ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Єгеній ТЕРЕЩЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. КІД-41
Євгеній ТЕРЕЩЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Юлія БОРОВА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: Юлія БОРОВА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Терещенко Євгеній Дмитрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних
керівник кваліфікаційної роботи Юлія БОРОВА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_____» _____2024р. № _____
2. Строк подання кваліфікаційної роботи «_____» _____ 2024р.
3. Вихідні дані до кваліфікаційної роботи: наукову літературу, статистичні дані, результати опитувань або експериментів, публікації, інформацію з веб-джерел, власний досвід використання технологій, що базуються на блокчейні та їх дослідження практичним застосуванням
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження технології блокчейн
2. Теоретичні та засади забезпечення безпеки даних з використанням технології блокчейну
3. Пропозиції щодо застосування технології блокчейну для захисту даних
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання«_____» _____ 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	26.02-22.03.2024	
2	Обробка матеріалу	23.03-05.04.2024	
3	Розробка теоретичної частини	06.04-10.04.2024	
4	Дослідження проектної частини	11.04-30.04.2024	
5	Виправлення недоліків	01.05-03.05.2024	
6	Висновки за результатами аналізу	04.05-08.05.2024	
7	Розробка презентації	09.05-11.05.2024	
8	Передзахист	14.05-17.05.2024	
9	Здача в деканат	25.05-1.06.2024	

Здобувач(ка) вищої освіти _____ Євгеній ТЕРЕЩЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юлія БОРОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 73 стор., 9 рис., 2 табл., 34 джерела.

Мета роботи – обґрунтування можливостей застосування блокчейн технологій для забезпечення безпеки даних.

Об'єкт дослідження – технологія блокчейн.

Предмет дослідження – можливості застосування блокчейн технологій для забезпечення безпеки даних.

Короткий зміст роботи: Враховуючи недоліки існуючих методів захисту інформації та постійний розвиток нових загроз, система захисту інформації потребує нових підходів та рішень. Основними проблемами, які значно впливають на повільне та проблематичне впровадження технології, є обмежена масштабованість, висока енерговитратність, відсутність нормативно-правової бази, що регулює використання технології, та недостатня кількість фахівців. Однак з кожним роком ці проблеми зменшуються, і тому технологія блокчейн вже зараз може бути ефективним засобом захисту інформації.

Досліджено, що найбільш доцільним типом для забезпечення безпеки інформації є гібридний блокчейн, який поєднує переваги обох типів технології, намагаючись при цьому обмежити їх недоліки і таким чином забезпечує всі аспекти інформаційної безпеки. З урахуванням цієї інформації, гібридний блокчейн є безпечним та надійним засобом для захисту інформації. Нами були сформовані пропозиції щодо застосування блокчейну для забезпечення безпеки даних, як включають: захист особистих даних, аутентифікацію ідентичності, трекінг походження даних, захист від кібератак, забезпечення цілісності даних.

КЛЮЧОВІ СЛОВА: БЛОКЧЕЙН, ХЕШУВАННЯ, АЛГОРИТМИ КОНСЕНСУСУ, СМАРТ-КОНТРАКТИ, БЕЗПЕКА ДАНИХ, ДЕЦЕНТРАЛІЗАЦІ

ABSTRACT

The text part of the qualifying work for obtaining a bachelor's degree:

73 pages, 9 figures, 2 tables, 34 sources.

The purpose of the work is to justify the possibilities of using blockchain technologies to ensure data security.

The object of research is blockchain technology.

The subject of the study is the possibilities of using blockchain technologies to ensure data security.

Summary of work: Given the shortcomings of existing information protection methods and the constant development of new threats, the information protection system needs new approaches and solutions. The main problems that significantly affect the slow and problematic implementation of the technology are limited scalability, high energy consumption, the absence of a legal framework regulating the use of the technology, and an insufficient number of specialists. However, these problems are decreasing every year, and therefore blockchain technology can already be an effective means of protecting information.

It has been studied that the most appropriate type for ensuring information security is a hybrid blockchain, which combines the advantages of both types of technology, while trying to limit their disadvantages and thus provides all aspects of information security. With this information in mind, hybrid blockchain is a safe and reliable means of protecting information. We have formulated proposals for the application of blockchain to ensure data security, including: personal data protection, identity authentication, data origin tracking, protection against cyber attacks, data integrity.

КЛЮЧОВІ СЛОВА: БЛОКЧЕЙН, ХЕШУВАННЯ, АЛГОРИТМИ КОНСЕНСУСУ, СМАРТ-КОНТРАКТИ, БЕЗПЕКА ДАНИХ, ДЕЦЕНТРАЛІЗАЦІЯ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут _____

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра (магістра)

Направляється здобувач(ка) _____ до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю _____
(код, найменування спеціальності)
освітньо-професійної програми _____
(назва)
на тему: «_____».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач(ка) Під час виконання бакалаврської роботи Терещенко Є. Д. показав хорошу теоретичну та практичну підготовку, знання матеріалу, вміння вирішувати самостійно питання і робити висновки. Зміст роботи відповідає завданню. Перелік використаних джерел свідчить про вміння розбиратися наукових питаннях та застосовувати їх при дослідженнях._____

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача(ки) _____ на оцінку «_____» та присвоїти йому(їй) кваліфікацію _____.

Керівник кваліфікаційної роботи _____ ___Юлія БОРОВА____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) _Терещенко Є.Д_ допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою _____ _____ _____
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську (магістерську) роботу

здобувача(ки) вищої освіти __Терещенко Євгеній Дмитрович_____

(прізвище, ім'я, по батькові)

на тему «Дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних»

Актуальність.

Блокчейн продовжує залишатися актуальною технологією через свою здатність забезпечувати безпеку, недійсність імутабельності та децентралізації. Він використовується в фінансах, логістиці, медицині та інших галузях для забезпечення прозорості та ефективності у даних та процесах.

Позитивні сторони.

1. Перевага роботи є всебічний та глибокий теоретичний аналіз блокчейн технологій та їх застосування для забезпечення безпеки даних.

2. Робота відзначається добре продуманою структурою і чіткістю викладу матеріалу. Логічна послідовність розділів, зрозумілий виклад складних технічних аспектів

Недоліки.

1. Незначним недоліком вашої роботи є обмежений огляд сучасної літератури.

2. Дослідження може не враховувати достатньо екологічних аспектів використання блокчейн технологій

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної бакалаврської (магістерської) роботи.

Висновок: *кваліфікаційна бакалаврська (магістерська) робота заслуговує оцінку "Відмінно", а здобувач(ка) _____ заслуговує присвоєння кваліфікації: бакалавр з комп'ютерної інженерії.*

Рецензент: _____ _____

науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП

*Актуальність теми***.** Тема дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних є надзвичайно актуальною в сучасному цифровому світі. Враховуючи постійне зростання обсягів цифрових даних та інформаційних технологій, збереження та захист цих даних стає все більшою проблемою для багатьох організацій та користувачів.

Блокчейн технологія, яка спочатку була розроблена для підтримки криптовалют, таких як Bitcoin, тепер виявляє потенціал для революції в галузі безпеки даних. Основна ідея блокчейну полягає в тому, що дані зберігаються у вигляді блоків, які постійно перевіряються та підтверджуються всіма учасниками мережі. Це забезпечує високий рівень надійності та непереборності даних. Однією з основних переваг застосування блокчейну є його децентралізований характер. Інформація зберігається на різних комп'ютерах у мережі, що ускладнює можливість зламу або втрати даних через атаки на централізовані сервери. Крім того, блокчейн може забезпечити прозорість та достовірність обміну даними. Кожна транзакція в мережі реєструється і не може бути змінена без згоди більшості учасників, що робить систему відкритою та надійною.

Застосування блокчейну для забезпечення безпеки даних має широкий спектр можливостей, включаючи фінансові транзакції, медичні записи, логістику, голосування та багато іншого. Водночас, важливо ретельно вивчити та розуміти потенційні обмеження та виклики, пов'язані з впровадженням цієї технології, такі як масштабованість, енергоефективність та правова база. Однак безсумнівно, застосування блокчейну для забезпечення безпеки даних є перспективним напрямом, який може значно підвищити рівень довіри та безпеки в цифровому середовищі.

Дослідники, такі як О. Баранов, О. Дубініна, І. Дунаєв, П. Кравченко, А. Кудь, І. Кузьмич, В. Рядінська, Р. Самсін, Б. Скрябін, О. Стащук, С. Теслюк, К. Токарєва, М. Уткіна, А. Харченко, М. Чупріна та інші, привернули увагу до ключових аспектів розвитку та характеристик технології блокчейн, а також до її

застосування та правового регулювання.

Мета і завдання дослідження. Метою кваліфікаційної роботи є обґрунтування можливостей застосування блокчейн технологій для забезпечення безпеки даних. Для досягнення поставленої мети необхідно вирішити наступні завдання:

– навести основні поняття захисту інформації та забезпечення безпеки даних;

– розглянути історію та розвиток технології блокчейн;

– проаналізувати застосування технології блокчейн для безпеки даних;

– навести ключові характеристики технології блокчейн;

– описати хешування у блокчейн та алгоритми досягнення консенсусу;

– навести класифікацію блокчейн-мереж;

– охарактеризувати смарт-контракти;

– надати пропозиції щодо застосування блокчейн технологій для забезпечення безпеки даних на прикладі фінансового сектору, державного сектору та логістики.

Об'єкт дослідження – технологія блокчейн.

Предмет дослідження – можливості застосування блокчейн технологій для забезпечення безпеки даних.

Методи дослідження. При написанні роботи використовувалися застосування методів аналізу та синтезу для використання елементів технології блокчейн для забезпечення безпеки даних. В роботі застосовано абстрактно-логічні методи, такі як дедукція, індукція, аналогія, перехід від конкретного до абстрактного та навпаки, побудова дефініцій понять, а також застосування поділу та класифікації. В роботі використані структурно-функціональний підхід, порівняльно-правовий підхід та інші загальнонаукові та спеціальні методи дослідження.

Теоретична значущість отриманих результатів полягає в узагальненні та систематизації знань про технологію блокчейн та її потенційні можливості для

забезпечення безпеки даних. Розглянуті в роботі теоретичні засади захисту інформації та розвиток блокчейну дозволяють глибше розуміти принципи функціонування цієї технології та її потенційний вплив на безпеку даних. Описані ключові характеристики, алгоритми та класифікація блокчейн-мереж допомагають уточнити розуміння процесів, що відбуваються в мережі блокчейн, та виявити їх можливості та обмеження.

Методична значущість полягає в розробці методів застосування технології блокчейн для забезпечення безпеки даних у різних сферах, таких як фінансовий сектор, державний сектор та логістика. Аналіз пропозицій щодо застосування блокчейну дозволяє виявити переваги та можливості використання цієї технології для підвищення рівня безпеки даних в різних галузях діяльності.

Практична значущість результатів полягає в можливості їх використання для розробки та впровадження систем захисту даних на основі технології блокчейн. Розглянуті у роботі практичні приклади застосування блокчейну дозволяють ідентифікувати конкретні сценарії використання технології для забезпечення безпеки даних і розробляти стратегії їх впровадження.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

1.1 Основні поняття захисту інформації та забезпечення безпеки даних

В епоху інформації, безпека даних стає ключовою проблемою. Здається, що кожен наш крок відображається у базах даних, і наша особиста інформація ніколи не була такою вразливою. У світі кіберпростору організації постійно виявляють слабкі місця у своїх системах і впроваджують нові заходи безпеки. Ці заходи повинні бути спрямовані на захист основних аспектів інформації: конфіденційності, цілісності і доступності, щоб бути ефективними проти кібератак.

Термін «інформація» має своє коріння у слові «Informatio» з англійської мови, що вказує на роз'яснення, повідомлення або виклад. Філософський погляд вбачає у ньому представлення оточуючого світу за допомогою даних. Існує багато визначень терміну «інформація» [2, с. 226]. В рамках нашого контексту ми використовуємо таке: «Інформація» – це документована або публічно розкрита інформація про явища та події, що відбуваються у громаді, державі та навколишньому середовищі.

У науковій літературі поняття «інформація» має іншу інтерпретацію. Воно описує інформацію про людей, речі, технології, інструменти, ресурси, події та явища, що відбуваються у всіх сферах життєдіяльності країни, громади та довкілля. Інформація може бути представлена у формі сигналів, зображень, знаків або іншими способами [26, с. 162].

У 1921 році англійський вчений Р. Фішер, один із піонерів математичної статистики, вперше ввів термін «інформація» у наукові дослідження. Він розумів під інформацією будь-які дані, що передаються усним, письмовим або іншими способами. Це трактування інформації вважається класичним і сформувалося на

так званому «докібернетичному» етапі визначення цього поняття [32, с. 15].

На сьогоднішній день науковці виокремлюють три основні підходи до визначення поняття «інформація» як теоретичної категорії: кібернетичний, філософський та правовий. Розвиток кібернетичного підходу розпочався у 40-х роках XX століття і пов'язаний з іменами американських вчених К. Шеннона та Н. Вінера. В їхніх роботах з кібернетики (математичної) теорії інформації та теорії передачі даних каналами зв'язку під інформацією розумілися всі види повідомлень, і були запропоновані ймовірнісні методи для визначення обсягу інформації, яка передається. Також була визначена схема системи передачі інформації: джерело – передавач – лінія зв'язку – приймач – адресат – джерело перешкод [2, с. 228].

Визначення інформації з точки зору кібернетики, незалежно від способу та мети її використання, мало свої особливості. По-перше, допускалось широке трактування інформації, що означало, що інформацією можуть бути не лише повідомлення, але і команди, заборони тощо. З точки зору форми, інформація могла бути представлена не лише мовою, але і будь-яким кодом, таким як генетичний, електронний імпульсний код, нервовий код, код гормонів і т. д. Цей підхід до визначення інформації дозволяв розглядати поширювачем інформації не лише людину, але і будь-які інші живі організми і явища неживої природи.

У чинному українському законодавстві вміщені різноманітні тлумачення терміну «інформація», що обумовлено необхідністю регулювання відповідних сфер громадського життя, враховуючи інформаційно-трансформаційні процеси у нашій країні. Перше офіційне визначення інформації з'явилося у Законі України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. Згідно з цим Законом, «інформація» – це будь-які дані або відомості, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [20].

Більш докладне розуміння терміну «інформація» закріплене у Законі України «Про захист економічної конкуренції» від 11 січня 2001 року № 2210-III. Згідно з цим Законом, «інформація» – це будь-які відомості у будь-якій формі та вигляді, що збережені на будь-яких носіях (включаючи листування, книги,

помітки, ілюстрації, фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), а також пояснення осіб та будь-які інші публічно оголошені або документовані відомості (п. 2 ст. 1) [19].

Зробивши аналіз визначень поняття «інформація» з різних законодавчих документів, можна зробити висновок, що «інформація» – це багатогранний термін, який охоплює будь-які дані або відомості, незалежно від їх форми, вигляду та способу збереження або передачі. Вона може бути представлена у різних форматах, включаючи текстовий, графічний, звуковий, а також в електронному або фізичному вигляді. Це підтверджує важливість і різноманітність інформаційних процесів у сучасному світі, де інформація виступає ключовим ресурсом для розвитку суспільства, економіки та технологій

Основні характеристики інформації включають такі аспекти [25, с. 162]:

1. Конфіденційність – здатність інформації захищатися від несанкціонованого доступу.

2. Цілісність – властивість інформації захищатися від несанкціонованого спотворення, руйнування або знищення.

3. Доступність – можливість інформації бути доступною та захищеною від несанкціонованого блокування.

4. Об'єктивність – здатність інформації об'єктивно відображати події, що відбуваються в світі.

Інформаційний процес можна поділити на кілька етапів, які складають життєвий цикл інформації [3, с. 151]:

1. Отримання інформації – це процес набуття, збору та накопичення документованої або публічно оголошеної інформації громадянами, юридичними особами або державою, відповідно до діючого законодавства України.

2. Обробка інформації – це сукупність операцій, які включають збір, введення, запис, перетворення, зчитування, зберігання, знищення та реєстрацію даних, здійснюваних за допомогою технічних та програмних засобів, включаючи обмін даними через канали передачі даних.

3. Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб та держави.

4. Зберігання інформації – це забезпечення належного стану інформації та її фізичних носіїв.

5. Знищення інформації.

6. Оновлення – процес формування інформації у джерелі її походження.

Всі аспекти людського життя безпосередньо пов'язані зі сферою інформації, яка має велике значення і потребує захисту від різних загроз, що можуть призвести до її порушення або руйнування. Сьогоднішня потреба у стабільному та постійному захисті інформації постійно зростає. Ефективне збереження інформації має велике значення для захисту інтересів країни. Ключовим чинником розвитку суспільства і країни є створення цивілізованого та безпечного інформаційного середовища. Останнім часом відбувається інноваційний стрибок у сфері управління, завдяки успішному впровадженню новітніх технічних розробок. У той же час зростає загроза зовнішнього втручання в інформаційні системи, і серйозність наслідків несанкціонованого втручання значно збільшилася. Це привернуло значну увагу з боку багатьох країн світу та спонукало до пошуку надійних рішень. Однією з головних ознак науково-технічного прогресу є стрімкий розвиток інформаційних технологій. Проте, з поширенням цих технологій у повсякденному житті та професійній сфері зростає проблема їх безпеки.

Інформаційна безпека, згідно з законодавством України, стосується захисту інформаційного середовища громадян, яке сприяє формуванню та використанню процесу розвитку на користь суспільства, підприємств і країни. Об'єктами безпеки інформаційного середовища є людина, суспільство та держава, а завданням інформаційної безпеки є захист їхніх інтересів. Захист інформації полягає у запобіганні розголошенню захищеної інформації та уникненні несанкціонованого та ненавмисного впливу на неї. Установлення системи захисту інформації становить головну мету інформаційної безпеки підприємства [2, с. 229].

Швидкий розвиток інформаційних технологій призвів до нових досягнень у

сфері інформаційної безпеки, що має вирішальне значення для сучасного суспільства. Проблеми розробки та впровадження заходів захисту інформації стосуються практично кожної науки через високий рівень автоматизації різних сфер діяльності. Серед всіх методів криптографія займає провідне місце у захисті даних від несанкціонованого втручання. Це відмінність від інших методів, які частково залежать від фізичних характеристик, оскільки криптографічні методи ґрунтуються переважно на особливостях інформації і не враховують властивостей матеріального середовища або характеристик обчислювальних пристроїв [6, с. 460].

Отже, захист інформації – це комплекс методів та засобів, спрямованих на забезпечення цілісності, конфіденційності та доступності інформації в умовах можливих загроз, незалежно від їх природного або штучного характеру. Реалізація заходів з захисту інформації спрямована на запобігання завданню шкоди власникам та користувачам цієї інформації.

