МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет комп’ютерних наук, фізики та математики

Кафедра комп’ютерних наук та програмної інженерії

Розробка системи електронного документообігу для організацій з використанням блокчейн-технологій

Кваліфікаційна робота (проєкт)

на здобуття ступеня вищої освіти «магістр»

Виконав: здобувач 2 курсу магістратури групи 241М
Спеціальність: 121 Інженерія програмного забезпечення
Освітньо-професійна програма: Інженерія програмного забезпечення
Пятько Сергій Сергійович
Керівник: Завідувач кафедри комп’ютерних наук та програмної інженерії ХДУ, доктор фізико-математичних наук, професор Песчаненко Володимир Сергійович
Рецензент: кандидатка технічних наук, доцентка кафедри програмних засобів і технологій, Захарченко Р. М. Херсонський національно-технічний університетю

Івано-Франківськ – 2024

ЗМІСТ

ВСТУП

На сьогоднішній день, зберігання та передавання великих об’ємів даних є критично важлививми для організацій. Останні роки характеризуються стрімким зростанням обсягів інформації, що вимагає використання більш ефективних і захищених технологій для її обробки. У цьому контексті особливої ваги набувають системи електронного документообігу, які дозволяють автоматизувати процеси управління документацією. Проте зі стрімким розвитком програм документообігу так само стрімко зростають і різного виду кіберзагрози які стають дедалі більшою проблемою з кожним роком. Ситуації коли у великої корпорації відбувається витік даних стають вже нормою у сучасному цифровому світі.

Блокчейн, як децентралізована технологія зберігання даних, став відповіддю на численні виклики у сфері безпеки інформаційних систем. За останні кілька років технологія зазнала значних удосконалень і розширила сферу свого застосування з фінансових операцій до багатьох інших галузей, включно з системами електронного документообігу. Використання блокчейну дозволяє створити систему, в якій кожен запис є незмінним і захищеним від несанкціонованих змін, що критично важливо для організацій, які працюють із чутливою інформацією.

Забезпечення конфіденційності та автентичності документів є ключовим аспектом ефективної роботи систем електронного документообігу. Блокчейн дає можливість реалізувати новий рівень захисту документів, оскільки кожен документ або транзакція записується в розподілену мережу, де вона може бути перевірена, але не змінена. Це створює додатковий рівень прозорості та безпеки в роботі організацій.

Метою цієї магістерської роботи є дослідження можливостей блокчейн-технологій для створення ефективної та безпечної системи електронного

документообігу, що дозволить організаціям мінімізувати ризики втрати або фальсифікації даних, підвищити ефективність управління документами та забезпечити дотримання стандартів інформаційної безпеки.

Актуальність: Актуальність теми полягає в необхідності забезпечення високого рівня безпеки та ефективності обробки, зберігання й обміну документами в сучасних організаціях.

Мета: Метою даного дослідження є розробка ефективної програми електронного документообігу з використанням блокчейн-технологій, яка забезпечить високу ступінь безпеки, прозорості та незмінності документів в організаціях. Очікуваний результат полягає в створенні такої системи, яка зможе автоматизувати процеси управління документами, підвищити їхню захищеність від несанкціонованого доступу та фальсифікації, а також зменшити вплив людського фактору на обробку й обмін документами.

Завдання:

1. Аналіз теоретичних основ блокчейн-технологій.
2. Дослідження сучасних систем електронного документообігу.
3. Аналіз існуючих рішень на основі блокчейн для документообігу.
4. Розробка концепції програми електронного документообігу.
5. Обґрунтування вибору методів реалізації.
6. Розробка та перевірка системи.
7. Розробка рекомендацій щодо впровадження.

Об`єкт дослідження: Об'єктом дослідження є системи електронного документообігу в організаціях. Це комплекс процесів та технологій, які забезпечують створення, обробку, зберігання, передачу та захист документів в електронному вигляді. Досліджуваний об'єкт охоплює такі аспекти, як безпечність обміну даними, ефективність управління документами, прозорість процесів документообігу.

Предмет: Предметом дослідження є технологічні аспекти впровадження блокчейн у системи електронного документообігу. Це включає в себе дослідження методів застосування блокчейн для забезпечення безпеки, прозорості, незмінності та ефективності обробки й зберігання електронних документів. Основна увага приділяється використанню смарт-контрактів, децентралізованих баз даних та криптографічних алгоритмів для оптимізації процесів документообігу в організаціях.

РОЗДІЛ 1: ОСНОВИ БЛОКЧЕЙН ТЕХНОЛОГІЙ

Визначення та історія розвитку блокчейн.

Блокчейн (blockchain) – "розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), який постійно довшає."[1]. Кожен блок містить набір транзакцій, хеш попереднього блоку і криптографічний підпис, що забезпечує цілісність інформації. Основновна відмінність блокчейну від баз даних традиційного формату це те що він не використовує звичайного центрального сховища, замість цього він використовує децентралізовану розподілену мережу. Система базується на принципах децентралізації, криптографії та консенсусу, саме ці три компоненти забезпечують блокчейн відмінним рівнем захисту.

Технологія блокчейн вперше була представлена у 2008 році анонімною особою або групою осіб під псевдонімом Сатоші Накамото у письмовій роботі "Bitcoin: A Peer-to-Peer Electronic Cash System"[2]. У цій роботі описувалася система, яка дозволяє здійснювати безпечні транзакції без необхідності в централізованому посереднику, що було реалізовано через використання блокчейн як основи для криптовалюти Bitcoin[3].

Перши coin, відомий як Genesis Block, був створений 3 січня 2009 року, це був перший задокументований випадок використання блокчейн технологій у реальних умовах[4]. Bitcoin став прикладом першої

децентралізованої валюти, він зміг довести ефективність децентралізованих технологій завдяки своїм безпеченим транзакціям та розподіленій мережі .

Після успішного Bitcoin, інші блокчейн-проекти почали з'являтися. У 2015 році було представлено Ethereum, основне унікальне для нього на тот момент нововведення було можливість використовувати спеціальні автоматизовані алгоритми під назвою смарт-контракти[5]. Смарт-контракти – це автоматизовані угоди, які виконуються лише після досягнення певних умов, що розширило можливості блокчейн для використання не лише в криптовалютних транзакціях, а й у багатьох інших сферах, таких як фінанси, логістика, страхування та документообіг .

З того моменту як блокчейн Ethereum почав стрімко розвиватись і глобалізуватись, технології почали набувати популярність не тільки як можливість фінансового апарата, але і чудовим способом зберігати та керувати інформацією завдяки своїй децентралізованій природі. Ці фактори спричинили зростання інтересу до блокчейн у різних галузях, включаючи банківську систему, охорону здоров'я, державне управління та корпоративний документообіг. На сьогодні блокчейн активно розвивається, і багато компаній та урядів почали впроваджувати цю технологію для підвищення ефективності та безпеки своїх процесів .

Блокчейн як технологія, еволюціонувала зі звичайної концепції яка підтримувала лише криптовалютні транзакції, то повноцінного багатофункціонального аппарата який займається обробкою і зберіганням даних у системах. Блокчейн 2.0 і 3.0 стали важливими етапами у розвитку технології. Вони зосереджені на інтеграції блокчейн у бізнес-процеси та соціальні структури, відкриваючи нові можливості для таких галузей, як управління ланцюгами постачань, правоохоронна діяльність, енергетика і документообіг.

Таким чином, розвиток блокчейн пройшов кількох етапів: від невідомо нікому технології яка стала популярна тільки зі різким ростом ціни Bitcoin, то фінансового апарату і в результаті до технології децентралізованої системи яка все більше інтегрується у сучасний цифровий світ. Це робить блокчейн ідеальною технологією для систем електронного документообігу, що потребують надійності, прозорості та захисту даних.

Принципи роботи блокчейн.

У технології блокчейн є декілька ключових принципів які забезпечують його безпеку та безперебійну роботу. Такими принципами є децентралізація, криптографічний захист, консенсусний механізм та незмінність даних. Той самий надійний захист та безпеку блокчейну забезпечує взаємозв'язок усіх цих чотирьох принципів, і їх робота.

Децентралізація є основною рисою блокчейн-технології, яка відрізняє її від традиційних централізованих систем зберігання та управління даними [6]. У традиційних системах існує лише один або два центральних вузла, які займаються забезпеченням та керуванням даними. Блокчейн, натомість, є розподіленою мережею, в якій кожен учасник (вузол) має копію всієї історії транзакцій і здатний самостійно перевіряти їхню достовірність. Саме така відсутність у потребі мати певних посредників або централізованих керівників у органах управління і є тим що забезпечує надійність та прозорість системи.

Учасник у цій системі має можливість прийняти на себе роль як споживання даних так і того хто ними керує і хберігає їх. Наприклад, у системах електронного документообігу на основі блокчейн кожен учасник мережі може зберігати копії документів, перевіряти їхню автентичність і долучатися до процесу їхньої передачі, такий вибір розподіленості ролей між користувачами забезпечує надійність системи.

Ключовим елементом технології блокчейн є використання криптографії для захисту даних і забезпечення цілісності інформації [7]. Кожен блок у ланцюжку містить криптографічний хеш попереднього блоку, який створюється за допомогою алгоритмів хешування. Ці алгоритми перетворюють вхідні дані у фіксований розмір рядка символів, так що навіть незначна зміна вхідних даних призведе до кардинальних змін у вихідному хеші. Таким чином, будь-які зміни в даних одного блоку призводять до розриву ланцюга і будуть відразу виявлені .

Ще одна особливість блокчейну це можливість використання ним асиметричного шифрування ключів і даних. Кожен користувач має пару криптографічних ключів – публічний і приватний. Публічний ключ використовується для ідентифікації користувача, а приватний – для підписання транзакцій. Така система дозволяє завжди визначати що нова транзакція була ініційована саме тим користувачем який і підписав її за допомогою свого приватного ключа, подібна система забезпечує анонімність і гарантує безпеку.

Для забезпечення узгодженості та верифікації транзакцій у децентралізованій мережі блокчейн використовується механізм консенсусу [8]. Консенсус – це процес, за допомогою якого всі учасники мережі погоджуються з поточним станом реєстру. Існує кілька різних механізмів консенсусу, які використовуються у блокчейн-системах, серед яких найпопулярнішими є Proof of Work (PoW) та Proof of Stake (PoS) [9, 10].

Механізм Proof of Work став відомим завдяки криптовалюті Bitcoin. Він передбачає, що учасники мережі (майнери) вирішують складні математичні задачі, які вимагають значних обчислювальних потужностей, перший учасник, який вирішить задачу, отримує право додати новий блок у блокчейн і отримати винагороду за свої зусилля. Цей процес передбачає що додавання нових блоків потребує

прикладання значних зусиль, що значно зменшує ризик атаки зі сторони зловмисника, оскільки йому треба буде вирішити задачі усіх попередніх блоків аби відновити інсформацію.

