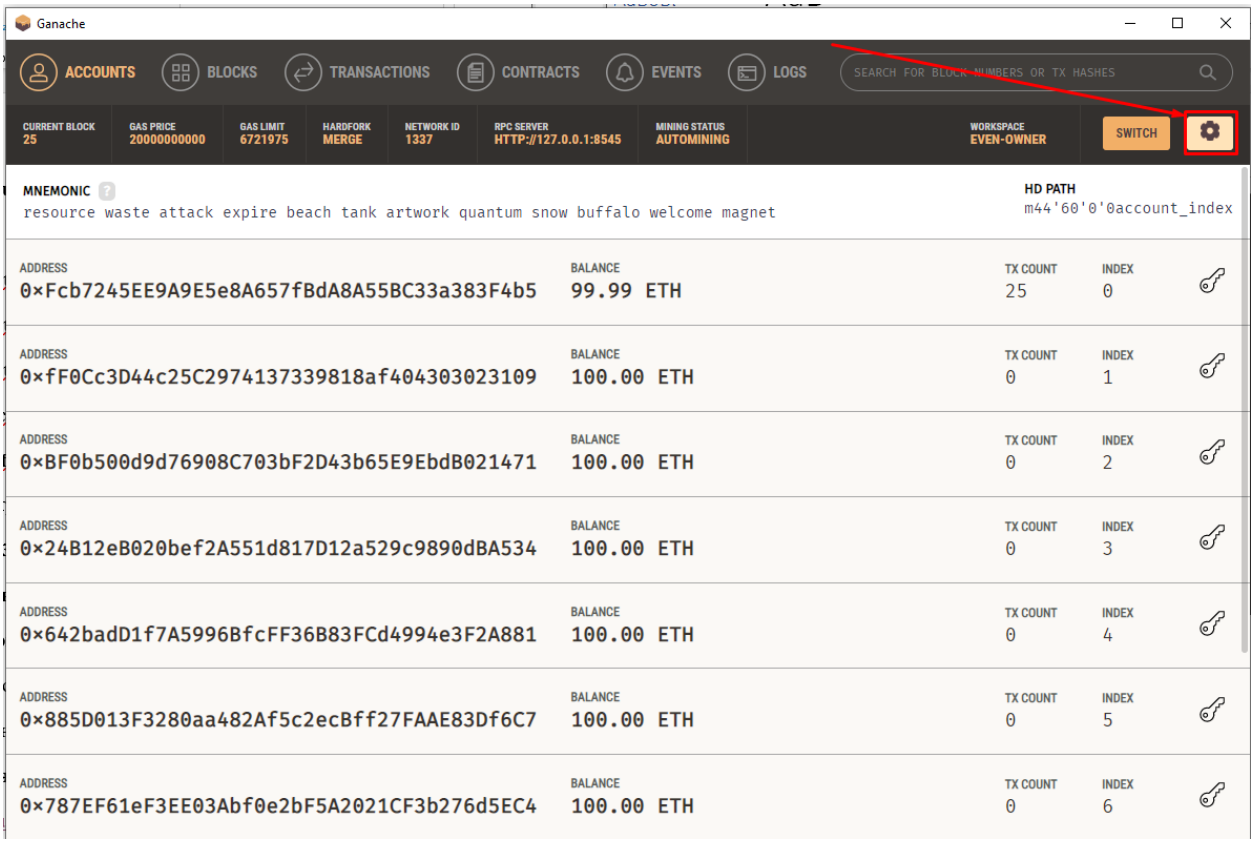

Рис 3.2 Головний екран додатку Ganache

Тут ми змінюємо параметри, як вказано на фото:

Переходимо на вкладку сервер, вказуємо Port Number на 8545 та Network ID на «1337» та натискаємо кнопку Restart. Такі числа ми встановлюємо через конфліктність GUI налаштувань програми та CLI начинки програми.

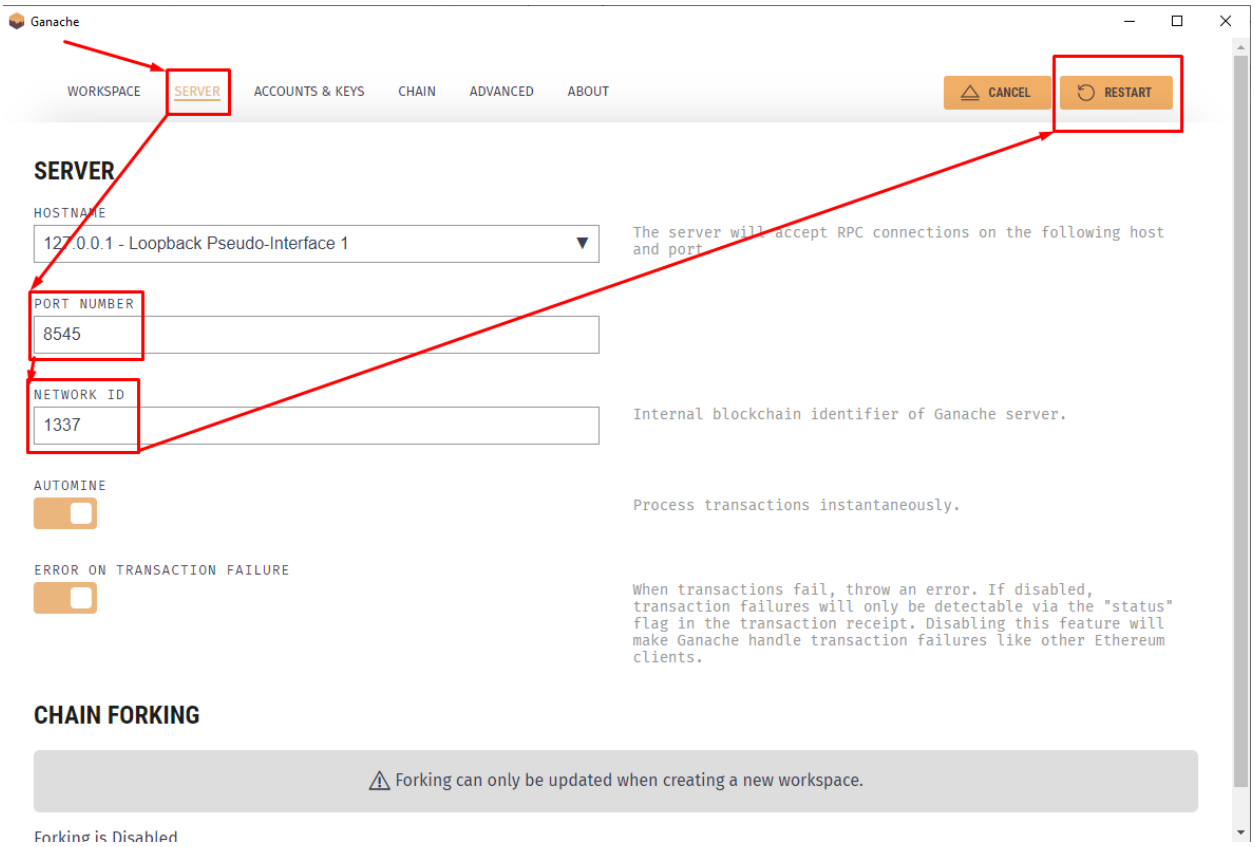

Рис 3.3 Екран налаштувань Ganache, вкладка Server

На цьому наше налаштування Ganache закінчено. Додаток залишається відкритим.

Наступним пунктом буде завантаження розширення MetaMask для браузеру та його синхронізація з Ganache.

https://chromewebstore.google.com/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn?hl=en

Після завантаження, нам потрібно створити акаунт, створивши пароль та захистивши акаунт mnemonic – 12ма унікальними кодовими фразами, які додаток запропонує сам.

Нажаль, MetaMask не відновить гаманці локальної мережі Ganache, якщо відразу після завантаження почати вводити його мнемонічну фразу. Далі нам потрібно заблокувати MetaMask натиснувши відповідну кнопку.

