МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»
Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»
Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему **«Система захисту електронного документообігу на основі технології блокчейн»**

здобувача Палагіна Владислава Олеговича

Науковий керівник: к.т.н., доцент Кулініч Олег Миколайович

_____

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., професор Джалладова І.А.

_____

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»
Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»
Форма навчання: очна (денна)

ПОГОДЖЕНО:
Керівник проектної групи (гарант)
освітньо-професійної програми «Кібербезпека»
к.ф.-м.н, доцент Г.В. Мамонова

_____
_____2024 р.

ЗАТВЕРДЖУЮ:
Завідувач кафедри системного
аналізу та кібербезпеки
д.ф.-м.н., проф. І.А. Джалладова

_____
_____2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Палагіна Владислава Олеговича

денної форми навчання

на підготовку кваліфікаційної бакалаврської роботи

на тему **«Система захисту електронного документообігу на основі технології блокчейн»**

Тему затверджено наказом ректора Університету від 30.04.2024р. № 726-ст

План кваліфікаційної бакалаврської роботи

Розділ 1	Методи та способи захисту інформації
Розділ 2	Суть, методи та моделі технології блокчейн
Розділ 3	Система технології блокчейн
Об'єкт дослідження:	Процес забезпечення цілісності та безпеки електронних документів за допомогою технології блокчейн
Предмет дослідження: технологія впровадження блокчейн у систему електронного документообігу.	
Мета кваліфікаційної бакалаврської роботи: розробка програмного забезпечення для системи електронного документообігу з використанням блокчейн-технології, що забезпечує незмінність та автентичність даних.	
Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети: 1. Дослідити концепцію електронного документообігу та його вимоги до безпеки. 2. Проаналізувати принципи та технології блокчейну. 3. Визначити необхідні компоненти для інтеграції блокчейну в систему електронного документообігу. 4. Розробити програмну реалізацію системи захисту електронного документообігу за допомогою блокчейну. 5. Здійснити інтеграцію блокчейну в існуючу інформаційну систему комерційного проекту.	
У розділі 1	Здійснено дослідження предметної галузі, описано основні загрози компрометації облікових даних та розглянуто методи їх протидії. Проаналізовано традиційні методи аутентифікації у клієнт-серверних програмах, а також розглянуто переваги використання блокчейн-технологій для забезпечення безпеки даних.
У розділі 2	Описано принципи роботи блокчейн та його застосування в системах електронного документообігу. Вивчено механізми функціонування блокчейну, включаючи створення, верифікацію та зберігання блоків даних. Розглянуто питання безпеки, цілісності та незмінності даних у блокчейні, а також використання криптографії для захисту інформації.
У розділі 3	На прикладному рівні описано процес розробки та впровадження елементів системи захисту електронного документообігу за допомогою блокчейн. Детально розглянуто архітектуру системи, включаючи компоненти та взаємодію між ними. Представлено програмну реалізацію створення блоків, хешування даних та забезпечення цілісності інформації.

Завдання підготував
науковий керівник

_____ к.т.н., доцент Кулініч О.М.

Завдання одержав
здобувач

_____ Палагін В.О

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатку і має 59 сторінок основного тексту, 22 рисунки, 2 сторінки додатку. Список використаних джерел містить 16 найменувань і займає 2 сторінки. Загальний обсяг роботи 67 сторінок.

Об'єкт дослідження. Процес забезпечення цілісності та безпеки електронних документів за допомогою технології блокчейн.

Мета роботи. Розробка програмного забезпечення для системи електронного документообігу з використанням блокчейн-технології, що забезпечує незмінність та автентичність даних.

Методи дослідження. Аналіз літературних джерел, системний аналіз, проектування програмного забезпечення, тестування програмного забезпечення.

Найважливіші та найвагоміші результати роботи. Розроблено програмне забезпечення яке демонструє основні принципи роботи та можливості для забезпечення безпеки та цілісності електронних документів. Впроваджено механізми хешування даних та цифрового підпису, що гарантують незмінність та автентичність документів.

Пропозиції щодо можливих напрямів продовження досліджень.

– Подальше вдосконалення алгоритмів захисту даних у системі електронного документообігу.

– Розробка інтерфейсів для інтеграції блокчейн-систем з іншими інформаційними системами підприємств.

– Дослідження можливостей використання інших криптографічних методів для підвищення безпеки електронних документів.

Ключові слова: блокчейн, інформаційна безпека, система електронного документообігу, електронний документ, цифровий підпис, технологія блокчейн.

Рік виконання кваліфікаційної бакалаврської роботи 2024.

Рік захисту кваліфікаційної бакалаврської роботи 2024.

ВІДГУК

на кваліфікаційну бакалаврську роботу
студента: Палагіна Владислава Олеговича гр. ІК - 401
на тему: «Система захисту електронного документообігу за допомогою блокчейн»

Актуальність теми. Тема кваліфікаційної роботи Палагіна Владислава «Система захисту електронного документообігу за допомогою блокчейн» є актуальною, оскільки впровадження блокчейн-технології в системи електронного документообігу забезпечує високий рівень безпеки та цілісності даних. Використання децентралізованих систем дозволяє уникнути єдиної точки відмови та знижує ризики несанкціонованого доступу або модифікації даних.

Повнота розкриття теми. Тема бакалаврської кваліфікаційної роботи розкрита в повному обсязі, про що свідчать результати, наведені в пояснювальній записці, новизна отриманих результатів та їх практична цінність.

Теоретичний рівень. Студент в своїй кваліфікаційній роботі самостійно виконав аналіз існуючих аспектів електронного документообігу та технології блокчейн, зібрав та попередньо підготував дані. В процесі роботи над кваліфікаційною роботою були використані сучасні методи досліджень, зокрема виконана розробка програмної реалізації запропонованих рішень.

Практична значущість. Отримані в кваліфікаційній роботі результати можуть бути використані для подальшої розробки та вдосконалення систем електронного документообігу з підвищеним рівнем безпеки. Розроблене програмне забезпечення має значний потенціал для впровадження в реальних умовах та може бути адаптоване для різних галузей.

Самостійність виконання роботи Кваліфікаційна робота Палагіна Владислава виконана у повному обсязі, самостійно в визначені строки та у відповідності до завдання. Оформлена у відповідності до нормативних вимог.

Переваги та недоліки роботи. Кваліфікаційна робота відзначається високим практичним рівнем, глибиною проведеного аналізу та інноваційністю запропонованих рішень.

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК. Результати представленої до захисту кваліфікаційної роботи свідчать про високий рівень підготовки її автора. Кваліфікаційна робота повністю відповідає вимогам, що висуваються до кваліфікаційних робіт освітньо-кваліфікаційного рівня бакалавра, і заслуговує оцінки «добре/82», а її автор Палагін Владислав заслуговує присвоєння йому ступеня бакалавра зі спеціальності «Кібербезпека».

Науковий керівник
к.т.н., доцент САтаК Кулініч О.М.

«___» червня 2024 р.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу

студента Палагіна Владислава Олеговича гр. ІК - 401

на тему: «Система захисту електронного документообігу за допомогою блокчейн»

Актуальність теми. Робота присвячена впровадженню блокчейн-технології в систему електронного документообігу. Ця тема є надзвичайно актуальною в сучасних умовах, коли інформаційна безпека та захист даних стають ключовими аспектами в діяльності будь-якої організації.

Наукова новизна. Дослідження полягає у розробці та вдосконаленні методів захисту документів на основі блокчейн, що враховують сучасні технологічні та організаційні вимоги.

Якість проведеного аналізу. Аналіз проведено на високому рівні, із застосуванням сучасних методів та підходів. Студент детально розглянув технологію блокчейн, її особливості та переваги, а також здійснив огляд сучасних систем електронного документообігу та їхніх недоліків.

Уміння користуватись літературними джерелами. Робота демонструє хороше вміння користуватися літературними джерелами. Використано широкий спектр наукових праць, статей та інших ресурсів, що свідчить про систематичний підхід до дослідження.

Практична цінність висновків і рекомендацій. Практична цінність дослідження полягає у можливості реального впровадження розробленої системи електронного документообігу на основі блокчейн. Запропоновані рішення можуть значно покращити безпеку та ефективність документообігу в організаціях, забезпечуючи високий рівень захисту конфіденційних даних.

Переваги та недоліки. Серед переваг роботи слід відзначити глибокий аналіз проблеми, детальний огляд сучасних технологій та практичну спрямованість дослідження. Однак, деякі аспекти можуть бути вдосконалені. Наприклад, у роботі відсутній детальний розгляд можливих ризиків та перешкод при впровадженні блокчейн-технології в існуючі системи електронного документообігу.

Загальний висновок і оцінка роботи. Загалом, дипломна робота справляє позитивне враження. Вона є актуальною, науково новою та має високу практичну цінність. Студент демонструє глибокі знання предмету та здатність до самостійного наукового дослідження.

Начальник відділу
інформаційних технологій
ТОВ « КК «ВЕРДИКТ» »

Дунський А.О.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

DES (Data Encryption Standard) – стандарт шифрування даних.
ECB (Electronic Code Book) – режим "електронної кодової книги" (проста заміна).
CBC (Cipher Block Chaining) – режим зчеплення блоків.
CFB (Cipher Feed Back) – режим зворотного зв'язку за шифротекстом.
AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування.
RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) – криптографічний алгоритм з відкритим ключем.
CRC32 (Cyclic Redundancy Check) – алгоритм знаходження контрольної суми.
MD5 (Message Digest 5) – 128-бітний алгоритм хешування.
SHA (Secure Hash Algorithm) – алгоритм криптографічного хешування.
ДСТУ - державні стандарти України.
ISO (International Organization for Standardization) – міжнародна організація зі стандартизації.
IEC (International Electrotechnical Commission) – міжнародна електротехнічна комісія.
IDT (Integrated Device Technology) – американська компанія, що займалася розробкою інтегральних мікросхем.
ЕДО – електронний документообіг.
ЕД – електронний документ.
ЕЦП – єдиний цифровий підпис.
SSL (Secure Sockets Layer) – рівень захищених сокетів.
TLS (Transport Layer Security) – захист на транспортному рівні.
POW (Proof-of-work) – доказ виконання роботи.
PoS (Proof-of-Stake) – підтвердження частки володіння.
UTXO (Unspent Transaction Output) – невитрачений результат транзакції.
СЕД – система електронного документообігу.
DeFi (Decentralized Finance) – децентралізоване фінансування.
GDPR (General Data Protection Regulation) – загальний регламент про захист даних.
EDMS (Document management system) – електронний документообіг.
DLT (Distributed Ledger Technology) – технологія розподіленого реєстру.

ВСТУП

Оцінка сучасного стану проблеми. Сьогодні електронний документообіг (ЕДО) стає невід'ємною частиною діяльності багатьох організацій та установ. Незважаючи на значний прогрес у впровадженні систем ЕДО, забезпечення безпеки даних залишається актуальною проблемою. У науковій літературі широко висвітлюються питання захисту інформації в електронному документообігу, проте наявні підходи мають ряд обмежень та вразливостей. Зокрема, традиційні методи криптографічного захисту не завжди можуть забезпечити необхідний рівень надійності, особливо в умовах активних кіберзагроз.

В останні роки блокчейн-технології привертають дедалі більше уваги як потенційний інструмент для підвищення безпеки ЕДО. Відомі дослідження у цій галузі проведено такими науковцями, як Сатоші Накамото, Віталік Бутерін, Дон Тапскотт та Алекс Тапскотт. В Україні значний вклад у розвиток блокчейн-технологій зробили В'ячеслав Куценко, Олександр Пушкар та Володимир Павленко.

Актуальність і перспективність тематики роботи. Актуальність дослідження обумовлена необхідністю подолання протиріч між вимогами до безпеки електронного документообігу та обмеженими можливостями традиційних методів захисту. Використання блокчейн-технологій відкриває нові перспективи для удосконалення систем ЕДО завдяки їх децентралізованій природі, високій стійкості до маніпуляцій та здатності забезпечити прозорість і незмінність даних.

Мета і завдання дослідження. Метою даної роботи є розробка програмного забезпечення для системи електронного документообігу з використанням блокчейн-технології, що забезпечує незмінність та автентичність даних.

Для досягнення цієї мети поставлені наступні завдання:

– Провести аналіз існуючих методів захисту електронного документообігу.

– Дослідити можливості застосування блокчейн-технологій для підвищення безпеки ЕДО.

– Розробити модель системи захисту ЕДО на основі блокчейн.

– Провести експериментальне дослідження розробленої системи та оцінити її ефективність.

Об’єкт, предмет, методи дослідження.

Об'єкт дослідження – процес забезпечення цілісності та безпеки електронних документів за допомогою технології блокчейн.

Предмет дослідження – методи та технології захисту електронного документообігу з використанням блокчейн.

Методи дослідження – аналіз літературних джерел, системний аналіз, проектування програмного забезпечення, тестування програмного забезпечення

Теоретична і методична значущість отриманих результатів. Теоретична значущість роботи полягає в розробці нових методів та підходів до забезпечення безпеки електронного документообігу з використанням блокчейн. На відміну від існуючих рішень, запропоновані підходи забезпечують високий рівень захисту даних завдяки децентралізованій природі блокчейн та використанню криптографічних алгоритмів.

Практичне значення одержаних результатів. Практична значущість роботи полягає в можливості впровадження розробленої системи захисту електронного документообігу на основі блокчейн в різних організаціях, що дозволить підвищити рівень безпеки, надійності та ефективності управління документами.

Інформація про апробацію результатів роботи та публікації. Основні наукові положення обговорювалися на науково-практичній конференції «Інтелектуальні методи аналізу загроз кібербезпеки (Київ, 2023).

РОЗДІЛ 1. МЕТОДИ ТА СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Методи криптографічного захисту інформації

Зі збільшенням використання Інтернету для обміну даними та комунікації, захист від кібератак стає критично важливим. Забезпечення конфіденційності та приватності даних постає як значний виклик для кібербезпеки. Конфіденційність передбачає захист інформації від несанкціонованого доступу та крадіжки, що можливо через криптографічне шифрування і розшифрування даних. Криптографія має на меті забезпечити безпеку критично важливих даних, незалежно від того, зберігаються вони локально чи передаються через незахищені канали.

Сучасна криптографія покладається на відкриті алгоритми шифрування, які вимагають обчислювальних ресурсів. Існує багато перевірених методів шифрування, які, за умови використання ключів та правильної реалізації алгоритмів, роблять зашифровані дані стійкими до криптоаналізу.

Цей підхід до інформаційної безпеки не тільки підвищує рівень захисту даних, але й сприяє розвитку методів криптографічного захисту, адаптованих до швидко змінних умов цифрового світу.