Питання захисту інформації має значний вплив на забезпечення інформаційної безпеки, яка виступає одним з важливих пріоритетів. Існує прямий зв'язок між захистом інформації та забезпеченням інформаційної безпеки, оскільки порушення заходів інформаційної безпеки може загрожувати не лише конфіденційності, але й цілісності та достовірності інформації. Інформаційна безпека передбачає захист конфіденційності та забезпечення захищеності конституційних прав і свобод людини та громадянина. Відповідно, забезпечення інформаційної безпеки передбачає забезпечення можливості доступу та використання інформації [3, с. 153].

Розповсюдження великих обсягів інформації, у тому числі за допомогою технологій великих даних, утворює величезні масиви, робота з якими передбачає вживання заходів для захисту та забезпечення доступу до неї. Організаційно-правові, технічні, програмно-апаратні та інші заходи інформаційної безпеки є важливою складовою цих заходів. Забезпечення захисту інформації може розглядатися перш за все як складова частина стану її захищеності [3, с. 153].

Захист даних – це практика забезпечення безпеки цифрової інформації від несанкціонованого доступу, порушення цілісності або крадіжки. Ця концепція включає всі аспекти інформаційної безпеки: від фізичного захисту обладнання, контролю доступу та логічної безпеки програмного забезпечення до організаційних політик і процедур.

Ефективні заходи безпеки допомагають захистити дані організацій від кіберзлочинів, людських помилок і внутрішніх загроз. Однак для забезпечення контролю над використанням власних даних також потрібні відповідні інструменти та технології. Ці інструменти можуть забезпечувати шифрування, редагування та маскування конфіденційної інформації. Ідеальна система інформаційної безпеки повинна також автоматизувати звітність, спростити аудиторські перевірки та допомогти виконати нормативні вимоги [7, с. 42].

У всьому світі організації інвестують у захист даних для захисту своїх брендів, інтелектуального капіталу, інформації про клієнтів і забезпечення контролю над важливими об’єктами інфраструктури. Недостатність або відсутність належних заходів безпеки даних може призвести до витоку інформації, що може призвести до серйозних фінансових втрат і втрати довіри споживачів. Дослідження показують, що більшість людей уникнули би співпраці з компанією, якщо б сталася витік даних, тому що надійне програмне забезпечення для захисту даних є невід’ємною частиною успішного бізнесу.

Таким чином, зробимо висновок, що захист інформації та забезпечення безпеки даних – це критично важливі аспекти для будь-якої організації, незалежно від її розміру чи сфери діяльності. Основні поняття в цій сфері включають заходи з фізичного та логічного захисту, політики та процедури безпеки, а також використання відповідних технологій та інструментів.

Важливо розуміти, що захист інформації не обмежується лише технічними аспектами, а також охоплює організаційні та правові положення, які регулюють доступ до інформації та її використання. Забезпечення безпеки даних передбачає виявлення, запобігання та реагування на потенційні загрози, що можуть призвести до несанкціонованого доступу, витоку чи порушення цілісності інформації.

Ефективний захист інформації та безпека даних вимагають комплексного підходу, який враховує як технічні, так і організаційні аспекти. Ретельне планування, впровадження відповідних політик та процедур, а також використання сучасних технологій допоможуть організаціям забезпечити надійний захист своєї інформації та даних.

1.2 Історія та розвиток технології блокчейн

Blockchain – термін, що складається з англійських слів «block» (блок) та «chain» (ланцюг). Блок – це файл з певними характеристиками, такими як частота створення, розмір та дані, які зашифровані криптографічними алгоритмами. Ланцюг – це послідовне поєднання блоків, при цьому кожен новий блок містить посилання на попередній. Цей метод зберігання даних унеможливлює підробку, оскільки будь-яка зміна в будь-якому блоку призведе до зміни його посилання, що викличе «ланцюгову реакцію» і відхилення змін [1, с. 2].

Ідея блокчейн-технології виникла ще в 1991 році, коли вчені-дослідники Стюарт Хабер та В. Скотт Сторнетт запропонували обчислювально-практичне рішення для тимчасового маркування цифрових документів, щоб забезпечити їх незмінність та неможливість підробки. Ця система використовувала криптографічно захищений ланцюг блоків для зберігання документів із позначками часу, а у 1992 році в неї були внесені покращення у вигляді додавання дерев Меркла. Це поліпшило ефективність системи та дозволило об'єднати кілька документів в один блок. Проте, не зважаючи на ці досягнення, ця технологія не знайшла широкого застосування, і патент втратив чинність у 2004 році, за чотири роки до того, як з'явився Bitcoin [4, с. 7].

У 2004 році Хел Фінні (Гарольд Томас Фінні II), комп'ютерний вчений та активіст з криптографії, представив нову систему під назвою RPoW, що скорочено від Reusable Proof Of Work. Ця система використовувала механізм Hashcash для

отримання невзаємозамінних токенів proof of work, але відмінністю було створення токенів з підписом RSA, які можна було передавати від особи до особи. Система RPoW вирішувала проблему подвійних витрат, зберігаючи власницькі права на токени, зареєстровані на довіреному сервері. Цей сервер був спеціально розроблений таким чином, щоб користувачі з будь-якої точки світу могли перевіряти його правильність та цілісність в реальному часі [4, с. 8].

У кінці 2008 року була представлена концепція децентралізованої системи електронних грошей під назвою Bitcoin у whitepaper. Цей документ був опублікований у списку криптографічної розсилки під псевдонімом Сатоші Накамото. В Bitcoin захист від подвійних витрат забезпечувався за допомогою алгоритму Hashcash proof of work та децентралізованого P2P-протоколу для відстеження та перевірки транзакцій. Це відрізнялося від підходу RPoW, який використовував апаратну функцію довірених обчислень. По суті, Bitcoin «майниться» за допомогою механізму proof-of-work окремими майнерами, а потім перевіряється децентралізованими нодами мережі. Перший блок Bitcoin було видобуто 3 січня 2009 року Сатоші Накамото, за що він отримав винагороду у розмірі 50 BTC. Хел Фінні став першим одержувачем Bitcoin, коли отримав 10 BTC від Сатоші Накамото у першій у світі транзакції з Bitcoin 12 січня 2009 року [9].

У 2013 році В. Бутерін, який був програмістом і співзасновником журналу Bitcoin Magazine, висловив думку, що для Bitcoin необхідна скриптова мова, яка дозволить створювати децентралізовані програми. Однак, не знайшовши підтримки спільноти, Бутерін вирішив розпочати розробку нової платформи розподілених обчислень на основі блокчейну, яка отримала назву Ethereum. У цій платформі була реалізована функція сценаріїв, відома як смартконтракти [10, с. 22].

Смартконтракти – це програми або скрипти, що запускаються та виконуються у блокчейні Ethereum. Вони можуть бути використані, наприклад, для здійснення транзакцій за умови виконання певних умов. Смартконтракти написані за допомогою певних мов програмування і компілюються в байт-код,

який потім може бути виконаний децентралізованою віртуальною машиною Ethereum (EVM), яка є повністю тьюринговою. Розробники також можуть створювати та публікувати додатки, які працюють у блокчейні Ethereum. Ці додатки зазвичай називаються dApp (децентралізованими додатками), і вже існує сотні dApp на платформі Ethereum, включаючи соціальні мережі, ігрові програми та фінансові біржі [14, с. 42].

Криптовалюта Ethereum відома як Ether і може бути переказана між акаунтами та використана для оплати комісій за обчислювальні потужності, які використовуються для виконання смартконтрактів. Сьогодні блокчейн-технологія привертає велику увагу і вже застосовується в різних програмах, не обмежуючись криптовалютами [16].

Основна відмінність між блокчейном та типовими базами даних полягає в тому, що бази даних використовують таблиці для зберігання інформації, тоді як блокчейн використовує блоки, які зв'язані між собою. Блокчейн є децентралізованою базою даних, тобто інформація зберігається на великій кількості комп'ютерів, що можуть знаходитись у будь-якій точці світу, без наявності центрального сервера. Ці комп'ютери відомі як вузли.

Блокчейн є прозорою системою, де кожен може отримати доступ до інформації про будь-який блок. Використання криптографічних алгоритмів у блокчейні гарантує незмінність блоків транзакцій та керує аутентифікацією. Хешування, що застосовується в цій системі, це криптографічна техніка, яка перетворює будь-який вхідний набір даних у стрічку фіксованої довжини. Хеш-функції в блокчейні повинні відповідати умові відсутності колізій, тобто неможливості отримати однаковий хеш для різних наборів вхідних даних [15, с. 85].

Хеші використовуються для вказівок на суміжні блоки у зв'язаному списку. У блокчейні вся інформацію у кожному блоку хешується для створення вказівника за допомогою бінарного дерева хешів, так званого дерева Меркла. Це означає, що зміна будь-якого фрагмента інформації призведе до зміни хешу самого блоку і, відповідно, усього ланцюжка. Крім того, у блокчейні використовуються цифрові

підписи, що ґрунтуються на криптографії з відкритим ключем. Відкритий ключ використовується для перевірки електронного підпису і доступний для всіх. Закритий ключ залишається конфіденційним і потрібний для створення електронного підпису [15, с. 86].

Хоча відкритий ключ можна обчислити за допомогою закритого, зворотний процес має бути практично неможливим, крім випадків застосування брут-форсу. Ініціатор транзакції підписує дані своїм закритим ключем, шифрує повідомлення за допомогою публічного ключа одержувача, а отримувач розшифровує дані за допомогою свого закритого ключа [16]. Таким чином, єдиний, хто може розшифрувати повідомлення, – це власник приватного ключа, для якого адресована транзакція. Підпис використовується для підтвердження того, що саме цей користувач ініціював транзакцію. Маючи повідомлення, підпис та публічний ключ підписанта, можна підтвердити його автентичність.

З огляду на історію та розвиток технології блокчейн можна зробити кілька важливих висновків:

1. Початки технології блокчейн сягають кінця 20 століття, коли було запропоновано ідеї, що лягли в основу сучасних концепцій.

2. Розвиток технології блокчейн став послідовним процесом, який включав удосконалення і доповнення оригінальних ідей, що зробило можливим її впровадження в різноманітних галузях.

3. Виникнення Bitcoin і Ethereum відіграли ключову роль у популяризації технології блокчейн і розширенні її можливостей, відкривши шлях для нових застосувань та інновацій.

4. Технологія блокчейн викликає зростаючий інтерес у різних галузях, таких як фінанси, логістика, медицина та громадський сектор, оскільки вона пропонує нові можливості для забезпечення безпеки, прозорості та ефективності.

5. У майбутньому технологія блокчейн може продовжити свій розвиток і стати ключовим інструментом для забезпечення інноваційного та стабільного цифрового середовища.

1.3 Застосування технології блокчейн для безпеки даних

Основні переваги технології блокчейн включають ряд ключових аспектів, таких як децентралізація, прозорість, надійність, швидкість та ефективність. Децентралізація забезпечує розподілене зберігання даних на різних комп'ютерах, що робить систему майже непридатною до взлому. Прозорість дає можливість користувачам перевіряти всі транзакції в реальному часі. Надійність гарантується за рахунок унікального хеш-коду кожного блоку, що ускладнює його модифікацію без відповідного впливу на весь блокчейн.

Крім того, блокчейн-технологія сприяє зниженню витрат на проведення транзакцій, оскільки всі операції можуть здійснюватися без посередницьких послуг. Наприклад, у банківській системі частина коштів йде на оплату послуг банку, але цю витрату можна значно зменшити за допомогою блокчейн-технології. Безпеку забезпечує криптографія та перевірка підписів, які дозволяють перевірити автентичність транзакцій. Надійність блокчейн-технології забезпечується її базуванням на математичних принципах та протоколах.

Одним з основних принципів технології блокчейн є консенсус, що означає, що кожен учасник мережі повинен погоджуватися з правильністю транзакцій. Якщо один учасник намагається провести фальшиву транзакцію, інші учасники відхилять її, не допустивши пройти. Це забезпечує безпеку та надійність мережі, а також дозволяє зберігати інформацію відкритою та анонімною. Крім того, технологія блокчейн дозволяє кожному користувачеві брати участь у децентралізованій мережі. Вона вже застосовується у різних галузях, таких як фінанси, логістика, медицина, нерухомість та інші, що свідчить про її потужний потенціал і можливість впливати на розвиток різних сфер діяльності, забезпечуючи безпеку, прозорість та ефективність [34].

Технологія блокчейну пояснює проблеми безпеки та довіри через кілька механізмів. По-перше, нові блоки завжди додаються лінійно та хронологічно до

кінця блокчейну, ускладнюючи зміну вмісту блоку після додавання. Це через те, що кожен блок має свій унікальний хеш, а також хеш попереднього блоку. Якщо дані будь-яким чином змінюються, змінюється і хеш-код, що важливо для забезпечення безпеки. Наприклад, якщо хакери намагаються змінити транзакцію від Amazon, то буде потрібно змінити кожен блок на шляху. Це потребує величезної обчислювальної потужності і ускладнює втручання в мережу. Для забезпечення довіри, мережі блокчейну використовують тести, що перевіряють комп'ютери перед приєднанням до мережі. Один з найпоширеніших тестів, використаних Bitcoin, – це «доказ роботи» [10, с. 26].

У системі доказу роботи комп'ютери мають вирішити складну обчислювальну математичну задачу, щоб «довести», що вони виконали роботу. Якщо цю задачу вирішено, комп'ютери отримують дозвіл на додавання блоку до блокчейну. Процес цього додавання, відомий як «видобування» у криптовалютному світі, складний. Хоча доказ роботи не гарантує повну безпеку від атак хакерів, він ускладнює їх можливість. Щоб здійснити успішну атаку, хакерам довелося б вирішити складні обчислювальні задачі на дуже великому рівні. Витрати на таку атаку майже завжди перевищують можливу вигоду [10, с. 27]. Основна мета блокчейну – дозволити записати та поширити цифрову інформацію, не дозволяючи її редагувати.

Блокчейн природно забезпечує повну цілісність інформації, що значно підвищує рівень захищеності системи від таких видів атак, як модифікація, імітація відправника, повторна передача повідомлення або відмова від повідомлення. Відповідно до Настанови з державних стандартів ТЗІ 1.1-003-99 [23], критеріями оцінки захищеності є сукупність вимог, що використовуються для оцінки ефективності функціональних послуг безпеки та коректності їх реалізації. Система з блокчейном відповідає критерію «ЦД-4. Абсолютна довірча цілісність» та «ЦЗ-3. Повна цілісність при обміні» [25, с.164].

Мережі блокчейн розподілені між усіма комп'ютерами учасників (консорціумна мережа). Кожен учасник може в реальному часі відслідковувати кожну транзакцію в мережі. Партнер також може відхилити неправильні

транзакції перед їх внесенням до реєстру. Це полегшує процес аудиту та значно знижує ризик шахрайства. Крім того, розробники створюють нові додатки для ланцюжка постачання та загальних робочих процесів, що відкриває нові джерела доходу через створення нових продуктів та послуг на основі блокчейну [18, с. 123].

Учасники децентралізованої мережі спільно зберігають інформацію в захищених криптографією блоках з даними. За допомогою алгоритмів консенсусу учасники вирішують, наскільки вони можуть довіряти один одному. Для мережі важливо, щоб транзакція була схвалена більшістю учасників мережі (поріг 51%), після чого новий блок буде доданий до ланцюга, який неможливо буде змінити пізніше [18, с. 123].

Оскільки мережа є децентралізованою, відсутній будь-який центральний хаб для зберігання усієї інформації або посередник, який координує взаємодію мережі між двома сторонами. Ця мережа різко відрізняється від традиційних централізованих мереж, де завжди присутній головний вузол, що відповідає за керування всією структурою. Блоки в ланцюжку блокчейну не можуть бути змінені або видалені, оскільки кожен наступний блок містить хеш попереднього блоку. Таким чином, будь-які спроби маніпулювати інформацією в блокчейні не залишаться непоміченими [25, с.165].

Враховуючи попередній досвід, блокчейн стає надійним засобом захисту від крадіжок інформації завдяки ускладненню процесів підробки блоків у ланцюзі. Тому очікується, що будуть спроби зловживання та маніпулювання цією технологією. Передбачається, що блокчейн залишиться стійким у постквантову еру, але для цього потрібно буде здійснити значні зусилля та витрати, які перевищать витрати на захист традиційних технологій.

На сьогоднішній день найбільшу вразливість в системі практичного застосування блокчейну становлять централізовані біржі. Саме через їх централізованість вони стають об'єктами численних атак. Головний принцип цієї архітектури є найбільш вразливим місцем, яке не можна виправити. Це призводить до зростання попиту на децентралізовані системи. Багато організацій

починають усвідомлювати переваги технології блокчейн і починають впроваджувати її в свою діяльність [15, с. 86].

Таким чином, зробимо висновок, що застосування технології блокчейн для безпеки даних демонструє значний потенціал у забезпеченні високого рівня захисту інформації. Ця технологія, завдяки своїм особливостям, таким як децентралізація, невідворотність та криптографічний захист, дозволяє створити безпечні та надійні системи зберігання та обміну даними. Вона дозволяє уникнути впливу централізованих точок вразливості, зменшує ризик маніпуляцій та підробки даних, а також забезпечує прозорість та надійність процесів обробки інформації. Однак важливо розуміти, що впровадження технології блокчейн вимагає обміркованого підходу та врахування специфіки конкретної ситуації. Тим не менше, в цілому можна зробити висновок, що застосування технології блокчейн для безпеки даних відкриває нові можливості для створення ефективних та безпечних інформаційних систем.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Ключові характеристики технології блокчейн

Блокчейн – це розподілена база даних, що постійно розширюється і містить список записів, відомих як блоки, із захистом від підробки та змін. Кожен блок включає в себе мітку часу і посилання на попередній блок у ланцюгу хешів. Ця технологія, яка була винаходом або результатом спільних зусиль людини чи групи людей, відомих під псевдонімом Сатоші Накамото, пережила значні зміни та здобула популярність у всьому світі після винайдення та формулювання принципів її функціонування [16].

Блокчейн представляє собою нову надійну технологію зберігання записів, що може радикально змінити підхід до створення та зберігання баз даних, дозволяючи розповсюджувати інформацію мережею без необхідності її копіювання між учасниками мережі. Таким чином, блокчейн створює нову основу для нового типу всесвітнього Інтернету. Хоча оригінальна розробка цієї технології була спрямована на створення нового слова в області криптовалют, таких як Bitcoin, ETH (Ethereum) і інші, з часом фахівці в галузі техніки почали виявляти нові можливості та варіації цього методу, як, наприклад, в системі документообігу на блокчейн [11, с. 26].