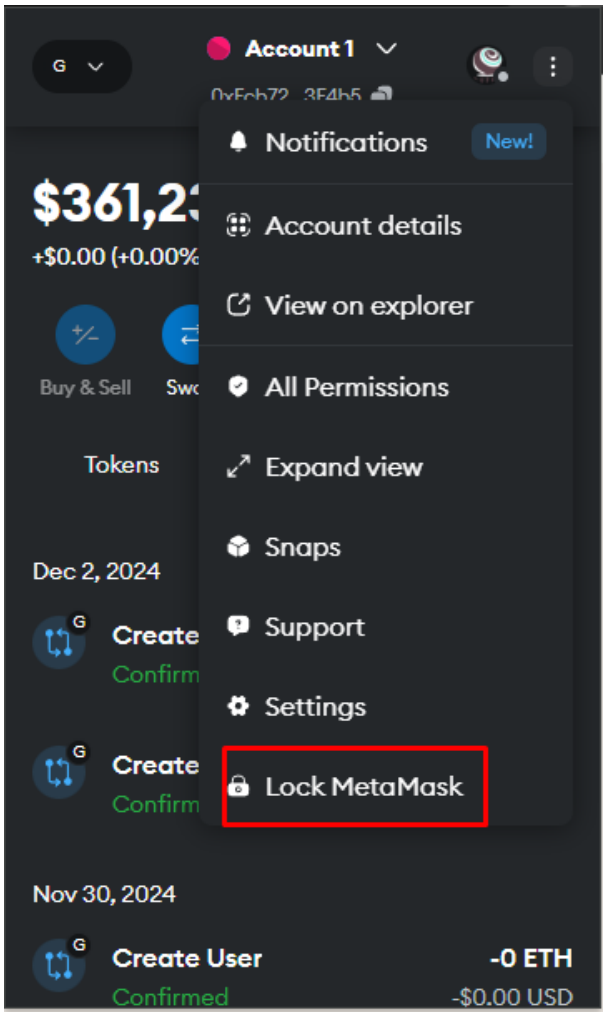

Рис 3.4 Діалогове вікно розширення MetaMask

Це потрібно для того, щоб відновити наші тестові гаманці, створені локальною мережею Ganache.

Далі ми натискаємо ”Forget Password?” та вводимо в новому pop-up вікні секретну фразу, яку нам згенерував додаток Ganache, а також довільний пароль:

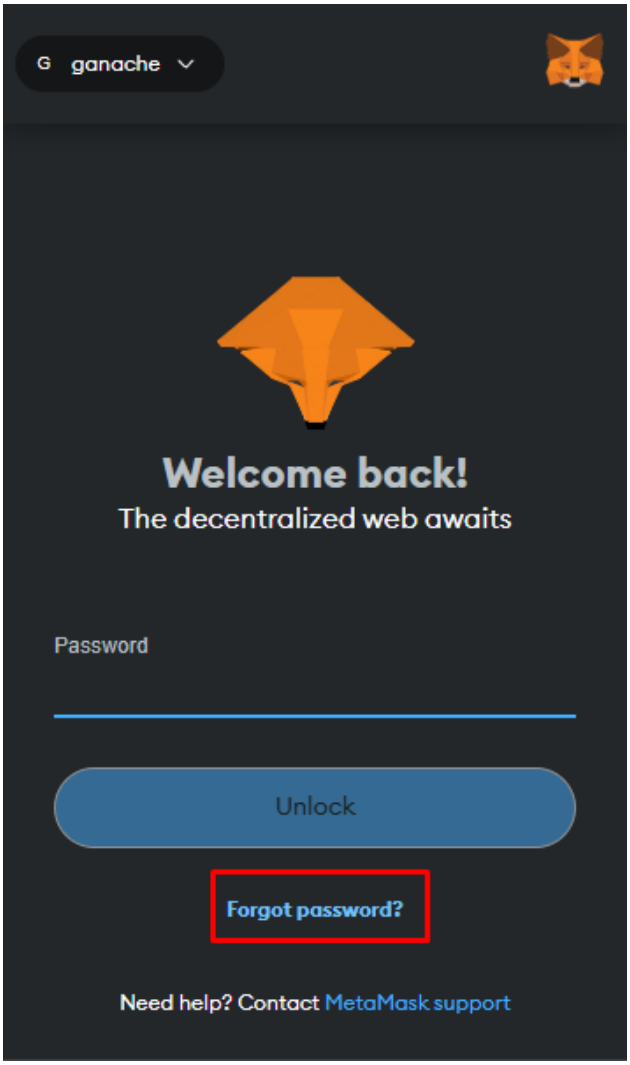

Рис 3.5 Діалогове вікно розширення MetaMask

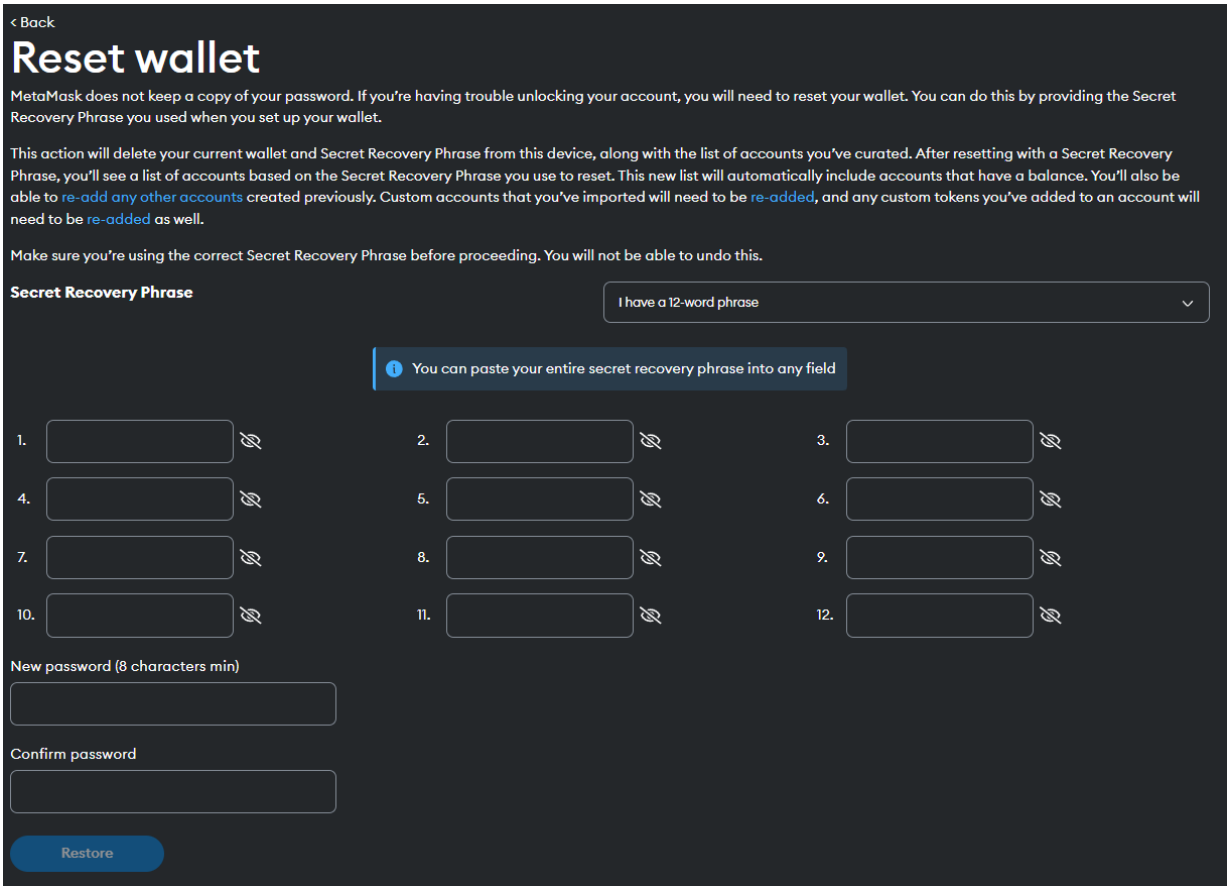

Рис 3.6 Діалогове вікно розширення MetaMask

Мнемонічну секретну фразу ми беремо з додатку Ganache, копіюючи/переписуючи кожне слово:

