ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Підвищення безпеки документообігу підприємців шляхом впровадження технології блокчейн»

на здобуття освітнього ступеня магістра
зі спеціальності 121 Інженерія програмного забезпечення
освітньо-професійної програми «Інженерія програмного забезпечення»

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

_____ Станіслав НЕМЧИН
(підпис)

Виконав: здобувач вищої освіти групи ПДМ-63
Станіслав НЕМЧИН

Керівник: Наталія ТРІНТІНА
канд.техн.наук, доц.

Рецензент: _____
науковий ступінь, вчене звання *Ім'я, ПРІЗВИЩЕ*

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення

Ступінь вищої освіти Магістр

Спеціальність 121 Інженерія програмного забезпечення

Освітньо-професійна програма «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____ Ірина ЗАМРІЙ
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Немчину Станіславу Вячеславовичу

1. Тема кваліфікаційної роботи: «Підвищення безпеки документообігу підприємців шляхом впровадження технології блокчейн»

керівник кваліфікаційної роботи Наталія ТРІНТІНА канд.тех.наук, доцент,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.
2. Строк подання кваліфікаційної роботи «19» грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література з питань електронного документообігу, криптографічного захисту інформації та блокчейн-технологій; існуючі моделі централізованих і децентралізованих систем зберігання документів; алгоритми криптографічного хешування (SHA-256); вимоги до забезпечення цілісності, незмінності та верифікації електронних документів.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз існуючих моделей і методів забезпечення безпеки електронного документообігу.
2. Дослідження можливостей застосування блокчейн-технологій для збереження та верифікації документів.

3. Розробка та експериментальна оцінка блокчейн-орієнтованого методу контролю цілісності документів.

5. Перелік ілюстративного матеріалу: *презентація*

1. Математична модель забезпечення цілісності документів.
2. Алгоритм реєстрації та верифікації документів.
3. Модифікований метод верифікації документів.
4. Практичний результат.
5. Варіанти використання користувачем системи верифікації документів.
6. Порівняльний аналіз існуючих підходів та запропонованого блокчейн-рішення.

6. Дата видачі завдання «31» жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	31.10-05.11.25	
2	Вивчення науково-технічних матеріалів з питань безпеки електронного документообігу	6.11-12.11.25	
3	Дослідження принципів та технологій блокчейн і хеш-ланцюгів	13.11-19.11.25	
4	Аналіз недоліків традиційних централізованих систем зберігання документів	21.11-27.11.25	
5	Дослідження криптографічних методів контролю цілісності документів	28.11-4.12.25	
6	Застосування блокчейн-орієнтованих підходів для підвищення безпеки та незмінності документів	4.12-10.12.25	
7	Оформлення роботи: вступ, висновки, реферат	11.12-13.12.25	
8	Розробка демонстраційних матеріалів	14.12-16.12.25	
9	Попередній захист роботи	18.12-19.12.25	

Здобувач вищої освіти _____ Станіслав НЕМЧИН
(підпис)

Керівник
кваліфікаційної роботи _____ Наталія ТРІНТІНА
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 82 стор., 10 табл., 4 рис., 40 джерел.

Мета роботи – Підвищення безпеки документообігу підприємців шляхом оптимізації процесів зберігання, верифікації та контролю цілісності документів на основі принципів децентралізованих систем.

Об'єкт дослідження – Процес електронного документообігу в підприємницькій діяльності.

Предмет дослідження – Методи та моделі забезпечення безпеки документів на основі принципів децентралізованих розподілених систем.

У роботі використано методи криптографічного хешування, методи математичного моделювання, методи аналізу ризиків, методи порівняльного аналізу та експериментального моделювання продуктивності алгоритмів.

Проведено огляд сучасних підходів до забезпечення безпеки документообігу, включно з централізованими системами, системами з використанням цифрових підписів та журналів змін. Виконано аналіз проблем їх застосування при обробці юридично значимих документів та оцінено ризики фальсифікації.

Розроблено концептуальну модель збереження документів у вигляді хеш-ланцюга, алгоритм формування блоків та модифікований метод перевірки цілісності, що включає двоетапну перевірку документа та структури ланцюга. Реалізовано програмний прототип, який забезпечує збереження документів, обчислення хешів, формування ланцюга, верифікацію, експорт та імпорт даних.

Проведено моделювання та експериментальне тестування продуктивності на різних обсягах документів і сценаріях використання. Результати показали, що

запропонована модель забезпечує підвищення швидкості перевірки цілісності у 5-8 разів у порівнянні з централізованими підходами та забезпечує 100% виявлення модифікацій документів.