Загальні вимоги до методів шифрування захисту інформації такі:

– зашифроване повідомлення має бути доступним для читання лише за наявності ключа (набору параметрів, що використовуються для шифрування повідомлення);

– кількість операцій, необхідних для визначення ключа шифрування, який використовується для фрагмента повідомлення та відповідного відкритого тексту, має бути не менше загальної кількості можливих ключів;

– кількість операцій, необхідних для розшифровки повідомлення шляхом сортування можливих ключів, повинна мати строго низьку оцінку і перевищувати можливості сучасних комп'ютерів (з урахуванням можливості використання

мережевих обчислень); знання алгоритму шифрування не повинно впливати на надійність захисту статі;

– навіть якщо використовується той самий ключ, незначна зміна ключа може призвести до значних змін у типі зашифрованого повідомлення

– алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до погіршення якості алгоритму шифрування.

Шифрування даних – це мистецтво захисту повідомлень шляхом їх перетворення на приховані тексти, тоді як зворотний процес отримання оригінальних текстів із прихованих текстів називається дешифруванням. Шифрування/дешифрування стає можливим за допомогою деяких ключів. Кожен алгоритм шифрування прагне зробити процес дешифрування якомога важчим без використання ключа, що використовувався під час шифрування. На рис. 1.1 показана загальна ідея шифрування та дешифрування. Існують три типи криптографічних технік: симетричний ключ, асиметричний ключ та хешування, показані на рис. 1.2.

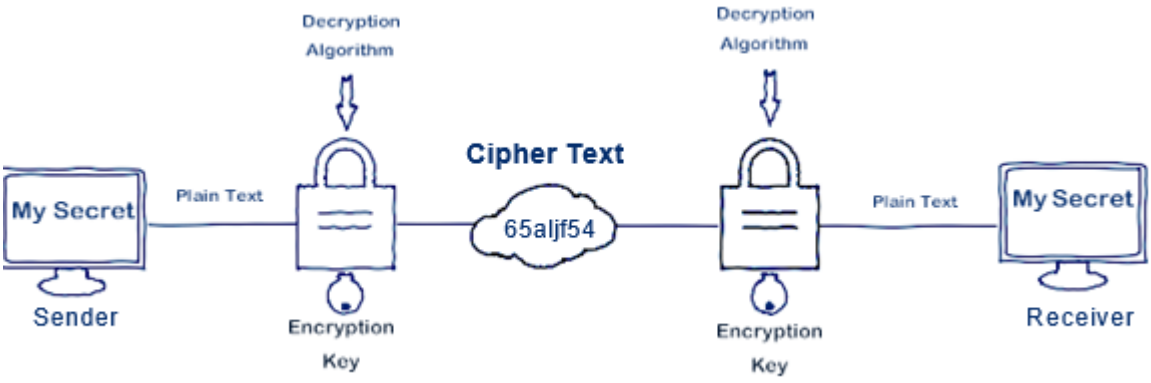

Рисунок 1.1 – Загальне уявлення про шифрування та дешифрування

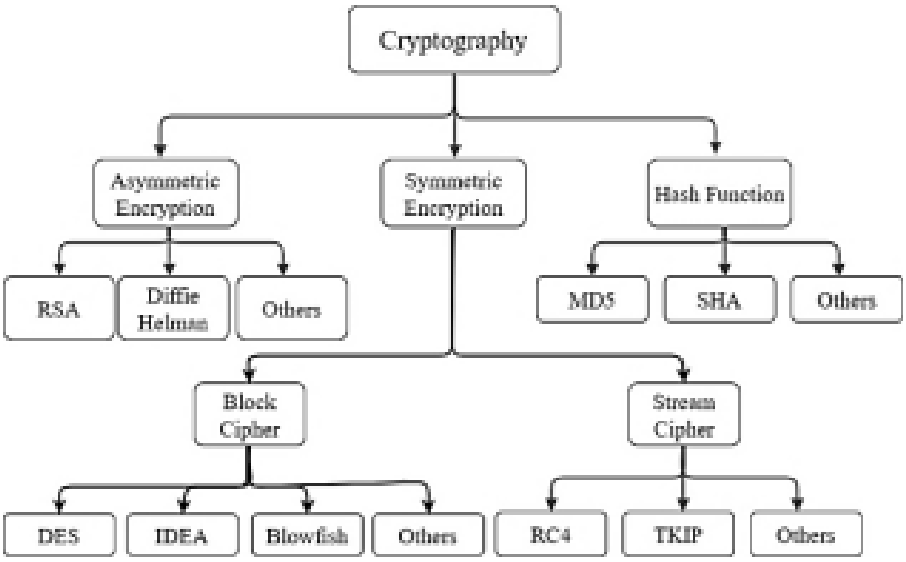

Рисунок 1.2 – Основна класифікація криптографії

1.1.1 Симетричні шифри

У техніці симетричного ключа і шифрування, і дешифрування виконуються на основі одного закритого ключа. Його також називають секретним ключем. Для обміну цим закритим ключем між відправником і одержувачем потрібен безпечний канал. Симетричні ключові криптографічні алгоритми поділяються на блочні та потокові шифри. У системах на основі блокового шифру дані обробляються або шифруються на основі групи бітів фіксованої довжини, яка називається блоком, тоді як у системах на основі потокового шифру дані обробляються на основі потоку бітів. Рисунок 1.3 ілюструє процес симетричного шифрування.

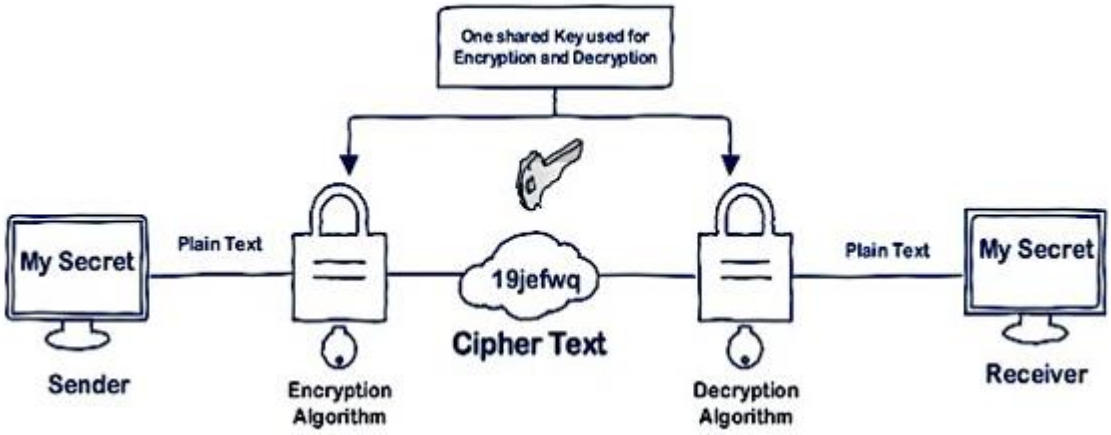

Рисунок 1.3 – Симетричне шифрування

DES [2], [3] є одним із основних симетричних алгоритмів блокового шифрування ключів, який приймає звичайні тексти як блоки, кожен з яких містить 64 біти, і перетворює зашифровані тексти, використовуючи ключі з 64 біт. З цих 64 бітів 8 бітів ключа використовуються для непарної парності, яка не враховуватиметься в довжині ключа. Тому існує 256 можливих способів знайти правильний ключ. Алгоритм DES виконує дві перестановки (початкову та кінцеву) і 16 кроків обробки, кожен з яких називається раундом, і для кожного раунду використовується окремий ключ.

DES базується на двох криптографічних операціях: підстановці та транспозиції. У кожному раунді DES виконуються деякі заміни та транспозиції. Перед початком першого раунду до звичайного тексту застосовується початкова перестановка. Наприклад, початкова перестановка замінює перший біт звичайного тексту на 58-й біт, а другий — на 50-й біт і так далі. Отриманий переставлений блок ділиться на дві половини, обидві мають 32 біти, і кожна з них проходить через 16 раундів процесів шифрування. Остаточна перестановка застосовується до комбінованого блоку, щоб отримати зашифрований текст. Повідомлялося, що DES є вразливим, тому його було замінено на 3DES [4]. Загальна робота DES пояснюється на рис. 1.4 [2], [3]. Існує три режими роботи DES. Це ECB, CBC і CFB.

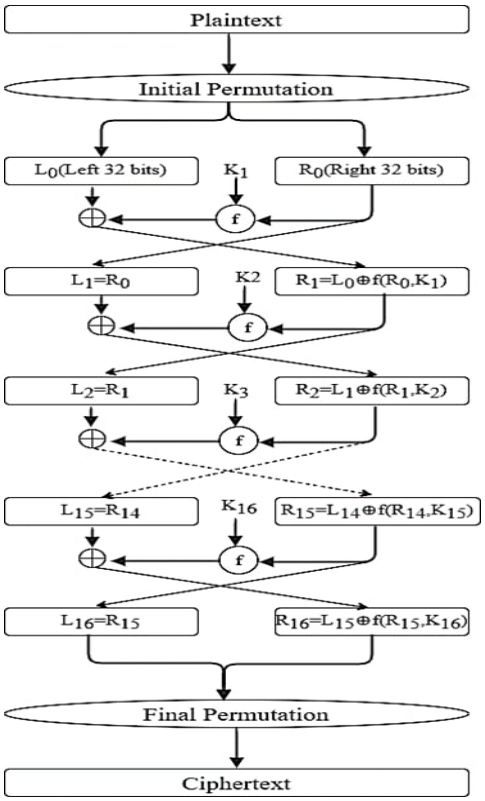

Рисунок 1.4 – Процес алгоритму DES

Advanced Encryption Standard (AES) [2], [5] – це алгоритм блокового шифрування, який прийшов на заміну DES і Triple DES. Він шифрує та розшифровує 128-бітний блок даних. Залежно від вибору розміру ключа, 128 біт, 196 біт або 256 біт, AES може приймати 10, 12 або 14 циклів шифрування. Кожен раунд складається з чотирьох операцій: замінити байти, клавіші shift, змішати стовпець і додати раундовий ключ. Однак операція змішування колонки не виконується в останньому циклі. У кожному раунді шифрування використовуються окремі раундові ключі, згенеровані з заданого ключа шифру. Дані, що підлягають шифруванню, розбиваються на блоки. Кожен блок представлений як масив даних, який відомий як масив стану. AES не є вразливим, як DES, і також відомо, що забезпечує хороший рівень безпеки [4]. Процес шифрування AES показано на рис. 1.5 [2], [5].

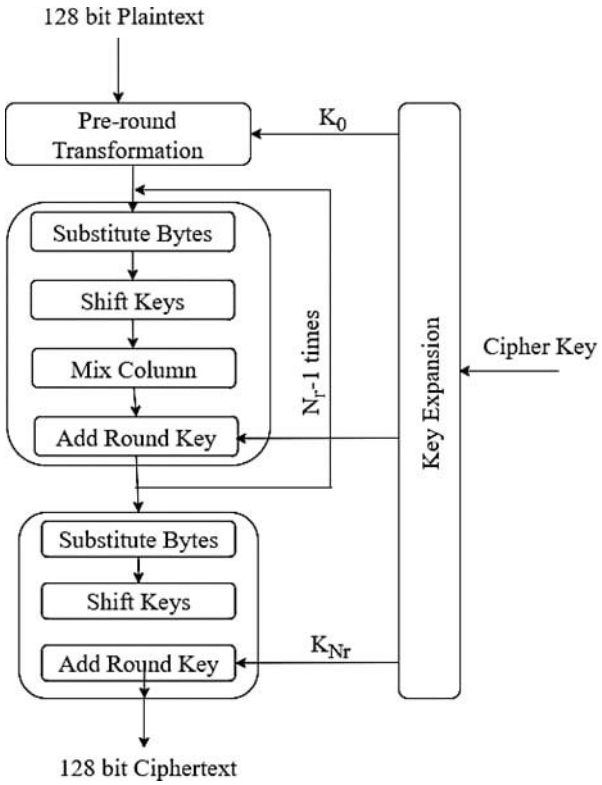

Рисунок 1.5 – Процес шифрування AES

1.1.2 Асиметричне шифрування

Криптографічні системи з асиметричним ключем вимагають двох ключів, один зберігається в секреті, а інший є відкритим. Шифрування здійснюється за допомогою відкритого ключа, тоді як секретний ключ використовується для розшифровки зашифрованого тексту. Обидва ці ключі математично пов’язані. Хоча асиметричні системи забезпечують вищий рівень безпеки, вони можуть не підходити для документів великого розміру. Це пояснюється тим, що швидкість низька порівняно з симетричними системами на основі ключів, і вони також реєструють більш високий рівень використання ЦП. Рис. 1.6 ілюструє процес асиметричного шифрування.

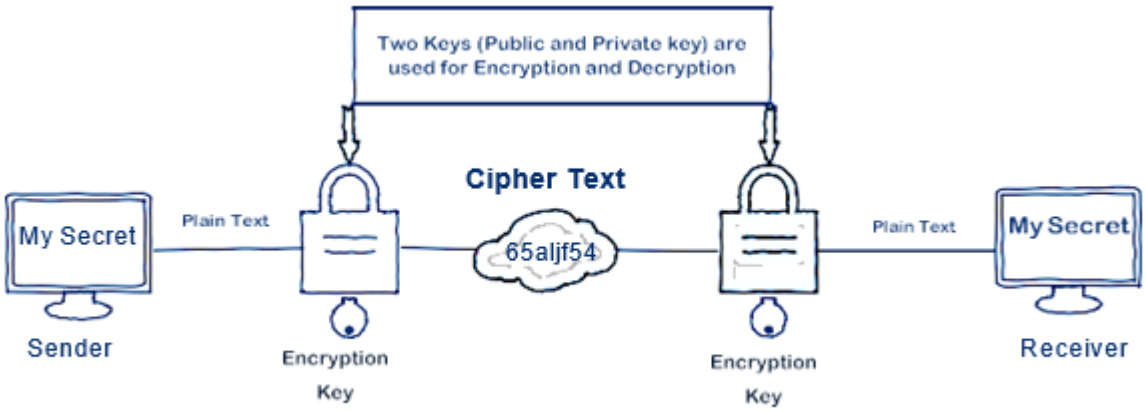

Рисунок 1.6 – Асиметричне шифрування

Прикладами криптосистем з відкритим ключем є Elgamal (автор Тахір Ельгамаль), RSA (автори: Рон Рівест, Аді Шамір і Леонардо Адлман), Diffie-Hellman і DSA, Digital Signature Algorithm (автор Девід Кравіц).