У Proof of Stake на відміну від свого попередника, учасники не потребують обчислювальних ресурсів, щоб додати нові блоки, а натомість використовують свої активи (зазвичай токени або монети) для забезпечення транзакцій. Програма аналізує активи усіх учасників і надає найбільше прав тому у кого більше всього активів. Цей метод є менш енергоємним порівняно з Proof of Work і поступово набирає популярності, особливо після переходу Ethereum на Proof of Stake у 2022 році .

Один із найважливіших принципів блокчейн-технології – це незмінність даних (immutability). Після того, як блок був доданий до блокчейну, змінити його або видалити практично неможливо. Це досягається за рахунок того, що кожен блок зберігає хеш попереднього блоку, і будь-яка спроба змінити дані у вже існуючому блоці змінить всі наступні блоки. Така архітектура гарантує, що всі транзакції, внесені у блокчейн, залишаються незмінними та доступними для перевірки у будь-який час .

Для систем електронного документообігу це означає, що будь-який документ, який був доданий до блокчейн, неможливо змінити без виявлення спроби фальсифікації. Це забезпечує високий рівень надійності і робить блокчейн ідеальним рішенням для управління критичними даними.

Застосування блокчейн у різних галузях

За доволі короткий час, технологія блокчейн технологій дуже сильно розвинулась, від чого набула широкої популярності не тільки у сфері фінансів а і в багатьох різних галузях, завдяки безперебійній

здатності забезпечувати безпеку, прозорість і децентралізацію у своїх системах. Технологія використовується у фінансах, охороні здоров'я, логістиці, урядових структурах, освіті, інтелектуальній власності, а також у системах електронного документообігу.

Найбільшою та найуспішнішою сферою застосування блокчейну можна безумовно виділити фінансові послуги, можливості блокчейну забезпечувати безпечні та швидкі транзакції з фінансами роблять його ідеальним кандидатом для роботи у цій сфері. Система децентралізованих фінансів (DeFi) дозволяє користувачам брати участь у фінансових операціях без традиційних фінансових інституцій. Децентралізовані біржі (DEX), такі як Uniswap, забезпечують торгівлю криптовалютами на основі смарт-контрактів без потреби в централізованій платформі. Більше того, саме в описі першої появи блокчейн технологій а саме у письмовій роботі Сатоші Накамото, блокчейн описується саме як механізм який вирішує проблему подвійних витрат у банківській сфері.

У сфері охорони здоров'я блокчейн допомагає у створенні безпечних і незмінних медичних записів, що можуть бути доступними для медичних працівників і пацієнтів без загрози підробки або втрати даних. Одним із прикладів використання блокчейн у медицині є зберігання та обмін медичними даними пацієнтів на децентралізованих платформах, подібний підхід дозволяє поліпшити контроль над конфіденційністю інформації та одночасно забезпечує доступ до необхідних даних для медичних фахівців.

Що однією галуззю робочого циклу де блокчейн чудово знаходить своє застосування є логістика. Ця сфера завжди потребувала ретельного контролю над ланцюгами постачання та обробки товарів та інформації, від виробника до споживача. Блокчейн значно підвищує прозорість та запобігає підробкам та шахрайству під час будь-яких процесів. Відомі компанії, такі як Walmart, вже використовують блокчейн для

відстеження продуктів харчування, забезпечуючи швидку ідентифікацію джерела продукції в разі виникнення проблем із якістю.

Для посилання на дослідження в логістиці можна звернутися до статті Carson et al. (2018), в якій розглядається вплив блокчейн на глобальні ланцюги постачання [11].

Ще однією потенційною сферою використання блокчейну є урядові структури, вони все більше починають звертати увагу на блокчейн як на спосіб забезпечення прозорості та зменшення корупції. Блокчейн використовується для створення реєстрів власності, які унеможливлюють підробку даних, крім того, технологія може використовуватися для впровадження електронного голосування, яке гарантує анонімність виборців і збереження цілісності результатів. Відомим прикладом є проект Estonian e-Residency, де уряд Естонії використовує блокчейн для захисту електронних послуг і документів[12].

Важливим аспектом використання блокчейн є захист інтелектуальної власності. Блокчейн дозволяє створювати незмінні записи прав на твори мистецтва, музичні твори, патенти тощо. Це дає можливість автоматично фіксувати момент створення твору та підтверджувати права на нього.

Блокчейн також знаходить застосування в освіті, де він використовується для збереження дипломів, сертифікатів та інших академічних документів. Такий підхід дозволяє перевіряти достовірність документів у будь-який момент часу, забезпечуючи автентичність даних і спрощуючи процеси перевірки кваліфікацій.

РОЗДІЛ 2: ПРОГРАМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Визначення електронного документообігу.

Для сучасних організацій та компаній електронний документообіг (ЕДО) є ключовим елементом для забезпечення стабільної роботи всіх процесів. Традиційні способи керування документами вже давно не підходять для використання і не можуть задовольнити навіть малий відсоток потреб організацій. Визначення електронного документообігу можна сформулювати як автоматизований процес створення, обробки, передачі та зберігання документів між учасниками бізнес-процесів з використанням інформаційно-комунікаційних технологій (ІКТ) без необхідності використання паперових носіїв. За допомогою електронного використання подібних систем мінімізуються ризики витрат, підробки документів або збоїв у роботі цілих систем.

Електронний документообіг дозволяє підвищити продуктивність організації завдяки зменшенню часу на підготовку та обробку документів, а також покращити контроль за виконанням завдань. Для забезпечення ефективної роботи програм документообігу використовують захищені канали шифрування, систему електронних підписів, та алгоритми захисту документів на кожному етапі їх обробки. Це дозволяє підприємствам не лише автоматизувати рутинні процеси, але й інтегрувати різні інформаційні системи для комплексного управління документами.

Сутність електронного документообігу полягає в тому, що всі етапи роботи з документами – від їх створення до архівування – виконуються в електронній формі, подібний підхід відкидає ризики пов’язані зі зберіганням документів у фізичному форматі, а саме пошкодження, втрата або несанкціонована зміна файлів. Процеси програм документообігу мають ряд етапів які використовуються для керування документами, це включає в себе: створення документів, їх зберігання, підпис, видалення та переміщення. Також системи контролю документ забезпечують зберігання інформації про час створення або

зміни документу, і інформації про того хто цей документ створив що є дуже важливим процесом аудиту в компаніях.

Електронний документообіг також сприяє більшій прозорості організаційних процесів. Використання подібних сучасних рішень у організаціях дозволяються суттєво зменшити кількість помилок та незрозумілостей які можуть виникати у процесах документообігу, кожна дія та помилка може бути відстежена, і виправлена або змінена. Такі рішення значно спрощують обмін документами між різними структурними підрозділами організацій та зовнішніми партнерами, покращують загальний користувацький досвід і зменшує напруження та тиск на робітників в організаціях. Окрім цього, важливо зазначити, що ЕДО також виступає основою для багатьох сучасних бізнес-систем, таких як системи управління відносинами з клієнтами (CRM), системи управління ресурсами підприємства (ERP) та інші корпоративні платформи, подібні рішення дозволяють корпораціям покращувати процеси обробки документи при цьому не змінюючи кардинально процес роботи.

Водночас, впровадження електронного документообігу вимагає ретельного дотримання нормативно-правових актів та стандартів, що регулюють порядок використання електронних документів, таких як Закон України "Про електронний документообіг" (2015). Згідно з цим документом, електронний документ має ту ж юридичну силу, що і паперовий, за умови дотримання вимог щодо його створення та підписання за допомогою електронного підпису, тому і розробка подібних систем є дуже серйозним процесом який має притримуватись усіх правил та норм.

Традиційні системи електронного документообігу.

Традиційні системи електронного документообігу (ЕДО) відіграють важливу роль у сучасних організаціях, забезпечуючи автоматизацію та централізоване управління документацією. Основним завданням таких систем є забезпечення збереження, обробки, передачі та захисту документів у цифровому вигляді, що дозволяє зменшити обсяги паперових документів та підвищити ефективність бізнес-процесів.

Традиційні системи ЕДО побудовані на основі централізованих баз даних та працюють за архітектурою "клієнт-сервер" [13]. У таких системах документи зберігаються на централізованих серверах, де до них мають доступ користувачі через спеціалізовані клієнтські програми або веб-інтерфейси. У таких системах зазвичай підтримується керування доступом до документів на основі ролей, версійність документів, їх маршрутизація та зберігання. До основних функцій традиційних систем належать:

- Створення та редагування документ**в** — можливість формування електронних документів у різних форматах.
- Зберігання документів — централізоване сховище, яке забезпечує надійне зберігання та захист даних.
- Маршрутизація та контроль — управління процесами узгодження документів, контроль виконання завдань.
- Пошук та індексація — можливість швидкого пошуку документів за ключовими словами, метаданими чи іншими атрибутами.

До традиційних систем ЕДО можна привести приклад програм які вже декілька років використовуються цивілізованим світом для обробки документів.

Microsoft SharePoint — одна з найбільш поширених систем для управління корпоративними документами та організації командної роботи [14]. Ця платформа дозволяє зберігати документи в єдиному централізованому сховищі, управляти правами доступу, забезпечувати колективну роботу над документами, а також інтегрувати документообіг

з іншими бізнес-додатками Microsoft, такими як Office 365 та Exchange Server.

Програмний продукт 1С: Документообіг є типовим прикладом системи ЕДО, яка широко використовується в країнах пострадянського простору [15]. Ця система забезпечує автоматизацію всіх етапів роботи з документами: від їх створення та реєстрації до узгодження, зберігання та архівування. Однією з головних особливостей цієї програми є її інтеграція з цсіма іншими продуктами 1С, що створює цілу екосистему в якій організації можуть організувати комплексне управління фінансами, обліком і документообігом в одній системі.

Alfresco — це відкрита платформа для управління контентом і документами, яка пропонує широкі можливості для інтеграції з іншими системами та розширення функціональності за допомогою відкритого API [16]. Програма Alfresco виставляє свою особливість як можливість підтримки відкритів стандартів та протоколів для обміну даними що робить її універсальним рішенням для різних організаційних потреб.

Проблеми та виклики традиційних рішень.

Не дивлячись на те що системи електронного документообігу вже давно стали невід’ємною частиною бізнес-процесів багатьох організацій, за рахунок того наскільки сильно вони спрощують обробку та керування документами, вони на жаль не позбавлені своїх багатьох викликів та проблем. Ці небезпеки ускладнюю подальший розвиток таких систем особливо на підвищені вимоги до безпеки, конфіденційності та масштабованості.