Запропонований підхід може бути використаний у системах електронного документообігу малого та середнього бізнесу, юридичних і бухгалтерських сервісах, а також у системах, де критичною є збереженість незмінної історії документів.

КЛЮЧОВІ СЛОВА: БЛОКЧЕЙН, ХЕШ-ЛАНЦЮГ, ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ, КРИПТОГРАФІЧНА ПЕРЕВІРКА, SHA-256, ЦІЛІСНІСТЬ ДАНИХ, ВЕРИФІКАЦІЯ ДОКУМЕНТА, ФАЛЬСИФІКАЦІЯ, МОДЕЛЮВАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Text part of the master's qualification work: 82 pages, 4 pictures, 10 table, 40 sources.

The purpose of the work is to enhance the security of entrepreneurs' document workflows by optimizing processes of storage, verification, and integrity control based on the principles of decentralized systems.

The object of research is the process of electronic document management in entrepreneurial activity.

The subject of research is the methods and models of ensuring document security based on the principles of decentralized distributed systems.

The study applies cryptographic hashing methods, mathematical modelling methods, risk assessment techniques, comparative analysis approaches, and experimental performance evaluation of algorithms.

A review of modern approaches to ensuring the security of document workflows has been carried out, including centralized systems, systems utilizing digital signatures and audit logs. The limitations of their application when processing legally significant documents have been analyzed, along with the risks of falsification.

A conceptual storage model based on a hash-chain structure has been developed, including a block formation algorithm and a modified integrity verification method that performs two-level validation of both the document and the chain structure. A software prototype has been implemented, providing document storage, hash computation, chain formation, verification, export, and import of data.

Simulation and experimental performance testing were conducted across various dataset volumes and use cases. The results show that the proposed model increases integrity verification speed by 5–8 times compared to centralized approaches and ensures 100% detection of document modifications.

The proposed approach can be applied in electronic document management systems for small and medium-sized businesses, in legal and accounting services, as well as in systems where preserving an immutable document history is critical.

KEYWORDS**:** BLOCKCHAIN, HASH CHAIN, ELECTRONIC DOCUMENT MANAGEMENT, CRYPTOGRAPHIC VALIDATION, SHA-256, DATA INTEGRITY, DOCUMENT VERIFICATION, FALSIFICATION, MODELLING, INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 12

ВСТУП 13

1. АНАЛІТИЧНИЙ ОГЛЯД ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОКУМЕНТООБІГУ 16

1.1 Аналіз проблематики методів перевірки знань 16

1.2. Основні загрози цілісності та достовірності документів 18

1.3. Огляд сучасних централізованих рішень документообігу 19

1.4. Методи і моделі захисту (хешування, криптографія, контроль версій) 22

1.5. Блокчейн у задачах захисту даних: стан досліджень 27

1.6. Недоліки існуючих підходів 31

2. ТЕОРЕТИЧНІ ЗАСАДИ БЛОКЧЕЙН-МОДЕЛІ ДЛЯ ДОКУМЕНТООБІГУ 34

2.1. Принципи та властивості технології блокчейн 34

2.2. Математична модель блоку документа 37

2.3. Модель хеш-ланцюга документів 41

2.4. Модель перевірки цілісності (валидація ланцюга) 44

2.5. Особливості розподіленого зберігання 46

2.6. Формулювання задачі підвищення безпеки 48

3. РОЗРОБКА МОДЕЛІ ТА АЛГОРИТМУ ПІДВИЩЕННЯ БЕЗПЕКИ ДОКУМЕНТООБІГУ 51

3.1. Вимоги до запропонованої моделі 51

3.2. Формальна постановка задачі 54

3.3. Математичний опис формування блоку 56

3.4. Алгоритм побудови хеш-ланцюга 61
3.5. Модифікований метод перевірки цілісності 64
3.6. Модель оцінки ризику фальсифікації 67
3.7. Теоретична оцінка ефективності 69
4. МОДЕЛЮВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО МЕТОДУ 73
4.1. Методика моделювання 73
4.2. Набір сценаріїв моделювання 75
4.3. Порівняння часу перевірки документів у різних моделях 77
4.4. Аналіз стійкості до модифікації документів 82
4.5. Порівняльний аналіз з традиційними підходами 87
4.6. Оцінка досягнення поставленої мети 89
ВИСНОВОК 92
ПЕРЕЛІК ПОСИЛАНЬ 96
ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 100
ДОДАТОК Б. ДЕМО-ВЕРСІЯ ЗАСТОСУНКУ 106