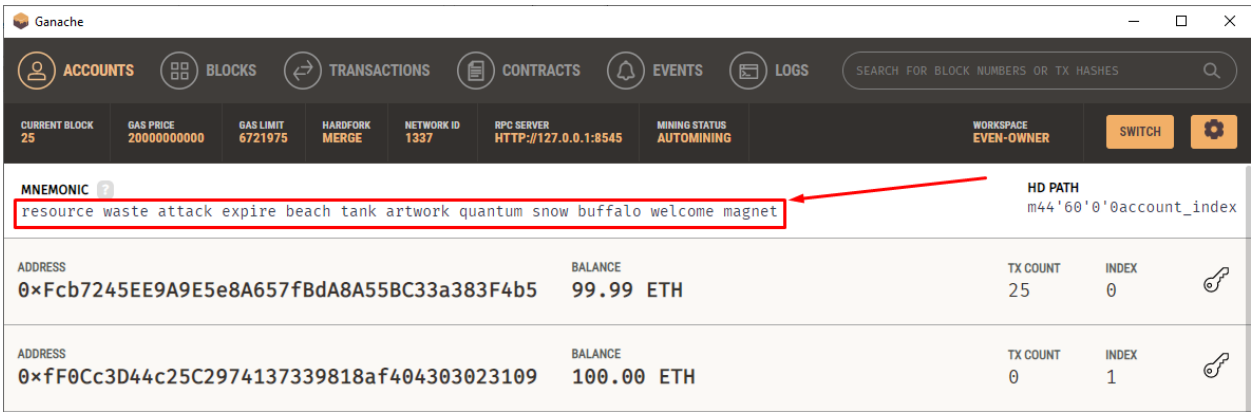

Рис 3.7 Діалогове вікно головного екрану Ganache

Після виконаних дій ми вводимо новий пароль та попадаємо назад в інтерфейс програми, де вже бачимо гаманці, які підтягнулися з локальної мережі Ganache:

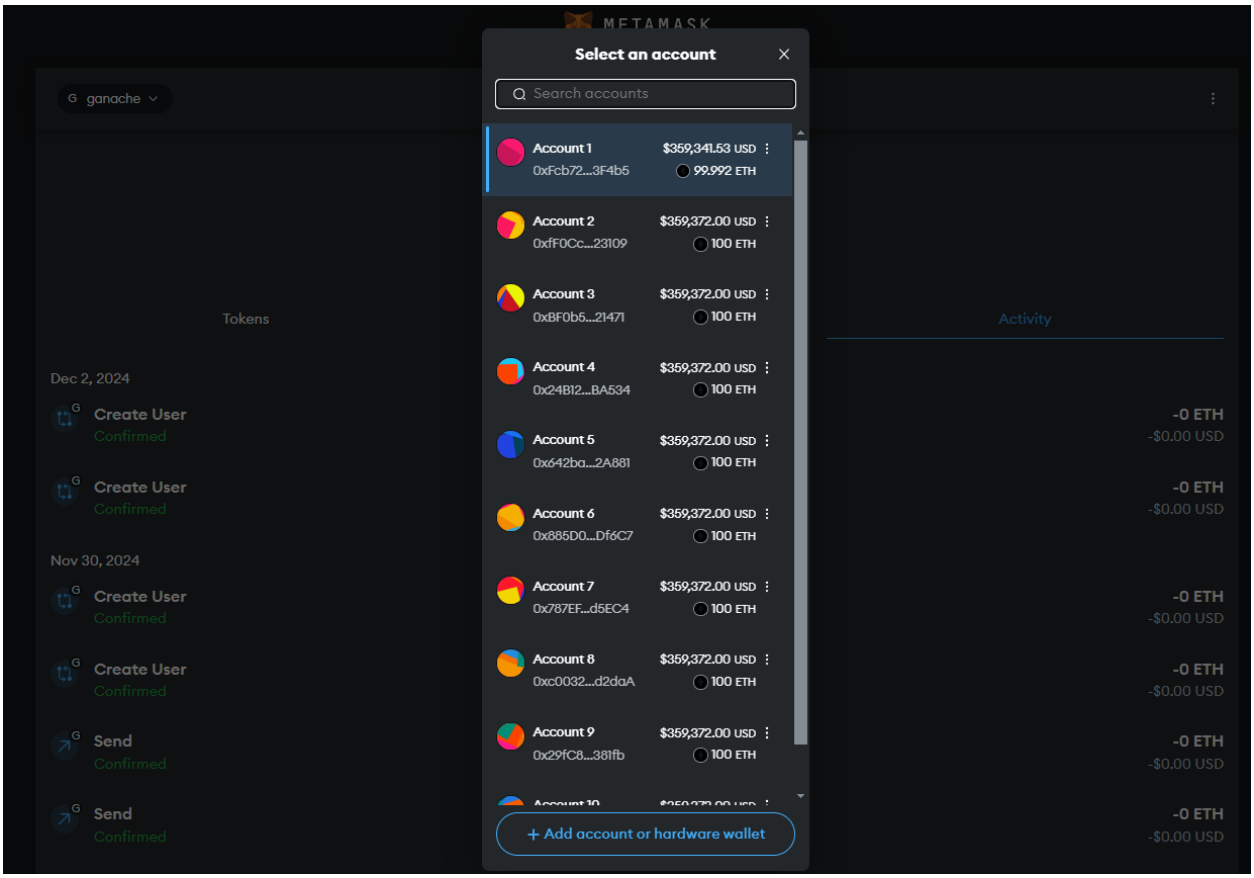

Рис 3.8 Діалогове вікно розширення MetaMask

Тепер нам залишилось створити тестову мережу в середині MetaMask, для цього натискаємо знизу кнопку “Add custom network”. Це потрібно для того, щоб використовувати не загальну мережу ETH, а нашу тестову, яку створив додаток Ganache.

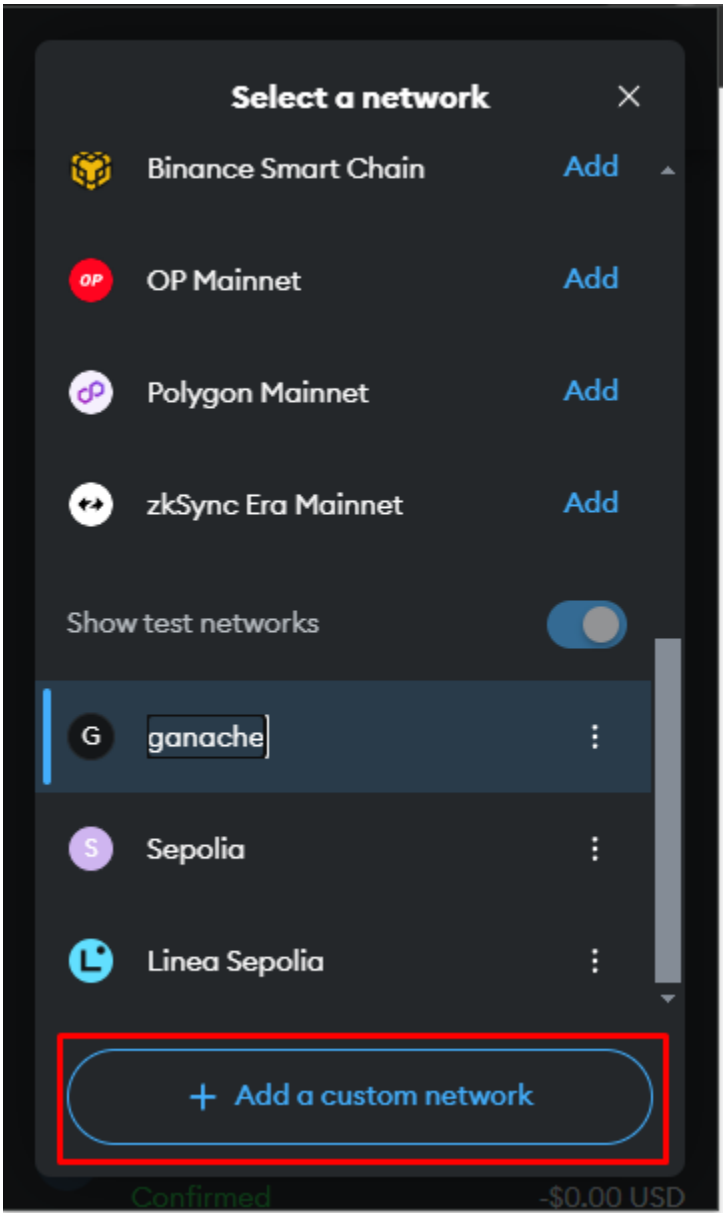

Рис 3.9 Діалогове вікно розширення MetaMask

Тут ми вказуємо ім’я мережі – ganache, URL та ChainId нашої мережі Ganache, та зберігаємо, а потім вибираємо у списку цю мережу.