Одна з головних проблем традиційних ЕДО полягає в їх централізованій архітектурі. Усі дані зазвичай зберігаються на одному або кількох серверах, які стають критичними точками відмови, подібний підхід означає що у випадку якогось сбою системи, або витоку

інформації уся інформація корпорації підпадає під велику загрозу без можливості скрити ще не зачеплені частини документів. Централізація також створює ризики для конфіденційності даних, оскільки неавторизований доступ до центрального сервера може призвести до витоку інформації або її знищення. За даними досліджень, понад 60% організацій, які використовують централізовані системи, стикаються з проблемами доступності даних через збої або атаки на сервери .

Одним із відомих прикладів витоку даних є інцидент у 2017 році, коли в результаті кібератаки на компанію Equifax, яка використовувала централізовану систему зберігання даних, були викрадені особисті дані понад 147 мільйонів користувачів [17], це є лише один із різних випадків того як велика організація стає жертвою витоку інформації, зловмисників або шахраїв.

Питання безпеки завжди було одним із ключових питань та викликів для традиційних систем ЕДО. Незважаючи на те що технології шифрування та захисту інформації розвиваються то неймовірних результатів на сьогоднішній день, і програми ЕДО активно оновлюють і імплементовують нові системи шифрів до своїх процесів, системи все ще залишаються неймовірно вразливими до зовнішніх та внутрішніх загроз. Найчастіше кіберзлочинці використовують фішингові атаки або зловмисне програмне забезпечення для отримання доступу до серверів, на яких зберігаються документи, тому під атакою завжди залишається людина яка працює у компанії та загальний людський фактор. Відомі також випадки, коли працівники компанії, що мають авторизований доступ до системи, зловживали своїми правами для викрадення або зміни важливої інформації. Наприклад, у 2020 році велика американська страхова компанія CNA Financial стала жертвою атаки програмного забезпечення-вимагача, що призвело до блокування доступу до важливих документів компанії [18]. Подібні ситуації змушують

дивитись на перспективи створення нових алгоритмів шифрування зовсім під іншим кутом, враховуючи навіть такі критичні ситуації.

Конфіденційність документів є ще одним проблемним аспектом, особливо для великих організацій, що працюють з персональними або фінансовими даними. Централізовані системи зберігання даних можуть стати мішенню для атаки, що наражає на ризик персональну інформацію користувачів. Для забезпечення відповідності сучасним стандартам захисту даних, таким як GDPR у Європі, традиційні системи повинні проходити складні та дорогі аудити безпеки.

Також необхідно враховувати проблеми технічних аспектів традиційних ЕДО а саме їх обмеженість у масштабованості. З ростом кількості користувачів та обсягу документів, які зберігаються і обробляються системою, продуктивність всіх алгоритмів та процесів може значною мірою сменшетись. Це особливо актуально для великих організацій або компаній з багатьма філіями, які мають доступ до однієї і тієї ж бази документів, оскільки розвиток успішних корпорацій можна привести іноді до геометричної прогресії. У таких випадках часто спостерігається уповільнення роботи системи, що впливає на ефективність бізнес-процесів. Для вирішення цієї проблеми можуть знадобитися значні інвестиції в оновлення серверного обладнання або інфраструктури, що ускладнює подальший розвиток системи.

Наприклад, у компаніях з тисячами співробітників і мільйонами документів виникають проблеми з синхронізацією, доступом і швидкістю обробки даних. У таких випадках традиційні системи можуть не справлятися з навантаженням, що призводить до затримок в обробці документів та зниження продуктивності працівників.

Підтримка традиційних систем ЕДО потребує значних фінансових і технічних ресурсів. Організації повинні не лише забезпечувати безперебійну роботу серверного обладнання, але й постійно оновлювати програмне забезпечення для забезпечення відповідності сучасним

вимогам безпеки та продуктивності. Це включає як регулярне впровадження нових функцій, так і виправлення вразливостей, що вимагає залучення фахівців з IT.

Наприклад, системи, такі як Microsoft SharePoint або OpenText, потребують постійних ліцензійних виплат та підтримки від спеціалістів, що підвищує загальну вартість володіння системою. Крім того, впровадження нових функцій чи оновлень може бути складним процесом, що вимагає детальної підготовки та тестування.

Складність інтеграції з іншими бізнес-системами також є проблемою для традиційних рішень. Більшість старих платформ ЕДО були розроблені як автономні рішення, що ускладнює їх інтеграцію з сучасними ERP, CRM та іншими бізнес-програмами. Це може призводити до дублювання процесів, необхідності ручного введення даних та збільшення кількості помилок при обробці інформації.

У багатьох випадках організаціям доводиться розробляти спеціалізовані модулі або API для інтеграції систем ЕДО з іншими бізнес-інструментами, що додатково збільшує витрати на розробку та підтримку.

РОЗДІЛ 3: ОГЛЯД ІСНУЮЧИХ РІШЕНЬ З ВИКОРИСТАННЯМ БЛОКЧЕЙН ДЛЯ ДОКУМЕНТООБІГУ

Огляд існуючих блокчейн-програм для документообігу.

На сьогоднішній день технологія блокчейн стрімко розвивається, знаходячи своє застосування в багатьох галузях, включаючи фінанси, охорону здоров'я, логістику та, зокрема, електронний документообіг. Традиційні системи управління документами часто стикаються з проблемами безпеки, прозорості та централізації, що робить їх вразливими до витоків інформації та маніпуляцій. Використання

блокчейн-технологій дозволяє розв'язати ці проблеми завдяки децентралізованій природі цієї технології, її незмінності та прозорості.

Вже існує кілька блокчейн-рішень, які спеціалізуються на забезпеченні безпечного зберігання, обробки та передачі документів. Серед них найбільшу популярність здобули такі платформи, як Storj, Factom та Chainpoint [19, 20, 21]. Кожна з цих платформ має свої унікальні характеристики та підходи до реалізації документного обігу, забезпечуючи користувачам високий рівень безпеки та надійності.

Storj – це децентралізована платформа для зберігання даних, яка використовує блокчейн-технології для забезпечення безпеки та ефективного розподілу інформації між різними вузлами мережі. Основна ідея Storj полягає в тому, щоб надати користувачам можливість зберігати файли у зашифрованому вигляді в децентралізованій хмарній інфраструктурі, що робить систему більш безпечною і стійкою до зовнішніх загроз у порівнянні з традиційними централізованими сховищами. Використання технології блокчейн у Storj дозволяє забезпечити прозорість операцій і автентичність даних, оскільки будь-які зміни в системі фіксуються в розподіленій книзі, що унеможливлює несанкціоноване втручання.

Принцип роботи Storj ґрунтується на кількох ключових аспектах, що забезпечують високу ефективність та надійність системи. Перш за все, дані перед зберіганням проходять шифрування на стороні клієнта, що гарантує конфіденційність інформації, навіть якщо один або кілька вузлів мережі будуть скомпрометовані. Це означає, що лише власник файлів має доступ до ключів шифрування, а оператори вузлів не можуть переглядати або змінювати дані. Завантажені файли поділяються на численні фрагменти, кожен з яких зберігається на різних вузлах. Такий підхід забезпечує не лише додатковий рівень захисту, але й дозволяє мінімізувати ризик втрати інформації у випадку виходу з ладу окремих вузлів.

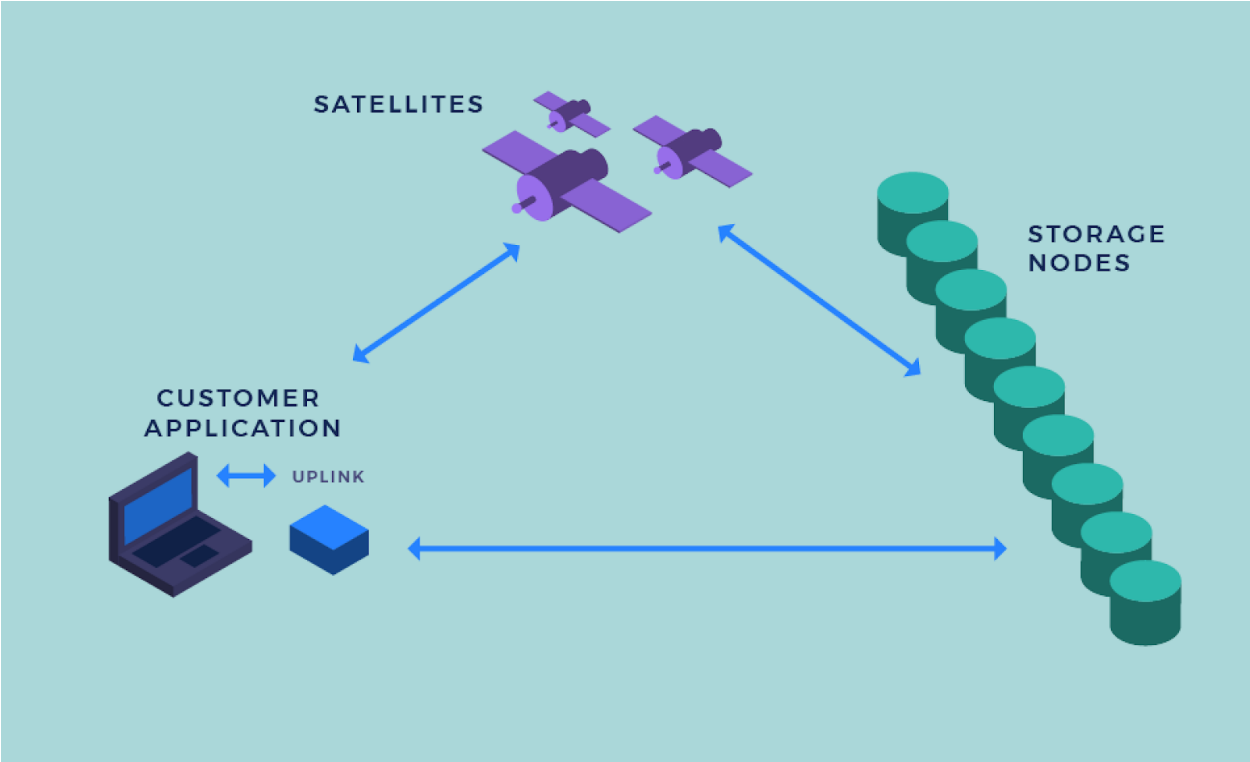


Фото 1. Структура роботи платформи Storj.