Проблема керування ключами вирішується за допомогою криптографії з відкритим або асиметричним ключем, концепції, запропонованої Вітфілдом Діффі та Мартіном Хеллманом у 1975 році. Шифрування з відкритим ключем – це асиметрична схема, у якій використовується пара ключів: відкритий ключ для шифрування даних і відповідний закритий ключ для розшифровки даних. На відміну від приватних ключів, відкриті ключі поширюються вільно. З його допомогою будь-який агент може зашифрувати інформацію, яка може бути розшифрована тільки за допомогою закритого ключа.

Хоча пара ключів математично пов’язана, розрахувати приватний ключ за допомогою відкритого ключа майже неможливо. Поява шифрування з відкритим ключем є технологічною революцією, яка дозволяє широко застосовувати потужні технології шифрування. Розглянемо коротко основний алгоритм асиметричного шифрування.

RSA — криптографічна система з відкритим ключем. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних додатків.

RSA був опублікований у 1977 році Рональдом Лінном Рівестом, Аді Шаміром і Леонардом Адлеманом у Массачусетському технологічному інституті (MIT).

Безпека алгоритму RSA базується на принципі факторизації складності. Алгоритм використовує два ключі - відкритий і закритий. Схема роботи шифру представлена на рис. 1.7:

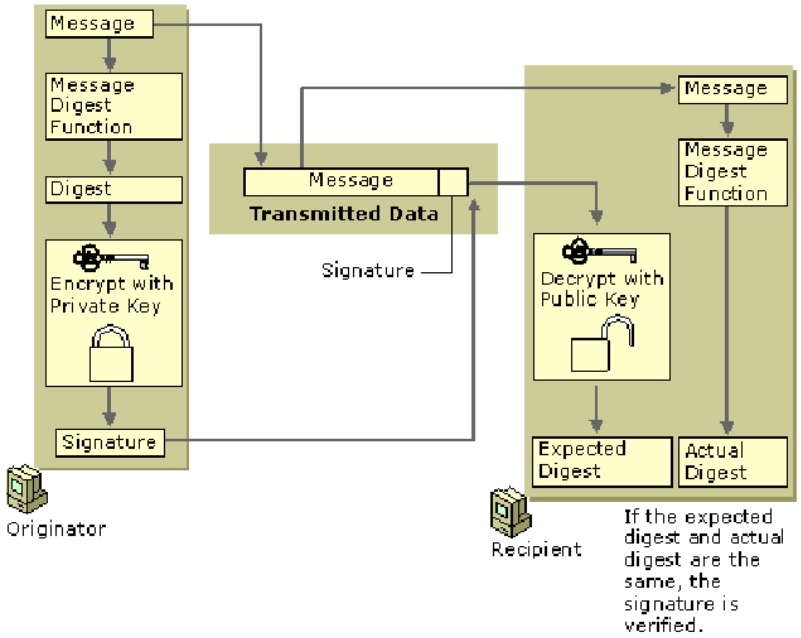

Рисунок 1.7 – Схема роботи шифру RSA

1.1.3 Хешування

Третій тип криптографічних алгоритмів хешування. У хешуванні вхідне повідомлення відображається в компактний бітовий рядок фіксованого розміру, який називається хеш. Хеш-функції — це односторонні функції, які є математичними алгоритмами, які відображають вхідне повідомлення довільного розміру в хеш фіксованого розміру або дайджест повідомлення. На рис. 1.8 представлена загальна концепція хеш-функції. Хеш-функції в основному використовуються для зберігання паролів і перевірки цілісності даних.

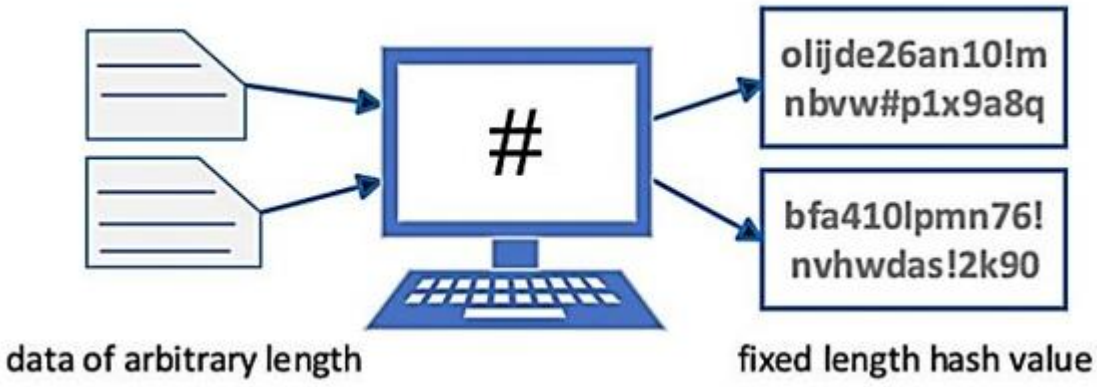

Рисунок 1.8 – Хеш-функція загальне поняття

Хеш-функції використовуються в технології блокчейн, де хеш є гарантією цілісності ланцюжка транзакції (платежів) і захищає її від несанкціонованих змін. Завдяки хешу і розподіленим обчислюванням зламати блокчейн дуже складно, на основі блокчейну існує багато криптовалют. Сама популярна — біткоїн — існує з 2009 року, і до цього часу її не було зламано.

Популярні алгоритми хешування:

– CRC32 – використовується для створення контрольних сум. Ця функція не є криптографічною. Існує кілька варіацій цього алгоритму, і число після «CRC» вказує на довжину отриманого хешу в бітах. Функція дуже проста і не вимагає ресурсів. Він використовується для перевірки цілісності пакетів даних у різних протоколах передачі даних.

– MD5 є старовинною, але все ще дуже популярною версією алгоритму шифрування, який створює 128-бітове хеш-значення. Хоча ця функція зараз не дуже стабільна, вона все ще часто використовується для шифрування паролів.

– SHA-1 — це криптографічна функція. Повертає 160-байтове хеш-значення. Зараз відбувається активний перехід на SHA-2, більш стабільну хеш-функцію.

1.2 Технічний захист інформації

В умовах сучасного динамічного розвитку суспільства, постійної модернізації технічної та соціальної інфраструктури інформація постає стратегічним об'єктом забезпечення дієвого обміну між усіма ланками сучасного світу. Інноваційні інформаційні технології, які дають змогу створювати, зберігати, передавати інформацію та забезпечувати ефективний захист, стали важливим фактором життя суспільства сьогодення й засобом підвищення ефективності управління всіма сферами суспільної діяльності. При цьому постає беззаперечна умова формування дієвого механізму захисту як персональної, конфіденційної, загальної, так і секретної інформації, що циркулює в умовах інформаційного простору. Сучасна інформаційна безпека вимагає постійного вдосконалення системи відповідно до збільшення ризику витоку інформації. Цей процес є безперервним і полягає в реалізації сучасних методів і способів поліпшення системи захисту інформації, постійного моніторингу, виявлення його слабких місць і потенційних каналів витоку інформації, постійному вдосконаленні систем за рахунок появи нових способів доступу до інформації ззовні. Роль інформаційної безпеки в організаційній системі заходів безпеки визначається своєчасністю й точністю управлінських рішень керівництва з урахуванням наявних ресурсів, прийомів і методів забезпечення інформаційної безпеки, а також на підставі чинних нормативно-методичних документів [6].

Технічні засоби захисту базуються на фізичних, апаратних і програмних засобах захисту. Організаційно технічні заходи передбачають блокування можливих каналів витоку інформації. Дієвий технічний захист інформаційного простору сьогодення характеризується такими методами:

– структуризація інформації за ступенем конфіденційності й забезпечення криптографічного захисту кожного ступеня при передачі інформації;

– розподіл інформаційних потоків з урахуванням відстані передачі інформації за напрям-ками трасування (локальна мережа, канали передачі повідомлень тощо);

– формування журналів атак із застосуванням сучасних механізмів обліку в разі спроб доступу сторонніх об’єктів в інформаційній системі та друкованих документах;

– забезпечення цілісності програмного забезпечення й інформації;

– застосування інноваційних засобів відновлення інформаційної безпеки на всіх рівнях впливу;

– обслуговування обладнання, систем і магнітних носіїв, формування ефективного фізичного захисту;

– створення, підтримка й удосконалення спеціальних служб захисту інформації.

В українському державному стандарті ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) [7] інформаційна безпека відноситься до стану системи, яка гарантує конфіденційність, доступність і цілісність інформації та забезпечує її автентичність, достовірність, надійність, не від-мову й відповідальність.

Основною властивістю забезпечення конфіденційності повідомлень є конфіденційність інформації, це дає змогу абстрагуватися від інших властивостей. Властивість конфіденційності інформації досягається за допомогою механізмів шифрування за допомогою ключа, що перетворює інформацію в нечитабельну форму для неавторизованих користувачів. З метою захисту конфіденційної інформації, що передається по відкритих каналах зв’язку, використовуються системи шифрування відкритого ключа, в яких відкритий ключ використовується для шифрування інформації, а секретний ключ – для її дешифрування. Принцип роботи таких систем заснований на обчислювальній складності зворотного перетворення інформації без використання секретного ключа.

1.2.1 Канали витоку інформації

Канали витоку інформації — це шляхи або методи, через які конфіденційні дані можуть бути ненавмисно або умисно розкриті неуповноваженим особам або організаціям. Розуміння та ідентифікація потенційних каналів витоку інформації є ключовим аспектом захисту даних у будь-якій організації.

Канали витоку інформації становлять серйозну загрозу для конфіденційності та безпеки даних в сучасному цифровому світі. Особливо це стосується електронної пошти та інших форм Інтернет-комунікації, які стали основними інструментами обміну інформацією. Нешифровані електронні листи та незахищені канали комунікації в соціальних мережах та месенджерах можуть легко стати мішенями для перехоплення. Це вимагає від організацій впровадження шифрування даних та використання захищених каналів комунікації для забезпечення конфіденційності передачі інформації.

Мобільні пристрої та застосунки створюють додаткові ризики для безпеки даних. Втрата або крадіжка смартфонів, ноутбуків та інших портативних пристроїв може призвести до неконтрольованого витоку конфіденційної інформації. Небезпечні застосунки, завантажені з неперевірених джерел, можуть містити шкідливе програмне забезпечення, що здатне красти або видаляти важливі дані. Тому критично важливо забезпечувати фізичну безпеку мобільних пристроїв та уважно ставитися до встановлення нових застосунків.

Зовнішні носії інформації, такі як флеш-накопичувачі та зовнішні жорсткі диски, також є потенційними джерелами витоку інформації. Їх втрата або несанкціонований доступ може призвести до неконтрольованого розповсюдження конфіденційних даних. Використання шифрування для зовнішніх носіїв є ефективним заходом для зниження ризику витоку інформації.

Хмарні сервіси та зберігання даних створюють додаткові виклики для захисту інформації. Незахищені хмарні сховища можуть стати легкою мішенню для хакерів, що шукають доступ до конфіденційної інформації. Належне шифрування даних та використання надійних хмарних платформ із суворими

політиками безпеки є необхідними для забезпечення безпеки інформації, збереженої в хмарі.

Не менш важливим є захист від внутрішніх загроз, таких як недбалість або зловмисні дії співробітників. Навчання персоналу основам кібербезпеки та впровадження строгих політик контролю доступу до інформації можуть значно знизити ризик внутрішніх витоків. Комплексний підхід до захисту інформації, що включає технічні, організаційні та фізичні заходи безпеки, є ключем до ефективного захисту даних від потенційних каналів витоку.

1.2.2 Несанкціонований доступ

Несанкціонований доступ є серйозною загрозою для інформаційної безпеки, оскільки зловмисники намагаються отримати доступ до систем, даних або ресурсів без належного дозволу. Ця проблема стосується як індивідуальних користувачів, так і організацій, ставлячи під загрозу конфіденційність, цілісність та доступність важливої інформації. Несанкціонований доступ може призвести до крадіжки конфіденційних даних, фінансових втрат, пошкодження репутації компанії та інших негативних наслідків.

Методи отримання несанкціонованого доступу дуже різноманітні. Зловмисники можуть використовувати слабкі або очевидні паролі, які легко вгадати або викрасти. Фішинг є іншим поширеним методом, який включає обман користувачів для отримання їх логінів і паролів через підроблені електронні листи або веб-сайти. Експлойти та вразливості в програмному забезпеченні також відкривають двері для несанкціонованого доступу, дозволяючи зловмисникам проникнути в системи через недоліки безпеки. Соціальна інженерія, яка включає маніпулювання людьми для отримання доступу або конфіденційної інформації, є ще одним ефективним інструментом у руках зловмисників.

Захист від несанкціонованого доступу вимагає комплексного підходу. Важливо використовувати складні паролі та регулярно їх змінювати, а також обмежувати доступ до систем на основі принципу найменших привілеїв.

Багатофакторна аутентифікація додає додатковий рівень захисту, ускладнюючи несанкціонований доступ. Регулярні оновлення програмного забезпечення є критично важливими для захисту від відомих вразливостей та експлойтів. Шифрування даних забезпечує, що навіть у разі витоку або крадіжки, інформація залишиться недоступною для несанкціонованого використання.

Навчання персоналу грає ключову роль у запобіганні несанкціонованому доступу. Освітні програми можуть підвищити обізнаність співробітників про кіберзагрози, вчить основам кібергігієни та ефективним методам протидії соціальній інженерії та фішингу. Впровадження цих заходів дозволяє створити багаторівневу систему захисту, яка значно знижує ризик несанкціонованого доступу та забезпечує надійний захист важливих інформаційних активів.

1.1.3 Загальна характеристика системи електронного документообігу

Паперовий документообіг був основною формою обробки, зберігання та передачі інформації в бізнесі та урядових структурах протягом багатьох років. Цей традиційний метод володіє певними перевагами, такими як фізична наочність та можливість легкого доступу без необхідності використання спеціального обладнання. Однак, незважаючи на ці переваги, паперовий документообіг має численні недоліки, що обмежують його ефективність у сучасному цифровому світі.

Недоліки паперового документообігу:

– Висока вартість: Паперовий документообіг вимагає значних витрат на друк, копіювання, поштові послуги та зберігання документів, що в сукупності створює значні витрати для організацій.

– Низька швидкість обробки: Процеси затвердження та обміну документами можуть тривати дні або навіть тижні, що значно знижує оперативність вирішення бізнес-завдань.

– Ризик втрати або пошкодження: Паперові документи схильні до втрати, крадіжки або пошкодження внаслідок природних катастроф, що може призвести до безповоротної втрати важливої інформації.