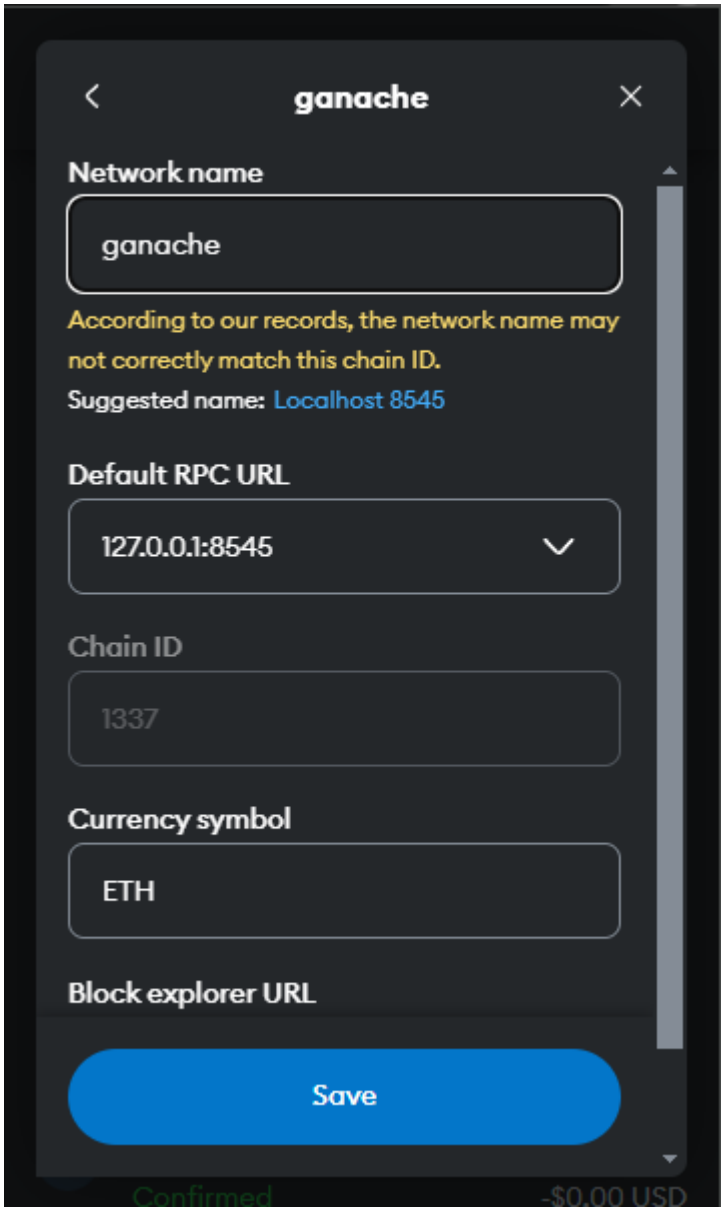

Рис 3.10 Діалогове вікно розширення MetaMask

На цьому налаштування Ganache та Metamask закінчено.

Далі ми переходимо до розбору коду та демонстрації роботи додатку.

3.3 Пояснення основного коду

Web3helpers.js використовується для:

Підключення до блокчейну через MetaMask або інші Ethereum-провайдери.

Завантаження даних блокчейну: облікових записів користувача, ID мережі, а також отримання розгорнутих смарт-контрактів (наприклад, Auth).

Абстрагування блокчейн-логіки: спрощує доступ до ключових функцій у React-компонентах.

src > JS Web3helpers.js > loadBlockchainData

```
1  import Web3 from "web3/dist/web3.min.js";
2
3  import Auth from "./build/contracts/Auth.json";
4
5  export const loadWeb3 = async () => {// Функція для підключення до Web3.
6    if (window.ethereum) {
7      window.web3 = new Web3(window.ethereum);
8      await window.ethereum.enable(); // Запит доступу до облікового запису користувача.
9    } else if (window.web3) {
10     window.web3 = new Web3(window.web3.currentProvider);// Використовуємо старий провайдер.
11   } else {
12     window.alert(
13       "Non-Ethereum browser detected. You should consider trying MetaMask!"
14       // Повідомляємо користувачу, що необхідно встановити MetaMask.
15     );
16   }
17 };
18
19 export const loadBlockchainData = async () => { // Функція для завантаження даних блокчейну.
20   const web3 = window.web3;// Отримуємо екземпляр Web3, створений у loadWeb3.
21   const accounts = await web3.eth.getAccounts();// Отримуємо список акаунтів (гаманців),
22   //підключених до провайдера. Перший акаунт буде поточним активним.
23   const networkId = await web3.eth.net.getId();// Отримуємо ідентифікатор мережі
24   // Network data
25   if (networkId) {// Перевіряємо, чи для поточної мережі є дані у Auth.json.
26     const auth = new web3.eth.Contract(
27       Auth.abi,// ABI (Application Binary Interface) смарт-контракту, потрібний для взаємодії з ним.
28       Auth.networks[networkId].address
29     );// Адреса розгорнутого смарт-контракту у відповідній мережі.
30     return { auth, accounts: accounts[0] };// Повертаємо екземпляр контракту і поточний акаунт.
31   }
32 };
33
```

Рис 3.11 Код файлу Web3helpers.js

Auth.sol

Цей контракт реалізує базову систему аутентифікації. Основні моменти:

Зберігання користувачів:

userCount — рахує кількість зареєстрованих користувачів.

usersList — мапінг (асоціативний масив), що зберігає дані користувача за його email.

Структура user: Містить інформацію про користувача: ім'я, email та пароль.

Функція createUser: Додає нового користувача до системи і викликає подію userCreated.

src > contracts > Auth.sol

```
pragma solidity >=0.4.22 <0.9.0; // Вказуємо версію компілятора, з якою цей контракт буде сумісний.

contract Auth{ // Оголошуємо контракт Auth, який буде використовуватись для керування користувачами.

    uint public userCount=0;

    mapping(string => user) public usersList;
    // Створюємо mapping (відображення), де ключем є email (тип string),
    // а значенням є структура user. Цей mapping зберігає зареєстрованих користувачів.
     struct user{
      string username;
      string email;
      string password;
   }

    // events

    event userCreated( // Оголошуємо подію, яка викликається при створенні нового користувача.
      string username,
      string email,
      string password
    );

   function createUser(string memory _username,string memory _email,string memory _password ) public {
     // Функція для створення нового користувача. Вона є публічною,
        // тобто її можуть викликати інші контракти або користувачі.

        userCount++;

        usersList[_email] = user(_username,_email,_password);// Додаємо нового користувача до mapping `usersList` з ключем _email.

        emit userCreated(_username,_email,_password);// Викликаємо подію `userCreated` для реєстрації створення нового користувача.
    }


}
```

Рис 3.12 Код файлу Auth.sol

Migrations.sol служить для управління процесом міграції смарт-контрактів. Він відстежує, які міграції були вже виконані, щоб уникнути повторного розгортання.

src > contracts > Migrations.sol

```
1   // SPDX-License-Identifier: MIT
2   pragma solidity >=0.4.22 <0.9.0;
3
4   contract Migrations {
5     // Контракт Migrations використовується для відстеження стану міграцій у проекті Truffle.
6     address public owner = msg.sender;
7     uint public last_completed_migration;
8
9     modifier restricted() {
10      // Змінна `owner` зберігає адресу власника контракту (адресу того, хто розгорнув контракт).
11      // `msg.sender` - це адреса того, хто викликає функцію.
12      require(
13        msg.sender == owner,
14        "This function is restricted to the contract's owner"
15        // Перевіряє, що функцію викликає лише власник контракту.
16      );
17      _;
18    }
19
20    function setCompleted(uint completed) public restricted {
21      // Функція `setCompleted` встановлює номер останньої завершеної міграції.
22          // Вона доступна лише власнику контракту завдяки модифікатору `restricted`.
23      last_completed_migration = completed;
24    }
25  }
26
```

Рис 3.13 Код файлу Migrations.sol

3.4 Демонстрація аутентифікації користувача використовуючи блокчейн технології

Для початку виконуємо команду *truffle migrate*, яка розгортає контракти на блокчейні згідно з файлами в migrations, зберігає інформацію про розгорнуті контракти у build/contracts, та забезпечує факт доступності контрактів для взаємодії через їх ABI та адресу.

Далі запускаємо додаток, виконуючи команду *npm start run* та попадаємо на сторінку реєстрації:

Рис 3.14 Сторінка реєстрації

Після введення імені, пошти та паролю та натискання кнопки «Зареєструватись», MetaMask звернеться до нас з запитом про проведення транзакції для реєстрації користувача, використовуючи наш гаманець.