Блокчейн – це система, яка забезпечує точний облік та ідентифікацію інформації, дозволяє розповсюджувати цю інформацію між користувачами мережі, одночасно працюючи з нею для кількох користувачів і фіксуючи час кожної транзакції. Цифровий кластер блокчейну призначений для зберігання змін в мережі, який може бути програмований не тільки для фіксації фінансових транзакцій, але й будь-яких інших значень, які існують у світі. Ця технологія дійсно може захистити дані, з якими працюється, зробивши їх більш доступними

й прозорими. Крім того, вона може значно зменшити витрати та скоротити час, необхідний для вирішення виникаючих проблем і виправлення помилок.

Блокчейн – це система обліку, розподілена серед спільноти, що дозволяє зберігати та обмінюватися інформацією в Інтернеті. У цій системі кожен учасник має свою власну копію інформації, і всі члени повинні одночасно підтверджувати будь-які оновлення. Це можуть бути операції, контракти, активи, посвідчення особи або будь-які інші дані, які можна ідентифікувати цифровим чином. Записи є стійкими, прозорими та доступними для пошуку, що дозволяє користувачам системи переглядати всю історію транзакцій. Кожне оновлення представляє собою новий блок, який додається до кінця кожного ланцюжка. Використання блокчейну для шифрування заміняє необхідність сторонніх посередників, що підвищує довіру та цілісність системи [9].

Блокчейн – це послідовний ланцюг блоків, що містять інформацію, і побудований згідно з певними правилами. Ця технологія може значно спростити відстеження сумнівних транзакцій та взагалі підвищити прозорість угод. Основна ідея полягає в розподіленому підтвердженні транзакцій, де учасники самостійно перевіряють та підтверджують їх автентичність, утворюючи блоки записів. Блокчейн – це децентралізована база даних, де всі блоки зв'язані між собою за допомогою криптографії.

Важливою концепцією блокчейн є децентралізація, де жоден комп'ютер чи організація не володіє мережею. Це означає, що інформація зберігається на різних незалежних серверах, що розповсюджені та не мають єдиного власника чи місця розташування. Децентралізація блокчейн значно знижує ризик фальсифікації даних, оскільки інформація розподілена по всій мережі, а не зосереджена в одному центрі. Це ускладнює спроби хакерів атакувати мережу, оскільки їм доведеться пошкодити дані у всіх блоках. Кожна зміна в блокчейні відображається для всіх учасників та потребує підтвердження більшістю, що ускладнює можливість здійснення атак [9].

Основна мета технології блокчейн полягає у надійному передаванні власності на цифрові активи в мережі, де відсутні посередники та встановлюється

недовірче середовище. Основою цієї технології є розподілене зберігання інформації, що дозволяє зберігати важливі дані одночасно на багатьох серверах (у всіх учасників мережі), забезпечуючи відкритість та надійність. Наприклад, блокчейн може зберігати історію банківських операцій клієнтів, транзакції, результати голосування, документи або медичні записи. Оскільки дані зберігаються одночасно у багатьох місцях і не можуть бути змінені без згоди всіх учасників, вони стають недоступними для фальсифікації та крадіжки [8, с. 118].

Отже, основна ідея використання блокчейну полягає у можливості дозволити недовірливим сторонам обмінюватися цінною інформацією безпечним та захищеним від фальсифікації способом. Блокчейн відрізняється своєю незмінністю даних, яка досягається завдяки застосуванню криптографії, а не залежить від довіри до будь-кого. Два основні криптографічні алгоритми, що використовуються в блокчейні, – це хеш-функції і електронні підписи, що гарантують цілісність транзакцій і забезпечують авторизацію.

Blockchain – це послідовність блоків даних, які генеруються та зберігаються на комп'ютерах учасників мережі. Основною концепцією блокчейн є транзакція – основний спосіб змінення стану даних. Кожен блок представляє собою структуру даних, яка містить список транзакцій. Вузли мережі блокчейн створюють транзакції, обмінюються ними та змінюють стан блокчейн. Зазвичай копії ланцюжків блоків зберігаються та обробляються незалежно одна від одної на різних комп'ютерах. Фактично, блокчейн є системою зберігання даних, яка не залежить від централізованого сервера або групи серверів.

Блокчейн працює за наступними правилами (рис. 2.1) [6, с. 461]:

1. Нові транзакції розсилаються до всіх вузлів.

2. Кожен вузол об'єднується в блок і намагається знайти хеш блоку транзакцій.

3. Коли такий хеш знайдений, блок відправляється в мережу.

4. Вузли приймають цей блок лише в разі, якщо всі транзакції в ньому є правильними.

5. Вузли висловлюють свою згоду з новими даними, починаючи роботу в

наступному блоку та використовуючи хеш попереднього як вихідні дані.

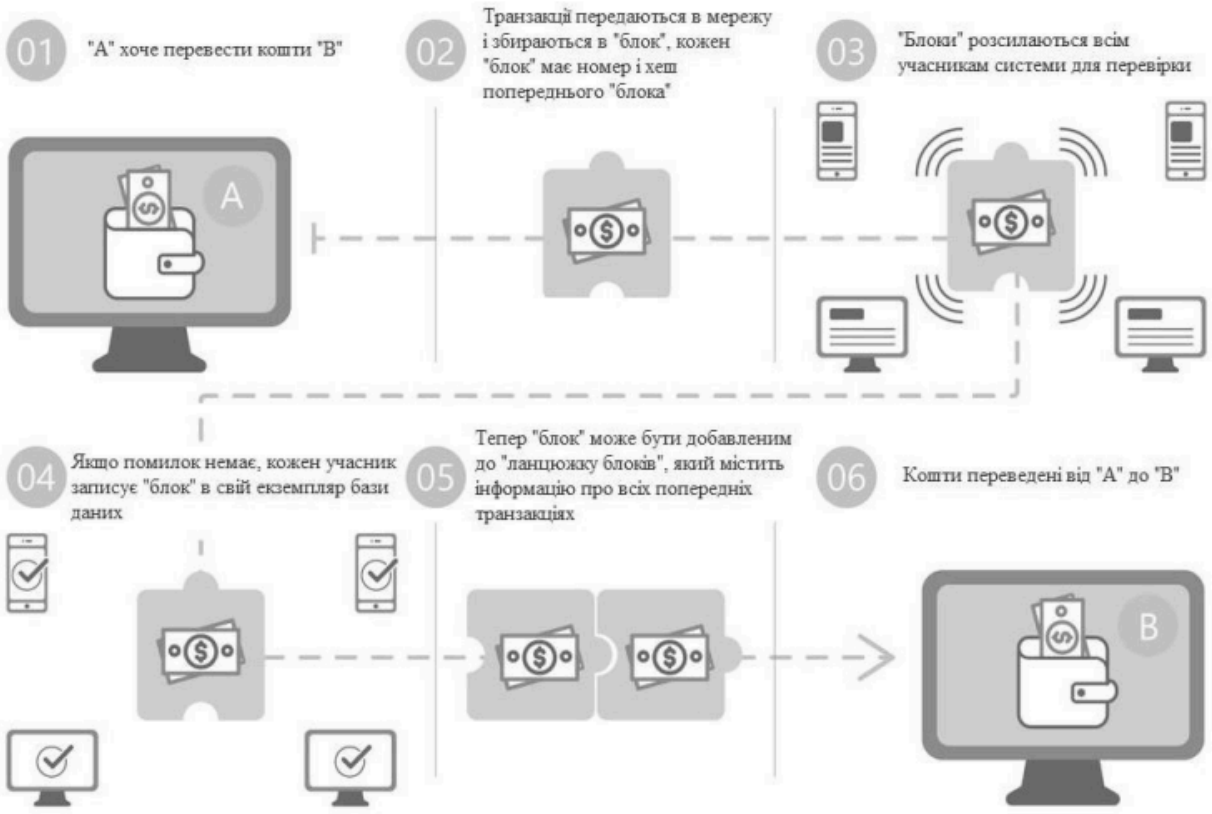


Рис. 2.1 – Схема роботи системи блокчейн [6]

Однією з найбільш перспективних та обіцяючих областей застосування блокчейн є технологія захищеного документообігу. Вона може стати значно безпечнішою, перш за все, завдяки веденню децентралізованого реєстру документів, який неможливо змінити або підкоригувати. Користувачі зможуть працювати з документами, маючи повну впевненість у їх автентичності та справжності.

Всі механізми технології блокчейн базуються на використанні наступних технологій та методів обробки та захисту даних [4]:

1. Асиметричні криптосистеми.

2. Хеш-функції або «хешування» даних (функції MD та SHA).

3. Хеш-таблиці для запису результатів операцій хешування в блоках транзакцій.

4. Смарт-контракти – це метод передачі даних (цифрових цінностей) від однієї особи до іншої.

5. Токени та використання механізму Proof of Concept (PoC) – доказ концепції як методу верифікації подій (підтвердження угоди) в системі.

Коли мова заходить про класифікацію блокчейнів, найбільш корисною є класифікація, запропонована творцем криптовалюти Ethereum В. Бутеріном, яка виокремлює три типи блокчейнів: публічні блокчейни з відкритим доступом, консорціумні блокчейни з відкритим доступом та приватні блокчейни з обмеженим доступом.

Публічний блокчейн з відкритим доступом – це блокчейн, який доступний для читання будь-якому користувачеві, кожен з яких може здійснювати транзакції. У такому випадку транзакції захищені криптографічними методами підтвердження, такими як підписання транзакції або підписання акцій. На даний момент цей тип є найпоширенішим і використовується в таких криптовалютах, як Bitcoin, Ethereum, Ripple та інші. Він особливо підходить для застосування у системах документообігу, де потрібна повна незалежність від третіх осіб, прозорість операцій і висока надійність системи. Крім того, публічний блокчейн забезпечує захист користувачів додатків від розробників, обмежуючи їхні можливості. У додатках на публічному блокчейні розробник не може самостійно змінювати код або дані. Основними характеристиками його є [4]:

1. Абсолютна доступність блоків для всіх користувачів.

2. Немає необхідності в довірі між користувачами.

3. Повна децентралізація та незалежність від посередників.

4. Безпека мережі забезпечується за рахунок криптографічних алгоритмів та використання великої кількості комп’ютерних систем.

Приватний блокчейн з відкритим доступом – це система, в якій право завіряти транзакції, вести аудит безпеки, вносити зміни в програмне забезпечення та бази даних належить тільки привілейованим користувачам, іншим же надається доступ лише для читання файлів. Така система вже не є повністю децентралізованою і залежить від певного кола осіб. Вона може бути корисною для державних структур і має такі основні властивості [9]:

1. Існування перевірених валідаторів.

2. Висока швидкість підтвердження транзакцій.

3. Відсутність можливості проведення атаки 51%.

4. Можливість видалення або зміни записів у ланцюжку.

5. Низька вартість транзакцій через відсутність необхідності великих обчислювальних потужностей.

Приватний блокчейн з закритим доступом має ті ж властивості, але з умовою, що прості користувачі не можуть стати учасниками мережі без підтвердження валідаторів і не завжди мають доступ до читання файлів ланцюжка. Така система повністю перестає бути відкритою і незалежною від третіх осіб. Отже, приватний блокчейн це технологія, яка централізовано визначає створення блоків, і всі права на здійснення транзакцій належать одній організації. Користувачі можуть лише читати інформацію для контролю, але лише надійні сайти можуть керувати базами даних та іншими програмами. Властивості даної системи включають [1, с. 4]:

1. Закритість даних від непривілейованих користувачів мережі.

2. Повна закритість мережі від неавторизованих користувачів.

3. Неможливість проведення атаки 51%.

4. Повна залежність від кола привілейованих користувачів.

5. Висока надійність і стійкість мережі за умови довіри до валідатора.

Ще однією перевагою приватного блокчейну є його більший рівень контролю з боку адміністрації. Суть полягає в тому, що приватний блокчейн, на відміну від публічного, дозволяє швидко оновлювати функціональність. Це робить його привабливим для організацій, які працюють з документами та системами бухгалтерського обліку та управління документами, оскільки він створює контрольоване та передбачуване середовище порівняно з публічним блокчейном.

Зведемо ці основні особливості трьох типів блокчейнів у таблицю 2.1:

Таблиця 2.1 – Порівняльна таблиця трьох типів блокчейнів

Особливості	Публічний блокчейн з відкритим доступом	Приватний блокчейн з відкритим доступом	Приватний блокчейн з закритим доступом
Доступ до блокчейну	Відкритий для всіх користувачів, можливість відправлення транзакцій та перевірки даних.	Відкритий для всіх користувачів, проте лише привілейовані користувачі можуть проводити аудит безпеки та вносити зміни.	Лише привілейовані користувачі мають доступ до мережі та можуть проводити аудит безпеки та змінювати дані.
Децентралізація	Повна децентралізація, незалежність від третіх осіб.	Часткова децентралізація, залежність від привілейованих користувачів	Можливий рівень децентралізації, залежить від управління адміністраторів
Керування	Відсутнє централізоване керування	Децентралізоване керування, проте з обмеженими можливостями для привілейованих користувачів	Централізоване керування адміністрацією мережі
Відкритість даних	Публічний доступ до всіх даних та транзакцій	Публічний доступ до даних, але обмеження для проведення аудиту та змін	Обмежений доступ до даних та можливості внесення змін
Швидкодія	Може бути менш ефективним через велику кількість вузлів та глобальну доступність	Може бути більш ефективним, оскільки має менше вузлів та обмежений доступ	Може бути найефективнішим, оскільки має обмежену кількість вузлів та контрольований доступ
Вартість	Дороге управління через велику кількість вузлів	Вартість управління залежить від розміру та складності мережі	Менша вартість управління через обмежену кількість вузлів та контрольований доступ

Джерело: складено автором самостійно

Таким чином, існують два основних типи блокчейнів: загальнодоступний і приватний. У загальнодоступному блокчейні будь-який користувач може читати дані та виконувати дії. У приватному блокчейні блоки формуються централізовано, і всі права на проведення операцій належать одній організації. У цьому випадку широкий загал може лише переглядати дані, тоді як тільки надійні вузли можуть керувати базами даних та іншими програмами. Приватний блокчейн

схожий на традиційні централізовані мережі, проте він має можливість ведення ланцюга блоків, що робить його застосовним для внутрішніх закритих мереж і систем захищеного документообігу в підприємствах або державних структурах, де необхідно зберігання конфіденційної інформації. Тому в даному випадку доцільним буде використання саме приватного блокчейну.

Блок транзакцій представляє собою електронну систему керування документами та спеціальну структуру для реєстрації групи транзакцій. Перш ніж транзакцію можна вважати дійсною, необхідно перевірити її формат та підписи, а потім записати групу транзакцій в спеціальну структуру – блок. Інформацію в блоках можна швидко перевірити, оскільки кожен блок завжди містить дані про попередній блок. Усі блоки можна організувати в один ланцюг, який містить інформацію про всі транзакції, що здійснені до цього часу в базі даних. Перший блок у ланцюзі, відомий як первинний блок (або Genesis block), розглядається окремо, оскільки він не має попереднього блоку [4].

Кожен блок містить заголовок, блокові дані та список транзакцій. Заголовок містить метадані для цього блоку, включаючи хеш-значення, хеш попереднього блоку, хеші транзакцій та додаткову службову інформацію. Кожен блок охоплює два типи інформації: специфічну, яка реєструє транзакції або смарт-контракти, та внутрішню, яка захищає блок і визначає його зв'язок з іншими. Блоки автоматично розповсюджуються мережею, перевіряються та зв'язуються через хеш-значення.

Структура заголовка блоку включає наступне (рис. 2.2) [9]:

1. Номер блоку, що також відомий як висота блоку.

2. Хеш-значення попереднього блоку.

3. Хеш-представлення даних блоку (для цього можна використовувати різні методи, наприклад, створити дерево та зберігання кореневого хешу або використання хешу всіх комбінованих даних блоку).

4. Відмітка часу.

5. Розмір блоку.

6. Значення nonce. Під час генерації блоку, nonce обирається випадковим чином, що використовується для генерації хешу заголовка блоку. Цей процес

створює криптографічний хеш при створенні першого ланцюжка.

Структура блоку даних включає наступне [9]:

1. Список транзакцій та подій книги, що входять до блоку.

2. Інші можливі дані.

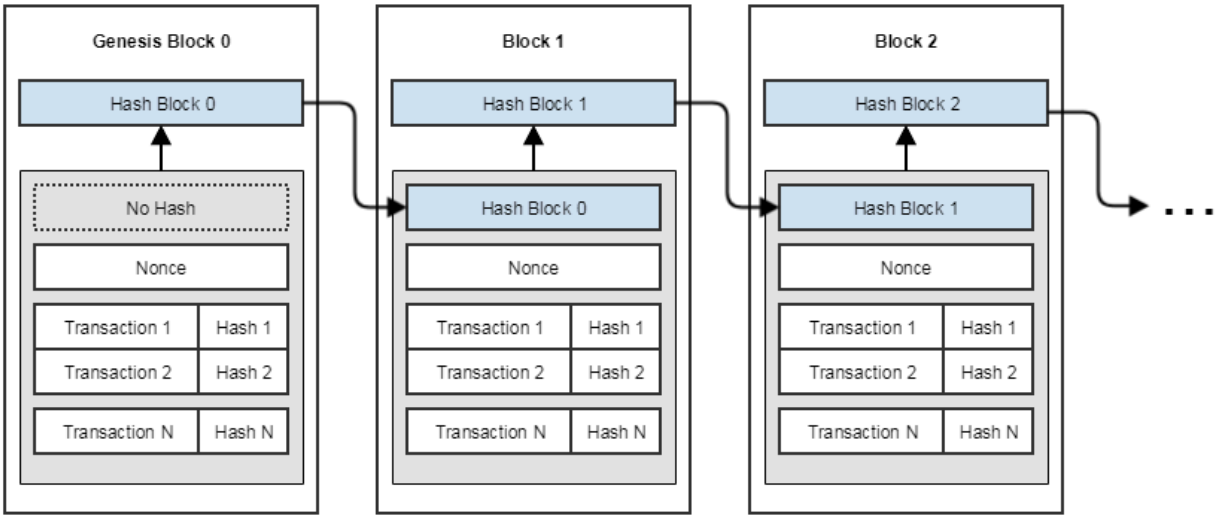


Рис. 2.2 – Структура блокчейну [9]

Блокчейн розпочинається з блоку генезису, до якого періодично додаються нові блоки. Кожен блок містить записи про здійснені транзакції. Вузли співпрацюють, щоб об'єднати ці блоки у ланцюг та сформувати книгу, яку неможливо змінити без перероблення затвердження (PoW). Кожен вузол блокчейну зберігає свою копію, а мережа потребує алгоритмічного оновлення, довіри та верифікації ланцюга. Цей процес легко контролювати та переглядати завдяки прозорості технології. Власні транзакції користувачів відображаються з унікальним буквено-цифровим ідентифікаційним номером, присвоєним кожній транзакції [6, с. 462].