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES — Advanced Encryption Standard (алгоритм симетричного шифрування)

API — Application Programming Interface (прикладний програмний інтерфейс)

Base64 — формат кодування двійкових даних у текст

CA — Certification Authority (центр сертифікації)

ECDSA — Elliptic Curve Digital Signature Algorithm (алгоритм цифрового підпису на еліптичних кривих)

JSON — JavaScript Object Notation (текстовий формат обміну даними)

JS — JavaScript (мова програмування)

PDF — Portable Document Format (формат документів Adobe)

RSA — Rivest–Shamir–Adleman (криптографічний алгоритм з відкритим ключем)

SHA-256 — Secure Hash Algorithm 256-bit (криптографічна хеш-функція)

SQL — Structured Query Language (мова структурованих запитів)

TLS — Transport Layer Security (протокол захисту передавання даних, наступник SSL)

XML — eXtensible Markup Language (розширювана мова розмітки)

DDoS – Distributed Denial of Service (розподілена атака на відмову в обслуговуванні)

CRM – Customer Relationship Management (система управління взаємовідносинами з клієнтами)

КЕП – кваліфікований електронний підпис

ЦЕП – цифровий електронний підпис (інколи – «цифровий електронний підпис» як синонім ЕЦП)

ЕЦП – електронний цифровий підпис

ЕЦД – електронний цифровий документ (у контексті електронного документообігу)

ВСТУП

Сучасний розвиток цифрової економіки супроводжується стрімким зростанням обсягів електронного документообігу, що стає фундаментальною складовою діяльності малого та середнього бізнесу, приватних підприємців, мережевих сервісів та платформ електронної комерції. Оцифрування бізнес-процесів, автоматизація взаємодії між учасниками ринку, відмова від паперових носіїв та розширення віддалених форматів роботи приводять до того, що електронний документ стає основним носієм юридично значимої інформації. У таких умовах питання цілісності, достовірності та захищеності документів набувають вирішального значення, оскільки їх порушення може спричинити значні фінансові, репутаційні та правові ризики.

Попри активний розвиток цифрових сервісів, більшість існуючих рішень електронного документообігу побудовані на централізованій архітектурі, де контроль за зберіганням, модифікаціями та історією документів зосереджений у одного оператора. Така централізація створює низку потенційних загроз: можливість несанкціонованих змін з боку адміністратора системи, ризик компрометації бази даних, відсутність прозорого механізму простеження історії змін, залежність від єдиної точки відмови. Проблема ускладнюється також тим, що підприємці та малі бізнеси часто використовують спрощені або застарілі рішення, які не забезпечують достатнього рівня криптографічного захисту та аудиту.

У відповідь на ці виклики в останні роки активно розвиваються блокчейн-орієнтовані підходи до захисту документів, які ґрунтуються на таких властивостях технології, як незмінність записів, криптографічне зв’язування блоків у хеш-ланцюг, розподілене зберігання та відсутність потреби у довіреному центральному адміністраторі. Блокчейн дозволяє забезпечити високий рівень достовірності та підтвердженого походження документів, оскільки будь-яка спроба модифікації файла веде до невідповідності хеш-ланцюга, що робить фальсифікацію очевидною для всіх учасників системи. Саме тому блокчейн дедалі частіше використовується

у фінансовому секторі, логістиці, охороні здоров'я, а також у задачах управління цифровими активами.

Однак впровадження блокчейн-моделей у документообіг підприємців потребує адаптації до практичних умов реального бізнесу. Відкриті публічні блокчейни мають високу вартість транзакцій та невисоку швидкодію, а приватні блокчейни часто є складними у розгортанні та адмініструванні. Тому постає завдання розроблення легковагової моделі, яка б поєднувала переваги блокчейн-технології з мінімальними витратами ресурсів, простотою інтеграції та можливістю застосування у невеликих бізнес-процесах.

Незважаючи на значну кількість досліджень у сфері застосування блокчейну, недостатньо вивченими залишаються питання інтеграції математичної моделі хеш-ланцюга документів, алгоритмів перевірки цілісності, оцінки ризику фальсифікації та формалізації процедури підтвердження справжності документа. Потребує уточнення й питання адаптації блокчейн-принципів до систем, де учасників небагато, а структура даних не потребує складних консенсус-алгоритмів. Також актуальною є проблема формального визначення ефективності таких рішень: вимірювання швидкодії перевірки, стійкості до підробок, складності компрометації зловмисником та витрат на забезпечення цілісності.