Нам потрібно сплатити network fee, тобто комісію в тестовій мережі ETH, натиснувши кнопку Confirm:

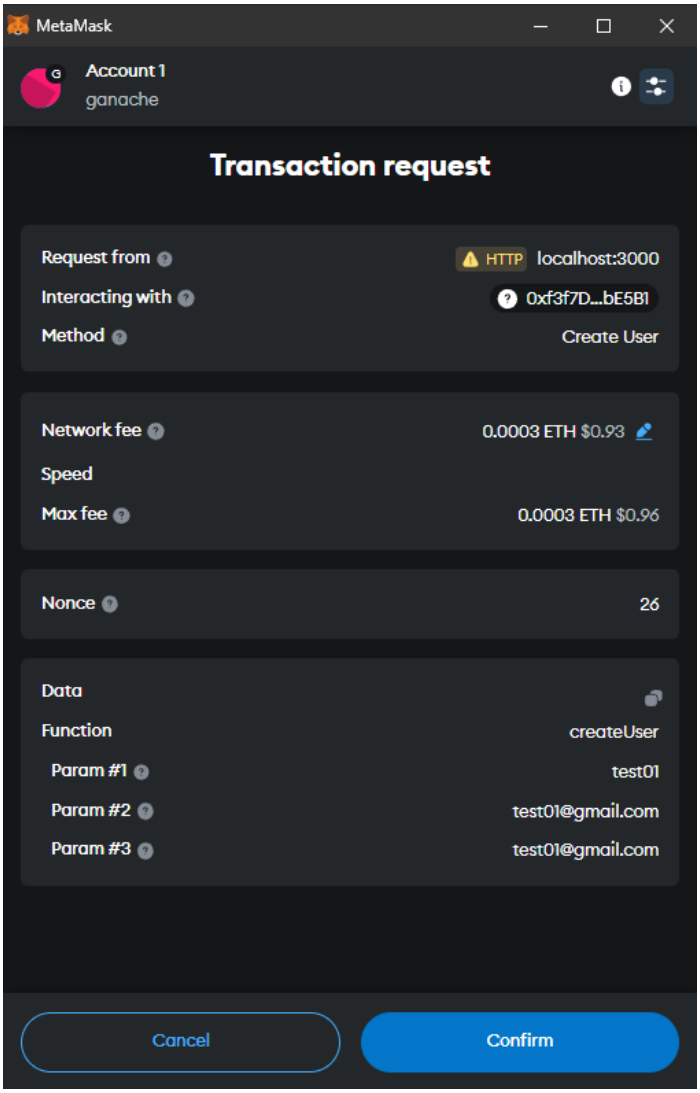

Рис 3.15 Діалогове вікно розширення MetaMask яке сповіщає про вхідну транзакцію

На цьому скріншоті ми можемо бачити деталі, тобто звідки прийшло звернення, з яким акаунтом створена інтеракція, назву методу з нашого коду, ціна податку на реєстрацію в мережі, значення Nonce яке репрезентує хешоване значення для внесення в блок, і інформацію, яку вводив юзер.

Далі користувача переміщує на сторінку логіну, де він може авторизуватись.

Рис 3.16 Сторінка логіну

Після натискання кнопки «Увійти» контракт, який містить пошту, пароль, та адресу нашого гаманця, перевіряється та у разі успіху перевірки, користувач попадає на головну сторінку, де йому відображається адреса

гаманця(акаунт),який був використаний для реєстації та пошта, яка була використана.

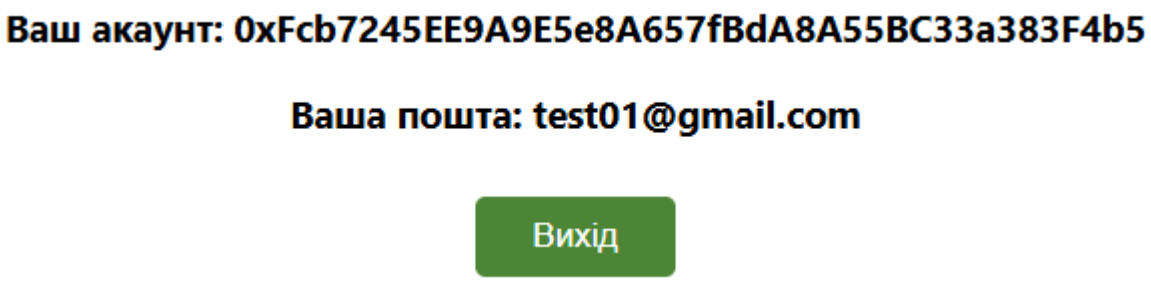

Рис 3.17 Головна сторінка

При натисканні кнопки вихід, контракт видаляє дані з localStorage та повертає користувача на сторінку входу.

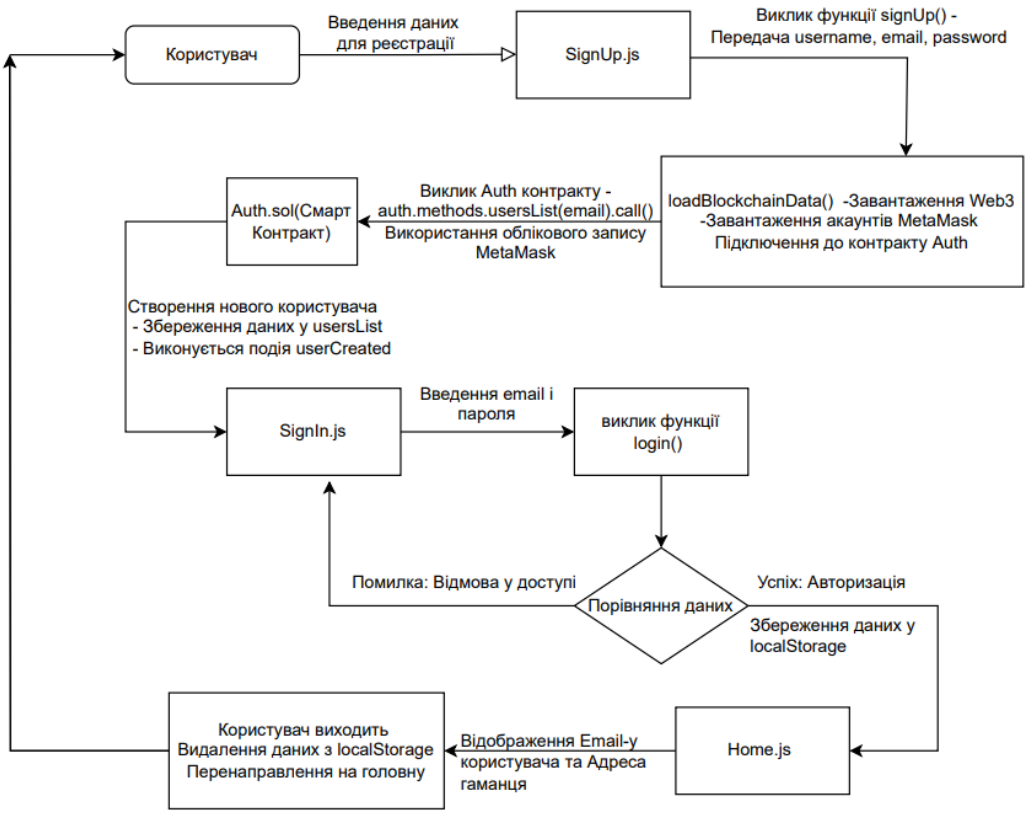

Рис. 3.18 – Діаграма роботи програми

Висновки

У цьому розділі було розглянуто архітектуру та принцип роботи рішення - блокчейн-додатка для аутентифікації користувачів. Було описано, як реалізовано процеси реєстрації, авторизації та виходу користувача, інтеграцію фронтенду (React) з блокчейном через MetaMask та Web3.js, а також роботу смарт-контрактів на Solidity.

Ця система демонструє ключові аспекти використання блокчейну для управління ідентифікацією користувачів:

Децентралізоване зберігання даних: Інформація про користувачів зберігається в смарт-контракті, забезпечуючи її незмінність та захист.

Інтеграція з Web3: Використання бібліотеки Web3.js для підключення до блокчейну та виконання транзакцій через локальну мережу Ganache.

Прозорість і безпека: Завдяки використанню MetaMask користувачі підтверджують транзакції, гарантуючи безпеку операцій.

Цей додаток є прикладом ефективного поєднання сучасних технологій, таких як React, Web3.js, Solidity і Truffle, для створення інноваційного рішення з використанням блокчейну.