– Виклики з архівуванням та пошуком: Управління великою кількістю паперових документів вимагає значних зусиль та часу для архівування та пошуку необхідних документів.

– Екологічний вплив: Великий обсяг використання паперу негативно впливає на довкілля, сприяючи вирубці лісів та забрудненню навколишнього середовища.

У відповідь на ці виклики, багато організацій активно переходять до електронного документообігу, який дозволяє автоматизувати багато процесів, пов'язаних з обробкою документів, забезпечує швидкий доступ до інформації, підвищує ефективність робочих процесів та зменшує екологічний вплив. Електронний документообіг значно знижує витрати на документообіг, підвищує швидкість обробки інформації та забезпечує високий рівень безпеки даних.

Запорукою успішного виконання роботи органів влади завжди є ефективна діяльність державних службовців і посадових осіб органів місцевого самоврядування. Проте традиційні методи обробки інформації дедалі менш ефективні для задоволення потреб громадян. Необхідно впровадити нову систему документообігу на основі електронного документообігу. Однак таку систему ще належить запровадити на практиці. Тому для вдосконалення процесу запровадження електронного документообігу в органах місцевого самоврядування України важливо розуміти, які саме системи електронного документообігу використовують українські органи місцевого самоврядування, та визначити їх основні проблеми.

Нині в Україні визначається Законами України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис», прийняті 22 травня 2003 року (набули чинності 1 січня 2004 року), а також низкою підзаконних нормативно-правових актів, прийнятих до їх виконання [9]. Цими актами, зокрема, встановлюються основні організаційно-правові засади

електронного документообігу, використання електронних документів, визначається правовий статус електронного цифрового підпису та регулюються відносини, що виникають при використанні електронного цифрового підпису. Мета законів полягає у наданні електронним документам юридичної сили, рівної паперовим. При цьому електронний цифровий підпис є тим інструментом, що дає змогу створити правові основи для електронного документообігу (у тому числі в мережі Інтернет), здійснювати різні трансакції тощо.

Для зрозуміння систем електронного документообігу необхідно оперувати такими поняттями, як електронний документообіг (ЕДО) та електронний документ (ЕД). Отже, електронний документообіг (ЕДО) – це єдиний механізм по роботі з документами, представленими в електронному вигляді, з реалізацією концепції «безпаперового діловодства». У свою чергу, електронний документ (ЕД) – це документ, створений за допомогою засобів комп'ютерної обробки інформації, підписаний електронним цифровим підписом (ЕЦП) і збережений на машинному носії у вигляді файлу відповідного формату [8].

Кожна система електронного документообігу працює за такими принципами [8]:

– однократна реєстрація документа, що дає змогу однозначно ідентифікувати документ у будь-якій інсталяції даної системи;

– можливість паралельного виконання операцій, що дає змогу скоротити час руху документів і підвищення оперативності їх виконання;

– безперервність руху документа, що дає змогу ідентифікувати відповідального за виконання документа (завдання) в кожен момент часу життя документа (процесу);

– єдина (або погоджено розподілена) база документної інформації, що дає змогу унеможливити дублювання документів;

– ефективно організована система пошуку документа, що дає змогу знаходити документ, володіючи мінімальною інформацією про нього;

– розвинена система звітності по різних статусах і атрибутах документів, що дає змогу контролювати рух документів по процесах документообігу і приймати управлінські рішення, ґрунтуючись на даних із звітів.

Особливий інтерес представляє використання технології блокчейн у системах електронного документообігу. Блокчейн дозволяє забезпечити незмінність та прозорість документообігу, а також автоматизувати виконання контрактів і затверджень без необхідності втручання третіх сторін. Застосування блокчейну може радикально покращити безпеку та ефективність обробки документів, забезпечуючи надійний захист від підробок та несанкціонованого доступу. Таким чином, інтеграція блокчейн технології в електронний документообіг відкриває нові можливості для створення максимально захищених, прозорих та ефективних систем управління документацією.

1.3 Проблеми безпеки в електронному документообігу

1.3.1 Конфіденційність ізоляції даних

Конфіденційність поділу даних є важливим аспектом електронного документообігу. У мережах документообігу, де передається і зберігається конфіденційна інформація, конфіденційність при поділі даних означає забезпечення відповідного поділу для кожного типу даних і рівня конфіденційності.

На першому рівні система повинна впроваджувати механізми контролю доступу, щоб гарантувати, що лише авторизовані користувачі можуть отримати доступ до конфіденційних даних. Це включає використання різних рівнів автентифікації, таких як паролі, двофакторна автентифікація та біометрія.

На другому рівні, де зберігаються дані, важливо використовувати механізми шифрування, щоб захистити конфіденційність даних, навіть якщо зловмисник отримає несанкціонований доступ до системи. Ефективне шифрування може бути використане для того, щоб гарантувати, що дані залишаться нечитабельними і

непридатними для використання, навіть якщо вони потраплять до рук зловмисника.

На третьому рівні передача даних через мережу також повинна бути захищена. Використання шифрування і протоколів безпеки, таких як SSL/TLS, гарантує, що дані, які передаються між користувачами і серверами, залишаються конфіденційними і не можуть бути перехоплені або прочитані несанкціонованими третіми особами.

1.3.2 Цілісність даних

Цілісність даних є одним з найважливіших аспектів інформаційної безпеки в будь-якій системі, включаючи електронний документообіг. Цілісність даних визначається як здатність інформації залишатися незмінною та неушкодженою протягом усього її життєвого циклу, від створення до знищення. Іншими словами, дані повинні залишатися недоторканими і незмінними, а будь-які зміни, внесені до них, повинні бути точно виявлені і відстежені.

У контексті електронного документообігу цілісність даних гарантує, що ніхто не може змінити документ або інформацію, і що вони залишаються недоторканими, якщо на це немає дозволу або схвалення. Це особливо важливо в сферах, де точність і цілісність даних є критично важливими, таких як фінанси, медицина і право.

Для гарантування цілісності даних використовуються різні методи, зокрема криптографічні хеш-функції, цифрові підписи та контрольні суми. Ці методи дозволяють перевірити, чи були дані змінені після їх створення або попереднього перегляду. Такі технології допомагають захистити цілісність електронних документів і забезпечити дотримання вимог законодавства щодо зберігання та захисту інформації.

1.3.3 Аутентифікація та авторизація

Аутентифікація та авторизація є важливими аспектами забезпечення безпеки в електронному документообігу. Процеси автентифікації підтверджують особу користувача та його право на доступ до системи. Для цього можуть використовуватися паролі, біометричні сканери, токени або інші методи ідентифікації. Авторизація визначає, які дії або ресурси користувач може виконувати після успішної автентифікації. Цей процес базується на правах доступу, наданих конкретному користувачеві або групі користувачів. Наприклад, після успішної авторизації адміністратор може мати права на редагування та видалення документів, тоді як звичайний користувач може мати права доступу, обмежені лише переглядом. Ефективна реалізація цих процесів може забезпечити безпеку електронного документообігу та запобігти несанкціонованому доступу і маніпуляціям з даними.

Висновки до розділу 1

Розглянуто методи криптографічного захисту інформації, такі як асиметрична криптографія та цифровий підпис. Описано технічний захист інформації, включаючи заходи на рівні програмного та апаратного забезпечення, такі як захист мережі, контроль доступу та механізми автентифікації. Розглянуті проблеми безпеки в електронному документообігу, які включають ризики шахрайства та фальсифікації даних.

Впровадження систем електронного документообігу на основі блокчейну виявляється більш перспективним та ефективним рішенням порівняно з іншими методами захисту інформації. Це дозволяє забезпечити високий рівень безпеки, прозорості та ефективності у вирішенні завдань електронного документообігу.

РОЗДІЛ 2. СУТЬ, МЕТОДИ ТА МОДЕЛІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

2.1 Загальна характеристика блокчейн

На сьогоднішній день, блокчейн займає ключове місце в професійному середовищі, ставши одним із найсуттєвіших технологічних проривів та інновацій. Ця технологія, заснована на принципах розподіленого реєстру, забезпечує можливість фіксації транзакцій та інших операцій у послідовність блоків без необхідності залучення посередника. З технічної точки зору, транзакції групуються у блоки, де кожен блок може містити численні транзакції і служить фундаментальною одиницею для верифікації даних учасниками мережі. Кожен блок також містить хеш-значення заголовка попереднього блоку, і таким чином утворює хеш-ланцюжок або блокчейн рис. 2.1. Оскільки всі блоки є ланцюжком, порядок блоків є детермінованим; отже, кожен блок може служити міткою часу вкладених транзакцій для вирішення проблеми подвійних витрат [11]. Кожен учасник підтримує копію всього блокчейну, тому кожен учасник може перевірити кожну транзакцію [12, 13].

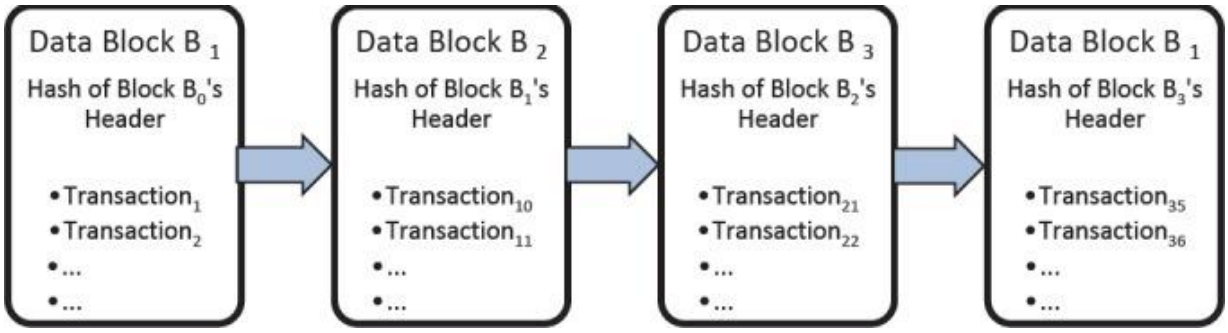

Рисунок 2.1 – Як блоки даних утворюють блокчейн

Виходячи з того, як ідентифікаційні дані визначені в мережі, можна розрізнити блокчейн-системи з дозволами та без дозволів. У блокчейні без дозволу учасники залишаються анонімними або використовують псевдоніми, і

кожен учасник може додавати нові блоки до ланцюжка. У дозволеному блокчейні ідентифікація кожного члена контролюється, а також його право перевіряти новий блок [14, 15]. У першому випадку транзакції перевіряються за допомогою підтвердження роботи (PoW), а в другому транзакції перевіряються за допомогою підтвердження частки (PoS) рис. 2.2.

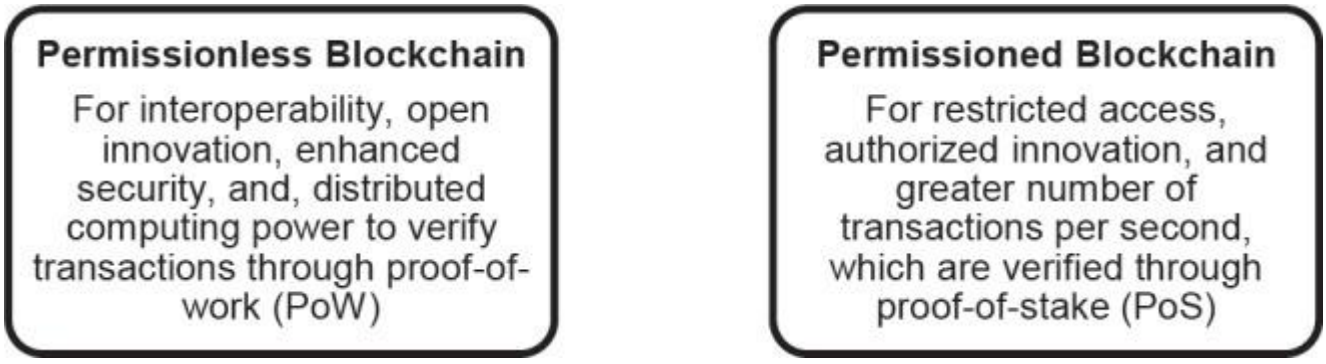

Рисунок 2.2 – Дозволене та бездозволене використання блокчейну

У статті Harvard Business Review [10] Янасіті та Лахані пояснюють, як технологія блокчейн працює на практиці; підкреслюючи п'ять основних принципів табл. 2.1.

Таблиця 2.1 – Як працює блокчейн [10]

№	Принцип блокчейна	Подробиці
1	Розподілена база даних	Кожен учасник блокчейну має доступ до всієї книги та її повної історії. Жоден член не може контролювати дані, у той час як кожен має можливість перевіряти транзакції безпосередньо, без посередників.
2	Одноранговa передача	Спілкування відбувається безпосередньо між членами без необхідності центрального органу (без посередників).

Продовж. табл. 2.1 – Як працює блокчейн [10]

3	Прозорість із псевдонімом	Кожна транзакція доступна для всіх, хто має доступ до блокчейну. Кожен користувач у блокчейні має унікальну буквено-цифрову адресу із 30 символів, яка його ідентифікує. Користувачі можуть залишитися анонімними або надати іншим докази своєї особи.
4	Незворотність записів	Після введення транзакції записи не можна змінити. Кожен блок містить хеш-значення заголовка попереднього блоку (звідси термін «ланцюжок»).
5	Обчислювальна логіка Блокчейн-транзакції можна прив’язати до обчислювальної логіки та, по суті, програмувати.	Блокчейн-транзакції можна прив’язати до обчислювальної логіки та, по суті, програмувати.

2.2 Особливості та переваги блокчейн

2.2.1 Архітектура технології блокчейн

Блокчейн складається з ланцюга блоків, які функціонують як розподілена, відмовостійка та спільна база даних. У цій структурі, записи зберігаються у вигляді блоків, які є взаємопов'язаними та хронологічно впорядкованими, забезпечуючи надійне зберігання даних. Кожен учасник мережі має доступ до всієї послідовності блоків, але блоки захищені від видалення або модифікації, що забезпечує цілісність і незмінність інформації.

У серці кожного блоку лежить набір транзакцій, які були попередньо перевірені. Блок містить унікальне хеш-значення, що забезпечує зв'язок з попереднім блоком у ланцюгу, створюючи безперервну послідовність. Генезисний блок, який є першим у ланцюгу, унікальний тим, що його хеш-значення встановлене в нуль, оскільки він не має попередника.