Застосування розподіленої мережі для зберігання даних у Storj забезпечує відмовостійкість системи. Навіть якщо кілька вузлів перестануть функціонувати, система може відновити зберігаються файли завдяки наявності копій на інших вузлах. Для перевірки цілісності даних використовуються алгоритми контролю, що постійно моніторять стан фрагментів файлів та забезпечують їх відновлення у разі втрат. Окрім цього, система винагороджує операторів вузлів за надання своїх ресурсів для зберігання фрагментів файлів, використовуючи криптовалюту STORJ як платіжний засіб. Це забезпечує децентралізацію інфраструктури та стимулює участь у мережі нових вузлів, що підвищує масштабованість та надійність системи.

Factom – це блокчейн-платформа, яка спеціалізується на зберіганні та верифікації даних, надаючи можливість впроваджувати децентралізовані системи управління документами та збереження важливої інформації. Основна мета цієї системи – забезпечити незмінність та безпеку даних, використовуючи розподілену мережу блокчейну для фіксації всіх змін, що відбуваються з документами та

іншими цифровими активами. Factom дозволяє зберігати дані за допомогою хешування інформації і подальшого збереження цих хешів у блокчейні, забезпечуючи тим самим високу ступінь захисту від модифікацій.

Принцип роботи Factom ґрунтується на тому, що дані не зберігаються безпосередньо в блокчейні, а лише хеші, які є криптографічними відбитками документів або транзакцій. Це дозволяє системі працювати з великими об'ємами інформації, зберігаючи лише невеликий фрагмент – хеш, який використовується для перевірки достовірності та цілісності даних. Цей підхід також знижує вартість зберігання, оскільки великі документи не потребують запису до блокчейну, а їх верифікація здійснюється шляхом звірки з хешем. Таким чином, Factom надає можливість підтверджувати автентичність будь-яких цифрових активів без необхідності зберігання повної інформації в блокчейні.

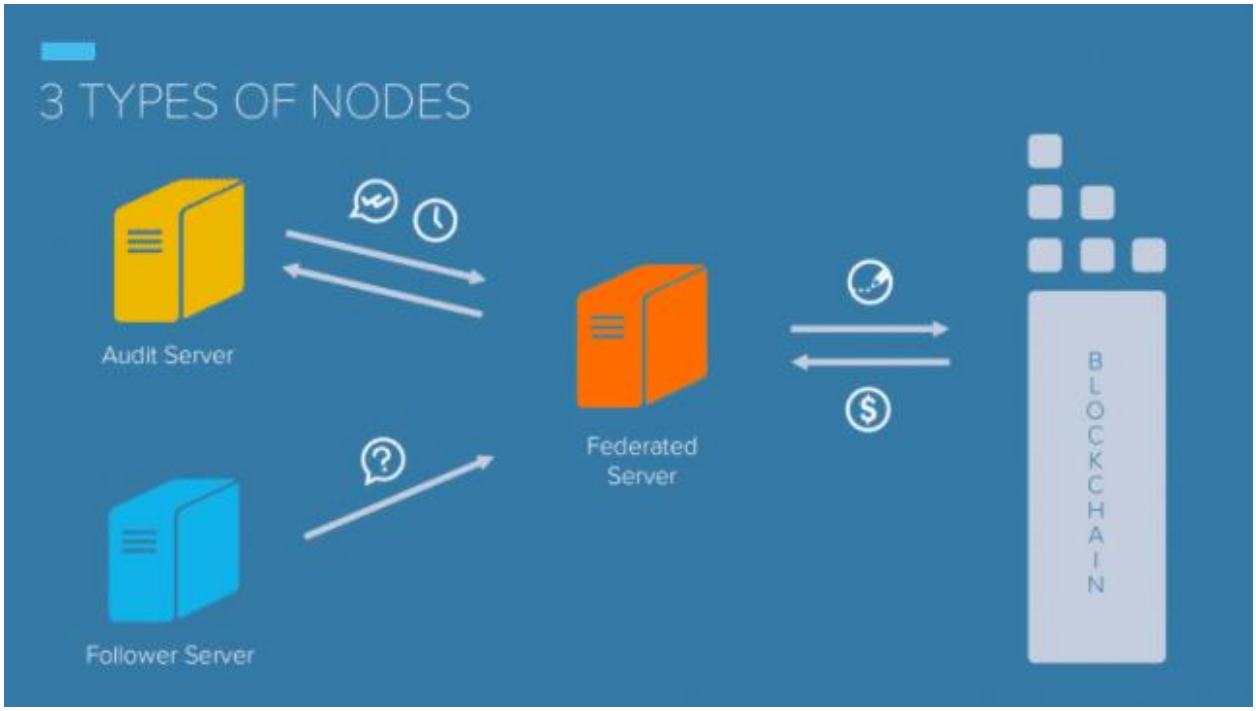


Фото 2. Структура платформи Factom.

Однією з ключових особливостей Factom є використання двох рівнів блокчейну: рівня основних транзакцій і рівня даних. Це дозволяє системі ефективно обробляти великі обсяги інформації, одночасно

забезпечуючи високу швидкість транзакцій і можливість гнучкого управління даними. Платформа використовує механізм консенсусу, який дозволяє децентралізовано підтверджувати верифікацію транзакцій без необхідності звертатися до центрального органу, що робить її надійною та стійкою до зовнішніх атак.

Chainpoint — це децентралізована платформа, яка надає механізм для перевірки достовірності та незмінності даних за допомогою блокчейну, зокрема блокчейну Bitcoin. Основним завданням Chainpoint є створення часових позначок (timestamp) для певних даних або документів, що дозволяє підтвердити факт їх існування на конкретний момент часу без необхідності розкриття самих даних. Цей підхід забезпечує збереження приватності інформації, водночас гарантує її автентичність і неможливість підробки або модифікації в майбутньому.

Принцип роботи Chainpoint ґрунтується на використанні криптографічних хешів. Коли користувач завантажує документ або дані до системи, Chainpoint генерує хеш, який є унікальним цифровим відбитком цих даних. Далі цей хеш записується в блокчейн Bitcoin, створюючи таким чином надійний і незмінний запис. У будь-який момент часу користувач може надати цей хеш та скористатися механізмами платформи для перевірки автентичності даних. Якщо дані були змінені, навіть найменша зміна спричинить зміну хешу, що дозволить легко виявити підробку.

Chainpoint дозволяє використовувати так звану "дерево Меркла" для оптимізації процесу запису і верифікації даних у блокчейні. Ця структура дозволяє групувати велику кількість хешів в один кореневий хеш, який записується до блокчейну, що значно знижує витрати на транзакції. В результаті, система може обробляти і записувати тисячі різних записів до блокчейну за допомогою однієї транзакції, забезпечуючи масштабованість і економічність рішення. Такий підхід робить Chainpoint ефективним інструментом для зберігання великих

обсягів даних у розподілених системах, де необхідна перевірка їх достовірності.

Chainpoint також підтримує можливість інтеграції з різними бізнес-додатками та інформаційними системами, що дозволяє використовувати його в різних галузях: від управління документами та юридичних записів до фінансових транзакцій. Це робить платформу привабливою для організацій, які прагнуть забезпечити довготривале збереження даних та їхню захищеність від модифікацій або фальсифікацій.

Порівняльний аналіз рішень з використанням блокчейн.

Розпочинаючи порівняльний аналіз рішень на основі блокчейн для електронного документообігу, слід зазначити, що кожна з програм — Storj, Factom та Chainpoint — має унікальні особливості та підходи до обробки даних, захисту інформації і реалізації блокчейн-технологій. Їхні принципи роботи базуються на різних архітектурних рішеннях, що дозволяє їм вирішувати проблеми документообігу в різних контекстах. Основними параметрами для порівняння є продуктивність кожної платформи, використання певних типів блокчейну, ціноутворення для користувачів, а також рівень захисту даних.

Платформа	**Storj**	**Factom**	**Chainpoint**
Продуктивність	Висока, завдяки децентралізованій архітектурі зберігання файлів на різних вузлах.	Швидке збереження хешів документів у блокчейні, масштабована система.	Швидке створення та верифікація хешів у блокчейні.

Тип блокчейну	Публічний Ethereum.	Приватний блокчейн з інтеграцією публічних (Bitcoin).	Публічний (Bitcoin).
Ціноутворення	Токен Storj, модель оплати за обсяг збережених даних та смуги пропускання.	Entry Credits, фіксована вартість транзакцій.	Оплата за кількість хешів.
Захист даних	Шифрування файлів перед завантаженням і зберігання на різних вузлах.	Криптографічні хеші документів, самі дані не зберігаються в блокчейні.	Криптографічні хеші, збереження лише доказів існування даних.
Інтеграція з іншими системами	Підтримка API та SDK, сумісність з Amazon S3.	Гнучкі API для інтеграції з бізнес-процесам.	API та SDK для легкої інтеграції в існуючі системи.

Таблиця 1. Порівняльна характеристика Storj, Factom та Chainpoint

Таблиця, представлена вище, слугує основою для порівняння трьох основних рішень у сфері електронного документообігу на базі блокчейн-технологій: Storj, Factom та Chainpoint. Вона відображає ключові характеристики цих платформ, такі як продуктивність, тип блокчейну, ціноутворення, захист даних та можливість інтеграції з іншими системами. Метою таблиці є допомогти у визначенні, яке з рішень найбільш підходить для використання в електронному документообігу в залежності від конкретних вимог та обмежень.

Storj відзначається високою продуктивністю та гнучкістю у зберіганні файлів завдяки децентралізованій архітектурі, що підвищує надійність і доступність даних. Важливою перевагою є його підтримка зберігання великих обсягів даних з розширеною сумісністю з іншими хмарними рішеннями, такими як Amazon S3. Це робить Storj ефективним рішенням для підприємств, які потребують високої масштабованості. Проте використання токенів для розрахунків може бути незручним для компаній, які не звикли працювати з криптовалютами.

Factom вирізняється своєю архітектурою з використанням приватного блокчейну та інтеграцією з публічним блокчейном (Bitcoin), що забезпечує високий рівень безпеки та ефективність в обробці документів. Ця платформа дозволяє зберігати хеші документів, а не самі дані, що підвищує конфіденційність і знижує вимоги до сховища. Однак, необхідність використовувати Entry Credits для здійснення транзакцій може бути складнішою у впровадженні для нових користувачів.

Chainpoint демонструє відмінну продуктивність у процесі створення та верифікації хешів завдяки використанню публічного блокчейну Bitcoin. Ця система є ефективною для зберігання доказів існування документів та їх підтвердження в блокчейні. Незважаючи на те, що Chainpoint не зберігає самі документи, його можливість інтеграції через API та SDK дозволяє легко вбудовувати цю технологію у вже існуючі системи електронного документообігу. Проте обмежений функціонал у роботі з великими обсягами даних може стати недоліком для масштабних проектів.