Після цього слідують всі або деякі з останніх транзакцій, які ще не записані в попередні блоки. Хеш-дерево використовується для транзакцій у блоці (деревоподібне хешування). Якщо хеш заголовка менше або дорівнює певній кількості числового значення, згенерований блок буде прийнятий іншими користувачами, його значення встановлюється періодично. Результат контрольної суми є незворотнім (функція SHA-256), за винятком випадкового пошуку, немає алгоритму отримання бажаного результату. Якщо хеш не задовольняє умові,

параметр nonce у заголовку змінюється, і хеш відображається в списку. Зазвичай для цього потрібна велика кількість перерахунків. Як тільки опція знайдена, вузол надсилає отриманий блок іншим підключеним вузлам, що керують блоком. Якщо помилок немає, блок вважається доданим до ланцюжка, і наступний блок повинен містити його хеш-значення [4].

Ще одним важливим елементом є ланцюжковий блок. Блоки створюються одночасно декількома майнерами. Блоки, що відповідають критеріям, надсилаються в мережу та додаються до бази даних розподіленого блоку. Часто кілька нових блоків в різних частинах мережі можуть мати однаковий попередній блок, що призводить до розгалуження ланцюга блоків. У такому випадку можливе паралельне розгалуження різних гілок. Під час подальшої ретрансляції блоків майнери починають враховувати основний ланцюжок, враховуючи складність хешу та довжину ланцюга. При рівні складності та довжині, три блоки обираються ланцюжку, який з'явився раніше. Транзакції, введені у відхилених гілках, втрачають статус підтвердження. База даних розподіленого блокчейну є постійно наростаючим ланцюжком блоків з записами всіх транзакцій. Його створення одночасно зберігається та синхронізується на декількох комп'ютерах згідно з формальними правилами. База даних містить незашифровану інформацію про всі транзакції, які підписані асиметричним шифруванням. Для уникнення подвійного витрачання однієї і тієї ж суми база даних використовує мітки часу, розділяючи їх на окремий ланцюжок блоків, кожен з яких містить хеш та серійний номер попереднього блоку. Кожен новий блок підтверджує транзакції, інформація про які включає додаткове підтвердження транзакцій у всіх попередніх блоках ланцюга. Редагування інформації вже включеного в ланцюжок блоку недоцільно, оскільки це потребує змін у всіх наступних блоках. Тому успішна атака подвійних витрат (перевитрата раніше витрачених коштів) є практично надзвичайно малоймовірною [4].

Отже, основний механізм функціонування блокчейну можна пояснити таким чином. Кожному блоку призначається унікальний цифровий підпис, який представляє собою хеш-суму з унікальним ідентифікатором. Завдяки

математичній функції всі блоки знаходяться у необхідному порядку, що дозволяє їм утворювати ланцюжок (оскільки термін «blockchain» буквально перекладається як «ланцюжок блоків»). При будь-якої спробі змінити порядок блоків система автоматично виявляє помилку через неузгодженість структури та ідентичності. Для того щоб убезпечити систему від зміни електронного підпису та перерахунку хешу, який система фактично визначить, блокчейн використовує кілька методів захисту інформації: Доказ роботи (Proof of Work) та Доказ володіння (Proof of Stake).

2.2 Хешування у блокчейн

Хешування виступає як фундаментальний елемент у технології блокчейн, що має значний вплив на цифрову безпеку та цілісність даних у мережі. Ця концепція, що є наріжним каменем у блокчейн-технології, виконує ключову роль, особливо у сфері криптовалют. Хеш-функція виходить за рамки простого шифрування даних, стаючи важливим компонентом криптографічних процесів, таких як доказ роботи (Proof-of-Work, PoW), який є необхідним для підтвердження та додавання нових блоків у блокчейн. Це зміцнює безпеку, а також забезпечує прозорість, верифікованість та незмінність розподіленого реєстру даних [9].

Хешування, що має велике значення в комп’ютерній науці, спочатку використовувалося для ефективного пошуку даних, а згодом стало основою криптографії та ключовим компонентом у цифровій безпеці. Сутність хеш-функції полягає у тому, що вона перетворює вхідний сигнал у рядок фіксованого розміру, у вигляді хеш-значення, за допомогою математичного алгоритму. Це перетворення є детермінованим і завжди дає однаковий вихідний результат для одного і того ж вхідного сигналу. Крім того, хеш-функція має односторонній характер, тобто неможливо відновити вхідний сигнал із хеш-значення (рис. 2.3).

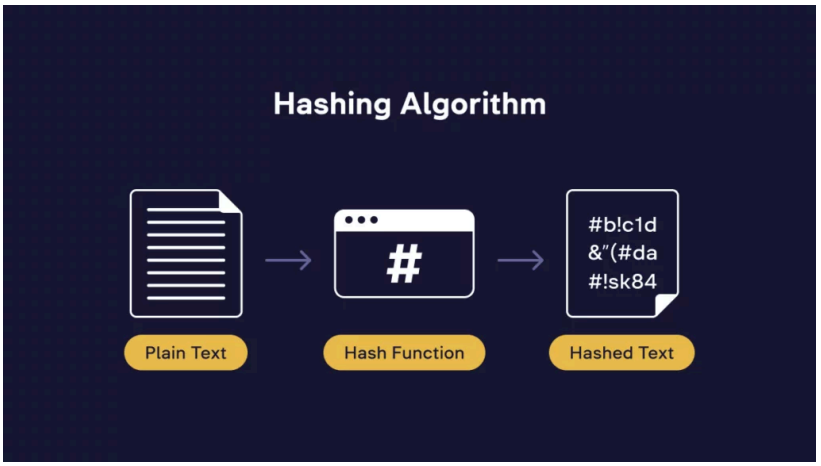


Рис. 2.3 – Алгоритм хешування [22]

Припустімо, що є юридичний договір, який необхідно зберегти в блокчейні. Замість того, щоб завантажувати весь текст контракту, мржна використати хеш-функцію, наприклад, SHA-256, для створення унікального хеш-значення. Цей хеш буде унікальним для даного документа та незмінним при будь-яких змінах в оригінальному документі. Таким чином, збереження лише хеш-значення дозволяє економити місце та підвищує конфіденційність. Пізніше, коли потрібно перевірити справжність контракту, можна застосувати хеш-функцію до поточної версії документа та порівняти отриманий хеш з тим, що зберігається в блокчейні. Це дозволяє підтвердити, що контракт не було змінено з моменту його збереження [22].

Отже, хешування не лише допомагає зекономити місце для зберігання даних, але й гарантує цілісність документа, оскільки навіть найменша зміна призводить до зміни хеш-значення. Це дозволяє зберігати фактичний зміст документа в конфіденційності, забезпечуючи його запис у блокчейні.

Біткоїн використовує алгоритм SHA-256 (Secure Hash Algorithm 256-біт). Кожен новий блок складається з заголовка (Block Header), тіла (Block Body), яке включає список транзакцій (List of Transactions), а також іншої службової інформації. Заголовок блоку (Block Header) є важливим компонентом, який майнери «маніпулюють», щоб знайти правильний хеш нового блоку (рис. 2.4).

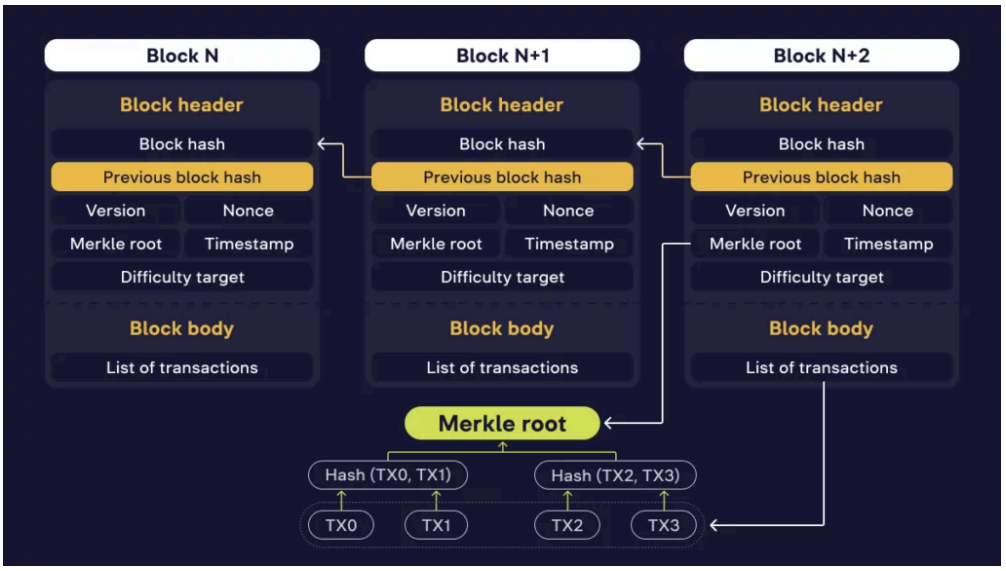


Рис. 2.4 – Алгоритм SHA-256 [26]

Розглянемо більш детально дані, які включаються до заголовка блоку в мережі Біткоїн (рис. 2.5):

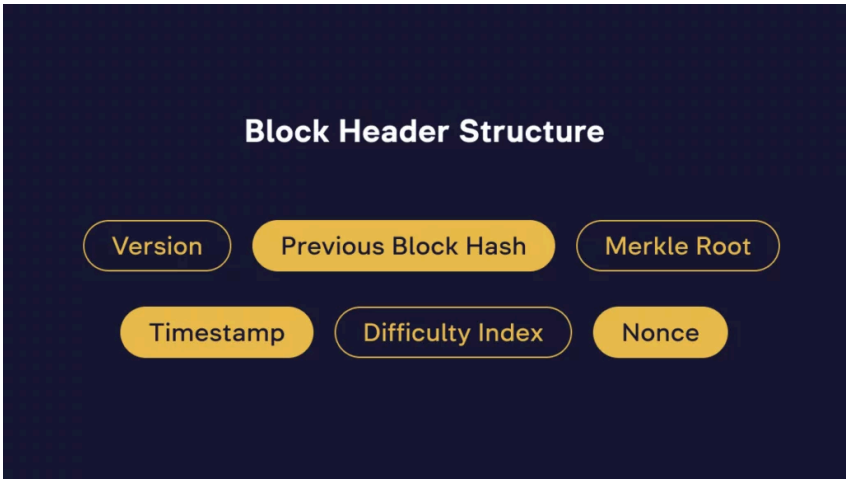


Рис. 2.5 – Заголовок блоку [26]

1. Версія блоку (Version): 4-байтове число, яке вказує на поточну версію блоку.

2. Попередній хеш блоку (Previous Block Hash): 32-байтовий хеш попереднього блоку в ланцюжку. Це критично важливий аспект безпеки блокчейну, оскільки створюється безперервний взаємозалежний ланцюжок, де кожен блок криптографічно пов'язаний зі своїм попередником.

3. Корінь Меркла (Merkle Root): 32-байтовий хеш, який представляє корінь дерева Меркла.

4. Тимчасова мітка (Timestamp): 4-байтове число, яке відображає час

створення нового блоку.

5. Цільова складність (Target Difficulty/Difficulty Index): 4-байтове число, яке визначає умови складності. Вона регулюється мережею з метою того, щоб новий блок створювався в середньому кожні 10 хвилин.

6. Випадкове число (Nonce): 4-байтове число, яке підбирають майнери. Вони часто змінюють Nonce і перераховують хеш-значення, щоб знайти відповідний, що задовольняє умовам складності.

Створення нового блоку включає об'єднання цих кількох елементів з випадковим числом (Nonce) і подальше застосування алгоритму хешування (наприклад, SHA-256) до цієї комбінації [26].

Версія блоку (з англ. Version) + Попередній хеш блоку (з англ. Previous Block Hash) + Корінь Меркла (з англ. Merkle Root) + Тимчасова мітка (з англ. Timestamp) + Цільова складність (з англ. Target Difficulty) + Випадкове число (з англ. Nonce)↓ Хешування (наприклад, за допомогою SHA-256) = Хеш

У цьому процесі майнери підбирають хеш для нового блоку, який відповідає поточному рівню складності мережі. Для цього необхідно неодноразово змінювати значення Nonce та перераховувати хеш-значення, доки не буде знайдене те, що відповідає заданим критеріям. В результаті виходить унікальний хеш, який представляє весь блок.

Хеші використовуються для заміни вказівників у звичайних структурах даних, таких як пов'язані списки та бінарні дерева. Властивість незмінності хешу одного блоку гарантує незмінність всього блокчейну. Отже, якщо хтось потребує доступу до певних даних у блоку, він може використовувати хеші у дереві Меркле для швидкого доступу до даних, замість того, щоб проходити по ним по одній. У випадку, коли транзакції зберігались б у лінійному порядку, пошук конкретної транзакції був би надзвичайно витратним. Використання хешів дозволяє представити загальний стан блокчейна, включаючи всі транзакції та їх послідовність на даний момент, одним числом – хешем найновішого блоку. Тому власність на хеш блоку забезпечує незмінність усього блокчейна (рис. 2.6) [9].

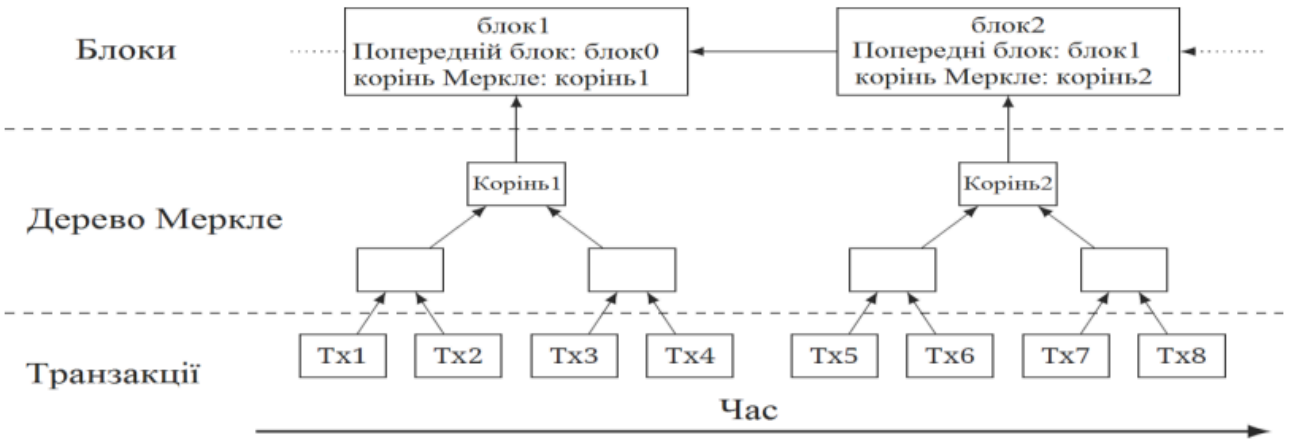


Рис. 2.6 – Графічне представлення хешування блоків транзакцій [9]

Таким чином, хешування в технології блокчейн гарантує недоторканність та безпеку криптотранзакцій, а також забезпечує стійкість та надійність блокчейну як системі, де довіра та безпека є ключовими. Хеш-функції в блокчейні забезпечують неперевершену безпеку та стабільність всього ланцюжка транзакцій. Кожен наступний блок транзакцій посилається на хеш попереднього блоку в реєстрі. Хеш самого блоку формується на основі всіх транзакцій у ньому, але вмість того, щоб обробляти транзакції окремо, вони групуються в одне хеш-значення за допомогою двійкового дерева хешів, відомого як дерево Меркле.

2.3 Алгоритми досягнення консенсусу

Алгоритм консенсусу – це механізм, що дозволяє всім учасникам мережі узгодити її поточний стан. Він забезпечує те, що кожен новий блок єдиний і погоджений всіма вузлами.

Основними завданнями алгоритму консенсусу є не лише досягнення загальної згоди, але й сприяння співпраці та кооперації, забезпечення рівних прав і відповідальностей для кожного вузла, а також включення всіх учасників у процес досягнення згоди. Ефективний алгоритм консенсусу має задовольняти кілька

критичних вимог [22]:

1. Децентралізація: механізми консенсусу повинні бути розроблені таким чином, щоб жодна особа не мала контролю над мережею. Це гарантує стійкість мережі до атак і залишає її незалежною навіть у разі збою вузла.

2. Безпека: алгоритми мають бути стійкими до атак і забезпечувати захист від маніпуляцій зловмисників, таких як подвійне витрачання коштів.

3. Масштабованість: з ростом кількості транзакцій у мережі алгоритми консенсусу повинні здати впоратися зі збільшеним навантаженням, не зашкоджуючи продуктивності чи безпеці.

4. Універсальність доступу: Кожен учасник мережі повинен мати змогу взаємодіяти з алгоритмом консенсусу, незалежно від своїх обчислювальних або фінансових можливостей.

Алгоритм досягнення консенсусу надзвичайно важливий для блокчейну, оскільки він дозволяє всім учасникам узгодити поточний стан мережі. Без таких алгоритмів було б складно переконатися, що кожен користувач бачить однакову інформацію, що може зробити систему вразливою перед атаками хакерів та шахраїв.

Існує різноманітність алгоритмів механізму консенсусу, кожен з яких працює за власними принципами. Один із найперших і найбільш відомих алгоритмів консенсусу – Proof-of-Work (PoW). Цей алгоритм передбачає, що майнери використовують спеціалізоване потужне обладнання для розв'язання складних математичних задач з метою створення нового блока. Основна мета полягає в знаходженні правильного хешу блока шляхом перебору тисяч варіантів за секунду. Перший майнер, який успішно знаходить потрібне значення, отримує право додати новий блок до ланцюга та винагороду в криптовалюті [4].

Майнери використовують різні методи видобутку криптоактивів, такі як використання відеокарт (GPU), центральних процесорів (CPU), програмованих логічних інтегральних схем (FPGA) та спеціалізованих мікросхем для (ASIC). Крім того, існують пули, де учасники об’єднують свої ресурси для збільшення шансів на успіх.

Proof-of-Stake (PoS) є екологічною альтернативою PoW. У цьому типі консенсусного алгоритму валідатори інвестують у криптовалюту системи, блокуючи певну кількість своїх монет на користь депозитного контракту, замість витрат на дороге обладнання для розв'язання складних завдань. Всі учасники беруть участь у перевірці блоків, і чим більше коштів має користувач на своєму рахунку, тим вища ймовірність того, що мережа дозволить йому створити новий блок. Замість майнерів, таких учасників називають валідаторами, і вони також отримують винагороду за свою роботу в криптовалюті. У мережах з алгоритмом PoS вузлам не потрібно конкурувати і виконувати велику кількість складних обчислень, що суттєво підвищує швидкість транзакцій [30].

Delegated-Proof-of-Stake (DPoS) розширює концепцію PoS. Цей механізм дозволяє учасникам мережі з великою кількістю активів обирати обмежену групу валидаторів, які будуть відповідати за створення нових блоків у блокчейні. Учасники мережі голосують за делегатів, використовуючи свої монети як голоси – чим більше монет вкладено в певного делегата, тим більший вплив має голос цього користувача. Делегати з найбільшою кількістю голосів отримують право на створення блоків і винагороду за свою роботу у вигляді транзакційних комісій або новостворених монет [30].