Кожен блок містить дві основні частини: заголовок та тіло. Заголовок включає метадані, такі як версію блоку, хеш попереднього блоку, хеш кореня дерева Меркла (структури даних, яка забезпечує ефективну перевірку та валідацію транзакцій), часову мітку та довільне число, яке використовується одноразово для криптографічних обчислень рис. 2.3. Тіло блоку, зі свого боку, містить дані або записи транзакцій, кожна з яких підписана учасниками для забезпечення автентичності рис. 2.4.

Така структура блокчейна не лише сприяє безпеці та прозорості транзакцій, але й уможливлює створення надійної системи, в якій дані захищені від несанкціонованих змін та втручань.

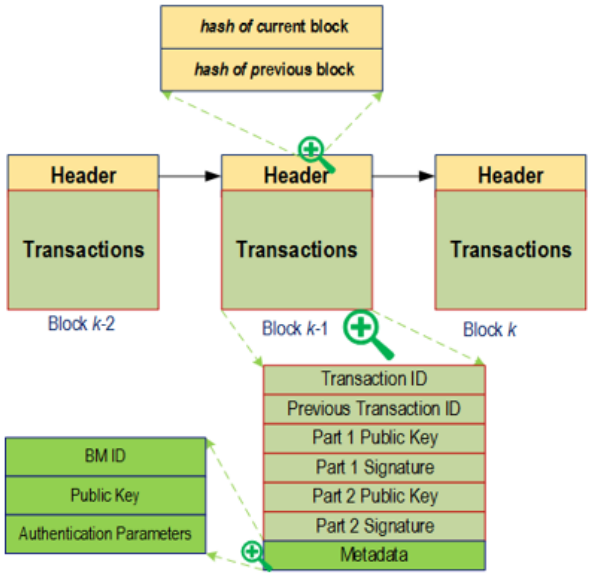

Рисунок 2.3 – Блоки в технології Blockchain

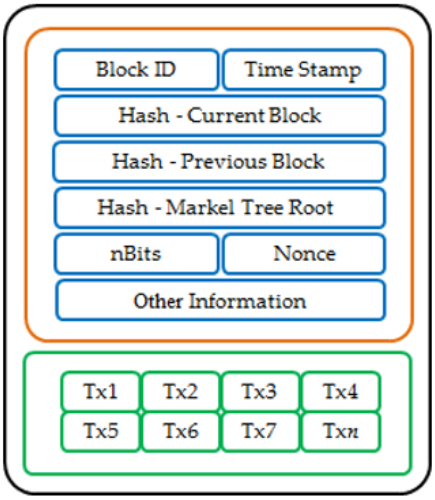

Рисунок 2.4 – Структура блоку

Незмінність технології блокчейн, безсумнівно, є однією з її найпривабливіших рис. Це стосується неможливості змінити або змінити інформацію. Технологія блокчейн найбільш відома здатністю забезпечувати постійну, незмінну мережу, це одна з її головних особливостей. Блокчейн незмінний, а це означає, що дані ніколи не можуть бути змінені. Крім того, усі мережеві вузли повинні затвердити дані, перш ніж вони будуть додані до блоку, що забезпечує безпечні транзакції. Майнінг – це процес додавання транзакцій до блоків шляхом їх перевірки.

Децентралізація стосується того факту, що немає нікого, хто відповідає за структуру чи будь-який керівний орган. Децентралізовані мережі обслуговуються групою вузлів. Це одна з ключових характеристик технології блокчейн. Традиційна централізована система транзакцій вимагає, щоб кожну транзакцію перевіряло центральне агентство, що, природно, спричиняє вузькі місця продуктивності та витрат рис. 2.5. Блокчейн усуває потребу в сторонніх розробниках на відміну від централізованого режиму. Узгодженість даних підтримується в розподілених мережах алгоритмами консенсусу. Децентралізована і відкрита книга, блокчейн — це і те, і інше. У відкритій книзі транзакції реєструються, і вони відкриті для всіх, тому книга є публічною.

Транзакції не контролюються жодною особою чи організацією. Існує одна копія книги для кожного з’єднання в мережі блокчейн.

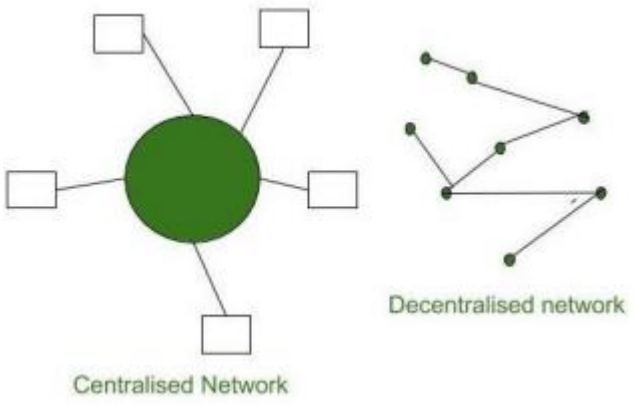

Рисунок 2.5 – Централізована та децентралізована мережа

Транзакції у блокчейні перевіряються швидко, і чесні майнери не допускають до мережі недійсних транзакцій. Однією з ключових особливостей блокчейна є те, що після включення транзакцій до блокчейну, вони стають незмінними та не можуть бути видалені або відкочені назад. Це забезпечує непорушність даних і дозволяє негайно виявляти будь-які нерегулярні транзакції. Структура блокчейну дозволяє перевіряти будь-яку транзакцію чи блок, роблячи збережені в ньому дані постійними та легкими для відстеження. Кожна транзакція в блокчейні біткойна реєструється в єдиній книзі, яка є доступною на всіх вузлах мережі, забезпечуючи повний слід кожної монети та вирішуючи проблему подвійних витрат.

У блокчейн-транзакціях зазвичай потрібен лише ідентифікатор одержувача, а додаткова інформація не розголошується, що забезпечує сторонам анонімність. Користувачі мають унікальну згенеровану адресу для взаємодії з блокчейном, що дозволяє їхній справжній особистості залишатися невідомою. Однак, через властиві обмеження блокчейну, абсолютне збереження конфіденційності не гарантується.

За моделлю невитрачених транзакцій (UTXO), створеною блокчейном Bitcoin, кожна транзакція повинна посилатися на попередню невитрачену транзакцію. Це дозволяє змінювати статус транзакцій з невитраченого на витрачений, коли транзакція фіксується в блокчейні, що сприяє виявленню та відстеженню шахрайства. Дані в блокчейні легко відстежуються та перевіряються, оскільки кожна транзакція перевіряється та забезпечується міткою часу. Всі учасники мережі мають доступ до цього запису та можуть використовувати спеціалізовані алгоритми для забезпечення цілісності і послідовності інформації у ланцюгу блоків.

2.3 Огляд сучасних систем електронного документообігу

Управління електронними документами охоплює складний набір операцій, включаючи створення, обробку, відправку, передачу, отримання, зберігання, використання та видалення електронних документів. Ці процеси доповнюються застосуванням перевірки цілісності та, за необхідності, підтвердженням отримання документа. Цей сучасний, орієнтований на технології підхід помітно підвищує операційну ефективність різноманітних організацій, починаючи від підприємств і організацій до урядових і місцевих адміністративних органів.

Вміле керування електронними документами відіграє ключову роль у підвищенні адміністративної ефективності підприємств і організацій. Це передбачає ретельне та своєчасне формування електронних документів, ретельний нагляд за їх виконанням, стратегічну організацію їх збереження, пошуку та застосування. Необхідність ефективного нагляду за електронними документами прискорила розробку спеціальних систем керування електронними документами.

Розвиток зв'язків з громадськістю в Україні зумовлює необхідність всебічного вдосконалення та постійного оновлення її науково-технічної та правової інфраструктури. Ця розробка передбачає розробку спеціалізованих правових стандартів і правил для регулювання сфери інформаційних і

документальних взаємодій. З цією метою законодавчий орган України, Верховна Рада, ініціативно прийняв кілька основних законів, зокрема:

- «Про електронні документи та електронний документообіг»;
- «Про електронний цифровий підпис»;
- «Про Національну програму інформатизації»;
- «Про телекомунікації»;
- "Про національну систему конфіденційного зв'язку";
- «Про захист інформації в інформаційно-телекомунікаційних системах».

Ці законодавчі акти встановлюють основні організаційно-правові положення, що регулюють обіг та використання електронних документів. Як наслідок, законодавча база не тільки підтримує, але й сприяє широкому впровадженню електронного документообігу на українських підприємствах, знаменуючи значний крок до модернізації та підвищення ефективності в державному та приватному секторах.

Система керування електронними документами (СЕД) являє собою складну суміш організаційних і технологічних структур, призначених для полегшення створення, контролю доступу та розповсюдження електронних документів у комп’ютерних мережах. Він ретельно контролює документообіг в організації, забезпечуючи безперебійну роботу.

Ключова перевага СЕД полягає в їхній здатності виконувати завдання керування документами з неперевершеною точністю та ефективністю, вміло обробляючи значні обсяги документів. Підтримувані формати файлів охоплюють різноманітний спектр, охоплюючи текстові документи, зображення, електронні таблиці, а також аудіо-, відео- та веб-документи.

Суть СЕД полягає в тому, щоб оптимізувати збереження електронних документів, підвищуючи простоту взаємодії з цими документами — чи то за допомогою пошуку на основі атрибутів, чи на основі вмісту. СЕД розроблено для автономного моніторингу змін документів, дотримання термінів, траєкторій документів і всіх версій документів.

Цілісний СЕД охоплює весь спектр бізнес-адміністрування в межах підприємства чи організації. Це охоплює від початкового завдання створення документа до його остаточного архівування, гарантуючи централізоване збереження документів у будь-якому можливому форматі, включаючи багатогранні складені документи. Крім того, СЕД призначені для об'єднання документообігу територіально розосереджених підприємств в уніфіковану систему, пропонуючи тим самим адаптивне керування документами. Ця адаптивність досягається завдяки точному розмежуванню шляхів руху документів і забезпеченню гнучкості маршрутизації документів.

У СЕД доступ до документів ретельно регулюється з чіткими розмежуваннями на основі ролей, компетенції та повноважень користувачів. Крім того, SED адаптовані до існуючої організаційної структури, методів ведення записів і бездоганної інтеграції з уже існуючими корпоративними системами.

Переважно, основні користувачі СЕД охоплюють великі державні установи, промислові підприємства, фінансові установи та будь-які організації, які мають справу з великим обсягом документів. Це підкреслює ключову роль СЕД в модернізації та оптимізації процесів управління документами в різних секторах.

Відповідно до основних принципів електронного документообігу він повинен функціонувати на таких засадах:

– єдиноразова реєстрація документа;

– можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання;

– безперервність руху документа;

– єдина база документальної інформації для централізованого зберігання документів і виключення можливості дублювання документів;

– ефективно організована система пошуку документа;

– розвинена система звітності за статусами і атрибутами документів, що дозволяє контролювати поетапний рух документів.

Як показали дослідження, переважна більшість вітчизняних підприємств автоматизують свій документообіг з використанням пакета програмного

забезпечення корпорації Microsoft, що пояснюється зручністю в експлуатації та широкими можливостями подальшого розвитку. Тому актуальним є огляд характеристик систем документообігу, що працюють на платформі Microsoft, визначення їх можливостей, технічних параметрів, вартості. Найцікавішими та поширеними СЕД на вітчизняному ринку є такі [16]:

– Система "Справа". Виробником даної системи є компанія "Електронні офісні системи". Система "Справа" призначена для автоматизації управлінської діяльності у вітчизняних міністерствах і відомствах, територіальних органах влади, на підприємствах різних сфер діяльності.

– DocsVision 2.0 "Архів-Діловодство". Виробником даної системи є компанія Digital Design. Система DocsVision 2.0 "Архів - Діловодство" являє собою закінчений додаток, призначений для створення архівів документів, автоматизації основних діловодних процедур і бізнес-процесів обробки документів в організації.

– "Кодекс: Документообіг". Компанією-виробником даної системи є ДП "Центр комп'ютерних розробок". Система "Кодекс: Документообіг" - це комплекс взаємозалежних систем діловодства, банків документів і корпоративних сервісів, що забезпечують автоматизоване розв' язання задач діловодства і документообігу в органах державної влади й інших організацій.

– "ГРАН-ДОК" для Microsoft Windows. Виробником даної системи є компанія Граніт-Центр. Система керування документами серії Documentum 4i дозволяє вирішувати широкий спектр задач автоматизації документообігу на підприємстві, пов'язаних з діяльністю різних підрозділів, а також автоматизувати типові бізнес-процеси.

– LanDocs. Виробником даної системи є компанія Ланіт. Система LanDocs призначена для комплексної автоматизації процесів діловодства і ведення архіву електронних документів.

– Lotus Notes. Виробником даної системи є компанія Lotus. Система Lotus Notes забезпечує розроблення і розміщення прикладних програм групового

забезпечення, дозволяє користувачам одержувати, відслідковувати, спільно використовувати і створювати інформацію для обробки документів.

– OPTiMA-WorkFlow. Виробником даної системи є компанія OPTiMA. Система OPTiMA-WorkFlow призначена для керування процесами створення, обробки, тиражування і збереження документів, а також для автоматизації основних процедур сучасного діловодства й організації документообігу.

– Documentum 4i. Виробником даної системи є компанія Documentum (Дистриб'ютор – компанія Документум Сервісіз). "Гран-Док" - система автоматизації діловодства і документообігу в державних і муніципальних структурах управління.

– У судовій системі України використовується автоматизована система керування документообігом "Діловодство".

Незважаючи на різноманіття систем автоматизації документообігу і діловодства, існують загальні вимоги, яким повинні відповідати ці системи:

- зручність і простота в адмініструванні та користуванні;
- масштабовуваність – здатність підтримувати будь-яку кількість користувачів; можливість нарощувати свою потужність має визначатися тільки потужністю відповідного апаратного забезпечення;
- розподіленість – підтримання роботи з документами в територіально розподілених організаціях та взаємодія з віддаленими користувачами;
- модульність – система має складатися з окремих модулів, інтегрованих між собою, що дає можливість замовникові вибирати й упроваджувати компоненти згідно зі своїми потребами;
- відкритість – наявність у системі відкритих інтерфейсів для можливої доробки та інтеграції з іншими системами;
- універсальність – можливість використання на різних апаратних платформах у середовищі різного системного програмного забезпечення.

Важливість оцінки можливостей і особливостей різноманітних систем автоматизації документообігу була підкреслена ретельним дослідженням, проведеним Лабораторією інформаційних систем Московського фізико-

технічного інституту. Це дослідження мало на меті окреслити ландшафт ринку електронного документообігу, виміряти проникнення різних систем і зафіксувати настрої користувачів щодо цих технологій. У рамках амбітного заходу дослідження ретельно вивчало російські та західні системи електронного документообігу, охоплюючи десять різних платформ.