Storj потребує децентралізованої мережі для зберігання даних, що може бути проблемою у випадку нестабільного інтернет-з'єднання чи недостатньо широкої мережі користувачів. Factom, хоча й забезпечує високу безпеку, може бути менш привабливим через складні механізми розрахунку за транзакції через Entry Credits. Chainpoint, попри

ефективність у створенні хешів, не підходить для зберігання великих обсягів інформації або роботи з великими наборами документів.

РОЗДІЛ 4: РОЗРОБКА СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ БЛОКЧЕЙН

Концепція та загальний огляд програми.

Після проведеного мною аналізу існуючих блокчейн-програм для електронного документообігу, таких як Storj, Factom та Chainpoint, було визначено сильні і слабкі сторони представлених рішень. Ключовими перевагами таких систем є високий рівень безпеки, прозорість та децентралізований характер зберігання даних, що значно знижує ризик витоку або втрати інформації. Однак, одним із найбільших викликів для користувачів є складність інтеграції блокчейн-рішень у вже існуючі корпоративні системи, які вони використовують щодня для управління процесами та документообігом. На практиці це означає, що підприємства не готові кардинально змінювати свої поточні робочі процеси, але прагнуть підвищити безпеку і ефективність, використовуючи нові технології.

На основі цього аналізу було прийнято рішення про розробку власної програми електронного документообігу з використанням блокчейн-технологій, яка, окрім безпечного зберігання даних та прозорості, буде мати унікальну особливість — інтеграцію з сучасними корпоративними системами, такими як ERP та CRM-системи [22, 23]. Це дозволить підприємствам безболісно впроваджувати нове рішення у свої робочі процеси, не змінюючи вже налагоджених моделей роботи.

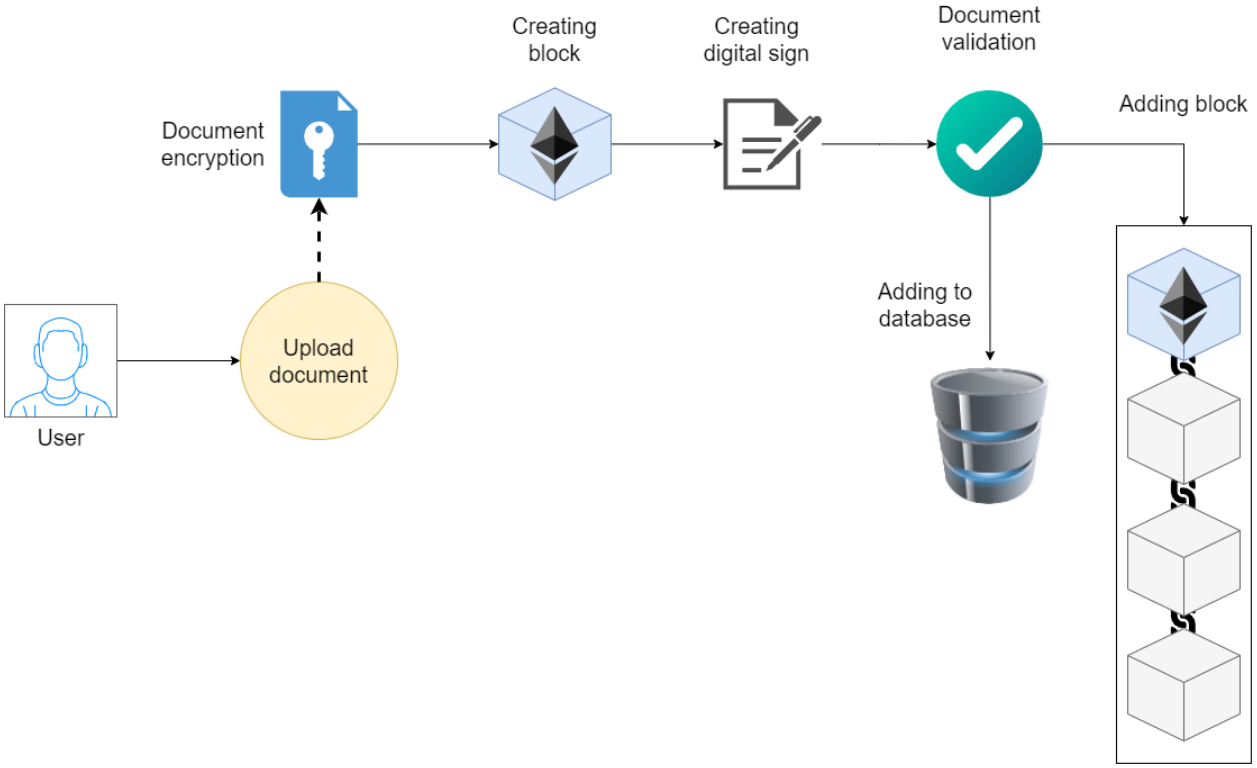
Концепція програми полягає в тому, щоб поєднати переваги блокчейн-технологій з гнучкістю, яку пропонують традиційні корпоративні системи. Це включає можливість автоматичного запису та валідації документів на блокчейні без необхідності повної заміни

існуючих систем. Програма матиме зручний API для інтеграції, підтримку стандартів обміну даними, а також можливість підключення до систем автентифікації, які вже використовуються у компаніях. Це рішення дозволить підприємствам плавно переходити на блокчейн-інфраструктуру, не ризикуючи перериванням бізнес-процесів і зберігаючи знайомі інтерфейси для користувачів.

Приклад використання такого продукту може виглядати таким чином: програма документообігу буде інтегрована з корпоративними системами за допомогою API (інтерфейс прикладного програмування), що дозволить обмінюватися даними між блокчейн-платформою та вже існуючими бізнес-додатками. Наприклад, компанія може використовувати популярну ERP-систему, як SAP або Oracle, для управління фінансовими операціями, контролю постачання та внутрішнього документообігу. Завдяки інтеграції, будь-який документ, який буде створений або оброблений у ERP, автоматично фіксуватиметься в блокчейн-мережі для збереження його прозорості та неможливості змін.

Уявімо конкретний сценарій: співробітник бухгалтерії компанії за допомогою ERP-системи створює платіжне доручення для постачальника. Коли документ готовий, система надсилає його до блокчейн-програми, де цей документ фіксується як незмінний запис. Після цього блокчейн забезпечує цифровий підпис та валідацію цього документа. Співробітники, що працюють з ERP, бачитимуть це як частину їхнього звичного процесу без необхідності заходити в нові інтерфейси або додаткові системи. Якщо ж виникне потреба перевірити легітимність документа, користувачі ERP зможуть це зробити безпосередньо з інтерфейсу ERP, оскільки інформація про документ і його стан буде синхронізована через API з блокчейн-програмою. Ключова перевага такої інтеграції — це те, що вона дозволяє користувачам взаємодіяти з блокчейн, навіть не усвідомлюючи, що вони

користуються блокчейн-технологіями. Для них це буде виглядати як автоматичний процес, де всі документи стають прозорими, незмінними та доступними для перевірки в будь-який момент. Це створює ефективну систему управління документами, яка мінімізує ризики втрати інформації, полегшує аудит та підвищує довіру до бізнес-процесів, залишаючи користувачів у звичному середовищі корпоративної системи.



Діаграма 1. Діаграма роботи програми.

Основний варіант архітектури програми буде включати в себе створення веб-додатку, який дозволить користувачам, у тому числі тим, хто не працює з корпоративними системами, напряму взаємодіяти з платформою документообігу. Цей додаток надасть доступ до таких функцій, як перегляд та валідація документів, створення нових документів, відслідковування їх змін та управління правами доступу. Така платформа буде веб-додатком з адаптивним дизайном, який можна використовувати як через браузер, так і через мобільні пристрої, що додасть мобільності для користувачів. Додатково це буде включати в себе інтеграцію у вигляді плагіну для браузера, наприклад, на кшталт

Metamask [24]. Це дозволить користувачам зберігати доступ до своїх документів безпосередньо у браузері та взаємодіяти з блокчейном напряму, коли вони працюють в інтернеті.

Вимоги до системи та ключові технічні аспекти.

Прототип програмного продукту програми документообігу буде включати в себе декілька окремих клієнтських програм, таких як: веб-додаток, мобільний додаток та плагін для браузерів. Платформа буде мати одну основну серверну частину яка буде відповідати за взаємодію з блокчейном. У цьому підрозділі будуть представлені вимоги до усіх компонентів програмного продукту.

Вимоги до веб-додатку. Основний веб-додаток служитиме як інтерфейс для користувачів для взаємодії з системою документообігу. Важливо, щоб цей додаток був максимально зручним, надійним та забезпечував швидкий доступ до всіх функцій. Ось ключові вимоги до веб-додатку:

1. **Кросплатформенність**: Веб-додаток повинен працювати на всіх основних браузерах (Chrome, Firefox, Safari, Edge), а також бути адаптованим до різних розмірів екрану, щоб забезпечити доступ як на десктопах, так і на мобільних пристроях.
2. **Захист даних**: Забезпечення безпеки передачі документів та їх шифрування під час зберігання та передачі між клієнтом і сервером є ключовою вимогою.
3. **Інтеграція з корпоративними системами**: Важливою є можливість інтеграції з існуючими системами документообігу, наприклад, через API або плагіни для браузера.
4. **Підтримка електронного підпису**: Веб-додаток має включати механізми для генерування та перевірки електронних підписів на документи.

Вимоги до мобільного додатку. Окрім веб-додатку, мобільний додаток є важливою частиною для забезпечення доступу до системи з будь-якої точки. Ключові технічні вимоги до мобільного додатку такі:

1. **Мультиплатформенність**: Мобільний додаток повинен підтримувати операційні системи iOS та Android. Для цього можна використовувати фреймворки на кшталт React Native або Flutter.
2. **Офлайн доступ**: Необхідно передбачити можливість роботи в офлайн-режимі з подальшою синхронізацією даних після відновлення підключення до мережі.
3. **Швидкий доступ до документів**: Мобільний додаток має забезпечувати швидкий доступ до ключових документів, з можливістю їх завантаження та редагування в межах дозволених функцій.
4. **Безпечна автентифікація**: Додаток має підтримувати двофакторну автентифікацію або біометричну автентифікацію для підвищення безпеки.

Вимоги до серверної частини. Серверна частина системи є ключовою для обробки запитів користувачів та взаємодії з блокчейном. Вимоги до серверної інфраструктури включають:

1. **Масштабованість**: Система повинна бути готова до обробки великої кількості одночасних запитів і підтримувати горизонтальне масштабування для забезпечення стабільної роботи.
2. **Інтерактивність з блокчейном**: Сервер повинен ефективно взаємодіяти з обраним блокчейном для запису та читання даних. Це включає підтримку функцій смарт-контрактів, створення транзакцій та збереження інформації на децентралізованих вузлах.
3. **API для зовнішніх систем**: Необхідно розробити REST або GraphQL API для забезпечення взаємодії з іншими корпоративними системами та мобільними додатками.