У рамках цієї кваліфікаційної роботи запропоновано математичну модель формування блоку документа, алгоритм побудови хеш-ланцюга, модифікований метод перевірки цілісності та модель оцінки ризику фальсифікації документа. Особлива увага приділяється формальному обґрунтуванню того, як криптографічні властивості SHA-256, хеш-ланцюги та контроль попереднього хешу забезпечують незмінність документа й підвищують загальний рівень інформаційної безпеки. Додатково в роботі проведено моделювання, що дозволило кількісно оцінити ефективність запропонованого підходу порівняно з традиційними централізованими рішеннями.

Результатом роботи стала також розробка демонстраційного веб-прототипу, що реалізує основні елементи блокчейн-орієнтованої моделі: формування блоків, хешування документів, перевірку цілісності, візуалізацію ланцюга та зберігання

даних. Такий прототип підтверджує практичну застосовність запропонованої моделі та дозволяє оцінити її поведінку у реальних сценаріях використання.

Таким чином, тема дослідження є актуальною як з теоретичної точки зору — оскільки спрямована на розвиток математичних моделей забезпечення цілісності документів — так і з практичної, адже пропонує реальне рішення, яке може підвищити рівень безпеки документообігу підприємців та зменшити ймовірність фальсифікації інформації.

1. АНАЛІТИЧНИЙ ОГЛЯД ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОКУМЕНТООБІГУ

1.1 Аналіз проблематики методів перевірки знань

Документообіг підприємців охоплює створення, передавання, зберігання та використання значної кількості документів, що супроводжують господарську діяльність: договорів, накладних, актів виконаних робіт, фінансових звітів, податкових декларацій, сертифікатів та іншої юридично значущої інформації. Особливість такого документообігу полягає у поєднанні високої динамічності бізнес-процесів із необхідністю забезпечення достовірності, точності та незмінності даних у кожному документі.

У підприємницькому середовищі документи часто формуються й передаються у стислі строки та залучають кількох суб’єктів — контрагентів, постачальників, підрядників, державні установи. Передача може здійснюватися через різні цифрові канали: електронну пошту, месенджери, CRM-системи, сервіси ЕДО або хмарні сховища. Така фрагментованість цифрових інструментів створює умови для втрати контролю над версіями документів і підвищує ризик їх ненавмисної чи умисної модифікації.

Більшість підприємців, особливо малого та середнього бізнесу, не використовують комплексні системи електронного документообігу. Натомість документи зберігаються у вигляді PDF-файлів, електронних таблиць, фотографій або неструктурованих архівів. У таких умовах складно забезпечити повноцінний аудит змін, перевірку автентичності та достовірності інформації після передачі контрагентам.

Документи можуть мати різний юридичний статус: одні підписуються КЕП/ЕЦП, інші передаються без формального підпису. Важливим є гарантування не тільки авторства, а й незмінності змісту після підписання та передачі.

Модифікація договору, накладної чи фінансового звіту може призвести до юридичних спорів, фінансових збитків або викривлення бухгалтерського обліку.

Суттєвим є також питання збереження історії змін. Підприємці часто працюють із документами, що неодноразово уточнюються (специфікації, технічні завдання, комерційні пропозиції). У більшості доступних інструментів контролю версій не вистачає або він реалізований поверхнево, що ускладнює відтворення стану документа на конкретний момент часу.

Важливим компонентом документообігу є довіра між сторонами. Документ, переданий однією стороною, повинен зберігати незмінність незалежно від того, у якій системі його зберігає інший учасник. За відсутності спільного надійного середовища зростає потреба у незалежних механізмах підтвердження цілісності.

Узагальнюючи, документообіг підприємців характеризується такими особливостями:

- високою динамічністю операцій та значним обсягом документів;
- використанням різнорідних цифрових каналів і форматів зберігання;
- відсутністю єдиної платформи контролю змін та автентичності;
- необхідністю гарантування цілісності та підтверджуваності документів;
- низьким рівнем формалізації процесів;
- критичною потребою у прозорій історії змін;
- важливістю створення технічного механізму довіри між незалежними учасниками.

Ці особливості обґрунтовують необхідність використання технологій, здатних забезпечити гарантовану незмінність та відтворювану історію документаційних записів. Одним із таких рішень є блокчейн, який завдяки криптографічній структурі та децентралізованій архітектурі забезпечує високий рівень контролю цілісності без участі центрального посередника.