РОЗДІЛ 4

РОЗРОБКА СТАРТАП ПРОЄКТУ

Цей розділ спрямований на формування інноваційного підходу до застосування блокчейн-технологій для управління ідентифікацією користувачів та пристроїв, проведення маркетингового аналізу потенційних переваг впровадження таких рішень, а також оцінку можливостей комерціалізації ключових науково-технічних розробок, висвітлених у попередніх розділах магістерської роботи. Зокрема, передбачається розробка концепції стартап-проєкту, орієнтованого на ефективну адаптацію до умов висококонкурентного ринку в умовах глобалізаційних процесів.

4.1. Опис ідеї проєкту

У даному розділі мною розглянуто підхід до керування ідентифікацією користувачів та пристроїв за допомогою блокчейн технологій. Мій проєкт спрямований на створення децентралізованої системи аутентифікації, яка підвищує безпеку та прозорість процесів ідентифікації, а також спрощує керування доступом у розподілених мережах. Використання блокчейн дозволяє забезпечити незмінність та надійність зберігання ідентифікаційних даних, що збільшує довіру користувачів та знижує ризики компрометації інформації.

Таблиця 4.1

Опис ідеї стартап-проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Застосування блокчейн технологій для управління ідентифікацією користувачів та пристроїв, що забезпечує децентралізовану та безпечну систему аутентифікації.	1. Підвищення рівня безпеки аутентифікації. 2. Зменшення ризиків компрометації даних. 3. Спрощення процесів керування доступом.	Компанії зможуть забезпечити безпечне зберігання та верифікацію ідентифікаційних даних, зменшити витрати на управління ідентифікацією, підвищити довіру клієнтів.

З особливою увагою досліджено алгоритм, який використовує блокчейн для безпечної аутентифікації та управління ідентифікацією. Це дозволить досягти переваг над конкурентами, недоліки і переваги яких наведено у таблиці 4.2.

Таблиця 4.2

Визначення 3х характеристик ідеї проєкту

№ п/п	Техніко-економічні характеристики ідеї	Потенційні товари/концепції користувачів	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
1	Децентралізована система аутентифікації	Традиційні централізовані системи			так
2	Незмінність данних у блокчейні	Системи з можливістю зміни даних			так

Продовження таблиця 4.2

3	Висока масштабованість	Обмежена масштабованість централізованих систем			так
4	Відсутність єдиного центру керування	Наявність єдиного центру, що може бути вразливим			так
5	Складність впровадження нової технології	Звичні для компаній рішення	так		

4.2 Технологічний огляд стартап проєкту

Для реалізації проєкту необхідно використовувати технології блокчейн-платформ (наприклад, Ethereum), смарт-контракти та інструменти для інтеграції з існуючими системами аутентифікації. Розробка додатка може бути здійснена з використанням мов програмування Solidity для смарт-контрактів та JavaScript для фронтенд-розробки.

Таблиця 4.3

Технологічна ймовірність ідеї проєкту

№ п/п	Ідея	Потенційні техн-ії	Наявність існуючої техн-ії	Доступність технологій
1	Блокчейн-платформа для аутентифікації	Ethereum, Hyperledger	Існуючі блокчейн-платформи	Доступні, деякі з відкритим кодом

Продовження таблиці 4.3

2	Смарт-контракти для управління доступом	Solidity, Chaincode	Інструменти для написання смарт-контрактів	Доступні, безкоштовні
3	Інтеграція з існуючими системами	API, SDK	Існуючі рішення для інтеграції	Доступні, можливі додаткові витрати
Обрана технологія реалізації проєкту: використання блокчейн-платформи Ethereum з розробкою смарт-контрактів для управління ідентифікацією та інтеграцією з існуючими системами через API.				

4.3 Аналіз можливості запуску стартап-проєкту на ринок

Дослідження ринкових перспектив розпочинається з аналізу попиту: оцінюється динаміка зростання ринку блокчейн-технологій, актуальність попиту на безпечні системи аутентифікації, а також масштаби ринку і його потенціал для впровадження таких рішень. (таблиця 4.4)

Таблиця 4.4

Попередня характеристика потенційного ринку стартап-проєкту

№ п/п	Показники стану ринку	Характеристика
1	Кількість прямих конкурентів, од	5
2	Загальний обсяг продажів, грн	50000000
3	Динаміка ринку	Стрімко зростає
4	Наявність обмежень для входу	Низькі

Продовження таблиці 4.4

5	Специфічні вимоги для стандартизації, специфікації	Відповідність стандартам безпеки та блокчейн-протоколів
6	Середня норма рентабельності в галузі, %	10

Ринок блокчейн-технологій для управління ідентифікацією швидко розвивається, що робить його привабливим для входження.

Наступним етапом є ідентифікація майбутніх клієнтів, визначення їхніх характеристик та складання орієнтовного списку вимог до продукту чи послуги, які відповідають потребам кожної з цих груп. (таблиця 4.5.) .

Таблиця 4.5

Ідентифікація майбутніх клієнтів стартап-проєкту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Готовність клієнтської бази	Вимоги споживачів до товару (послуги)
1	Підвищення безпеки ідентифікації	Фінансові установи, телекомунікаційні компанії, постачальники IoT-пристроїв	Різний рівень готовності до впровадження нових технологій	Висока безпека, масштабованість, сумісність з існуючими системами

Наступним кроком стане аналіз ринкового середовища, що передбачає ідентифікацію факторів, які сприяють успішному впровадженню проєкту, а

також виявлення перешкод і потенційних ризиків, які можуть ускладнити реалізацію.

Таблиця 4.6

Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Складність впровадження нової технології	Компанії можуть бути не готові до переходу на блокчейн	Проведення навчання та надання консультацій
2	Регуляторні обмеження	Відсутність нормативної бази для блокчейн-рішень	Співпраця з регуляторами, участь у розробці стандартів

Таблиця 4.7

Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Зростаючий інтерес до блокчейн	Більше компаній зацікавлені у впровадженні блокчейн.	Активна маркетингова стратегія, участь у конференціях
2	Потреба в безпеці	Збільшення кількості кібератак стимулює попит на безпечні рішення	Розробка додаткових функцій безпеки, акцент на перевагах блокчейн

На наступному етапі проводиться аналіз пропозиції, в ході якого визначаються ключові характеристики конкурентного середовища на ринку,

включаючи основних гравців, рівень конкуренції та унікальні переваги існуючих рішень.

Таблиця 4.8

Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Тип конкуренції: монополістична	Наявність кількох компаній з подібними рішеннями	Необхідність виділятися інноваціями
2.Рівень конкурентної боротьби: міжнародний	Конкуренція з іноземними компаніями	Орієнтація на глобальний ринок
3. Галузева ознака: технологічна	Швидкий розвиток технологій	Постійне оновлення продукту
4. Конкуренція за видами товарів: функціональна	Різні підходи до управління ідентифікацією	Інвестиції в R&D
6. За інтенсивністю: брендова	Важливість бренду в прийнятті рішення	Розвиток власного бренду

Після оцінки загального рівня конкуренції здійснюється детальний аналіз конкурентного середовища в галузі, використовуючи модель п'яти сил Майкла Портера. Ця модель дозволяє оцінити вплив основних чинників: загрозу появи нових конкурентів, силу постачальників, силу покупців, загрозу замінників та рівень конкурентної боротьби між існуючими гравцями. (таблиця 4.9)

Таблиця 4.9

Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Існуючі компанії з подібними продуктами	Нові стартапи	Постачальники технологій блокчейн	Компанії, що потребують безпечної ідентифікації	Традиційні системи аутентифікації

Результатом проведення аналізу є висновок: конкуренція присутня, але ринок ще формується, що створює можливості для входження з інноваційним продуктом.

На основі проведеного аналізу конкурентного середовища та унікальних особливостей ідеї проєкту було визначено й обґрунтовано ключові фактори конкурентоспроможності, які представлені в таблиці 4.10. Також проведено детальне порівняння сильних і слабких сторін стартап-проєкту, результати якого наведені в таблиці 4.11, що дозволяє оцінити перспективи успішної реалізації проєкту на ринку.