Щоб забезпечити ретельну оцінку, дослідницька група залучила 239 професіоналів із різних галузей, у тому числі кінцевих користувачів систем керування електронними документами, а також адміністраторів і технічних експертів. Цей широкий спектр перспектив допоміг створити точну картину поточної динаміки ринку.

Кульмінацією цього масштабного дослідження стала розробка складної математичної моделі. Ця модель послужила основою для обчислення загального рейтингу проаналізованих систем, пропонуючи цінну інформацію про їхні відносні позиції. Такий аналітичний підхід не лише висвітлює поточні уподобання та тенденції у сфері електронного документообігу, але також забезпечує орієнтир для майбутніх технологічних досягнень та очікувань користувачів.

2.4 Переваги та недоліки існуючих підходів до захисту

Прийняття блокчейну забезпечує безпрецедентний рівень прозорості та відстеження в електронному документообігу, де кожна транзакція або обмін документами реєструється в публічній книзі, доступній для всіх учасників. Це дозволяє з великою точністю перевіряти автентичність документів і відстежувати історію їх змін, значно зміцнюючи довіру між сторонами та спрощуючи процес аудиту за допомогою відповідності та підзвітності. Така технологія віщує нову еру ефективності та швидкості обробки документів, автоматизуючи процеси та усуваючи потребу в посередниках, що в свою чергу скорочує час і витрати, пов’язані з традиційною обробкою документів.

Однак, блокчейн не позбавлений проблем. Масштабованість стає значною перешкодою, оскільки мережа намагається підтримувати продуктивність зі збільшенням обсягу транзакцій, що може призвести до затримок і збільшення витрат. Технологія блокчейну є складною, що вимагає певного рівня технічної експертизи для її розуміння та впровадження, створюючи перешкоди для широкого прийняття без значних інвестицій у навчання та розвиток.

Додатково, децентралізований і глобальний характер блокчейна створює лабіринт регуляторних проблем, оскільки юрисдикції в усьому світі борються з тим, як регулювати цю нову технологію. Це ускладнює дотримання нормативних вимог, особливо під час керування електронними документами через кордон. Екологічні занепокоєння, пов'язані з високим споживанням енергії деякими реалізаціями блокчейну, зокрема механізмом консенсусу PoW, також викликали дебати щодо стійкості технології, спонукаючи до пошуку більш енергоефективних альтернатив.

2.5 Аналіз рішень на основі блокчейну

Щоб провести аналіз рішень на основі блокчейну, важливо глибоко зануритися в застосування технології, переваги та обмеження, контекстуалізовані прикладами та посиланнями на реальні ресурси. Блокчейн, технологія розподіленої книги, знайшла застосування в різних секторах, включаючи фінанси, охорону здоров’я, ланцюг поставок тощо.

Біткойни та інші криптовалюти є одними з перших і найвидатніших прикладів застосування технології блокчейн, пропонуючи модель децентралізованого фінансування (DeFi), яка усуває потребу в традиційних банківських системах та посередниках. Це знижує комісії за транзакції та розширює доступ до фінансових послуг, особливо в регіонах, де банківські послуги відсутні. Проте мінлива природа криптовалют та асоціації з незаконною діяльністю викликають певні занепокоєння. Додатково, проблеми масштабованості, зокрема обмежена здатність обробки транзакцій у біткойнів,

призводять до збільшення комісій та сповільнення часу обробки під час пікових навантажень. Детальний аналіз впливу біткойна на фінансовий сектор, включаючи його переваги та обмеження, можна знайти в оригінальному документі Сатоші Накамото про біткойн та подальших дослідженнях фінансових експертів на платформах, таких як Financial Times або Bloomberg, що надають глибоке розуміння цієї теми.

В охороні здоров'я блокчейн пропонує системи керування даними пацієнтів, які забезпечують безпечні та незмінні записи, підвищуючи конфіденційність і сприяючи ефективному обміну інформацією між медичними постачальниками. Це може значно вдосконалити діагностику, плани лікування та загальні результати для пацієнтів. Проте існують виклики, зокрема, інтеграція з наявними IT-системами, дотримання нормативних вимог конфіденційності даних, таких як GDPR, та потреба в культурних та організаційних змінах у медичній сфері. Академічні дослідження та тематичні дослідження, опубліковані на платформах, як-от PubMed або Journal of Medical Internet Research, детально розглядають потенціал та обмеження блокчейн-додатків у сфері охорони здоров'я, надаючи цінне уявлення про перспективи та перешкоди їхнього впровадження.

У сфері управління ланцюгом поставок блокчейн пропонує значні переваги для підвищення прозорості та відстежуваності, дозволяючи споживачам перевіряти автентичність і походження продуктів. Наприклад, компанія Walmart використовує блокчейн для відстеження ланцюжка поставок листової зелені, значно скорочуючи час відстеження продукції з декількох днів до лічених секунд. Однак, існують і певні обмеження при впровадженні блокчейну в ланцюги поставок, включаючи необхідність уніфікації галузевих стандартів, складності інтеграції з існуючими логістичними системами, а також забезпечення точності даних, що вводяться в систему. Приклад використання блокчейну компанією Walmart та дослідницькі статті в логістичних журналах надають цінне розуміння потенціалу та викликів блокчейну в контексті управління ланцюгом поставок, що доступні на корпоративному веб-сайті Walmart та в академічних публікаціях.

В енергетичному секторі блокчейн пропонує можливість створення децентралізованих енергетичних мереж, які дозволяють споживачам купувати та продавати надлишкову енергію безпосередньо один одному без залучення центральної енергосистеми, що може сприяти більш ефективному розподілу ресурсів та зниженню витрат. Однак, цей підхід супроводжується рядом викликів, включаючи технічні складнощі управління потоками енергії в розподіленій системі, нормативні бар'єри, а також необхідність значних інвестицій у розвиток інфраструктури. Дослідження та звіти про пілотні проекти, опубліковані в енергетичних журналах і на веб-сайтах таких організацій, як Міжнародне енергетичне агентство, надають цінну інформацію щодо доцільності, переваг та проблем застосування блокчейну у сфері енергетики.

2.6 Технологічні аспекти блокчейну в контексті електронного документообігу

Інтеграція технології блокчейн в системи електронного документообігу являє собою значну еволюцію в тому, як документи керуються, перевіряються та захищаються в цифровій сфері. Технологія Blockchain пропонує децентралізовану, захищену від втручання книгу, яка може трансформувати традиційні системи управління електронними документами (EDMS), підвищуючи безпеку, прозорість і довіру між учасниками.

2.6.1 Криптографічний захист

В основі технології блокчейн лежить криптографічний захист, який забезпечує конфіденційність, цілісність і автентичність даних, що зберігаються в блокчейні. Кожен блок у блокчейні містить набір транзакцій (у цьому контексті обмін документами або їх модифікація), які захищені за допомогою криптографічних алгоритмів.

Хеш-функції є ключовими елементами у забезпеченні безпеки електронних систем. Вони дозволяють зв'язувати блоки даних між собою, створюючи

унікальний цифровий відбиток, відомий як хеш, для кожного блоку. Цей хеш генерується на основі інформації, що міститься всередині блоку, і будь-які зміни в цьому вмісті призводять до створення нового хешу. Це означає, що якщо хеш блоку змінено, це одразу ж сигналізує про можливе втручання. Така властивість робить хеш-функції незамінними для систем електронного документообігу, де вище за все цінується автентичність та цілісність документів.

Крім того, блокчейн використовує криптографію публічно-приватного ключа для забезпечення безпечного обміну даними між учасниками. Кожна особа має унікальну пару ключів: приватний ключ, який зберігається в таємниці та використовується для підписання транзакцій, та публічний ключ, який може бути відкрито наданий іншим для перевірки підпису. Цей механізм забезпечує, що лише уповноважені особи мають доступ до документів, їх підпису або модифікації, значно підвищуючи рівень безпеки електронних документів.

2.6.2 Незмінність

Після додавання транзакції до блокчейну змінити її стає майже неможливо. Ця незмінність забезпечується механізмом консенсусу та криптографічним зв’язуванням блоків.

Механізми консенсусу в мережах блокчейну, такі як PoW або PoS, відіграють ключову роль у підтвердженні дійсності транзакцій. Вони дозволяють учасникам мережі досягти загальної згоди щодо стану бази даних, і після досягнення цього консенсусу, інформація про транзакції назавжди реєструється в блокчейні. Це особливо важливо в контексті електронного документообігу, оскільки забезпечує, що будь-які документи, які були видані, отримані або підтверджені, фіксуються постійно, запобігаючи будь-яким несанкціонованим змінам або спробам відмовитися від них.

У структурі блокчейну кожен блок містить хеш свого попередника, утворюючи безперервний і безпечний ланцюг. Ця властивість робить будь-яку спробу змінити інформацію в одному з блоків вкрай складною, оскільки це

вимагало б змінити всі наступні блоки в ланцюжку, що є обчислювально непрактичним завданням у розподіленій мережі. Така структура забезпечує незмінність історії документів, забезпечуючи високий рівень довіри та безпеки в електронному документообігу.

2.6.3 Децентралізація

Блокчейн працює в одноранговій мережі, де жодна особа не контролює всю систему. Ця децентралізація означає, що електронні документи не зберігаються в центральному сховищі, а розподіляються між кількома вузлами, зменшуючи ризик втрати даних, підробки та централізованих атак.

Технологія розподіленої книги (DLT), зокрема DLT Blockchain, відіграє ключову роль у забезпеченні безпеки та доступності документів у системах електронного документообігу. Ця технологія дозволяє зберігати копії документів на багатьох комп'ютерах одночасно, що забезпечує високий рівень резервування та доступності. Така функція стає незамінною в умовах, де втрата або тимчасова недоступність критично важливих документів може призвести до серйозних наслідків.

Децентралізований характер DLT сприяє створенню прозорості та довіри між усіма учасниками системи. Завдяки спільному доступу до однакової інформації, кожен учасник має можливість переглядати одну й ту ж версію історії документів, що значно спрощує співпрацю та взаємодію між різними організаціями. Така прозорість і відкритість інформації зменшує потребу в центральному регулюючому органі, тим самим сприяючи більшій довірі між сторонами.

2.6.4 Розумні контракти

Автоматизація процесів документообігу за допомогою систем електронного документообігу та смарт-контрактів відкриває нові можливості для підвищення

ефективності та забезпечення відповідності вимогам управління документацією. Смарт-контракти, що використовуються в таких системах, можуть автоматизувати різноманітні процеси, пов'язані з документами, включаючи робочі процеси затвердження, перевірку документів та перевірку їх відповідності встановленим стандартам. Це означає, що, наприклад, смарт-контракт може бути програмований таким чином, щоб автоматично здійснювати платіж після того, як документ про доставку буде не тільки отриманий, але й перевірений на відповідність умовам контракту. Однією з ключових переваг використання смарт-контрактів у системах електронного документообігу є забезпечення вищої відповідності процесів управління документами до попередньо встановлених правил і процедур. Смарт-контракти можуть гарантувати, що кожна дія з документом буде виконана в строгій відповідності до визначених параметрів, значно знижуючи ризик людської помилки та сприяючи більшій прозорості та надійності у процесах обігу документації. Це не тільки покращує ефективність робочих процесів, але й забезпечує більшу впевненість у відповідності цих процесів нормативним і законодавчим вимогам.

Висновки до розділу 2

Технологія блокчейн є трансформаційною силою в різних галузях, пропонуючи інноваційні рішення для давніх проблем управління даними та безпеки. У цьому розділі описано ключові аспекти технології блокчейн та надано огляд її загальних характеристик, особливостей та переваг. Тут досліджуються фундаментальні принципи, що лежать в основі блокчейну, включаючи його децентралізовану природу, криптографічну безпеку і незмінність.

Цей розділ дасть уявлення про стан сучасних систем електронного документообігу та окреслить поточні підходи до управління документами та виклики, які вони створюють для безпеки та ефективності. Розглядаються сильні та слабкі сторони традиційних методів захисту документів і підкреслюється необхідність у надійних рішеннях, здатних протистояти загрозам, що виникають у цифровому середовищі, яке швидко розвивається.

РОЗДІЛ 3. СИСТЕМА ТЕХНОЛОГІЇ БЛОКЧЕЙН

У розділі описано технологію та компоненти, використані для побудови програмної моделі та реалізації системи, а також представлено простий приклад процесу шифрування електронних документів за допомогою блокчейну.

3.1 Функціональність системи електронного документообігу на основі блокчейн

Система електронного документообігу, що базується на криптографії та технології блокчейн, використовує алгоритм формування блоків з початкових даних. Кожен блок гарантує цілісність і незмінність вхідних даних і містить службову інформацію, необхідну для роботи блокчейну. Ланцюжок являє собою єдиний зв'язаний список.

Блок даних містить наступні поля (рис 3.1):

– Індекс: вказує на номер блоку в ланцюжку;

– Мітка часу. Мітка часу, що вказує на час створення транзакції;

– Ім'я користувача. Ім'я користувача, який виконав транзакцію;

– Ім'я файлу. Ім'я файлу, доданого в систему; Ім'я файлу;

– Значення файлу, виражене шістнадцятковим числом;

– Хеш; унікальне значення, створене зі збережених даних, згенероване за алгоритмом SHA256;

– Попередній хеш. Покажчик на попередній хеш-блок. Необхідний для зв'язування блоків в єдиний ланцюжок.