4. **Захист даних**: Серверна частина має підтримувати захищене шифрування та механізми аутентифікації для забезпечення конфіденційності користувачів.

Вимоги до блокчейну. Вибір блокчейну є одним із ключових рішень у проєкті, адже саме блокчейн буде використовуватися для зберігання й підтвердження документів. Для цієї системи необхідно обрати блокчейн з такими характеристиками:

1. **Тип блокчейну**: Найкращим вибором є приватний або гібридний блокчейн, щоб забезпечити необхідний рівень конфіденційності при зберіганні документів та водночас використовувати переваги децентралізації.
2. **Продуктивність**: Блокчейн повинен забезпечувати високу швидкість транзакцій для обробки документів у реальному часі. Для цього можуть бути обрані платформи з високою пропускною здатністю, наприклад, Hyperledger або Corda.
3. **Можливість інтеграції**: Обраний блокчейн має мати прості механізми для інтеграції з корпоративними системами та можливість створення смарт-контрактів для автоматизації документальних процесів.
4. **Безпека**: Забезпечення безпеки та цілісності даних через алгоритми консенсусу, а також захист від атак типу "51%" є критично важливим.

Використання смарт-контрактів для автоматизації процесів.

Смарт-контракти – це програми, які виконуються автоматично на блокчейні за умови виконання певних заздалегідь визначених умов. У контексті системи документообігу це означає, що смарт-контракти дозволяють автоматично виконувати процедури, пов'язані з обробкою, затвердженням, перевіркою або передачі документів без необхідності

втручання людини чи інших зовнішніх учасників. Смарт-контракти забезпечують автоматизацію ключових процесів, включаючи укладання угод, проведення перевірок документів, обробку транзакцій і моніторинг виконання зобов'язань.

Залежно від складності та функціоналу смарт-контракти можуть бути різними:

Прості смарт-контракти – це контракти, які виконують прості дії, такі як автоматичне зберігання або передача документів після підтвердження отримання необхідних підписів. Вони можуть виконувати елементарні операції, такі як підтвердження згоди сторін або автоматичне зберігання документів у захищеній базі даних.

Мультифункціональні смарт-контракти – ці контракти підтримують складніші умови та дії. Вони можуть виконувати взаємодію між кількома сторонами або системами, перевіряти стан виконання певних етапів процесу, генерувати звіти, чи навіть запускати автоматичні оплати за надані послуги після успішного виконання документа.

Смарт-контракти для динамічного керування документами – ці контракти використовуються для процесів, де документи проходять через кілька етапів затвердження. Контракт забезпечує, щоб кожен етап був виконаний, перед тим як документ переходить до наступного стану, наприклад, коли документ повинен пройти через різні рівні затвердження.

Після аналізу видів смарт-контрактів і окреслення потреб свого продукту я обрав декілька видів смарт-контрактів які будуть інтегровані у мій програмний продукт.

По-перше, необхідним буде смарт-контракт для електронних підписів, який забезпечуватиме підтвердження автентичності документів на кожному етапі їх обробки. Цей контракт зберігатиме електронні

підписи на блокчейні, що дозволить гарантовано підтвердити особу підписанта і забезпечити цілісність документа.

По-друге, важливим елементом стане смарт-контракт для автоматичного розподілу документів, який відповідатиме за передачу документів на наступні етапи обробки залежно від статусу попередньої дії. Наприклад, після затвердження документа контракт автоматично передасть його до відповідного відділу для подальшої обробки, зменшуючи ризик людських помилок і затримок.

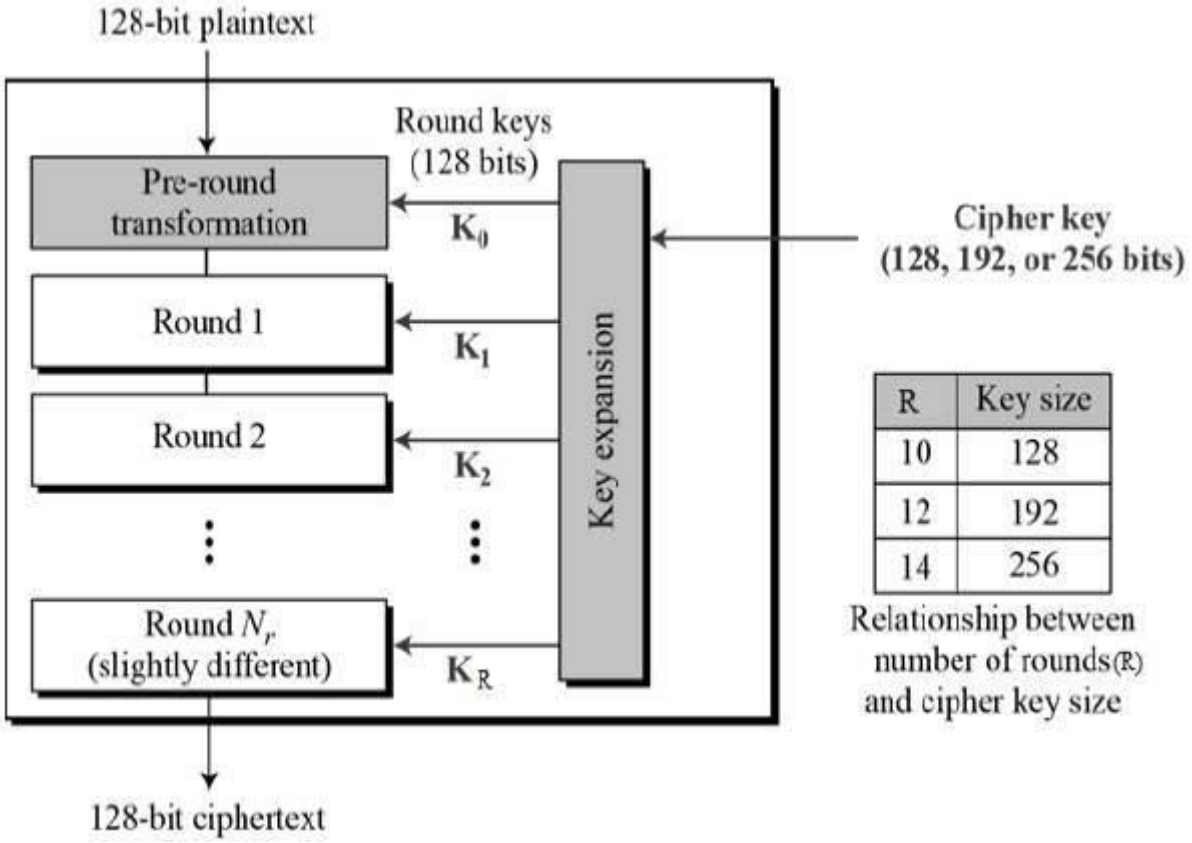
Третім важливим типом смарт-контракту є контракт для перевірки статусу виконання угод. Цей контракт надасть можливість моніторити виконання угод або зобов'язань, автоматично перевіряючи умови, такі як строки виконання чи етапи реалізації. Завдяки цьому, користувачі отримуватимуть сповіщення про будь-які затримки або виконання зобов'язань, що сприятиме своєчасному реагуванню на зміни в процесі.

І останнім не менш важливим контрактом буде смарт-контракт для перевірки звітності та аудиту. Цей контракт дозволить зберігати всю інформацію про дії з документами на блокчейні, створюючи умови для детального аудиту та звітності, завдяки такій прозорості, користувачі зможуть відстежувати кожен етап життєвого циклу документа, що підвищить надійність і довіру до системи в цілому. Всі ці смарт-контракти разом забезпечать ефективність, безпеку і зручність використання системи електронного документообігу, що, в свою чергу, сприятиме її прийняттю в корпоративному середовищі.

Захист і безпека даних у системі.

У системах електронного документообігу, які використовують блокчейн, важливо зосередити увагу на безпеці та захисті даних. Одним із ключових інструментів забезпечення безпеки є шифрування. Документи, що зберігаються чи передаються через систему, будуть

зашифровані за допомогою сучасних криптографічних алгоритмів, наприклад AES-256 [25]. Це гарантує, що навіть у випадку несанкціонованого доступу до документа, його зміст залишиться недоступним для сторонніх осіб. Шифрування забезпечує конфіденційність даних як під час передачі, так і зберігання в блокчейні.



Діаграма 2. Структура роботи алгоритму шифрування AES-256

Алгоритм шифрування AES-256 працює шляхом перетворення відкритого тексту в зашифрований через послідовність математичних операцій. Основою алгоритму є симетричне шифрування, що означає використання одного й того ж ключа для шифрування і розшифрування даних. Ключ має довжину 256 біт. Процес включає кілька етапів, таких як підстановка, перестановка і змішування блоків даних, при цьому всі операції виконуються на рівні байтів.

Ще одним важливим аспектом є застосування цифрового підпису для верифікації. Цей механізм дозволяє підтвердити цілісність і справжність документів, оскільки кожен документ буде підписаний автором за

допомогою унікального цифрового підпису. Верифікація підпису здійснюється за допомогою криптографічних ключів, що зберігаються в блокчейні. Це робить неможливим несанкціоноване редагування чи підробку документа. До того ж, цифровий підпис стане підтвердженням авторства та дозволить відстежити, хто і коли створив або затвердив документ, що підвищує рівень довіри до системи.

Блокчейн, зі свого боку, забезпечує додатковий рівень захисту завдяки своїй децентралізованій природі. Кожен запис у блокчейні є незмінним, що дозволяє фіксувати будь-які зміни або спроби маніпуляцій з документами чи їх метаданими. Оскільки блокчейн є розподіленою системою, всі користувачі мають доступ до повного ланцюга записів, що робить спроби несанкціонованих змін надзвичайно складними.

Отже, система передбачає кілька рівнів безпеки: шифрування для захисту змісту, цифровий підпис для підтвердження автентичності та блокчейн для забезпечення незмінності і прозорості усіх дій із документами. Усе це забезпечує високий рівень захисту даних і надійність роботи системи в корпоративних умовах.

РОЗДІЛ 5: ТЕХНІЧНА РЕАЛІЗАЦІЯ СИСТЕМИ

Вибір платформи для розробки блокчейн-системи.

Після проведеного аналізу існуючих технологій та потреб мого проєкту блокчейн документообігу, мною був обраний ряд технологій та компонентів які будуть використовуватись у якості інструментів для розробки програмного продукту моєї системи. Рішення приймається не тільки на основі потреб програми, а і на основі того наскільки обрані компоненти будуть мати інтеграцію один з одним, оскільки платформа документообігу повинна надавати доступ до себе через веб-додаток,

мобільний додаток, браузерний плагін і також мати стабільну серверну частину для можливості швидкої відповіді на запити користувачів.