Proof-of-Activity (PoA) поєднує принципи PoW і PoS. Процес розпочинається аналогічно PoW: майнери використовують спеціалізоване обладнання для обчислення правильного хеша нового блоку. Після успішного видобутку блоку майнер оголошує про його знаходження та відправляє дані в мережу, після чого система переходить до механізму PoS. Для того, щоб новий блок був доданий у блокчейн, він повинен бути підписаний певною кількістю PoS-майнерів. Винагороду за створення блоку потім розподіляють між учасниками, які беруть участь у процесах PoW і PoS.

Proof-of-Burn (PoB) – це механізм консенсусу, що передбачає «спалення» монет, тобто їх відправлення на адресу, з якої неможливо їх вилучити. У системах, що використовують PoB, майнери або валідатори «знищують» або «спалюють» певну кількість монет, щоб підтвердити свою участь у мережі. Це надає їм шанс

бути обраними для створення нового блоку та отримання винагороди за його додавання до блокчейну. Такий механізм стимулює учасників здійснювати довгострокові інвестиції у мережу, оскільки для отримання права на майнінг вони повинні вкласти значну суму перед тим [31].

Proof-of-Importance (POI) є аналогом PoS, де право на видобуток нового блоку надається активному користувачеві, який не лише має більше коштів на рахунку, але й проводить більше часу у мережі. Proof-of-Capacity (PoC) – екологічний аналог PoW, право на видобуток блоку надається майнеру з більшим доступним простором на жорсткому диску [4].

Крім того, існують інші типи алгоритмів консенсусу, такі як Proof-of-Location (PoL), який відстежує місцезнаходження цифрових активів за допомогою маячків для запобігання шахрайству в мережі, і Proof-of-Elapsed-Time (PoET), який генерує випадковий час очікування для блоку, і перша нода, яка прокидається після цього часу, отримує право на валідацію та додавання блоку до ланцюга. У кожного з вищезгаданих типів алгоритму консенсусу існують як свої переваги, так і недоліки. Наведемо їх у таблиці 2.2:

Таблиця 2.2 – Переваги та недоліки різних алгоритмів

Тип алгоритму	Переваги	Недоліки
PoW	Надійність, високий рівень безпеки	Неекологічність та висока енергозатратність
PoS	Висока швидкість обробки транзакцій, енергоефективність	Нижчий рівень безпеки порівняно з PoW, менший рівень децентралізації
DPoS	Висока швидкість обробки транзакцій	Схильність до централізації
PoA	Обробляє велику кількість транзакцій в секунду, стійкість до кібератак та шахрайства	Схильність до централізації
PoB	Високий рівень безпеки, стимулювання довгострокової участі	Марнотратство ресурсів
PoL	Висока енергоефективність та децентралізація	Низький рівень масштабованості, складність обчислень

Джерело: складено автором самостійно

Таким чином, алгоритми досягнення консенсусу надалі відіграють важливу роль у криптовалютному середовищі. Без них суть блокчейн-технологій втрачала б свою сутність. Proof-of-Work, як ключове нововведення у біткоїні, ілюструє

ефективність консенсусних алгоритмів у досягненні угоди між учасниками без централізованого органу. Проте пошуки надійних та ефективних альтернатив тривають через високу енерговитратність та обчислювальні витрати PoW. Багато досліджень спрямовані на розробку та впровадження нових консенсусних алгоритмів, які можуть бути більш екологічними, доступними та масштабованими. Це відкриває нові можливості для подальшого розвитку технологій. Механізми консенсусу залишаються важливою складовою блокчейну, а їх постійний розвиток та удосконалення лишаються ключовими для успіху криптовалют та блокчейн-технологій загалом.

2.4 Класифікація блокчейн-мереж

Блокчейн-проєкти постійно еволюціонують та вдосконалюються, і часто вони використовують розробки один одного, оскільки багато з них базуються на відкритому вихідному коді. Кожна блокчейн мережа має свої особливості та характеристики, а також чітко визначені межі можливого застосування. Найзручнішим способом класифікації блокчейн мереж є їх розподіл за рівнем відкритості, що дозволяє їх розділити на публічні (відкриті), приватні та гібридні. Ступінь відкритості часто залежить від кількох факторів, включаючи доступність вихідного коду протоколу блокчейн системи [32].

Ще одним важливим фактором є можливість підключення нового вузла до мережі без отримання дозволу. Ця можливість є ключовою характеристикою відкритої блокчейн мережі порівняно з закритою. Більшість публічних блокчейн мереж дозволяють підключатися новим користувачам за допомогою сумісного клієнтського додатку і спілкування з іншими вузлами мережі. Рівень участі користувача визначається самим користувачем і залежить від його особистих (фінансових та технічних) можливостей. В закритих блокчейн мережах підключення та відключення користувачів регулюються певними вузлами або

групою вузлів, які мають вищий рівень повноважень порівняно з іншими учасниками мережі.

1. Публічний блокчейн тісно пов'язаний з криптовалютами, які виступають базовим сценарієм, що сформував технологію в її поточному вигляді. Криптовалюти та супутні фінансові інструменти продовжують активно розвивати технологію та вирішувати архітектурні обмеження перших реалізацій. Проте капітал завжди привертає значну увагу зловмисників, і публічні блокчейн-мережі, що генерують та обслуговують цифрові активи, постійно піддаються різноманітним атакам.

Хоча найпоширеніші атаки безпосередньо не впливають на блокчейн-мережі, вони спрямовані на розкрадання активів, доступ до яких забезпечується за допомогою приватного ключа. У публічних мережах кожна транзакція, така як переказ криптовалюти з одного гаманця до іншого, підписується асиметричним електронним підписом. Цей додатковий криптографічний шар є необхідним у публічній мережі, де учасники анонімні та не довіряють один одному [28].

Використання асиметричного механізму цифрового підпису відрізняється від традиційного асиметричного шифрування. Підпис здійснюється закритим або приватним ключем, а перевірка підпису – відкритим або публічним ключем, що дозволяє будь-якому учаснику перевірити підпис транзакції. Значення відкритого ключа обчислюється на основі закритого ключа, а зворотне перетворення вимагає значних обчислень, які на сьогоднішній день практично неможливо виконати.

Приватний ключ, що генерується користувачем, надає доступ до адреси в блокчейні, де зберігається цифровий актив. Володіючи значенням приватного ключа, користувач фактично контролює та може розпоряджатися цифровим активом, який прив'язаний до цього ключа. Публічний ключ використовується як адреса блокчейну або гаманця, а також для підпису та аутентифікації інформації в інших блоках іншими учасниками мережі. Пара публічного та приватного ключа може розглядатися як блокчейн-гаманець [28].

Хоча вектор атак на отримання доступу до приватного ключа не прямо

пов'язаний з блокчейн-мережею, заходи для зниження цього ризику вживаються, включаючи архітектурні особливості блокчейн-мережі. Наприклад, децентралізовані сервіси стають популярними, оскільки вони не зберігають приватні ключі та персональні дані на своїх серверах і діють як посередники для виконання заявок на купівлю та продаж активів [24, с. 272].

Додатковий рівень захисту цифрових активів може бути забезпечений за допомогою технології мультипідпису, що вимагає кількох підписів для підтвердження транзакції. Участь кількох користувачів з приватними ключами, які зберігаються окремо, у процесі підтвердження транзакції значно підвищує безпеку гаманця.

Архітектура, криптографічні функції та алгоритми консенсусу в децентралізованій блокчейн-мережі також можуть бути потенційно використані для атак, що загрожує базовому принципу блокчейна – незмінності даних. Нижче подано основні види атак на інфраструктуру публічних блокчейн-мереж, багато з яких наразі лише теоретичні та обговорюються як концептуальні.

Складові блокчейн-стеку, що є вразливими, та рішення, що базуються на них, включають інтерфейсні елементи, користувацькі програми (наприклад, гаманці) та централізовані платформи (наприклад, біржі). В порушеннях цих систем у більшості випадків відбувається захоплення приватного ключа, що може призвести до: компрометації вузлів мережі; порушення безпеки ключів та криптографічних функцій.

2. Приватний блокчейн, також відомий як закритий блокчейн, функціонує на основі контролю доступу, який обмежує учасників мережі. У таких мережах одна або кілька організацій контролюють доступ, що робить транзакції залежними від третіх сторін. Лише учасники транзакції мають доступ до інформації про неї, тоді як інші залишаються відокремленими від неї.

Очевидно, що приватний блокчейн дозволяє кращий контроль над інфраструктурою для організації або групи компаній. Це стосується як загальних аспектів IT (наприклад, можливість швидкого оновлення функціоналу), так і аспектів інформаційної безпеки. Модель загроз для приватних блокчейнів вже не

включає ряд атак, що характерні для публічних блокчейнів. Наприклад, атака 51% або Сівіл, стають важкими для виконання через те, що всі вузли перебувають під контролем у довірених зонах. Хоча гіпотетично зловмисник може отримати доступ до підконтрольного вузла, вартість атаки значно зростає через необхідність подолання корпоративного периметра різних організацій та використання заходів інформаційної безпеки [9].

Контроль доступу є фундаментальною функцією приватної блокчейн-мережі, де новий учасник не може приєднатися без дозволу оператора мережі. Це гарантує, що доступ до інформації відбувається згідно з класичними принципами інформаційної безпеки, де доступ мають лише авторизовані учасники. Ще однією особливістю приватних мереж є можливість використання алгоритмів консенсусу, оптимізованих для довіреної мережі. За допомогою спрощених протоколів взаємодії між автентифікованими учасниками мережі можна досягти більшої пропускної спроможності та масштабованості. У порівнянні з публічними мережами, деякі приватні мережі можуть обробляти значно більшу кількість транзакцій за секунду, завдяки використанню таких алгоритмів, як Byzantine/Crash Fault Tolerance, Raft, Proof-of-Authority та інші [9].

Конфіденційність даних у приватних блокчейнах досягається через контроль прав на читання та запис даних у реєстрі. Деякі приватні блокчейн-платформи надають можливість використання додаткових інструментів захисту даних, щоб уникнути ситуацій, коли кілька учасників мережі роблять транзакції, які інші не можуть бачити, навіть у зашифрованому вигляді.

3. Гібридний блокчейн представляє собою поєднання публічних і приватних ланцюгів, об'єднуючи особливості обох підходів. Суттєву відмінність від інших систем можна помітити на рівні консенсусу. Натомість стандартної відкритої або закритої системи, де кожен може перевіряти блоки, або лише одна особа має можливість призначати валідаторів, гібридний ланцюг розглядає декілька рівноправних сторін як валідаторів.

Гібридний блокчейн пропонує такі функції, як цілісність, прозорість та безпека. Учасники гібридного блокчейну приймають рішення про те, хто може

брати участь у мережі та які транзакції будуть публічними. Хоча транзакції в гібридному блокчейні не обов'язково є публічними, вони можуть бути перевірені за необхідності. Кожна транзакція в гібридному блокчейні може бути приватною, а водночас відкритою для перевірки, якщо це потрібно. Однак головну роль в гібридному блокчейні відіграє незмінність: кожна транзакція записується один раз і не може бути змінена [28].

Гібридний блокчейн забезпечує більшу безпеку порівняно з публічним або приватним блокчейном, оскільки навіть група осіб, яка контролює мережу, не може змінити основну властивість блокчейну – його незмінність, тим самим не піддавши ризику безпеку транзакцій. Учасники блокчейну можуть лише визначати, які транзакції є публічними, а які – ні.

Як тільки користувач отримує доступ до гібридного блокчейну, він може повністю брати участь у діяльності мережі. Однак особистість користувачів залишається конфіденційною перед іншими учасниками. Це зроблено для забезпечення приватності користувачів. Інформація про особи користувачів розкривається тільки в процесі їх взаємодії між собою, і тільки цим особам, які взаємодіють. Незважаючи на обмежену анонімність осіб користувачів у межах мережі, вони мають повну анонімність поза межами мережі гібридного блокчейну. Гібридна блокчейн-мережа забезпечує всі переваги публічного блокчейну, такі як безпека, прозорість, незмінність та децентралізованість, але в той же час обмежує можливість вільного доступу до транзакцій. Ураховуючи всі свої особливості, гібридна мережа блокчейну має ряд переваг:

1. Робота в закритій екосистемі: гібридний блокчейн може працювати в закритій екосистемі, що забезпечує захист від витоку інформації.

2. Захист від атаки 51%: гібридний блокчейн не піддається атакам 51%, оскільки хакерам важко отримати доступ до мережі.

3. Захист конфіденційності та взаємодія зі світом: гібридний блокчейн забезпечує захист конфіденційності та одночасну взаємодію зі світом поза мережею.

4. Низька вартість транзакцій: транзакції у гібридному блокчейні є

дешевими, оскільки для їх перевірки потрібно лише кілька вузлів. Це робиться завдяки перевірці транзакцій лише впливовими вузлами, у публічному блокчейні це вимагає тисяч вузлів.

Таким чином, з класифікації блокчейн-мереж видно, що різні типи – публічні, приватні і гібридні – мають свої особливості. Приватні мережі надають вищий рівень конфіденційності, але менше відкритості, в той час як публічні мережі – навпаки. Гібридні мережі поєднують переваги обох типів, забезпечуючи ефективність та безпеку. Незалежно від типу, безпека залишається ключовою складовою, і важливо ретельно розглядати методи захисту при використанні блокчейну.

2.5 Смарт-контракти

Смарт-контракт – це інструмент, який уніфікує комп'ютерні мережі шляхом поєднання протоколів з користувацьким інтерфейсом. Вони дозволяють створювати протоколи, де обидві сторони можуть взяти на себе зобов'язання через блокчейн мережу, незалежно від взаємного знання чи довіри. Учасники можуть бути впевнені в виконанні зобов'язань, оскільки у разі невиконання умов контракт анулюється. Смарт-контракти зазвичай базуються на Ethereum, оскільки це надійна криптоплатформа [18, с. 124].

Ці контракти працюють за допомогою простих операторів, які записані в коді у ланцюжку блоків. Мережа комп'ютерів виконує дії, коли виконані та перевірені певні умови. Ці дії можуть включати виділення коштів, реєстрацію об'єктів, відправлення повідомлень та інше. Після завершення транзакції блокчейн оновлюється, що гарантує незмінність операцій.

У смарт-контракті може бути будь-яка кількість умов, що дозволяє учасникам переконатися у виконанні завдання. Для встановлення умов необхідно визначити представлення транзакцій та їх даних у ланцюжку блоків, встановити

правила, що регулюють транзакції, дослідити можливі винятки та розробити структуру для вирішення суперечок.

Після цього розробник може програмувати смарт-контракт, але організації, які використовують блокчейн для бізнесу, все частіше надають шаблони, веб-інтерфейси та інші онлайн-інструменти для спрощення створення смарт-контрактів. Переваги смарт-контрактів включають [16]:

1. Швидкість, ефективність та точність: контракт виконується негайно при виконанні умови, що унеможливлює потребу в ручній обробці документів та узгодженні помилок.

2. Довіра та прозорість: зашифровані записи транзакцій блокчейна спільно використовуються учасниками, що усуває потребу у третіх сторонах та сумнівів у чесності операцій.

3. Безпека: записи транзакцій зашифровані, а їх зміна потребує зміни всього ланцюжка, ускладнюючи можливість злому.

4. Економія: смарт-контракти усувають потребу у посередниках та зменшують часові затримки та комісії.

Проте смарт-контракти також мають вразливості, які можуть бути використані для маніпуляції кодом та викрадення максимально можливих сум за короткий час. Одна з потенційних вразливостей полягає у можливості цілочисельного переповнення (integer underflow). Це дозволяє зловмиснику, якому не має коштів на рахунку, відправити один токен і отримати у відповідь мільярди токенів. Інша форма цілочисельного переповнення полягає в тому, що коли баланс досягає максимального значення і зловмисник отримує один токен, цей процес починається заново.

Третя вразливість стосується неналежного контролю доступу, що призводить до можливості незахищеного зняття коштів з контракту. Четверта вразливість полягає в незахищеному самознищенні, яке дозволяє сторонньому зловмисникові «вбити» контракт і надіслати кошти на будь-яку адресу.

Ці вразливості можуть призвести до серйозних наслідків для користувачів, які тримають криптовалюту на основі Ethereum або токени на онлайн-платформі.

Якщо зловмисник створить шкідливий смарт-контракт і атакує платформи, що використовують цей контракт, користувачі ризикують втратити свої кошти [32].

Таким чином, по закінченні другого розділу, зробимо наступні висновки: нами була ретельно розглянута та проаналізована технологія блокчейн, включаючи її архітектуру та унікальні особливості. На підставі цього аналізу було зроблено висновок щодо переваги технології блокчейн, зокрема, у незмінності, децентралізації, прозорості та конфіденційності.

Також проведено порівняльний аналіз трьох типів протоколів досягнення консенсусу та різних видів блокчейн-мереж, включаючи публічні, приватні та гібридні. Показано основні переваги, проблеми та недоліки кожного з них. Зроблено висновок, що гібридний блокчейн є найбільш доцільним для захисту інформації, оскільки він поєднує переваги обох типів технології, при цьому намагаючись зменшити недоліки. Враховуючи цю інформацію, гібридний блокчейн визнається безпечним та надійним методом захисту інформації.

Додатково, розглянуто смарт-контракти, написані на основі публічних блокчейн-мереж, які мають певні недоліки в сфері забезпечення інформаційної безпеки. Смарт-контракти, засновані на гібридних блокчейн-мережах, можуть ефективно усунути ці недоліки та стати важливим інструментом для безпечної передачі інформації.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

3.1 Безпека даних у фінансовому секторі

Враховуючи великий потенціал, блокчейн може бути застосований у багатьох сферах. Один з найкращих способів використання полягає в забезпеченні цілісності для заходів кібербезпеки. Нижче наведено деякі приклади застосування блокчейну у майбутньому для підвищення рівня кібербезпеки:

1. Захист особистих повідомлень: з ростом кількості соціальних мереж збільшується обсяг зібраних метаданих під час користування ними. Багато користувачів захищають свої дані та сервіси ненадійними паролями. Компанії, які займаються обміном повідомлень, можуть використовувати блокчейн для захисту даних, що є більш ефективним варіантом, ніж поточне шифрування. При відповідній реалізації у системах обміну повідомленнями, блокчейн може запобігти подібним кібератакам у майбутньому.

2. Безпека Інтернету речей: хакери використовують периферійні пристрої, такі як термостати та маршрутизатори, для доступу до систем в цілому. З розвитком систем штучного інтелекту, хакерам стало легше отримати доступ до загальних систем, таких як домашня автоматизація через периферійні пристрої, наприклад, «розумні» перемикачі. Більшість пристроїв Інтернету речей мають недостатні засоби безпеки. Блокчейн може використовуватися для захисту таких систем шляхом децентралізації адміністрування, що дозволяє пристроям самостійно приймати рішення з питань безпеки. Це ускладнює атаки на централізовані системи керування пристроями, що робить їх практично неможливими.