Таблиця 4.10

Обгрунтування можливої конкурентоспроможності

№ п/п	Фактори конкурентоспроможності	Обґрунтування
1	Інноваційність технології	Використання блокчейн для управління ідентифікацією є новим підходом
2	Високий рівень безпеки	Блокчейн забезпечує незмінність та захист даних
3	Масштабованість рішення	Можливість легко адаптувати систему під потреби клієнта

Таблиця 4.11

Порівняльний аналіз сторін проєкту

№ п/п	Фактори конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з власною системою						
			-3	-2	-1	0	1	2	3
1	Інноваційність технології	18				+			
2	Високий рівень безпеки	20		+					
3	Масштабованість рішення	17			+				

Фінальним кроком аналізу ринкових можливостей для впровадження проєкту є складання SWOT-аналізу. У цьому аналізі враховуються сильні (Strengths) та слабкі (Weaknesses) сторони проєкту, а також можливості (Opportunities) і загрози (Threats), визначені на основі попереднього аналізу ринкових факторів. Результати цього аналізу представлені у вигляді матриці в таблиці 4.12, що дозволяє сформувати комплексне уявлення про перспективи реалізації проєкту в ринкових умовах.

Таблиця 4.12

SWOT-аналіз стартап проєкту

Сильні сторони: • Інноваційна технологія • Високий рівень безпеки • Масштабованість	Слабкі сторони: Відсутність відомого бренду Складність впровадження для деяких клієнтів
Можливості: Зростаючий ринок блокчейн Потреба в безпечних системах	Загрози: Конкуренція з боку традиційних рішень Регуляторні обмеження

4.4. Розроблення ринкової стратегії проєкту

Першим етапом розроблення ринкової стратегії є визначення стратегії охоплення ринку, що включає ідентифікацію цільових груп потенційних споживачів. У цьому процесі аналізуються їхні потреби, очікування та характеристики, що дає змогу сформувати сегментований підхід до просування продукту чи послуги. Результати цього етапу систематизовані у таблиці 4.13.

Таблиця 4.13

Вибір таргет-груп можливих клієнтів

№ п/п	Опис профілю таргет-групи можливих клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Фінансові установи	Висока	Високий	Середня	Середня
2	Телекомуніка ційні компанії	Середня	Середній	Низька	Легка
3	Постачальник и IoT-пристроїв	Низька	Зростаючий	Низька	Легка
Цільовими групами обрано фінансові установи, телекомунікаційні компанії та постачальників IoT-пристроїв.					

За результатами проведеного аналізу було обрано стратегію охоплення ринку – диференційований маркетинг, який спрямований на врахування специфічних потреб кожного цільового сегмента. Для ефективної роботи в цих сегментах розроблено базову стратегію розвитку, що враховує ключові пріоритети та заходи, необхідні для успішної реалізації проєкту. Основні аспекти стратегії викладені в таблиці 4.14.

Таблиця 4.14

Визначення основи стратегії розвитку

№ п/п	Обраний шлях розвитку	Шлях охоплення ринку	Основні конкурентоспроможні позиції	Базова стратегія розвитку
1	Впровадження блокчейн-рішення в фінансових установах	Охоплення фінансового сектору	Висока безпека, відповідність регуляторним вимогам	Стратегія фокусування
2	Розширення на телекомунікаційний ринок	Охоплення телеком-сегменту	Масштабованість, інтеграція з IoT	Стратегія диференціації

Обрана стратегія поведінки конкуренції– стратегія лідерства за рахунок інновацій.

Таблиця 4.15

Визначення основи для стратегії поведінки конкуренції

№ п/п	Чи є проєкт першим на ринку?	Чи претендує стартап на аудиторію конкурентів?	Копіювання рішень у конкурентів	Стратегія конкурентної поведінки
1	Так, у певних сегментах	Шукає нових споживачів	Ні, пропонує унікальні рішення	Стратегія лідерства за рахунок інновацій

На основі аналізу вимог споживачів та обраних стратегій охоплення ринку була сформована стратегія позиціонування. Вона визначає ключові переваги проєкту, які виділяють його серед конкурентів, та формує унікальну пропозицію цінності, що відповідає потребам цільових сегментів. Стратегія спрямована на створення позитивного сприйняття продукту чи послуги в очах потенційних клієнтів. (таблиця 4.16).

Таблиця 4.16

Визначення позиційної стратегії

№п/п	Вимоги до товару ЦА	Основна стратегія	Основні позиції націлені на конкурентоспроможність свого стартап проєкту	Вибір асоціацій, які мають сформувати комплексну позицію власного проєкту
1	Висока безпека, відповідність стандартам	Стратегія фокусування	Інноваційність, надійність	Безпека, інновації, довіра

4.5. Розроблення маркетингової програми стартап-проєкту

Маркетингова програма є основою успішного запуску продукту, що поєднує комплекс завдань і заходів соціального, економічного, науково-технічного, виробничого та організаційного характеру. Вона визначає ресурси, які будуть залучені, та джерела їх отримання, і будується на чітко окреслених цілях та часових рамках. Ця програма спрямована на систематичну реалізацію маркетингових стратегій, оптимально поєднуючи інструменти маркетингу, з урахуванням планового періоду та відповідного фінансового забезпечення.

Першим етапом у розробці маркетингової програми є формування концепції товару, який буде пропонуватися споживачеві. Для цього необхідно узагальнити результати попереднього аналізу конкурентоспроможності товару, визначивши його унікальні переваги, які задовольняють вимоги цільових груп споживачів і вирізняють продукт серед конкурентів.

Таблиця 4.17

Визначення основних переваг потенційного товару

№ п/п	Потреба	Пропозиції нашого товару	Переваги нашого товару над товаром конкурента
1	Безпечна ідентифікація	Захист даних від компрометації	Незмінність даних у блокчейні
2	Масштабованість	Легке розширення системи	Децентралізована архітектура
3	Відповідність стандартам	Спрощення відповідності регуляторним вимогам	Прозорість та аудиторність блокчейн

Наступним етапом є розробка трирівневої маркетингової моделі товару, яка охоплює:

1. **Ядро продукту (основна ідея):** визначення ключової цінності продукту або послуги, тобто основної потреби споживача, яку він задовольняє.
2. **Реальний продукт:** деталізація фізичних або технічних характеристик товару, включаючи його дизайн, функціональність, якість, упаковку, бренд та інші атрибути, які формують сприйняття продукту.
3. **Розширений продукт:** визначення додаткових послуг або переваг, які супроводжують товар (наприклад, гарантії, післяпродажне обслуговування, доступність інформаційної підтримки або персоналізовані рішення).

Цей підхід дозволяє повністю структурувати продукт, враховуючи не лише його матеріальну складову, але й створення цінності для споживача через процес його надання та супровідні послуги.

Таблиця 4.18

Опис рівнів товару

Рівні товару	Сутність та складові
Ядро продукту	Забезпечує безпечне та масштабоване управління ідентифікацією користувачів та пристроїв
Реальний продукт	Властивості: інноваційність, безпека, масштабованість
	Назва: Blockchain ID Management System
Розширений продукт	До продажу: Консультації, демонстрація продукту
	Після продажу: Технічна підтримка, оновлення, навчання персоналу

Наступним кроком є визначення оптимальної системи збуту, в рамках якої приймаються ключові рішення щодо:

1. **Каналів збуту:** вибір між прямими (безпосередній продаж споживачам) та непрямими (через посередників) каналами, враховуючи специфіку продукту та цільову аудиторію.
2. **Стратегії покриття ринку:** вибір між інтенсивним (максимально широке розповсюдження), селективним (обмежена кількість партнерів) або ексклюзивним (співпраця з одним або кількома ключовими дистриб'юторами) підходами.
3. **Логістики:** розробка схеми доставки товару, що включає способи транспортування, складування, управління запасами та забезпечення своєчасного постачання.
4. **Цінової політики:** встановлення рівнів цін і умов співпраці для дистриб’юторів, роздрібних мереж чи кінцевих споживачів. (таблиця 4.19).

Таблиця 4.19

Основи системи збуту

№ п/п	Канали збуту	Стратегія покриття ринку	Логістка	Цінова політика
1	Довготривалі контракти, індивідуальні умови	Розробка під потреби клієнта, інтеграція, підтримка	Непрямий збут через партнерів	Динамічна в залежності від ситуації на ринку

Фінальним етапом є розробка концепції маркетингових комунікацій, яка базується на обраній стратегії позиціонування, специфіці поведінки клієнтів і враховує ключові елементи(таблиця 4.20).

Таблиця 4.20

Концепція маркетингових комунікацій

№ п/п	Орієнтація клієнтів стартапу	Методи розповсюдження проєкту	Основні позиції для рекламування	Завдання рекламного агенства
1	Шукають безпечні та інноваційні рішення	Професійні конференції, галузеві видання, онлайн-платформи	Безпека, інновації, довіра	Показати переваги рішення, викликати інтерес до продукту

У основі маркетингових комунікацій компанія використовуватиме цільовий маркетинг, орієнтований на конкретні сегменти, та акцентуватиме на перевагах свого рішення.