Фронтенд частина веб-додатку розроблятиметься з використанням бібліотеки React, яка вже довела свою ефективність у створенні масштабованих та інтерактивних користувацьких інтерфейсів. Саме продуктивність та гнучкість цієї бібліотеки робить його відмінним кандидатом для створення такої комплексної платформи. Великий спектр додаткових бібліотек значно спрощує та пришвидшує процес розробки завдяки масі готових рішень інтеграції з іншими системами.

Для мобільної версії платформи обрано **React Native**, оскільки ця технологія дозволяє розробляти кросплатформенні мобільні додатки з використанням тієї ж самої логіки та структури, що й у веб-додатку. Це значно прискорює процес розробки та спрощує підтримку двох версій програми — веб- та мобільної. Крім того, React Native дозволяє використовувати спільний код між платформами, що знижує витрати на розробку та оптимізує загальну продуктивність системи.

Для серверної частини був обраний Node js. Він є популярним вибором для створення серверних частин платформ завдяки своїй гнучкості та простоті використання. Node js має великий обсяг бібліотек та додатків які спрощують процес розробки і покращують інтеграцію з різними платформами. Подібна інтеграція стає особливо важливою враховуючи те що природа мого продукту буде основана навколо взаємодії з платформами блокчейн. Також Node js славиться для створення масштабованих серверних модулів завдяки своїй асинхронній архітектурі та високій продуктивності. Це дозволяє ефективно обробляти одночасні запити, що є важливим для документообігу, де велика кількість користувачів може одночасно взаємодіяти з системою.

Основним елементом, який забезпечуватиме захист даних і прозорість, стане приватний блокчейн, заснований на платформі Quorum. Вибір даного компоненту є критично важливим для усієї

структури моєї програми. Quorum — це форк Ethereum, оптимізований для корпоративних рішень, що дозволяє створювати приватні мережі з підтримкою конфіденційних транзакцій. Його висока продуктивність і високий рівень приватності робить цей блокчейн ідеальним кандидатом для платформи документообігу для корпорацій. Приватність цього блокчейну забезпечує максимальний контроль над доступом до даних та їх безпекою, що є критично важливим для документообігу.

Останнім елементом для архітектури є вибір сервісу для розгортання блокчейн платформи. Для виконання цієї задачі було обрано Amazon Web Services (AWS) [27]. AWS пропонує надійні сервіси для хмарного хостингу та управління блокчейн-мережами, зокрема підтримку Quorum. Хмарна інфраструктура AWS дозволяє легко масштабувати систему відповідно до потреб користувачів, забезпечуючи високу продуктивність та стійкість до збоїв.

Таким чином вибір технологій та компонентів для розробки програми документообігу з використанням блокчейн технологій був зроблений ретельно з урахуванням усіх сучасних стандартів розробки програмного забезпечення та з урахуванням потреб майбутнього продукту. Головним плюсом є те що представлені технологій мають високий рівень маштабованості що дозволяє повноцінний подальший розвиток програми і додавання нових технологій.

Опис архітектури і основних компонентів.

Після того як технології розробки програми були обрані, та їх використання затверджене, був розписаний план взаємодії усіх цих програм та компонентів які разом утворювали архітектуру платформи.

Фронт-енд частина яка розроблена за допомогою React буде представляти собою користувацький інтерфейс який буде створений по стандартам та принципам UI/UX дизайну для забезпечення найкращого

користувацького досвіду перебування на сайті [28]. Компонентна архітектура React дозволяє створювати кожний функціональний елементи (наприклад, завантаження документів, відстеження їхнього стану, або підписання) окремо один від одного, завдяки чому вони можуть бути використані окремо в різних частинах веб-додатку, а також такий підхід забезпечує швидкодію сайту що покращує користувацький досвід. Фронтенд безпосередньо взаємодіє із серверною частиною за допомогою API-запитів. Коли користувач завантажує документ або підписує його, ці дані відправляються через HTTP-запити на сервер, який працює на Node.js.

Node.js на сервері виконує роль мосту між клієнтом (React) і блокчейном (Quorum). Коли користувач виконує будь-яку дію з документами (надсилає їх, видаляє, змінює) то задача серверу отримати цей запит, перевірити його валідність, зберегти у базі даних або файловій системі (за необхідності), та обов’язково згенерувати транзакцію запису цієї дії на платформі блокчейн. Node.js обробляє логіку взаємодії з блокчейном, використовуючи Quorum API для створення смарт-контрактів і транзакцій.

Quorum, як приватний блокчейн, служить ядром безпеки та прозорості системи. Кожна важлива дія з документами, така як створення, підписання, редагування або видалення, записується у вигляді транзакцій у блокчейн. Використання приватного блокчейну на основі Quorum забезпечує конфіденційність і контрольованість доступу, оскільки лише авторизовані учасники мережі мають змогу бачити та взаємодіяти з даними. Інтеграція Quorum з серверною частиною на Node.js відбувається через спеціальну бібліотеку для взаємодії з блокчейном,web3.js що забезпечує зручний інтерфейс для роботи з блокчейн-запитами.

Для того аби можна було зберегти повноцінні доступ до системи через мобільні пристрої буде створений мобільний додаток з

використанням React Native. Мобільний додаток, побудований на React Native, використовуватиме ті ж самі API, що і веб-додаток, для взаємодії з сервером і блокчейном. Основна перевага React Native полягає в можливості використовувати спільну кодову базу для мобільних додатків на iOS та Android, що зменшує витрати на розробку та підтримку. За допомогою мобільного додатку користувачі зможуть користуватися абсолютно усіма можливостями платформи використовуючи лише свої мобільні пристрої.

І загалом вся ця інфраструктура буде розгорнута на платформі Amazon Web Services (AWS), що надасть можливості для легкого масштабування системи, та керувати її ресурсами. AWS надасть хмарні сервери для розгортання Node.js сервера, забезпечуючи швидку та стабільну роботу системи. Блокчейн платформа Quorum також може бути розгорнута на AWS що забезпечить можливість легкого та надійного керування вузлами системи. рім того, AWS надає інтегровані засоби безпеки для захисту від атак і забезпечення конфіденційності даних.

Таким чином була створенна архітектура роботи платформи документообігу з використанням блокчейн технологій, складений план дозволяє розписати всі етапи розробки та розбити її на декілька модулів що зручно при роботі з компандою та перспективно для подальшого масштабування програми.

Алгоритм функціонування програми.

Реалізація системи подібного формату де дії користувачів з документами такі яка (створення, видалення, зміна) записуються не тільки у серверну частину а ще і блокчейн, потребують спеціального функціоналу для роботи. Для зручного та масшатабованого способу взаємодії серверної частини Node js та блокчейну були розроблені

спеціальні алгоритми з використанням бібліотеки web3.js. Web3.js — це популярна JavaScript бібліотека, яка дозволяє взаємодіяти з блокчейн-мережею Ethereum та іншими сумісними мережами. Вона використовується для взаємодії з блокчейном через смарт-контракти, надсилання транзакцій, отримання інформації про блоки та події, а також управління криптографічними ключами.

У цьому підрозділі ми розглянемо декілька алгоритмів програми які відповідають за взаємодію з блокчейном.

```
const hre = require("hardhat");

async function main(){
   const [deployer] = await hre.ethers.getSigners();

   console.log("Deploying contract with account", deployer.address);

   const DocumentRegistry = await
hre.ethers.getContractFactory("DocumentRegistry");
   const documentRegistry = await DocumentRegistry.deploy();

   console.log("Contract deployed to: ", documentRegistry.runner.address);
}

main().catch((error) => {
   console.error(error);
   process.exitCode = 1;
})
```

Блок коду 1. Скріпт deploy.js.

У блоку коду вище представлений функціонал скріпту для деплою документу задача якого це деплой та запуск смарт контракту DocumentRegistry на блокчейн Ethereum.

Робота алгоримту:

- Спочатку сервер підключається до адерси людини яка деплоїть смарт-контракт.
- Далі алгоритм завантажує смарт-контракт DocumentRegistry.
- Після чого викликається функція deploy() для деплою смарт-контракту.
- Для вилову помилок була написана функція catch яка перевіряє роботу алгоритму на певні помилки (наприклад якщо на адресі не вистачить коштів аби заплатити за комісію)

Зі сторони роботи програми це виглядає так, коли користувач завантажує документ, серверна частина зберігає файл у сховищі або локальній базі даних. Потім хеш файлу розраховується і відправляється на блокчейн, де він записується в смарт-контракті. Далі система дозволяє легко перевіряти цілісність документа перевіряючи його хеш зі записом у блокчейні. Якщо хеші збігаються то документ не був змінений.

Далі розглянемо смарт-контракт який відповідає з збереження документа.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract DocumentRegistry{
    struct DocumentMeta{
        string hash;
        uint256 timestamp;
        uint256 userId;
```

```
    }

    mapping(string => DocumentMeta) public documents;

    event DocumentStored(string hash, uint256 timestamp, uint256 userId);

    function storeDocumentMeta(string memory hash, uint256 timestamp,
uint256 userId) public {

        require(bytes(documents[hash].hash).length == 0, "Document already
exists");