3. Захист DNS та DDoS: Атака типу «відмова в обслуговуванні» (DDoS) стає фактом, коли користувачам цільового ресурсу, такого як мережний ресурс, сервер

або веб-сайт, відмовляють у доступі або обслуговуванні. Ці атаки призводять до відключення або уповільнення роботи систем ресурсів. З іншого боку, система доменних імен (DNS) дуже централізована, що робить її ідеальною метою для хакерів, які можуть проникнути у зв'язок між IP-адресою та ім'ям веб-сайту. Ця атака призводить до недоступності веб-сайту та навіть перенаправлення користувача на інші шахрайські веб-сайти. Однак блокчейн можна використовувати для зменшення таких атак за рахунок децентралізації DNS-записів. Застосування децентралізованих рішень у блокчейні допоможе захистити окремі вразливі точки, які використовуються хакерами [9].

4. Децентралізація сховища: злам та крадіжка бізнес-даних є основною причиною занепокоєння для організацій. Більшість компаній залишаються при централізованій формі зберігання даних. Для отримання доступу до всіх цих даних хакерам потрібно лише сконцентруватися на одній вразливій точці. Внаслідок таких атак конфіденційні дані, як фінансові звіти, цінні папери та документи, можуть потрапити у руки злочинця. Використання блокчейну для забезпечення децентралізованої форми зберігання даних допоможе захистити конфіденційні дані. Цей підхід знижує ризик ускладнених або навіть неможливих атак хакерів на системи зберігання даних. Багато компаній, що надають послуги зберігання, досліджують можливості захисту даних за допомогою блокчейну. Команда Apollo Currency є прикладом організації, яка вже успішно впровадила технологію блокчейну у свої системи (Apollo Data Cloud) [22].

5. Програмне забезпечення: блокчейн може бути використаний для забезпечення цілісності програм та запобігання встановленню шкідливого програмного забезпечення. Подібно до використання хешів MD5, блокчейн може застосовуватися для перевірки дій, таких як оновлення прошивки та виправлення помилок у версіях, щоб запобігти проникненню шкідливого програмного забезпечення на комп'ютери. У випадку MD5 новий ідентифікатор програмного забезпечення порівнюється з хешами, доступними на веб-сайтах постачальників. Проте цей метод не є абсолютно надійним, оскільки хеші, доступні на платформі постачальника, можуть бути вже скомпрометовані. Однак за використання

технології блокчейн хеші постійно записуються у ланцюжок, а інформація, що записана у блоках, не піддається зміні чи редагуванню програмного забезпечення.

6. Перевірка кіберфізичних систем: підробка даних та неправильна конфігурація систем, разом із відмовою компонентів, порушують цілісність інформації, що генерується кіберфізичними системами. Однак можливості технології блокчейн щодо цілісності та перевірки інформації можуть використовуватися для автентифікації статусу будь-якої кіберфізичної інфраструктури. Інформація, отримана про компоненти інфраструктури за допомогою блокчейна, може бути надійнішою для всього ланцюжка поставок.

7. Захист передачі даних: блокчейн може бути використаний у майбутньому для запобігання несанкціонованому доступу до даних під час їх передачі. Використовуючи повне шифрування, передача даних може бути захищена для запобігання доступу до неї зловмисників, незалежно від того, чи є ці зловмисники приватними особами чи організаціями. Такий підхід призведе до загального підвищення надійності та цілісності даних, що передаються через блокчейн.

Криптовалюти виступили піонерами в застосуванні технології блокчейну. У контексті численних криз і конфліктів людство почало шукати альтернативні способи збереження своїх фінансів, що призвело до появи недовіри до банків та фінансових установ. Поява абсолютно нового продукту негайно привернуло увагу багатьох. Капіталізація криптовалют почала стрімко зростати і досягла обсягів, що перевищують або рівні річному ВВП розвинених країн. Багатьох привабила відсутність централізованого органу, який би контролював обіг валют. Серед переваг криптовалют порівняно з банками можна виділити доступність цілодобово, фіксований розмір комісії незалежно від місцезнаходження, швидка обробка транзакцій, збереження анонімності, простота початку використання послуг за умови наявності пристрою з підключенням до інтернету, відсутність централізованого сервера з даними користувача та неможливість відхилення транзакцій за різних обставин. Тим часом, банки можуть збанкрутіти, а валюта певної країни може швидко втратити свою цінність, у той час як криптовалюти, як правило, не прив'язані до ситуації на певній території. Однак вони також не

можуть похизуватися стабільністю, тому були створені так звані стейблкоїни – криптовалюти, прив'язані до резервів звичайної валюти або певних товарів, таких як дорогоцінні метали або нафта. Їх курс коливається відповідно до активу, до якого вони прив'язані. Фінансові установи також можуть відчути переваги використання блокчейну, інтегруючи його у свою систему платежів [1, с. 7].

Приклад проведення транзакцій через Blockchain наведений на рис. 3.1:

```python
from ecdsa import SigningKey, SECP256k1
import hashlib

# Створення криптогаманця А
private_key_A = SigningKey.generate(curve=SECP256k1)
public_key_A = private_key_A.verifying_key.to_string()

# Адреса криптогаманця А зазвичай є хешем його публічного ключа
address_A = hashlib.sha256(public_key_A).hexdigest()

# Створення криптогаманця Б
private_key_B = SigningKey.generate(curve=SECP256k1)
public_key_B = private_key_B.verifying_key.to_string()
address_B = hashlib.sha256(public_key_B).hexdigest()

# Сума переказу
amount = 10

# Підписання транзакції від А до Б
transaction_data = f"{address_A}->{address_B}:{amount}"
signature_A = private_key_A.sign(transaction_data.encode())

# Перевірка підпису Б
try:
    public_key_A.verify(signature_A, transaction_data.encode())
    print("Підпис вірний.")
except ecdsa.BadSignatureError:
    print("Неправильний підпис.")
```

Рис. 3.1 – Приклад проведення транзакцій через Blockchain

Простий приклад коду на мові Python, який демонструє створення та підписання транзакції між двома криптогаманцями. Для цього прикладу використовується бібліотека ecdsa для роботи з еліптичними кривими, що зазвичай використовується для підписування транзакцій у біткойні та інших криптовалютах.

Хешування SHA-256 наведена на рис. 3.2:

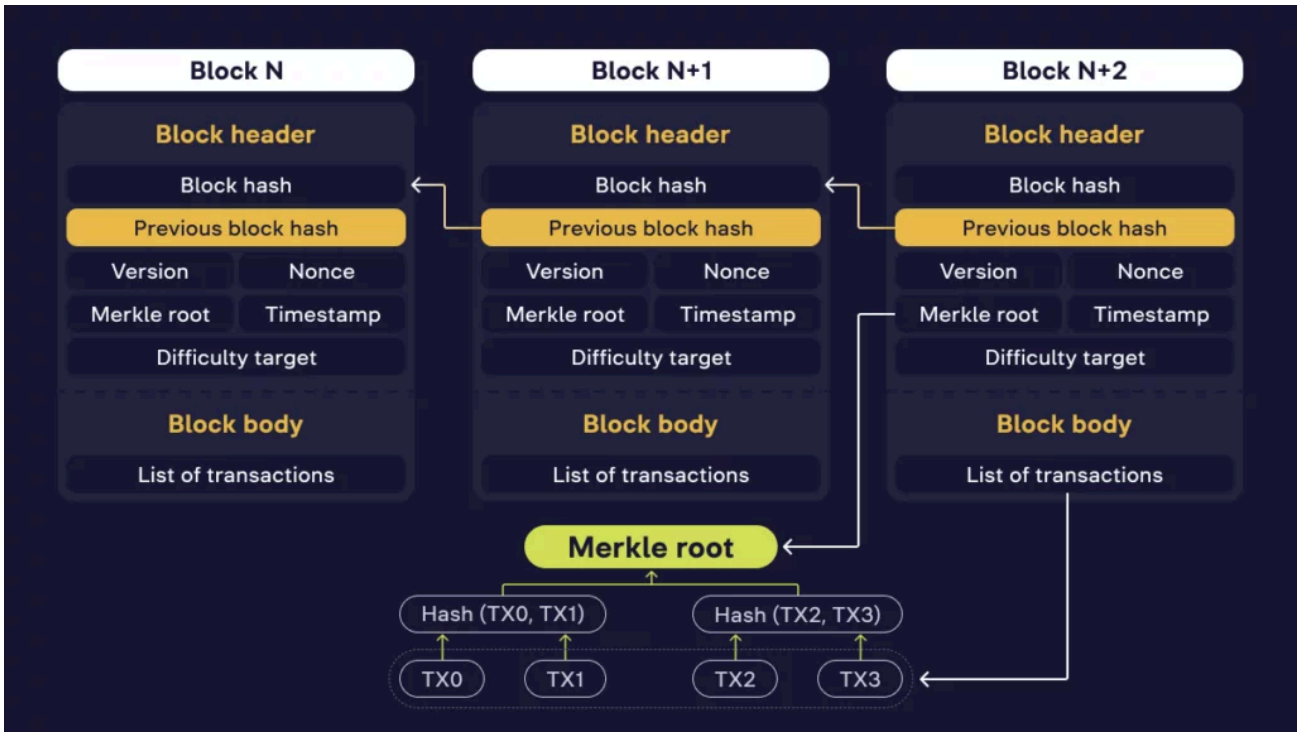


Рис. 3.2 – Хешування SHA-256

Також наведемо приклад роботи хешування SHA-256 на рис. 3.3:

```python
import hashlib

# Вхідне повідомлення
message = "Hello, world!"

# Перетворення рядка в байтовий формат
message_bytes = message.encode('utf-8')

# Хешування вхідного повідомлення за допомогою SHA-256
hash_result = hashlib.sha256(message_bytes).hexdigest()

# Виведення отриманого хешу
print("SHA-256 хеш вхідного повідомлення:", hash_result)
```

Рис. 3.3 – Приклад роботи хешування SHA-256

У цьому коді ми спочатку конвертуємо рядок у байтовий формат, оскільки бібліотека hashlib очікує байтові дані для хешування. Потім ми використовуємо метод sha256 для створення об'єкту хешування SHA-256 та метод hexdigest() для

отримання закодованого у шістнадцятковому форматі рядка, який представляє собою фактичний хеш.

Наведемо рекомендації щодо застосування блокчейн-технологій у фінансовому секторі:

1. Децентралізовані системи ідентифікації: використання блокчейну для створення децентралізованих систем ідентифікації може забезпечити безпеку даних у фінансовому секторі. Кожен користувач може мати унікальний цифровий ідентифікатор, який зберігається у безпечному та незмінному блокчейні, забезпечуючи високий рівень захисту від кіберзлочинців.

2. Блокчейн для обробки платежів: застосування блокчейну для обробки фінансових транзакцій може забезпечити безпеку даних та уникнення шахрайства. Транзакції можуть бути збережені у розподіленій мережі, що робить їх відстеження та верифікацію надійними та безпечними.

3. Системи смарт-контрактів для автоматизації операцій: використання смарт-контрактів на блокчейні дозволяє автоматизувати фінансові операції і забезпечує їх виконання відповідно до зазначених умов без можливості маніпуляції чи зміни даних.

4. Аудит та внутрішня перевірка: блокчейн може бути використаний для забезпечення прозорості та відстеження дій в системі фінансових установ. Кожна транзакція та зміна даних може бути зафіксована у блокчейні, що дозволяє здійснювати аудит та внутрішню перевірку з високою точністю

5. Захист від кібератак: розподілена природа блокчейну робить його менш вразливим до кібератак. Застосування цієї технології може допомогти уникнути порушень безпеки даних та зберегти конфіденційність фінансових інформаційних потоків.

Особисто використовувався криптогаманець для зберігання і відправлення криптовалюти. Однією з переваг такого використання є безпека. Криптогаманці зазвичай мають різні рівні безпеки, включаючи можливість налаштування двофакторної аутентифікації та використання криптографічних ключів. Додатково, використання криптогаманця дозволяє зберігати і керувати

криптовалютою без посередництва банків чи інших фінансових установ. Це дає більший контроль користувачеві над його фінансами.

Таким чином, ця технологія може створити безпечну, ефективну та децентралізовану інфраструктуру для фінансових операцій, забезпечуючи високий рівень захисту від шахрайства та забезпечуючи швидкість та доступність для всіх користувачів. Зараз, коли індустрія фінансових послуг активно адаптується до цифрової ери, впровадження технології блокчейн стане ключовим фактором у формуванні майбутнього ландшафту. Від оптимізації платіжних систем до модернізації відповідності нормативним вимогам, блокчейн має потенціал трансформувати традиційні бізнес-моделі та практики, відкриваючи нову еру ефективності, безпеки та прозорості фінансових послуг.

Блокчейн-рішення в галузі фінтех та інших фінансових послуг вже успішно демонструють свою готовність до адаптації та інновацій. Прогнозується, що в майбутньому їх потенціал лише зростатиме, що дозволить їм ще глибше інтегруватися у наше повсякденне життя. У сфері банківської справи технологія блокчейн може зробити банки більш ефективними та безпечними, прискоривши міжнародні грошові перекази, забезпечивши чіткий запис операцій, мінімізуючи ризик людської помилки та виключивши посередників з ланцюжка операцій.

Проте важливо врахувати, що впровадження технології блокчейн потребує вирішення великої кількості технічних, регуляторних та конфіденційних питань. Потрібно розробляти стандарти та правила, які б забезпечували регулювання цієї нової системи та захищали інтереси користувачів. В цілому, технологія блокчейн вже робить значний внесок у розвиток та оптимізацію різних галузей, включаючи платіжну, банківську та кредитну. Проте її потенціал ще далеко не вичерпаний. У майбутньому ця технологія може суттєво змінити фінансовий ландшафт, забезпечуючи більшу безпеку, швидкість, прозорість та доступність для всіх користувачів.

3.2 Державний сектор

Використання блокчейну у державному секторі відкриває широкі можливості. Переваги цієї технології можна успішно використовувати для організації виборів, фінансових операцій, охорони здоров'я, критичної інфраструктури, майнових реєстрів та освіти.

Наприклад, Американський центр контролю захворювань висловлює намір використовувати блокчейн для збереження інформації про випадки захворювань важкими або заразними хворобами, такими як гепатит, COVID-19 та інші. Якщо в одному штаті реєструється випадок захворювання, то сусідні штати мають негайно отримувати повідомлення і вживати всі необхідні заходи для захисту населення. Це дозволить краще контролювати поширення захворювань, швидко реагуючи та обмежуючи дії осіб у зонах спалахів інфекцій [8, с. 120].

Міністерство внутрішньої безпеки США ідентифікує 16 галузей критичної інфраструктури, таких як енергетика, транспорт, медицина, фінанси та інші. Навіть коротка перебіжка часу, протягом якої система перестає функціонувати, може призвести до серйозних економічних втрат для країни або навіть до загибелі осіб. Тому використання блокчейну є оптимальним рішенням для цих секторів, і вони широко впроваджують цю технологію [8, с. 120].

У серпні 2019 року Міністерство енергетики США висловило підтримку проекту «Енергетичний інтернет», який базується на блокчейні. Цей проект дозволяє власникам будинків придбавати електроенергію від різних джерел, таких як вітряні ферми, за допомогою розподіленої мережі. Це сприятиме оптимізації споживання енергії, оскільки споживачі матимуть можливість вибирати час споживання залежно від ціни: чим більше попит, тим вища ціна [34].

Інший цікавий проект, який підтримується Міністерством охорони довкілля Японії, спрямований на створення системи обміну та вимірювання відновлюваної енергії. Цей проект використовує криптовалюту для обміну енергією, де ціна формується на основі попиту та вартості передачі енергії.

У Малаккі, малайзійському місті, ведуться роботи щодо створення міста майбутнього на базі технології блокчейн. Це місто буде орієнтоване на розкішні готелі, вілли з видом на море, шале та водні атракції. Першим кроком буде випуск власної криптовалюти DMI, яка буде використовуватися для оплати послуг. Туристи також матимуть змогу обмінювати свою валюту на монети DMI та проводити оплату за допомогою телефонів або комп'ютерів. Планується, що це інноваційне блокчейн-місто зможе привабити близько трьох мільйонів туристів щорічно [8, с. 121].

У 2018 році двадцять дві країни Європейського Союзу підписали документ щодо можливостей використання блокчейну для трансформації електронних сервісів у Європі. Згідно з останніми даними, у проекти вже було вкладено близько 350 мільйонів євро. Європейські експерти вважають, що майбутнє всіх громадських сервісів пов'язане з технологією блокчейн, оскільки громадяни будуть впевнені у захисті та надійності своїх персональних даних [8, с. 121].

В Естонії було створено велику онлайн-платформу з доступом до ідентифікаційних даних, медичних записів та «держави в смартфоні». 99% медичних даних оцифровано і доступно з будь-якого пристрою, а всі ці дані зберігаються у блокчейні. Грузія та Швеція впровадили систему реєстрації прав власності на землю та продажу нерухомості на основі технології блокчейн, що призвело до зменшення рівня корупції у цих галузях. Мальта успішно використовує блокчейн для зберігання студентських дипломів, шкільних табелів та нагород, що допомагає зберігати особисту інформацію конфіденційною, зменшує бюрократію та спрощує доступ до ресурсів [6, с. 462].

Українська платформа «Дія» використовує технологію блокчейн для збереження критично важливих даних. У 2017 році Кабінет Міністрів уклав угоду з американською компанією BitFury з метою переведення державних реєстрів на блокчейн, що спростить реєстрацію фізичних осіб та підприємств. Міністерство аграрної політики також презентувало оновлений земельний кадастр на блокчейні, що полегшить роботу підприємців. Багато інших країн також приєдналися або приєднуються до використання технології блокчейн. Цікаво, що з

експериментуванням з цією технологією не тільки передові країни світу, але й досить бідні держави Африки та Близького Сходу. Блокчейн має великий потенціал стати популярним та надійним інструментом у сферах, які мають стратегічне значення для держави, і забезпечувати постійний доступ до даних, зберігаючи при цьому їх безпеку та надійність.

Протягом багатьох століть, питання чесних виборів залишається актуальним. Корупція, такі як підкуп виборців та учасників виборчих комісій, фальсифікація голосів та інші нелегальні практики, призводять до конфліктів та спричиняють зростання недовіри до виборчої системи. Застосування технології блокчейну для проведення виборів унеможливить будь-які види підкупу, оскільки автоматизований процес підрахунку голосів.