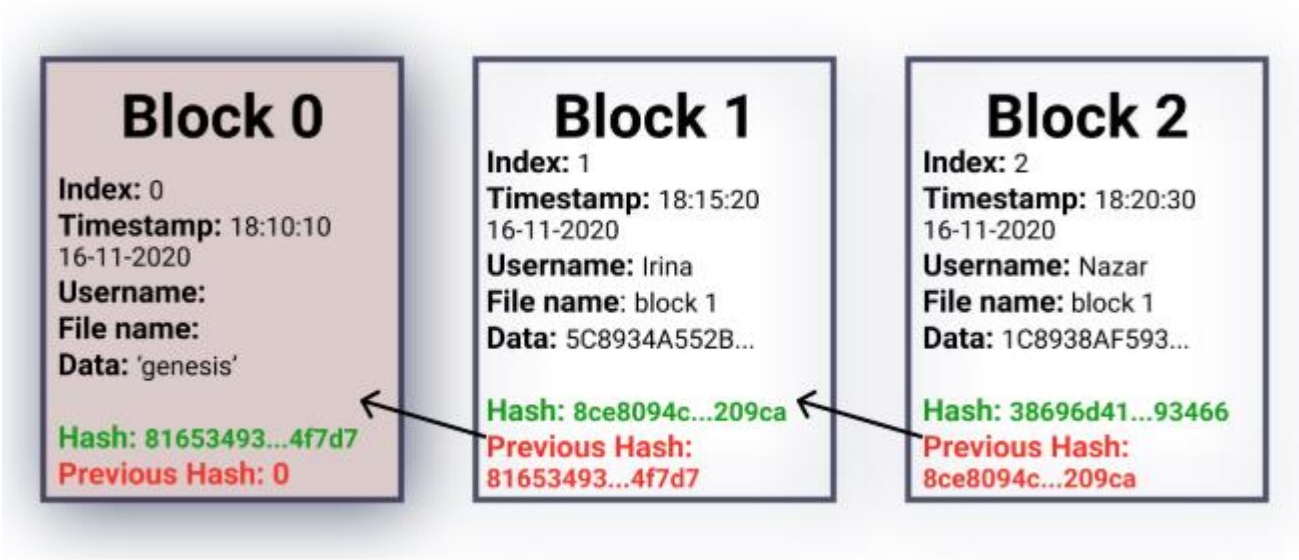

Рисунок 3.1 – Ланцюжок блоків blockchain

При створенні блоку даних всі збережені дані в блоці хешуються за допомогою алгоритму SHA256 і результат записується в поле Hash. Цей метод забезпечує незмінність даних. Це пов'язано з тим, що якщо змінити хоча б один символ в одному з полів блоку, хеш-функція поверне зовсім інший результат. Система може легко виявити це втручання і неточність ланцюжка, повторно хешуючи блок і порівнюючи його зі збереженим хешем.

Цифрові підписи можна застосовувати в системі для підтвердження авторства. Цифрові підписи в першу чергу використовуються для автентифікації користувачів у системі. Коли користувач підписує документ, він зберігається в блокчейні для цілей автентифікації. Зробивши блокчейн компонентом серверної інфраструктури, можна забезпечити незмінність і простежуваність збережених записів.

Алгоритм RSA з відкритим ключем. Цей алгоритм дозволяє підписувати та перевіряти повідомлення. Коли користувач реєструється в системі, генерується приватний ключ, необхідний для підписання ЕД.

Схема цифрового підпису виглядає наступним чином:

– Генерується пара відкритого та закритого ключів;
– Аліса підписує документ закритим ключем і надсилає його в систему

– Боб перевіряє справжність підпису за допомогою відкритого ключа Аліси.

Для побудови СЕД на основі блокчейн необхідно визначити основні етапи зберігання ЕД у децентралізованому сховищі з накладеним ЦС.

Вхідними даними від авторизованого користувача є документ. Результатом всіх етапів є підписана версія файлу, що зберігається в сховищі. Основним процесом роботи програмного забезпечення є зберігання електронних документів. Результатом всіх внутрішніх процесів зберігання електронних документів є безперервний ланцюжок блоків, які складають сховище ЕД в оверлеї КП. Аутентифікація користувача відбувається після введення правильного логіну та паролю, користувач є авторизованим в системі і може виконувати певні дії відповідно до своїх прав в системі. Авторизований користувач може завантажувати документи для подальшого дослідження.

3.2. Алгоритм та розробка блокчейн системи

Для розробки програмного забезпечення для прикладу роботи сиcетми електронного документобігу за допомогою блокчейн було розроблено та реалізовано просту імплементацію блокчейну на платформі Node.js.

Node.js - це вільна та відкрита платформа для виконання JavaScript коду на сервері. Вона побудована на JavaScript runtime (виконавче середовище JavaScript) Chrome's V8 Engine, що забезпечує високу швидкодію виконання коду. Node.js дозволяє розробникам створювати скальовані та ефективні серверні застосунки, використовуючи JavaScript, який раніше був обмежений до веб-браузера. Він активно використовується для створення веб-серверів, мережевих додатків, API, а також для реалізації інших серверних застосунків. Через асинхронну та подієву модель програмування, Node.js є особливо ефективним у високонавантажених додатках, де обробка багатьох запитів може виконуватися паралельно без блокування основного потоку виконання.

При створенні блоку в системі блокчейн використовуються кілька ключових компонентів, які гарантують цілісність та безпеку інформації. Першим з них є ідентифікатор блоку (індекс), який вказує на позицію блоку в ланцюгу. Другий компонент - це попередній хеш, що є унікальним ідентифікатором попереднього блоку. Це створює безперервний ланцюг, де кожен блок підтверджує попередній. Найважливішим елементом є дані, які включаються в блок. У якості даних для хешування я обрав ім'я відправника, ім'я отримувача, та текст, який замінює електронний документ. Це дозволяє створити унікальний відбиток кожного блоку, який відображає всю необхідну інформацію про транзакцію. Після хешування ці дані стають незмінними та неспроможними до модифікації, що додає до надійності та цілісності системи блокчейн.

Для кращого розуміння процесу створення та валідації блоків, була розроблена детальна блок-схема, яка ілюструє основні етапи роботи коду (рис. 3.2). Вона включає опис створення блоків, додавання їх до ланцюжка, а також перевірку цілісності ланцюжка.

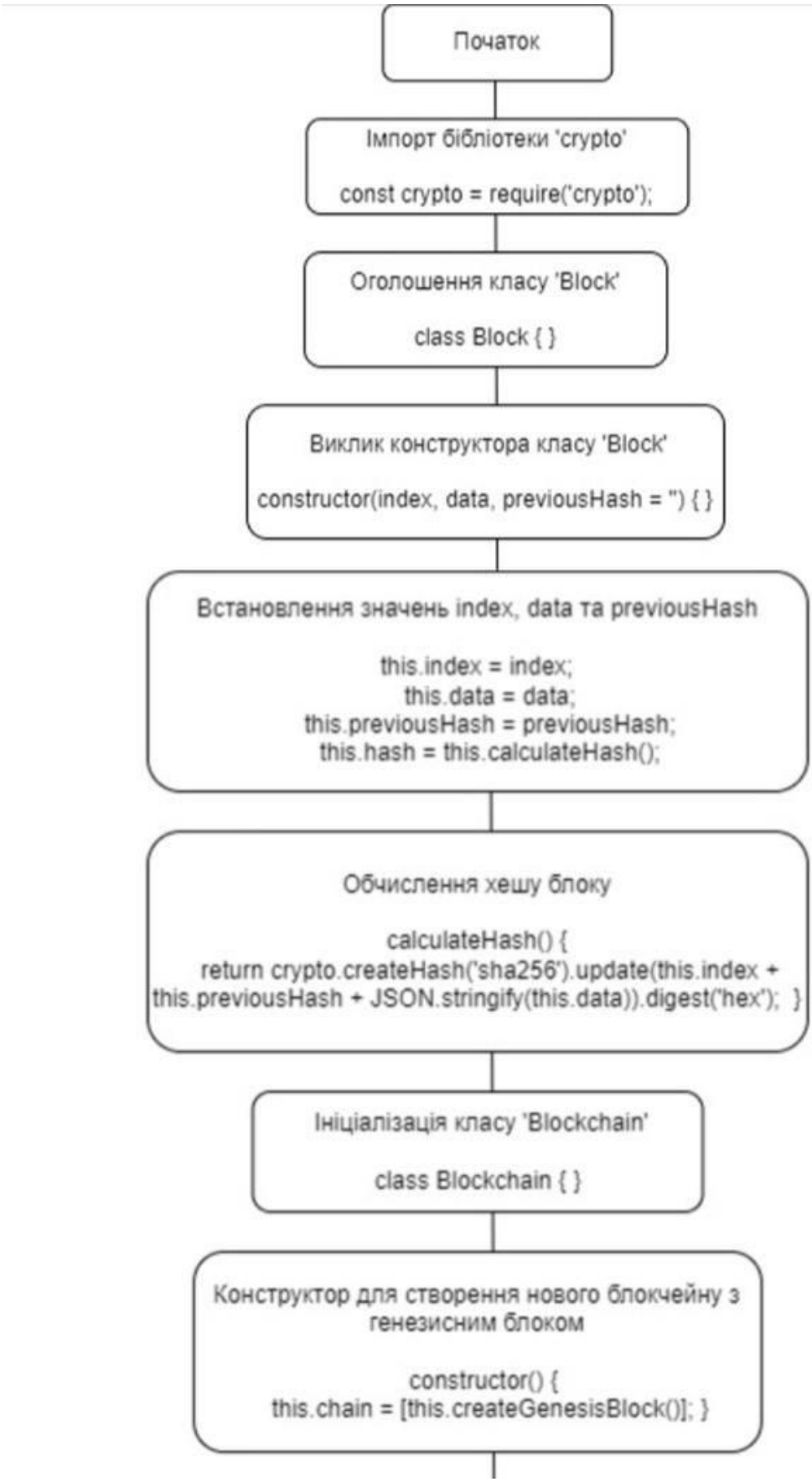

Рисунок 3.2 – Блок-схема алгоритму роботи програмної реалізації блокчейну частина 1

Рисунок 3.3 – Блок-схема алгоритму роботи програмної реалізації блокчейну частина 2

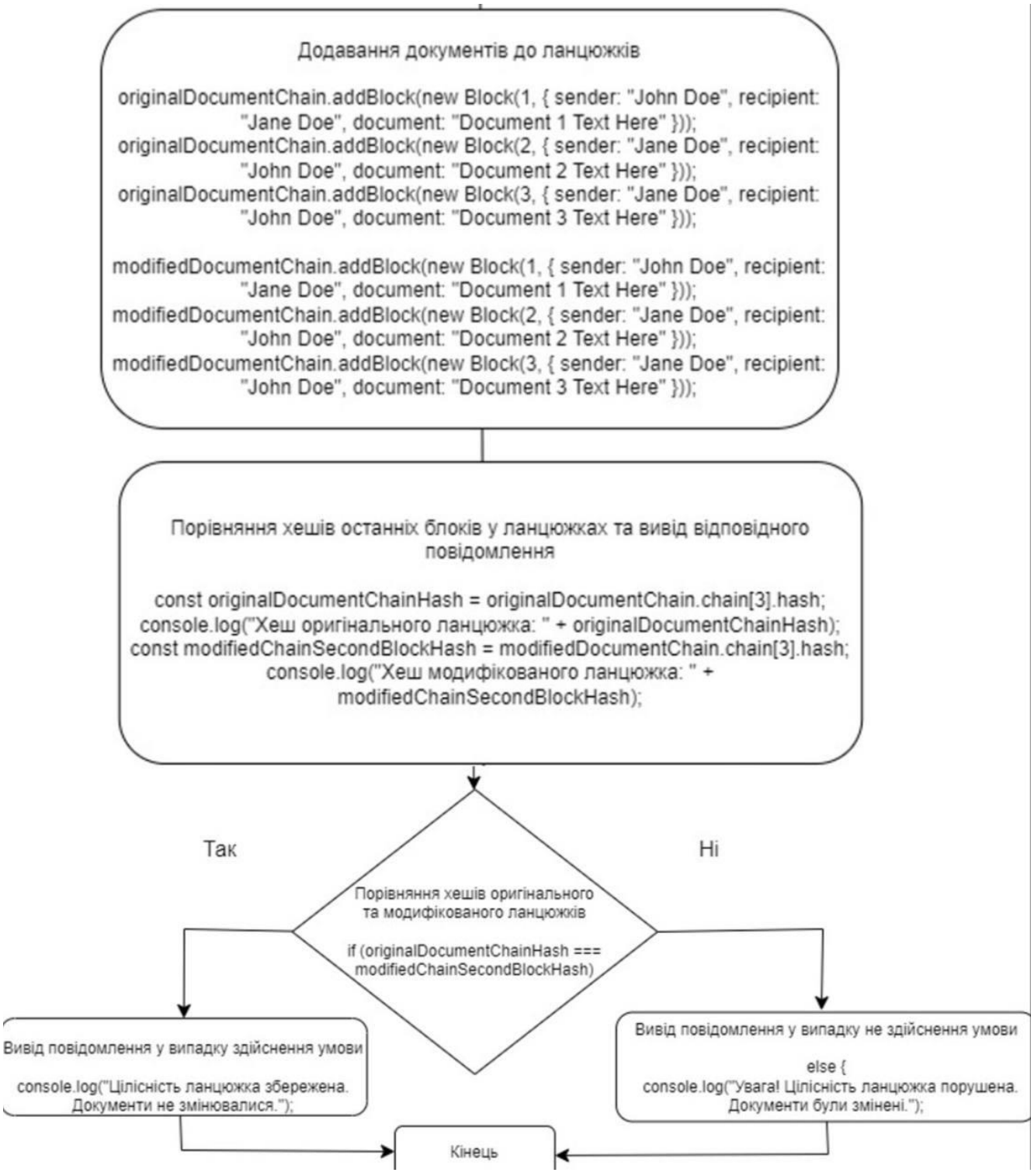

Рисунок 3.4 – Блок-схема алгоритму роботи програмної реалізації блокчейну частина 3

Короткий опис схеми алгоритму:

– Блок: Кожен блок містить дані, індекс, хеш попереднього блоку та свій власний хеш.

– Блокчейн: Ланцюжок блоків, який починається з "Genesis Block". Нові блоки додаються до кінця.

– Додавання блоків: Кожен новий блок обчислює свій хеш на основі даних і хеша попереднього блоку.

– Перевірка цілісності: Порівнюються хеші останніх блоків двох ланцюжків. Якщо вони збігаються, дані не змінювались; якщо ні, то дані були змінені.

У випадку моєї реалізації блокчейну, я вирішив не використовувати часову мітку у створенні блоків. Це було зроблено з метою спрощення та акцентування уваги на процесі хешування даних. Оскільки моя основна мета полягала у демонстрації роботи блокчейна та валідації інформації за допомогою хешування, використання часової мітки не є обов'язковим. Це дозволяє краще зосередитися на самому процесі створення та валідації блоків, що є ключовим аспектом розуміння функціонування системи блокчейн.

3.3 Переваги електронного документообігу на основі блокчейн

У сучасному цифровому середовищі безпека електронних документів є дуже важливою. Адже електронні документи зберігають і передають конфіденційну інформацію, таку як персональні дані, фінансові звіти, комерційні таємниці та інші конфіденційні дані. Захист цих документів необхідний для того, щоб захистити їх від несанкціонованого доступу, втрати та зміни даних.

Електронні документи можуть зазнавати різноманітних загроз від хакерів та кіберзлочинців, які прагнуть отримати доступ до конфіденційної інформації з метою підробки, шахрайства або шпигунства. Порушення безпеки може призвести до серйозних фінансових втрат, репутаційних збитків та інших негативних наслідків для компаній та організацій.