Висновки

У розділі проведено маркетинговий аналіз реалізації технології застосування блокчейн для управління ідентифікацією користувачів та пристроїв та оцінено можливості виходу на ринок. Встановлено, що існує значний потенціал для комерціалізації проєкту як на внутрішньому, так і на міжнародному ринках завдяки інноваційності та актуальності запропонованого рішення. Продукт наділений такими характеристиками, як безпека, масштабованість та відповідність сучасним вимогам. Конкурентами можуть бути компанії, які пропонують традиційні системи аутентифікації, однак наше рішення вирізняється значними перевагами завдяки використанню блокчейн-технологій. Серед таких переваг — підвищений рівень безпеки, прозорість процесів і децентралізований підхід. Основною проблемою може стати складність інтеграції нової технології в існуючі системи, але результати проведеного аналізу свідчать про доцільність подальшої імплементації стартап-проєкту. Він демонструє високий потенціал для успішного впровадження на ринку і досягнення комерційного успіху.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У магістерській дисертації було досліджено застосування блокчейн-технологій для управління ідентифікацією користувачів та пристроїв. Було проаналізовано історію розвитку технології блокчейн, її ключові особливості, архітектуру, а також сучасні інструменти та протоколи для її впровадження. Проведено детальний розбір основних механізмів роботи, таких як смарт-контракти, механізми консенсусу та децентралізовані ідентифікаційні системи (DID).

У ході дослідження були розглянуті існуючі виклики та проблеми централізованих систем ідентифікації, такі як вразливість до атак, залежність від третіх сторін та обмежена масштабованість. Запропоновано використання блокчейн-рішень для їх подолання, що дозволяє підвищити рівень безпеки, прозорості та автономності користувачів.

Практичне впровадження результатів дослідження показало ефективність використання блокчейн-технологій у побудові сучасних ідентифікаційних систем, зокрема шляхом інтеграції з платформами, такими як MetaMask, Ganache та Truffle, а також розробки смарт-контрактів на Solidity.

Отже, підводячи підсумки, можна стверджувати, що блокчейн-технології є перспективним напрямком для модернізації систем ідентифікації. Їх впровадження дозволить підвищити безпеку, надійність та зручність використання ідентифікаційних систем, забезпечуючи користувачів і організації новими можливостями для взаємодії у цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What Is a One Time Password? [Електронний ресурс] // CM. – 2020. – Режим доступу до ресурсу: https://www.cm.com/glossary/what-is-one-time-password/.
2. Bezrukava P. What is an OTP (One Time-Password)? [Електронний ресурс] / Polina Bezrukava // BSG World. – 2024. – Режим доступу до ресурсу: https://bsg.world/blog/what-is-the-one-time-password/.
3. What is: Multifactor Authentication [Електронний ресурс] // Microsoft. – 2020. – Режим доступу до ресурсу: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661.
4. What is Multi-Factor Authentication (MFA)? [Електронний ресурс] // Amazon. – 2018. – Режим доступу до ресурсу: https://aws.amazon.com/what-is/mfa/.
5. What is two-factor authentication? [Електронний ресурс] // Microsoft. – 2021. – Режим доступу до ресурсу: https://www.microsoft.com/en-ie/security/business/security-101/what-is-two-factor-authentication-2fa.
6. Two-Factor Authentication (2FA) [Електронний ресурс] // Duo. – 2021. – Режим доступу до ресурсу: https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa.
7. Facial Recognition: how it works and its safety [Електронний ресурс] // Signicat. – 2024. – Режим доступу до ресурсу: https://www.signicat.com/blog/face-recognition.

8. About Face ID advanced technology [Електронний ресурс] // Apple. – 2018. – Режим доступу до ресурсу: https://support.apple.com/en-us/102381.
9. What Are Finger Scanners and How Do They Work? [Електронний ресурс] // Lifewire. – 2021. – Режим доступу до ресурсу: https://www.lifewire.com/understanding-finger-scanners-4150464.
10. Beyond the Iris: Retina Scan for Future Biometric Security? [Електронний ресурс] // Aratek. – 2024. – Режим доступу до ресурсу: https://www.aratek.co/news/beyond-the-iris-retina-scan-for-future-biometric-security.
11. Speech recognition Overview [Електронний ресурс] // Microsoft Learn. – 2024. – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/azure/ai-services/speech-service/speaker-recognition-overview.
12. What Is Behavioral Biometrics? [Електронний ресурс] // LexisNexis. – 2024. – Режим доступу до ресурсу: https://risk.lexisnexis.com/global/en/insights-resources/article/what-is-behavioral-biometrics#:~:text=Behavioral%20biometrics%20invisibly%20helps%20verify,strong%20foundation%20for%20establishing%20trust..
13. What is Cryptographic Identity? [Електронний ресурс] // GoTeleport. – 2024. – Режим доступу до ресурсу: https://goteleport.com/learn/what-is-cryptographic-identity/.
14. What is Cryptographic Authentication and Why Are Leading Companies Moving Away from Risk-Based Authentication? [Електронний ресурс] // Prove. – 2022. – Режим доступу до ресурсу: https://www.prove.com/blog/what-is-cryptographic-authentication-

why-are-leading-companies-moving-away-from-risk-based-authentication.

15. What is MAC Address? [Електронний ресурс] // Geeksforgeeks. – 2024. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/mac-address-in-computer-network/.
16. What is an IMEI number? [Електронний ресурс] // Thales. – 2023. – Режим доступу до ресурсу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/inspired/basics-of-phone-security/imei-number#:~:text=The%20IMEI%20(International%20Mobile%20Equipment,all%20valid%20mobile%20phone%20equipment..
17. What is a serial number? [Електронний ресурс] // Lenovo. – 2024. – Режим доступу до ресурсу: https://www.lenovo.com/us/en/glossary/serial-number/.
18. What is a SIM card number? [Електронний ресурс] // Currys. – 2024. – Режим доступу до ресурсу: https://www.currys.co.uk/techtalk/mobile/how-to-find-your-sim-card-number-on-android.html#:~:text=A%20SIM%20card%20number%2C%20also,authenticate%20it%20on%20their%20systems..
19. What Is An IP Address? How Does It Work? [Електронний ресурс] // Fortinet. – 2024. – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/what-is-ip-address.
20. What is a User Agent? [Електронний ресурс] // WhatIsMyBrowser. – 2024. – Режим доступу до ресурсу: https://www.whatismybrowser.com/detect/what-is-my-user-agent/faq/what-is-a-user-agent.

21. History of Blockchain [Електронний ресурс] // Geeksforgeeks. – 2023. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/history-of-blockchain/.
22. Blockchain Structure [Електронний ресурс] // Geeksforgeeks. – 2024. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/blockchain-structure/.
23. What are the 4 different types of blockchain technology? [Електронний ресурс] // Techtarget. – 2024. – Режим доступу до ресурсу: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology#:~:text=There%20are%20four%20main%20types,consortium%20blockchains%20and%20hybrid%20blockchains..
24. What are smart contracts? [Електронний ресурс] // IBM. – 2024. – Режим доступу до ресурсу: https://www.ibm.com/topics/smart-contracts#:~:text=Smart%20contracts%20are%20typically%20used,intermediary\'s%20involvement%20or%20time%20loss..
25. GDPR & Blockchain: At the intersection of data privacy and technology [Електронний ресурс] // PSABDB. – 2023. – Режим доступу до ресурсу: https://psabdp.com/psa-bdp-blog/gdpr-blockchain-at-the-intersection-of-data-privacy-and-technology#:~:text=The%20key%20difference%20between%20a,the%20data%20is%20distributed%2Fstored..
26. Understanding Blockchain\'s Authentication Process [Електронний ресурс] // Verix. – 2022. – Режим доступу до ресурсу: https://www.verix.io/blog/blockchain-

authentication#:~:text=Understanding%20Blockchain\'s%20Authentication%20Process,stored%20in%20a%20decentralised%20ledger..

27. What is Web3? [Електронний ресурс] // Mckinsey. – 2023. – Режим доступу до ресурсу: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3.
28. Decentralized Identifiers (DIDs) v1.0 [Електронний ресурс] // W3. – 2022. – Режим доступу до ресурсу: https://www.w3.org/TR/did-core/.