У багатьох сферах, зокрема у сфері охорони здоров'я, блокчейн вже використовується для збереження даних пацієнтів та медичних записів. Ці дані можуть бути зашифровані з використанням публічних та приватних ключів, що забезпечує доступ до них лише авторизованим користувачам. Впровадження блокчейну дозволить пацієнтам перевірити, чи зроблені всі відповідні записи лікарями, і гарантувати, що дані не будуть видалені або змінені без дозволу. Пацієнти матимуть доступ до повного ланцюжка записів усіх лікарів у хронологічній послідовності, що сприяє уникненню непорозумінь між медичним персоналом. Крім того, це допоможе у запобіганні шкоди від хакерських атак, оскільки дані пацієнтів будуть захищені високим рівнем конфіденційності та безпеки. Багато подібних проектів вже успішно реалізовано та активно використовуються.

Використання технології блокчейну для реєстрації прав власності особи над певним майном є дуже цілком обґрунтованим. Спочатку, питання забезпечення безпеки всіх збережених даних виявляється крайньо важливим, оскільки в разі їх втрати особа може втратити змогу підтвердити своє право власності над певним об'єктом, або процес відновлення прав може стати дуже складним. Крім того, як вже зазначалося, блокчейн гарантує незмінність усіх записів, створених з моменту початку функціонування мережі. Тому зловмисникам, які намагатимуться

заволодіти чужим майном шахрайськими методами, не вдасться це зробити. Крім того, в разі атаки на один з вузлів мережі, працездатність та вміст блокчейну не будуть порушені [14, с. 56].

Розумні контракти, як новий вид укладання домовленостей між особами чи групами осіб, є однією з переваг технології блокчейну. Умови договору, їх виконання та результат прописуються в коді контракту. Головною перевагою цих контрактів є відсутність потреби в третіх осіб, які регулювали б виконання умов договору кожною стороною. Оскільки розумні контракти вбудовуються в блокчейн, вони отримують всі переваги цієї технології. Потенційна сфера застосування смарт контрактів є широкою, а їх використання значно зменшує витрати на нотаріальні послуги та послуги третіх осіб, в тому числі адвокатів [34].

Таким чином, використання блокчейн-технології у державному секторі може мати значний позитивний вплив на ефективність, безпеку та прозорість адміністративних процесів. Ця технологія може допомогти у ряді сфер, включаючи реєстрацію прав власності, зберігання медичних даних, ведення обліку громадських послуг та багато інших. Завдяки властивостям блокчейну, таким як незмінність даних, децентралізація та шифрування, державні органи можуть забезпечити високий рівень безпеки та довіри до систем управління. Також блокчейн дозволяє створити ефективні та прозорі процеси взаємодії між різними сторонами, що сприяє уникненню корупції та покращує якість обслуговування громадян. Хоча використання блокчейну у державному секторі може потребувати значних витрат на впровадження та технічну підтримку, його переваги у довгостроковій перспективі можуть бути важливими для покращення ефективності та довіри до державних інституцій. Використання блокчейну у державному секторі може бути важливим кроком у напрямку модернізації та оптимізації адміністративних процесів.

3.3 Логістика

Використання технології блокчейну в логістиці є ілюстрацією успішного використання розподіленого реєстру для вирішення наступних проблем:

1. Обігу документів.
2. Відстеження вантажів.
3. Аутентифікації.
4. Надання своєчасної інформації про зміни.
5. Забезпечення прозорості процесів.
6. Здійснення платежів та виставлення рахунків.
7. Розрішення спорів.

У 2021 році обсяг світового ринку логістики становив $9,5 трлн, а очікується, що протягом наступних 5 років (з 2022 по 2027 рік) він зросте до $13,3 трлн. Незважаючи на постійне збільшення обсягів постачання, людський фактор, складність документообігу та велика кількість контрагентів суттєво уповільнюють процес і підвищують вартість послуг [16].

Використання технології блокчейну може вирішити ці проблеми, поліпшити комунікацію, усунути неточності в документації і збільшити ВВП, заощадивши галузі приблизно $40 млрд. Однією з головних проблем постачання є недостатня достовірність інформації через неповноту або недоступність даних для контролю, що сприяє контрабанді та втратам вантажу. Непрозорий процес формування вартості постачання змушує компанії переплачувати [21].

Можливості блокчейну дають змогу зробити ланцюжки постачання прозорими та перевіряти інформацію щодо вантажу, що нівелює розбіжності та підробки в документації. Інформація, збережена в блокчейні, не може бути змінена, що гарантує постійну достовірність даних від постачальників сировини до кінцевої локації та зменшує кількість маніпуляцій з товаром.

Замовник може також переглядати попередні результати роботи контрагента (затримки постачання, оплату). Для контролю умов перевезення можна

використовувати RFID-мітки, що передають дані безпосередньо в блокчейн. У разі несанкціонованого розкриття пакування або порушення умов зберігання можна буде швидко й точно визначити вину та етап, на якому виникла проблема.

Оптимізація документообігу можлива завдяки використанню смартконтрактів, які автоматизують виконання умов, дозволяючи [17, с. 256]:

1. Негайно виставляти штрафи при пошкодженні товару під час перевезення, без очікування судового розслідування.

2. Швидко проводити операції підтвердження, що допомагає прискорити просування вантажів ланцюгом поставок.

3. Полегшити контроль відстежуваності товарів від постачальника сировини до полиці в магазині.

4. Зменшити витрати на оформлення документів, що зараз становлять 10–15% від плати за доставку.

5. Блокчейн дозволяє отримати повну інформацію про походження товару та його виробництво, забезпечуючи незмінність даних у реєстрі. Це підвищує довіру клієнтів до бренду і робить ланцюг поставок більш прозорим.

Хоча ринок блокчейну та смартконтрактів постійно росте, впровадження технології може зустрітися з труднощами, такими як навчання персоналу та інтеграція з існуючими робочими процесами. Додаткові витрати та проблеми із стандартизацією можуть ускладнити процес. Недоліки включають незмінність смартконтрактів, яка не дозволяє змінювати умови в разі обставин, що не залежать від постачальника. Однак впровадження блокчейну вже має позитивний вплив на різноманітні галузі, включаючи логістику, і поширюється як у великих, так і в малих компаніях [24].

Ланцюги поставок можуть допомогти значно зменшити відслідковування походження товарів. В даний момент складно відстежити партії продуктів, які поставляються невеликими підприємствами або фермерами. У разі виявлення недоброякісних або забруднених товарів одним з отримувачів майже неможливо досягти вилучення цих продуктів у інших. Компанії IBM та Walmart працюють над системою відстежування, яка допоможе їм швидко виявляти «погані» товари

та подавати сигнали про необхідність їх вилучення. Наприклад, якщо певний ресторан або магазин отримав партію товару, яка викликала недуги у покупців, вони можуть швидко відстежити цю партію, ідентифікувати дистриб'ютора та постачальника продукції за допомогою блокчейн системи. Якщо товар дійсно пошкоджений, то постачальник отримає мітку, всі, хто купував такі товари або мали з ними справу, отримають повідомлення про небезпеку. Крім того, цю систему можна використовувати для позначення продуктів з мітками «органічний», «вибір року» або іншими для підтвердження їх валідності [27].

Таким чином, незалежно від того, як використовується блокчейн, ключовим компонентом є його здатність до децентралізації. Ця функція видаляє єдину цільову точку, яка може бути зламана. В результаті стає абсолютно неможливо проникнути в системи або сайти, контроль доступу, зберігання даних та мережевий трафік яких, більше не знаходяться в одному місці.

Мережа блокчейн успішно забезпечує збереження цілісності даних, завдяки наявності численних копій бази даних та можливості змінювати її лише після перевірки правильності інформації іншими учасниками мережі. Це гарантує захист інформації від будь-яких ненавмисних чи несанкціонованих змін, а також від змін під час зберігання, обробки чи передачі даних. Механізм підтвердження операцій за допомогою складних математичних функцій перешкоджає будь-яким спробам маніпулювання даними, забезпечуючи їх незмінність та правильність. Завдяки цим заходам інформація залишається стабільною та достовірною, що забезпечує надійність операцій та прийняття правильних рішень, а також можливість зберігання даних у їх первісному стані.

Застосування блокчейн-технологій для забезпечення безпеки даних має великий потенціал і може бути корисним у різних сферах. Сформуємо пропозиції щодо застосування блокчейну для забезпечення безпеки даних:

1. Захист особистих даних: використання блокчейну для збереження особистих даних може забезпечити їхню безпеку і конфіденційність. Блокчейн забезпечує надійний механізм шифрування та безпечного доступу до даних, що робить його відмінним вибором для зберігання чутливої інформації, такої як

медичні записи, фінансові дані або особисті ідентифікаційні дані.

2. Аутентифікація ідентичності: блокчейн може бути використаний для створення безпечних систем автентифікації, що дозволяють користувачам підтверджувати свою ідентичність без ризику зламу або шахрайства. Це може бути корисно для банківських операцій, онлайн-платежів, входу до систем електронної пошти та багатьох інших випадків, де потрібна надійна ідентифікація користувачів.

3. Трекінг походження даних: блокчейн може слугувати як прозорий реєстр для відстеження походження даних, забезпечуючи достовірність та недоступність для змін. Це особливо корисно для галузей, де важливо визначити точне походження даних, наприклад, у ланцюгу постачання, наукових досліджень або обміні медичною інформацією.

4. Захист від кібератак: блокчейн може забезпечити додатковий шар захисту від кібератак шляхом розподіленого зберігання даних та механізмів шифрування. Це може допомогти у запобіганні несанкціонованого доступу до даних та маніпуляцій з ними.

5. Забезпечення цілісності даних: блокчейн дозволяє підтвердити цілісність даних, оскільки будь-які зміни в інформації реєструються у вигляді нових блоків. Це дозволяє виявити будь-які спроби зміни чи видалення даних, забезпечуючи їхню недоступність для втручання без авторизації.

Ці пропозиції відображають різноманітні можливості використання блокчейну для забезпечення безпеки даних у різних контекстах.

ВИСНОВКИ

По закінченні дослідження відмітимо досягнення поставленої мети та вирішення завдань. Нами був проведений аналіз головної мети забезпечення безпеки інформації під час передачі даних у комп'ютерних мережах. Додатково, були розглянуті основні загрози безпеці інформації та проблеми несанкціонованого доступу. Враховуючи недоліки існуючих методів захисту інформації та постійний розвиток нових загроз, зроблено висновок про те, що система захисту інформації потребує нових підходів та рішень. Основними проблемами, які значно впливають на повільне та проблематичне впровадження технології, є обмежена масштабованість, висока енерговитратність, відсутність нормативно-правової бази, що регулює використання технології, та недостатня кількість фахівців. Однак з кожним роком ці проблеми зменшуються, і тому технологія блокчейн вже зараз може бути ефективним засобом захисту інформації.

У другому розділі дослідження була розглянута та проаналізована технологія блокчейн, її структура та особливості. На підставі отриманих даних зроблено висновок про ряд переваг технології блокчейн, зокрема: незмінність, децентралізація, прозорість та конфіденційність. Було проведено порівняльний аналіз трьох типів протоколів досягнення консенсусу, а також публічних, приватних та гібридних мереж блокчейн. Крім цього, визначено основні переваги, проблеми та недоліки різних типів блокчейну. Досліджено, що найбільш доцільним типом для забезпечення безпеки інформації є гібридний блокчейн, який поєднує переваги обох типів технології, намагаючись при цьому обмежити їх недоліки і таким чином забезпечує всі аспекти інформаційної безпеки.

З урахуванням цієї інформації, гібридний блокчейн є безпечним та надійним засобом для захисту інформації. Детально розглянуто смарт-контракти, написані на базі публічних мереж блокчейн, та виявлено ряд

недоліків у сфері забезпечення інформаційної безпеки. Тому було зроблено висновок про те, що смартконтракти на базі гібридних мереж блокчейн зможуть усунути ці недоліки та стануть ефективним засобом для безпечної передачі інформації.

Блокчейн може створити безпечну, ефективну та децентралізовану інфраструктуру для фінансових операцій, забезпечуючи високий рівень захисту від шахрайства та забезпечуючи швидкість та доступність для всіх користувачів. Зараз, коли індустрія фінансових послуг активно адаптується до цифрової ери, впровадження технології блокчейн стане ключовим фактором у формуванні майбутнього ландшафту. Від оптимізації платіжних систем до модернізації відповідності нормативним вимогам, блокчейн має потенціал трансформувати традиційні бізнес-моделі та практики, відкриваючи нову еру ефективності, безпеки та прозорості фінансових послуг.

Блокчейн-рішення в галузі фінтех та інших фінансових послуг вже успішно демонструють свою готовність до адаптації та інновацій. Прогнозується, що в майбутньому їх потенціал лише зростатиме, що дозволить їм ще глибше інтегруватися у наше повсякденне життя. У сфері банківської справи технологія блокчейн може зробити банки більш ефективними та безпечними, прискоривши міжнародні грошові перекази, забезпечивши чіткий запис операцій, мінімізуючи ризик людської помилки та виключивши посередників з ланцюжка операцій.

Українська платформа «Дія» використовує технологію блокчейн для збереження критично важливих даних. У 2017 році Кабінет Міністрів уклав угоду з американською компанією BitFury з метою переведення державних реєстрів на блокчейн, що спростить реєстрацію фізичних осіб та підприємств. Міністерство аграрної політики також презентувало оновлений земельний кадастр на блокчейні, що полегшить роботу підприємців. Багато інших країн також приєдналися або приєднуються до використання технології блокчейн.

У багатьох сферах, зокрема у сфері охорони здоров'я, блокчейн вже використовується для збереження даних пацієнтів та медичних записів. Ці дані

можуть бути зашифровані з використанням публічних та приватних ключів, що забезпечує доступ до них лише авторизованим користувачам. Впровадження блокчейну дозволить пацієнтам перевірити, чи зроблені всі відповідні записи лікарями, і гарантувати, що дані не будуть видалені або змінені без дозволу. Пацієнти матимуть доступ до повного ланцюжка записів усіх лікарів у хронологічній послідовності, що сприяє уникненню непорозумінь між медичним персоналом. Крім того, це допоможе у запобіганні шкоди від хакерських атак, оскільки дані пацієнтів будуть захищені високим рівнем конфіденційності та безпеки. Багато подібних проектів вже успішно реалізовано та активно використовуються.

Незалежно від того, як використовується блокчейн, ключовим компонентом є його здатність до децентралізації. Ця функція видаляє єдину цільову точку, яка може бути зламана. В результаті стає абсолютно неможливо проникнути в системи або сайти, контроль доступу, зберігання даних та мережевий трафік яких, більше не знаходяться в одному місці. Застосування блокчейн-технологій для забезпечення безпеки даних має великий потенціал і може бути корисним у різних сферах. По закінченню третього розділу нами були сформовані пропозиції щодо застосування блокчейну для забезпечення безпеки даних, як включають: захист особистих даних, аутентифікацію ідентичності, трекінг походження даних, захист від кібератак, забезпечення цілісності даних.

Основні переваги використання блокчейн-технологій:

1. Децентралізоване зберігання даних: це одна з ключових особливостей блокчейну, де інформація зберігається в блоках та розподіляється між безліччю учасників мережі. Це зменшує вразливість до атак на централізовані сховища даних.

2. Криптографічна безпека: блокчейн використовує потужні криптографічні алгоритми для захисту даних і забезпечення цілісності блоків. Використання хешування та цифрових підписів забезпечує неможливість зміни або підроблення даних без відповідних дозволів.

3. Незмінність даних: кожен блок містить хеш попереднього блоку,

утворюючи ланцюжок. Це унеможливлює зміну даних і захищає їх від можливих маніпуляцій.

4. Контроль доступу та приватність: блокчейн дозволяє контролювати доступ до даних і забезпечує їхню приватність, що є важливим для роботи з конфіденційною інформацією.

5. Відсутність посередників: блокчейн дозволяє уникнути посередників, оскільки інформація зберігається та підтверджується всіма учасниками мережі, що зменшує ризики шахрайства.

У цьому дослідженні було детально розглянуто використання технології блокчейн у різних сферах, зокрема в фінансовій галузі, логістиці, охороні здоров'я та управлінні даними. Одним з найпоширеніших застосувань блокчейну є криптовалюти, які змінили підходи до транзакцій, зберігання та обміну вартостями. Важливо зазначити, що використання криптовалют та відповідних інструментів, таких як криптогаманці, стає все більш поширеним як серед окремих користувачів, так і в бізнесі. На особистому прикладі я можу поділитися власним досвідом використання криптогаманця Trust Wallet. Цей криптогаманець забезпечує високий рівень безпеки та зручності для зберігання і управління різними криптовалютами. Trust Wallet підтримує широкий спектр криптовалют, що дозволяє користувачам ефективно керувати своїми активами. Крім того, інтеграція з різними децентралізованими додатками (dApps) дає можливість безпосередньо з гаманця брати участь у фінансових операціях, торгівлі на децентралізованих біржах та користуватися іншими сервісами, заснованими на блокчейні. Однією з переваг такого використання є безпека. Криптогаманці зазвичай мають різні рівні безпеки, включаючи можливість налаштування двофакторної аутентифікації та використання криптографічних ключів. Додатково, використання криптогаманця дозволяє зберігати і керувати криптовалютою без посередництва банків чи інших фінансових установ. Це дає більший контроль користувачеві над його фінансами.

Отже, дослідження показало, що блокчейн має значний потенціал для

трансформації багатьох галузей, а власний досвід використання Trust Wallet підтверджує практичність і зручність цієї технології у повсякденному житті. Це ще раз підкреслює важливість подальшого вивчення та впровадження блокчейну для покращення ефективності та безпеки різних процесів.