Безпека електронних документів важлива для забезпечення відповідності законодавчим і нормативним вимогам щодо захисту даних. У багатьох країнах і галузях існують суворі правила щодо обробки та зберігання конфіденційної інформації, наприклад, GDPR у Європейському Союзі та HIPAA у США. Недотримання цих правил може призвести до значних штрафів та інших юридичних дій.

Впровадження систем електронного документообігу на основі блокчейну пропонує численні переваги порівняно з іншими варіантами цифрового документообігу. Перш за все, блокчейн, як розподілена база даних, надає безпеку та надійність, що є важливими аспектами у сфері документообігу. Кожен блок в ланцюжку блоків містить хеш попереднього блоку, що робить маніпулювання даними майже неможливим. Це забезпечує високий рівень цілісності та безпеки документів.

Моя проста модель блокчейну призначена для демонстрації, як можна застосувати цю технологію для забезпечення безпеки та цілісності електронних документів.

У моєму коді створюється два ланцюжки документів: оригінальний (рис. 3.5) та змінений (рис. 3.6). Оригінальний ланцюжок містить набір документів, що імітуються, а змінений ланцюжок є копією оригінального, до якого вносяться зміни у тексті деяких документів.

```
let originalDocumentChain = new Blockchain();

originalDocumentChain.addBlock(new Block(1, { sender: "John Doe", recipient: "Jane Doe", document: "Document 1 Text Here" }));
originalDocumentChain.addBlock(new Block(2, { sender: "Jane Doe", recipient: "John Doe", document: "Document 2 Text Here" }));
originalDocumentChain.addBlock(new Block(3, { sender: "Jane Doe", recipient: "John Doe", document: "Document 3 Text Here" }));
```

Рисунок 3.5 – Створення ланцюжка документів та збереження його хешу

```
let modifiedDocumentChain = new Blockchain();

modifiedDocumentChain.addBlock(new Block(1, { sender: "John Doe", recipient: "Jane Doe", document: "Document 1 Text Here" }));
modifiedDocumentChain.addBlock(new Block(2, { sender: "Jane Doe", recipient: "John Doe", document: "Document 2 Text Here CHANGE" }));
modifiedDocumentChain.addBlock(new Block(3, { sender: "Jane Doe", recipient: "John Doe", document: "Document 3 Text Here" }));
```

Рисунок 3.6 – Створення ланцюжка зі зміненим документом та збереження його хешу

Після того, як дані додані до ланцюжка, вони захищені від будь-яких змін через криптографічний механізм хешування. На рисунку 3.7 представлена перевірка цілісності ланцюжка, яка полягає у порівнянні хешів останніх блоків оригінального та зміненого ланцюжків. Якщо хеші збігаються, це свідчить про те, що документи залишаються незмінними. У цьому випадку виводиться повідомлення "Цілісність ланцюжка збережена. Документи не змінювалися" (рис. 3.8).

```
const originalDocumentChainHash = originalDocumentChain.chain[3].hash;
console.log("Хеш оригінального ланцюжка: " + originalDocumentChainHash);
const modifiedChainSecondBlockHash = modifiedDocumentChain.chain[3].hash;
console.log("Хеш модифікованого ланцюжка: " + modifiedChainSecondBlockHash);


if (originalDocumentChainHash === modifiedChainSecondBlockHash) {
  console.log("Цілісність ланцюжка збережена. Документи не змінювалися.");
} else {
  console.log("Увага! Цілісність ланцюжка порушена. Документи були змінені.");
}
```

Рисунок 3.7 – Порівняння ланцюжків та виведення відповідного повідомлення

```
PS C:\Users\palag\OneDrive\Рабочий стол\кнеу\Диплом\practice> node blockchain.js
Цілісність ланцюжка збережена. Документи не змінювалися.
PS C:\Users\palag\OneDrive\Рабочий стол\кнеу\Диплом\practice>
```

Рисунок 3.8 – Позитивний результат перевірки цілісності

Проте, якщо будь-який документ у зміненому ланцюжку був модифікований, хеші останніх блоків різняться, що свідчить про порушення цілісності ланцюжка. У цьому випадку виводиться повідомлення "Увага! Цілісність ланцюжка порушена. Документи були змінені" (рис. 3.9). Такий підхід дозволяє виявити та відслідкувати будь-які зміни в електронних документах, забезпечуючи високий рівень надійності та цілісності електронного документообігу.

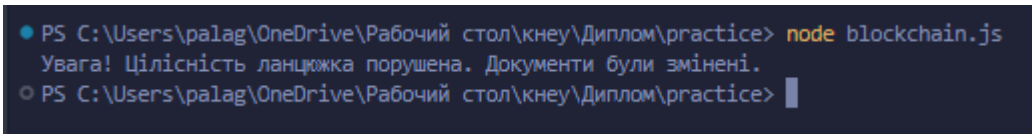

Рисунок 3.9 – Негативний результат перевірки цілісності

Використання блокчейну для електронного документообігу дозволяє покращити співпрацю та обмін інформацією між різними учасниками екосистеми. Блокчейн забезпечує безпеку та конфіденційність даних, що дозволяє сторонам взаємодіяти між собою без посередництва та страху зазіхання на конфіденційність своїх даних. Це сприяє покращенню комунікації та співпраці між різними суб'єктами бізнесу та організаціями.

Висновки до розділу 3

У цьому розділі було досліджено технологію блокчейн та її застосування для створення системи електронного документообігу (СЕД). Було розроблено та реалізовано просту модель блокчейну на платформі Node.js, яка демонструє основні принципи роботи та можливості для забезпечення безпеки та цілісності електронних документів.

Блокчейн пропонує прозорість та незмінність, що дозволяє відстежувати історію змін документів та гарантувати, що жодна сторона не зможе змінити або видалити документи без відома інших учасників. Також він може допомогти покращити співпрацю та обмін інформацією між різними учасниками екосистеми СЕД. Завдяки децентралізованому характеру блокчейну сторони можуть взаємодіяти без посередників, що може призвести до економії часу та коштів, а також до покращення комунікації та ефективності.

ВИСНОВКИ

У дипломній роботі розглянуто створення і використання блокчейн технології для захисту електронного документообігу. Основна мета полягала у демонстрації, як блокчейн може забезпечити цілісність і незмінність документів, що є критичним для багатьох сфер діяльності.

Було розроблено просту модель блокчейну, що дозволяє створювати, зберігати та перевіряти документи. Кожен документ зберігається в окремому блоці, який містить хеш попереднього блоку, що забезпечує зв’язність і захист від несанкціонованих змін. У прикладі було показано, як зміна одного документа в середині ланцюжка призводить до зміни хешів наступних блоків, що легко виявляється при перевірці цілісності.

Переваги використання блокчейну для електронного документообігу включають:

1. Безпека: Використання криптографічних хешів забезпечує захист від несанкціонованих змін та підробок.

2. Прозорість: Всі транзакції з документами зберігаються у вигляді незмінного ланцюжка, що дозволяє відстежити всі зміни та перевірити їх походження.

3. Незмінність: Документи, що зберігаються у блокчейні, не можуть бути змінені без виявлення цієї зміни, що гарантує довіру до збережених даних.

4. Доступність: Блокчейн забезпечує децентралізоване зберігання, що підвищує надійність системи навіть при виході з ладу окремих вузлів.

На основі проведених досліджень та розробленої моделі можна зробити висновок, що блокчейн технологія є ефективним інструментом для захисту електронного документообігу. Вона забезпечує високий рівень безпеки, прозорості та незмінності даних, що особливо важливо для сфер, де потрібна висока надійність і довіра до збереженої інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ю.Мінгальова. Новітні криптографічні методи захисту інформації. С. 2. URL: http://eprints.zu.edu.ua/13902/1/Mingaleva3.pdf.

2. Stallings W. Cryptography and network security: principles and practice. Pearson Education, Limited, 2010. 744 p.

3. A cryptographic key management scheme for implementing the Data Encryption Standard / W. F. Ehrsam et al. *IBM systems journal*. 1978. Vol. 17, no. 2. P. 106–125. URL: https://doi.org/10.1147/sj.172.0106 (date of access: 15.04.2024).

4. Advani N., Rathod C., Gonsai A. M. Comparative study of various cryptographic algorithms used for text, image, and video. *Advances in intelligent systems and computing*. Singapore, 2018. P. 393–399. URL: https://doi.org/10.1007/978-981-13-2285-3_46 (date of access: 15.04.2024).

5. Katz J., Lindell Y. Introduction to Modern Cryptography. 2014. Vol. 2 : Chapman & Hall/CRC Cryptography and Network Security Series.

6. Рибальский О.в, Хахановський В.г, Кудінов В.а. Основи інформаційної безпеки та технічного захисту інформації. Київ : М-ВО ВНУТР. СПРАВ УКРАЇНИ НАЦ. АКАД. ВНУТР. СПРАВ, 2012. 104 с.

7. Manzhai O.v. Procedure analysis of the special investigative actions through cyberspace in countries of common and continental law. *Internal security*. 2012. Vol. 1, no. 4. P. 141–152.

8. Виадук телеком. *Віадук-Телеком. Розробка документоорієнтованих баз даних*.
URL: https://www.viaduk.net/viaduk/web5ua.nsf/0/ACC6E5C6C0A30BD9C225726F0051E265.

9. Про Закон України "Про електронний цифровий підпис" : Лист Вищ. госп. суду України від 03.07.2003 р. № 01-8/746. URL: https://zakon.rada.gov.ua/laws/show/v_746600-03#Text.

10. Iansiti M, Lakhani KR. The Truth About Blockchain. *Harvard Business Review.* 2017. [cited 2018 09 November]; January-February 2017

11. Wright C. S. Bitcoin: a peer-to-peer electronic cash system. *SSRN electronic journal*. 2008. URL: https://doi.org/10.2139/ssrn.3440802 (date of access: 15.04.2024).

12. Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the american medical informatics association*. 2017. Vol. 24, no. 6. P. 1211–1220.

13. Peterson K. A blockchain-based approach to health information exchange networks. 2016.

14. Dubovitskaya A. Secure and trustable electronic medical records sharing using blockchain. *AMIA annu symp proc*. 2017. P. 650–659.

15. Krawiec R. Blockchain: opportunities for health care. *Deloitte*. 2016.

16. 2.2. Огляд сучасних систем електронного документообігу | Коментар. *Мего-Інфо - Юридичний портал України №1, Коментар ЦПК, КПК, КУПАП, ККУ, ЦК*. URL: http://mego.info/матеріал/22-огляд-сучасних-систем-електронного-документообігу.

ДОДАТОК А

Програмна реалізація моделі блокчейну на платформі Node.js

```
const crypto = require('crypto');

// Клас для представлення кожного блоку у ланцюжку
class Block {
  // Конструктор для створення нового блоку з заданими даними та попереднім хешем
  constructor(index, data, previousHash = '') {
    this.index = index; // Індекс блоку у ланцюжку
    this.data = data; // Дані, що зберігаються у блоку
    this.previousHash = previousHash; // Хеш попереднього блоку у ланцюжку
    this.hash = this.calculateHash(); // Обчислення хешу поточного блоку
  }

  // Функція для обчислення хешу поточного блоку
  calculateHash() {
    // Використання алгоритму SHA-256 для хешування індексу, попереднього хешу, мітки
часу та даних блоку
    return crypto.createHash('sha256').update(this.index + this.previousHash +
JSON.stringify(this.data)).digest('hex');
  }
}

// Клас, що представляє блокчейн
class Blockchain {
  // Конструктор для створення нового блокчейну з генезисним блоком
  constructor() {
    this.chain = [this.createGenesisBlock()]; // Ланцюжок блоків, починаючи з
генезисного блоку
  }

  // Функція для створення генезисного блоку
  createGenesisBlock() {
    return new Block(0, "Genesis Block", "0"); // Генезисний блок з індексом 0,
попереднім хешем "0" та статичними даними
  }

  // Функція для отримання останнього блоку у ланцюжку
  getLatestBlock() {
    return this.chain[this.chain.length - 1];
  }

  // Функція для додавання нового блоку до ланцюжка
  addBlock(newBlock) {
    // Встановлення попереднього хешу нового блоку як хешу останнього блоку у
ланцюжку
    newBlock.previousHash = this.getLatestBlock().hash;
    // Обчислення хешу нового блоку
```

```
    newBlock.hash = newBlock.calculateHash();
    // Додавання нового блоку до ланцюжка
    this.chain.push(newBlock);
  }
}

// Створення двох блокчейнів з однаковими даними
let originalDocumentChain = new Blockchain();
let modifiedDocumentChain = new Blockchain();

// Додавання документів до ланцюжків
originalDocumentChain.addBlock(new Block(1, { sender: "John Doe", recipient: "Jane
Doe", document: "Document 1 Text Here" }));
originalDocumentChain.addBlock(new Block(2, { sender: "Jane Doe", recipient: "John
Doe", document: "Document 2 Text Here" }));
originalDocumentChain.addBlock(new Block(3, { sender: "Jane Doe", recipient: "John
Doe", document: "Document 3 Text Here" }));

modifiedDocumentChain.addBlock(new Block(1, { sender: "John Doe", recipient: "Jane
Doe", document: "D123ocument 1 Text Here" }));
modifiedDocumentChain.addBlock(new Block(2, { sender: "Jane Doe", recipient: "John
Doe", document: "Document 2 Text Here" }));
modifiedDocumentChain.addBlock(new Block(3, { sender: "Jane Doe", recipient: "John
Doe", document: "Document 3 Text Here" }));

// Порівняння хешів останніх блоків у ланцюжках та вивід відповідного повідомлення
const originalDocumentChainHash = originalDocumentChain.chain[3].hash;
const modifiedChainSecondBlockHash = modifiedDocumentChain.chain[3].hash;

if (originalDocumentChainHash === modifiedChainSecondBlockHash) {
  console.log("Цілісність ланцюжка збережена. Документи не змінювалися.");
} else {
  console.log("Увага! Цілісність ланцюжка порушена. Документи були змінені.");
}
```

Короткий звіт подібності

UNICHECK
by Turnitin

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

ID перевірки:
1016354236

Дата перевірки:
12.06.2024 22:18:58 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.06.2024 23:06:26 EEST

ID користувача:
100005746

Назва документа: Палагін_КБ_бакалвр.робота

Кількість сторінок: 46 Кількість слів: 9471 Кількість символів: 81293 Розмір файлу: 1.43 MB ID файлу: 1016158166

18.7%
Схожість

Найбільша схожість: 5.42% з джерелом з Бібліотеки (ID файлу: 10001138)

15.3% Джерела з Інтернету 383 ..... Сторінка 48

14.7% Джерела з Бібліотеки 397 ..... Сторінка 51

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 2