        documents[hash] = DocumentMeta(hash, timestamp, userId);
        emit DocumentStored(hash, timestamp, userId);
    }
}
```

Блок коду 2. Смарт-контракт DocumentRegistry.

Цей смарт-контракт дозволяє зберігати документи, хешувати їх для перевірки автентичності, а також надає можливість отримати інформацію про документ. Його функціонал виглядає таким чином:

- storeDocumentMeta : Функція для додавання нового документа. Вона отримує на вхід хеш документа та його назву, перевіряє, чи такий документ уже існує, і зберігає інформацію у блокчейні.

У програмі буде використовуватись декілька смарт-контрактів для взаємодії з документами, вони будуть виконувати важливу роль в функціонуванні платформи забезпечуючи автоматичні процеси.

Тестування і перевірка працездатності системи.

Тестування блокчейн програм є критично важливим етапом під час розробки подібної платформи, оскільки подібний процес передбачає підтвердження правильності функціонування системи та гарантування її безпеки. Основні типи тестування включають в себе функціональне тестування, тестування продуктивності та тестування безпеки.

Функціональне тестування є стандартним етапом в розробці будь-якого програмного продукту і не є чимось унікальним виключно для блокчейну. На цьому етапі проводится перевірка того чи всі функції системи відповідають вимогам які були описані на етапі проєктування. Це включає в себе тестування основних функцій системи, таких як створення, підписання, зберігання та передачу документів.

Тестування продуктивності оцінює те як система справляється з навантаженням при високій активності користувачів. Тут буде важливо протестувати швидкість обробки транзакцій, час, необхідний для підтвердження операцій у блокчейні, та загальну стійкість системи під час пікових навантажень. Особливу увагу на цьому етапі під час тестування блокчейн програми необхідно приділити тому наскільки оптимально смарт-контракти використовують газ під час своєї роботи [29]. Комісія за газ це - “це поширений термін для позначення вартості, яку певні користувачі блокчейн-протокол сплачують мережевим валідаторам кожного разу, коли хочуть виконати якусь функцію в блокчейні” [29]. Тобто газ це певна комісія яку необхідно сплачувати при роботі з блокчейном, ца цим треба особливо уважно слідкувати людям які займаються розробкою смарт-контрактів для платформи, оскільки абсолютно кожна функція у контракті використовує газ для роботи, економія повинна стимулювати програмістів писати чистий та оптимізований код.

Тестування безпеки є особливо критичним для блокчейн додатків, оскільки це саме те за що блокчейн і використовують. Для блокчейн програми треба проводити аудити безпеки, перевіряючи, як система

реагує на спроби злому, а також чи забезпечуються належні механізми шифрування та аутентифікації.

Конкретно для моє програми були проведені такі тестувальні процедури.

- Були перевірені функції шифрування та розшифрування яка відіграють критичну роль у забезпеченні безпеки програми.
- Були проведене тестування верифікаційних підписів для підтвердження
  автентичності документів.
- Був проведений аудит безпеки для виявлення потенційних загроз та вразливостей системи.
- Була проведена перевірка на швидкість обробки транзакцій у блокчейні під різними умовами навантаження.
- Було проведено тестування на стабільність інтеграції програми з існуючими корпоративними системами, аби впевнитися що цей функціонал працює без збоїв.

Проведені тести підтвердили високий рівень захисту системи, показали високі показники продуктивності при високому навантаженні, та аналіз підтвердив що всі функції шифрування та розшифрування працюють без проблем.

Можливі удосконалення та майбутні напрями розвитку.

Після того як розробку основного функціоналу прототипу програми документообігу було завершено, був розроблений план розвитку цієї програми у майбутньому. Розробка нового та покращення вже існуючого функціоналу підвищить працездатність платформи, привабливість для користувачів та конкурентоспроможність програми на ринку. Було розглянуто декілька напрямків для розширення функціоналу, що можуть забезпечити додаткові переваги системі.

Одним із можливих удосконалень є інтеграція з хмарними сервісами для зберігання документів. Це дозволить розширити можливості зберігання великих обсягів даних поза блокчейном, при цьому зберігаючи метадані в блокчейні для забезпечення безпеки та контролю доступу. Подібне рішення грано вплине на загальну картину платформи оскільки це розширить той саме функціонал який робить її унікальною а саме інтеграція з сучасними системами які використовують більшість корпорацій та користувачів сучасності.

Ще одним важливим напрямом розвитку є впровадження механізмів автоматизації на основі смарт-контрактів. Прототип програмного продукту на даний момент має основні смарт контракти для роботи з документами, проте їх функціонал завжди можна покращити або доповнити, одним з варіантів є це написання більш просунутих смарт-контрактів як матимуть алгоритми автоматизації різних процесів. Ці контракти можуть бути використані для автоматичного виконання певних умов або дій при роботі з документами, наприклад, автоматичного затвердження або передачі документа після виконання певних критеріїв. Це дозволить підвищити ефективність процесів і зменшити людський фактор у повсякденних операціях, що особливо важливо в корпоративному середовищі.

Також варіантом яки зараз стає все більш актуальним це є додавання функції штучного інтелекту. Наприклад, система могла б використовувати алгоритми машинного навчання для аналізу вмісту документів та рекомендацій щодо їхнього зберігання, обробки або розподілу. Або завжди гарним рішенням є створення інтелектуального помічника на платформі для спрощення роботи користувачам. Ці нововведення допомогли б спростити управління документами в умовах великого обсягу інформації.

Реалізація цих удосконалень не лише підвищить функціональність системи, але й збільшить її привабливість для організацій, які прагнуть

оптимізувати свої бізнес-процеси та підвищити безпеку документів. Ширший спектр можливостей для інтеграції та автоматизації зробить систему більш універсальною, що позитивно вплине на попит на неї в корпоративному секторі.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи на тему “Розробка програми документообігу яка використовує блокчейн технології” були досягнені усі цілі та розв’язані всі задачі які були поставлені на початкових етапах розробки.

Перш за все, мною був проведений ґрунтовний аналіз існуючих рішень у сфері електронного документообігу, заснованих на блокчейн технологіях. На основі цього аналізу були виділені сильні та слабкі сторони різних платформ, що дозволило визначити ключові аспекти, які варто інтегрувати в нову програму для досягнення конкурентних переваг.

Після цього була розроблена архітектура системи, що відповідає вимогам сучасних користувачів та забезпечує інтеграцію з корпоративними системами. Після аналізу існуючих технологій та популярних рішень для розробки програмного забезпечення були обрані найоптимальніші технології для розробки проєкту на всі етапи (фронеенд, бек-енд, блокчейн).

Після того як аналіз рішень у сфері блокчейн документообігу був завершений та спроєктована архітектура програми був розроблений прототип програмного продукту, який задовольняє всі технічні та функціональні вимоги, поставлені на початку роботи. Прототип було протестовано з технічної точки зору та з боку користувачів для забезпечення належної функціональності та зручності у використанні. Особлива увага була приділена захисту даних, де були використані шифрування та верифікація транзакцій у блокчейні для забезпечення максимального рівня безпеки.

Отже, в результаті виконання роботи було розроблено комплексне рішення для документообігу на основі блокчейн технологій, яке забезпечує високу продуктивність, безпеку, зручність для користувачів

та інтеграцію з існуючими корпоративними системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Визначення Blockchain (https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD#:~:text=%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD%20(%D0%B0%D0%BD%D0%B3%D0%BB.,%D0%B1%D0%BB%D0%BE%D0%BA%D1%96%D0%B2)%2C%20%D1%8F%D0%BA%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%82%D1%96%D0%B9%D0%BD%D0%BE%20%D0%B4%D0%BE%D0%B2%D1%88%D0%B0%D1%94.). Дата візиту ресурсу: 24.10.24
2. Сатоші Накамото (https://uk.wikipedia.org/wiki/%D0%A1%D0%B0%D1%82%D0%BE%D1%81%D1%96_%D0%9D%D0%B0%D0%BA%D0%B0%D0%BC%D0%BE%D1%82%D0%BE). Дата візиту ресурсу: 24.10.24
3. Bitcoin whitepaper (https://bitcoin.org/bitcoin.pdf). Дата візиту ресурсу: 24.10.24
4. Genesis Block (https://en.bitcoin.it/wiki/Genesis_block). Дата візиту ресурсу: 24.10.24
5. Ethereum (https://ethereum.org/en/whitepaper/). Дата візиту ресурсу: 24.10.24
6. Decentralization in blockchain(https://www.chiliz.com/what-is-decentralization-in-blockchain/#:~:text=Decentralization%20within%20blockchain%20means%20the,a%20copy%20of%20the%20network) Дата візиту ресурсу: 24.10.24
7. Криптографія (https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF

%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F). Дата візиту ресурсу: 24.10.24

8. Механізм консенсусу (https://www.zfort.com.ua/blog/mekhanizmi-konsensusu-v-blokcheini-yak-ce-pracyuye). Дата візиту ресурсу: 24.10.24
9. Proof of work (https://academy.binance.com/uk/articles/proof-of-work-explained). Дата візиту ресурсу: 27.10.24
10. Proof of Stake (https://academy.binance.com/uk/articles/proof-of-stake-explained). Дата візиту ресурсу: 27.10.24
11. Carson et al. (2018) (https://onlinelibrary.wiley.com/doi/abs/10.1002/gps.4756). Дата візиту ресурсу: 27.10.24
12. Estonian e-Residency (https://www.e-resident.gov.ee/). Дата візиту ресурсу: 27.10.24
13. Клієнт-серверна архітектура (https://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%96%D1%94%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%BD%D0%B0_%D0%B0%D1%80%D1%85%D1%96%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0#:~:text=%D0%90%D1%80%D1%85%D1%96%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0%20%D0%BA%D0%BB%D1%96%D1%94%D0%BD%D1%82%2D%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%20%D1%94%20%D0%BE%D0%B4%D0%BD%D0%B8%D0%BC,%D1%82%D0%B0%20%D0%BE%D0%B1%D0%BC%D1%96%D0%BD%20%D0%B4%D0%B0%D0%BD%D0%B8%D0%BC%D0%B8%20%D0%BC%D1%96%D0%B6%20%D0%BD%D0%B8%D0%BC%D0%B8.). Дата візиту ресурсу: 27.10.24
14. Microsoft Share Point (https://www.microsoft.com/en-us/microsoft-365/sharepoint/collaboration). Дата візиту ресурсу: 27.10.24

15. 1С (https://1c-dn.com/1c_enterprise/what_is_1c_enterprise/). Дата візиту ресурсу: 27.10.24
16. Alfresco (https://docs.alfresco.com/). Дата візиту ресурсу: 27.10.24
17. Equifax (https://uk.wikipedia.org/wiki/Equifax). Дата візиту ресурсу: 27.10.24
18. CNA Financial кібер атака (https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack). Дата візиту ресурсу: 27.10.24
19. Storj (https://www.storj.io/). Дата візиту ресурсу: 27.10.24
20. Factom (https://factom.pro/). Дата візиту ресурсу: 27.10.24
21. Chainpoint (https://chainpoint.org/). Дата візиту ресурсу: 27.10.24
22. ERP система визначення (https://uk.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D1%96%D0%B2_%D0%BF%D1%96%D0%B4%D0%BF%D1%80%D0%B8%D1%94%D0%BC%D1%81%D1%82%D0%B2%D0%B0). Дата візиту ресурсу: 28.10.24
23. CRM система, визначення (https://www.creatio.com/ua/crm/what-is-crm).
24. Metamask (https://en.wikipedia.org/wiki/MetaMask). Дата візиту ресурсу: 28.10.24
25. AES-256 визначення (https://www.vpnunlimited.com/ua/help/cybersecurity/aes-256) Дата візиту ресурсу: 28.10.24
26. Quorum (https://www.kaleido.io/blockchain-platform/quorum). Дата візиту ресурсу: 28.10.24
27. Amazon Web Services (AWS) (https://aws.amazon.com/). Дата візиту ресурсу: 28.10.24

28. UI/UX визначення (https://prjctr.com/mag/uxui-questions). Дата візиту ресурсу: 28.10.24
29. Газ, визначення (https://www.kraken.com/uk-ua/learn/what-is-a-blockchain-gas-fee). Дата візиту ресурсу: 28.10.24