Загальний висновок полягає в тому, що застосування блокчейн-технологій в сфері забезпечення безпеки даних має великий потенціал. Вони надають можливості для створення безпечних, незмінних та децентралізованих систем збереження та передачі інформації. Використання гібридних блокчейн-мереж та смарт-контрактів може забезпечити відсутність недоліків, що характерні для інших типів блокчейнів. Хоча є деякі виклики, такі як обмежена масштабованість та відсутність нормативно-правової бази, що регулює використання технології, з кожним роком ці проблеми стають менш значущими. Отже, використання блокчейн технологій може стати ефективним рішенням для забезпечення безпеки даних у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балазюк О.Ю., Пилявець В.М. Технологія блокчейн: дослідження суті та аналіз сфер використання. *Економіка та суспільство*. 2022. №43. С. 1-8. URL: https://economyandsociety.in.ua/index.php/journal/article/download/1701/1636/
2. Банах С. Поняття та особливості інформації як теоретичної категорії. *Актуальні проблеми правознавства.* 2019. Вип. 4. С. 226-231. URL: http://dspace.wunu.edu.ua/bitstream/316497/38405/1/Банах.pdf
3. Баран М.В. Захист інформації у контексті забезпечення інформаційної безпеки. *Аналітично-порівняльне правознавство.* 2022. №3. С. 150-155. URL: http://journal-app.uzhnu.edu.ua/article/view/264943/260924
4. Блокчейн і децентралізовані системи: навч.посібник для студ.закл.вищ.осв. У трьох частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. Харків: ПРОМАРТ, 2022. 460 с.
5. Блокчейн у логістиці. URL: https://blog.whitebit.com/uk/blockchain-in-logistics/ (дата звернення 06.05.2024).
6. Дмитрик О.О., Артеменко К.В. Безпека та прозорість: як блокчейн змінює платіжні системи та фінансовий сектор. Ю*ридичний науковий електронний журнал*. 2023. №4. С. 460-463. URL: http://lsej.org.ua/9_2023/114.pdf
7. Захист інформації в автоматизованих системах управління: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с. URL: https://moodle.znu.edu.ua/pluginfile.php/1142772/mod_resource/content/1/Zahyst_informacii_ASU.PDF
8. Кобійчук В.В., Рожкова М.С. Дослідження застосування блокчейн-технологій у діяльності світових підприємств: методичний підхід. *Приазовський економічний вісник.* 2020. Випуск 4(21). С. 118-123. URL: http://pev.kpu.zp.ua/journals/2020/4_21_ukr/22.pdf
9. Ковальчук Л.В., Кудін А.М., Кучинська Н.В. Вступ до технології блокчейн та

криптовалют. Ч.1. Теоретичні засади функціонування блокчейн-технологій: навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 142 с. URL: https://moodle.znu.edu.ua/pluginfile.php/1121555/mod_resource/content/1/Vstup_do_tekhnolohii_blokchein_kryptovaliut_1.pdf

10. Костюк П.П. Використання технології блокчейн для забезпечення інформаційної безпеки. *Сучасний захист інформації.* 2020. №3. С. 22-28. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2440/2338
11. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. Харків : ПРОМАРТ, 2019. 452 с.
12. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99 від 28 квітня 1999 р. №22. ДСТСЗІ СБУ, 1999. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
13. Кудирко О. В. Інновації в логістиці: перспективи використання технології блокчейн у ланцюгах поставок. *Науковий вісник Ужгородського національного університету. Серія «Міжнародні економічні відносини та світове господарство».* 2017. Вип. 15 (1). С. 158–163. URL: http://www.irbis-nbuv.gov.ua/
14. Кудь А.А. Трансформація економічних відносин та способів їх реалізації в умовах розвитку цифрових технологій. *Вісник Львівського університету. Серія економічна.* 2022. Випуск 62. С. 42–58. URL: http://dx.doi.org/10.30970/ves.2022.62.0.6204
15. Куліковський А. Технологія Blockchain як складова інформаційної безпеки. Кібербезпека: освіта, наука, техніка. 2019. №4. Т.4. С. 85-89. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/84/93
16. Литовченко А. Історія Blockchain: від заснування до широкого розповсюдження. URL: https://thepage.ua/ua/experts/istoriya-blockchain-vid-zasnuvannya-do-shirokogo-rozpovsyudzhennya (дата звернення 01.05.2024).
17. Мазуренко О. К. Технології Blockchain в інформаційному забезпеченні

логістичних послуг. *Бізнесінформ.* 2019. №12. С. 255-261. URL: https://www.business-inform.net/export_pdf/business-inform-2019-12_0-pages-255_261.pdf

18. Мануілов Я.С. Використання технології «блокчейн» у телекомунікаціях. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2021. Том 32 (71) № 3. С. 123-127. URL: http://www.tech.vernadskyjournals.in.ua/journals/2021/3_2021/22.pdf
19. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. URL: https://zakon.rada.gov.ua/laws/show/2210-14#Text (дата звернення 01.05.2024).
20. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 01.05.2024).
21. Стащук О.В., Теслюк С.А., Кузьмич І.В. Перспективи використання технології блокчейн у фінансовому секторі. *Електронний журнал «Економіка та суспільство».* 2022. № 40. URL: https://www.economyandsociety.in.ua/index.php/journal/article/view/1562/1503
22. Сурган І. Що таке алгоритм досягнення консенсусу в блокчейні? URL: https://incrypted.com/ua/
23. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99 від 28 квітня 1999 р. №22. ДСТСЗІ СБУ, 1999. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf
24. Уткіна М.С., Харченко А.Л. Blockchain як революційне явище у сфері технологій та права інтелектуальної власності. *"Young Scientist"*. 2020. № 4. С. 472. URL: https://molodyivchenyi.ua/index.php/journal/article/view/2092/2071
25. Четверіков І.О., Петренко А.І. Технологія blockchain в системі захисту інформації. Моделювання та інформаційні системи в економіці : зб. наук. пр. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана» ; [редкол.: О. Є. Камінський (відп. ред.) та ін.]. Київ : КНЕУ, 2020. Вип. 99. С. 162–169. URL: https://kneu.edu.ua/userfiles/zb_mise/99/14.pdf
26. Що таке хеш у блокчейні? URL:

https://blog.whitebit.com/uk/what-is-a-hash-in-blockchain/

27. Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків. *Підприємництво та інновації*. 2020. № 12. С. 206–214. URL: https://doi.org/10.37320/2415-3583/12.36
28. Badzar A. Blockchain for Securing Sustainable Transport Contracts and Supply Chain Transparency. Master's Thesis. Lund University. Helsingborg, Sweden. 2016. URL: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8880383&fileOId=8880390
29. Blockchain set to transform collateral lending. 2018. URL: https://www.ing.com/Newsroom/News/Blockchain-set-to-transform-collaterallending.htm (дата звернення 05.05.2024).
30. Casey M. J., Wong P. Global Supply Chains Are About to Get Better, Thanks to Blockchain. Harvard Business Review. 13 March 2017. URL: https://hbr.org/2017/03/global-supplychains-are-about-to-get-better-thanks-to-Blockchain.
31. Clavin J. Blockchains for Government: Use Cases and Challenges. 2020. URL: https://dl.acm.org/doi/fullHtml/10.1145/3427097.
32. Schroeder M. Spór o pojęcie informacji. *Studia Metodologiczne.* 2015. № 34. S.11–36.
33. State land cadastre transeferred to blockchain technology. 2017. URL: https://ti-ukraine.org/en/news/derzhavnyi-zemelnyi-kadastrpereishov-na-tekhnolohiiu-blokchein/ (дата звернення 05.05.2024).
34. YouTeam Editorial Team. 10 Use Cases of Blockchain Technology in Banking 2023. URL: https://youteam.io/blog/10-use-cases-ofblockchain-technology-in-banking/ (дата звернення 05.05.2024).

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра
Комп'ютерної інженерії

Презентація бакалаврської роботи на тему: «Дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних»

ВИКОНАВ: СТУДЕНТ ГРУПИ КІД-41
Терещенко Євгеній Дмитрович

1

Слайд 1

Мета, Об'єкт предмети досліджень та актуальність теми

Мета роботи – обґрунтування можливостей застосування блокчейн технологій для забезпечення безпеки даних.

Об'єкт дослідження – технологія блокчейн

Предмет дослідження – можливості застосування блокчейн технологій для забезпечення безпеки даних.

Актуальність теми – Блокчейн продовжує залишатися актуальною технологією через свою здатність забезпечувати безпеку, недійсність імутабельності та децентралізації. Він використовується в фінансах, логістиці, медицині та інших галузях для забезпечення прозорості та ефективності у даних та процесах.

2

Слайд 2

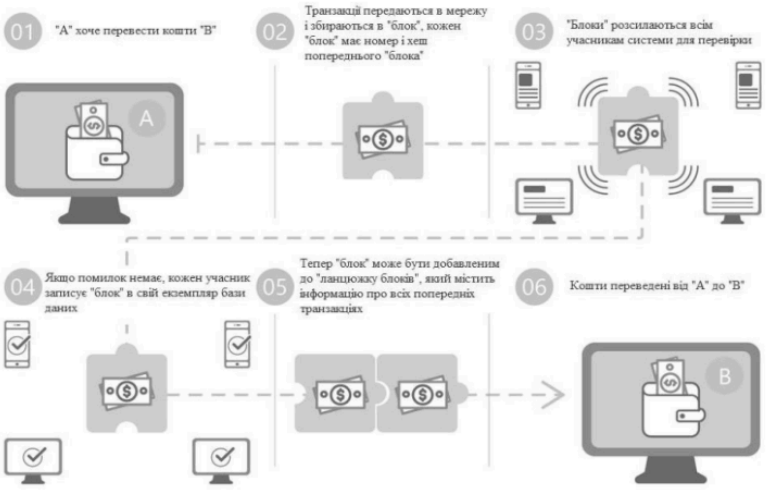
Порівняльна таблиця трьох типів блокчейнів

Особливості	Публічний блокчейн з відкритим доступом	Приватний блокчейн з відкритим доступом	Приватний блокчейн з закритим доступом
Доступ до блокчейну	Відкритий для всіх користувачів, можливість відправлення транзакцій та перевірки даних.	Відкритий для всіх користувачів, проте лише привілейовані користувачі можуть проводити аудит безпеки та вносити зміни.	Лише привілейовані користувачі мають доступ до мережі та можуть проводити аудит безпеки та змінювати дані.
Децентралізація	Повна децентралізація, незалежність від третіх осіб.	Часткова децентралізація, залежність від привілейованих користувачів	Можливий рівень децентралізації, залежить від управління адміністраторів
Керування	Відсутнє централізоване керування	Децентралізоване керування, проте з обмеженими можливостями для привілейованих користувачів	Централізоване керування адміністрацією мережі
Відкритість даних	Публічний доступ до всіх даних та транзакцій	Публічний доступ до даних, але обмеження для проведення аудиту та змін	Обмежений доступ до даних та можливості внесення змін
Швидкодія	Може бути менш ефективним через велику кількість вузлів та глобальну доступність	Може бути більш ефективним, оскільки має менше вузлів та обмежений доступ	Може бути найефективнішим, оскільки має обмежену кількість вузлів та контрольований доступ
Вартість	Дороге управління через велику кількість вузлів	Вартість управління залежить від розміру та складності мережі	Менша вартість управління через обмежену кількість вузлів та контрольований доступ

3

Слайд 3

Перевага проведення транзакцій через Blockchain



4

Слайд 4

Приклад проведення транзакцій через Blockchain

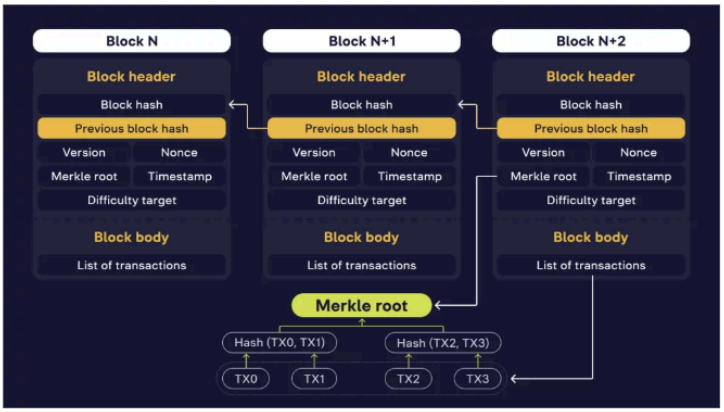
```python
from ecdsa import SigningKey, SECP256k1
import hashlib

# Створення криптогаманця A
private_key_A = SigningKey.generate(curve=SECP256k1)
public_key_A = private_key_A.verifying_key.to_string()

# Адреса криптогаманця A зазвичай є хешем його публічного ключа
address_A = hashlib.sha256(public_key_A).hexdigest()

# Створення криптогаманця B
private_key_B = SigningKey.generate(curve=SECP256k1)
public_key_B = private_key_B.verifying_key.to_string()
address_B = hashlib.sha256(public_key_B).hexdigest()

# Сума переказу
amount = 10

# Підписання транзакції від A до B
transaction_data = f"{address_A}->{address_B}:{amount}"
signature_A = private_key_A.sign(transaction_data.encode())

# Перевірка підпису B
try:
    public_key_A.verify(signature_A, transaction_data.encode())
    print("Підпис вірний.")
except ecdsa.BadSignatureError:
    print("Неправильний підпис.")
```

Простий приклад коду на мові Python, який демонструє створення та підписання транзакції між двома криптогаманцями. Для цього прикладу використовується бібліотека ecdsa для роботи з еліптичними кривими, що зазвичай використовується для підписування транзакцій у біткойні та інших криптовалютах.

5

Слайд 5

хешування SHA-256



6

Слайд 6

Дослідження переваг та недоліків різних алгоритмів

Тип алгоритму	Переваги	Недоліки
PoW	Надійність, високий рівень безпеки	Неекологічність та висока енергозатратність
PoS	Висока швидкість обробки транзакцій, енергоефективність	Нижчий рівень безпеки порівняно з PoW, менший рівень децентралізації
DPoS	Висока швидкість обробки транзакцій	Схильність до централізації
PoA	Обробляє велику кількість транзакцій в секунду, стійкість до кібератак та шахрайства	Схильність до централізації
PoB	Високий рівень безпеки, стимулювання довгострокової участі	Марнотратство ресурсів
PoL	Висока енергоефективність та децентралізація	Низький рівень масштабованості, складність обчислень

Слайд 7

Приклда роботу хешування SHA-256

```python
import hashlib

# Вхідне повідомлення
message = "Hello, world!"

# Перетворення рядка в байтовий формат
message_bytes = message.encode('utf-8')

# Хешування вхідного повідомлення за допомогою SHA-256
hash_result = hashlib.sha256(message_bytes).hexdigest()

# Виведення отриманого хешу
print("SHA-256 хеш вхідного повідомлення:", hash_result)
```

У цьому коді ми спочатку конвертуємо рядок у байтовий формат, оскільки бібліотека hashlib очікує байтові дані для хешування. Потім ми використовуємо метод sha256 для створення об'єкту хешування SHA-256 та метод hexdigest() для отримання закодованого у шістнадцятковому форматі рядка, який представляє собою фактичний хеш.

Слайд 8

Дослідження власного використання криптогаманцю який працює на блокчейн

9

Слайд 9

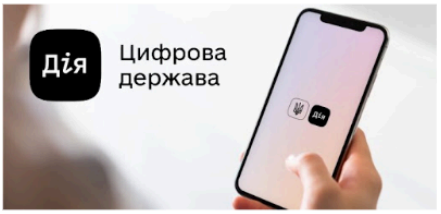
Дослідження Використання Blockchain в логістиці

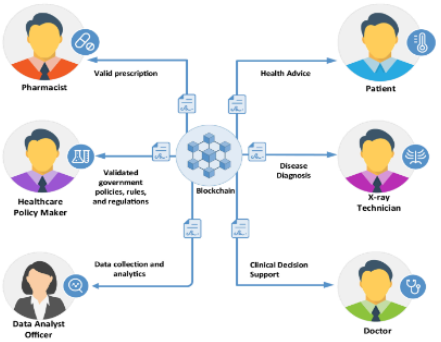
У 2021 році обсяг світового ринку логістики становив $9,5 трлн, а очікується, що протягом наступних 5 років (з 2022 по 2027 рік) він зросте до $13,3 трлн. Незважаючи на постійне збільшення обсягів постачання, людський фактор, складність документообігу та велика кількість контрагентів суттєво уповільнюють процес і підвищують вартість послуг. Використання технології блокчейну може вирішити ці проблеми, поліпшити комунікацію, заощадивши галузі приблизно $40 млрд.

10

Слайд 10

Дослідження Використання Blockchain у Державному секторі

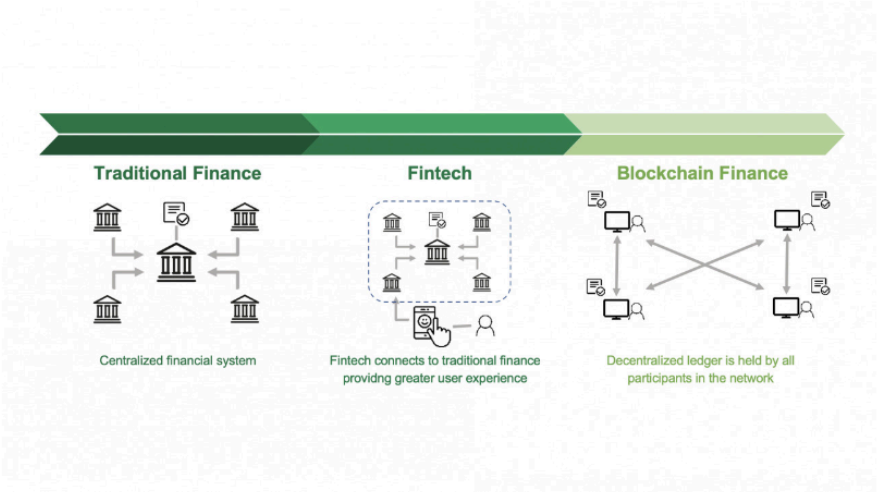




11

Слайд 11

Дослідження Використання Blockchain у фінансовому секторі



12

Слайд 12

Висновок

У цій роботі було розглянуто і проведено аналіз та дослідження переваг технології блокчейн, такі як незмінність, децентралізація, прозорість та конфіденційність дають великий потенціал для втілення їх в основні галузі по всьому світу для зменшення витрат, прискорення та оптимізацію процесів

Використання блокчейн-технологій може ефективно забезпечити безпеку даних у різних сферах. Децентралізоване зберігання даних, криптографічна безпека, незмінність даних, контроль доступу та відсутність посередників - основні переваги цієї технології. Хоча є виклики, такі як обмежена масштабованість та відсутність регулюючої бази, з кожним роком ці проблеми стають менш актуальними. Таким чином, блокчейн може стати важливим засобом для забезпечення безпеки інформації у майбутньому.

Слайд 13

Висновок продовження

Проаналізувавши застосування блокчейн технологій в державному секторі, фінансовому секторі та логістиці можна зробити висновок, що ця технологія збільшує продуктивність та безпеку даних зменшуючи витрати та прибираючи людський фактор. Дослідивши найпопулярніші алгоритми технології блокчейн ми бачимо практичне застосування їх для поліпшення інших процесів та зменшення негативного впливу на зовнішнє середовище: використання алгоритму PoW - для обігріву приміщень щоб попросту не витрачати енергію, що виділяється при важких обчисленнях

Слайд 14

Висновок продовження

дослідження показало, що блокчейн має значний потенціал для трансформації багатьох галузей, а власний досвід використання Trust Wallet підтверджує практичність і зручність цієї технології у повсякденному житті. Це ще раз підкреслює важливість подальшого вивчення та впровадження блокчейну для покращення ефективності та безпеки різних процесів.

Слайд 15

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Євгеній ТЕРЕЩЕНКО

Назва: Дослідження можливостей застосування блокчейн технологій для забезпечення безпеки даних

Координатор: Юлія БОРОВА

Підрозділ: ННІІТ

Коефіцієнт подібності 1:20.3

Коефіцієнт подібності 2:8.5

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… …… *Дата Підпис Наукового*