1.2. Основні загрози цілісності та достовірності документів

Забезпечення цілісності та достовірності документів є критично важливим аспектом діяльності підприємців, оскільки будь-яке несанкціоноване втручання в документообіг може спричинити фінансові втрати, юридичні наслідки та порушення договірних зобов'язань. У сучасних умовах цифровізації бізнесу зростає кількість загроз, пов'язаних як із технічними, так і з організаційними аспектами управління документами. Їх можна умовно поділити на технічні, організаційні, людські та зовнішні (юридичні та регуляторні) ризики.

Однією з ключових загроз є несанкціоноване редагування або підробка документів. У централізованих системах зберігання інформації дані контролюються однією стороною або розміщуються на одному сервері, що створює можливість модифікації документів без залишення слідів. Особливо ризиковими є зміни у фінансових звітах, договорах, актах виконаних робіт та іншій юридично значущій документації.

Суттєву небезпеку становлять технічні ризики, пов'язані з перехопленням даних під час передавання документів. Використання застарілих або некоректно налаштованих засобів шифрування підвищує ймовірність атак типу «Man-in-the-Middle», що дозволяють змінювати або підмінювати документи у процесі комунікації.

Проблемою також є відсутність достовірної та захищеної історії змін. У централізованих БД журнали подій можуть бути змінені або видалені адміністраторами системи, що унеможливлює відновлення точної послідовності операцій. Це створює труднощі при аудиті, вирішенні спорів і оцінці справжності документів.

Вразливим місцем є і система доступу. Компрометація облікових записів, слабкі паролі, відсутність багатофакторної автентифікації та некоректні налаштування прав доступу відкривають шлях для внутрішніх і зовнішніх зловмисників. Значна частина інцидентів безпеки пов'язана саме з людським

фактором — недбалістю персоналу, помилками під час обробки документів або навмисними діями співробітників.

Сучасні атаки включають також спроби масового шифрування або знищення документів за допомогою шкідливого ПЗ, наприклад ransomware. За відсутності дубльованої або розподіленої системи зберігання такі атаки можуть призвести до повної втрати критично важливих даних.

Організаційні ризики пов’язані з недостатньою формалізацією бізнес-процесів, відсутністю політик щодо управління документами, нерегулярними аудитами та хаотичним використанням різних інструментів документообігу. Це призводить до розривів між версіями документів, втрати узгодженості та неможливості підтвердити їхній справжній стан у конкретний момент часу.

До зовнішніх чинників належать юридичні та нормативні ризики, коли документи не відповідають вимогам стандартів, або можуть бути поставлені під сумнів у суді через відсутність механізмів верифікації їх походження та історії змін.

Узагальнюючи, сучасні загрози демонструють потребу у вдосконаленні систем документообігу й впровадженні рішень, які забезпечують незмінність записів, захищений аудит, прозорість історії змін та можливість незалежної перевірки достовірності документів. Одним із найбільш ефективних підходів для цього є блокчейн-технологія, що ґрунтується на криптографічному захисті та забезпечує математично гарантовану цілісність даних.

1.3. Огляд сучасних централізованих рішень документообігу

Системи електронного документообігу (ЕДО) широко використовуються підприємцями та організаціями для автоматизації створення, передачі, зберігання та узгодження документів. Більшість сучасних рішень працюють на основі централізованої архітектури, у якій усі дані зосереджені в одному логічному центрі — сервері або хмарній інфраструктурі, що контролюється однією організацією. Така модель визначає функціональність, можливості та обмеження системи,

зокрема у сфері забезпечення цілісності, достовірності та незмінюваності документів.

Централізовані системи ЕДО, включаючи як державні сервіси (M.E.Doc, СОТА, Дія.Едок), так і комерційні платформи (Microsoft 365, Google Workspace, BAS Документообіг, M-Files, DocuSign у корпоративному режимі), забезпечують широкий спектр функцій: створення документів, їх реєстрацію, маршрутизацію, роботу з КЕП/ЕЦП, управління правами доступу, журналювання операцій та архівування. Попри це, їхня архітектура передбачає повну залежність від оператора системи, який контролює базу даних, журнали подій та механізми доступу.

Основними технічними елементами таких систем є центральний сервер або кластер, база даних документів, модуль автентифікації, клієнтські додатки, механізми цифрового підпису та модуль маршрутизації. Уся логіка обробки та зберігання інформації зосереджена на стороні постачальника або адміністратора, що створює єдину точку контролю та потенційну точку відмови.

Типові механізми безпеки — шифрування (AES-256, RSA-2048, TLS 1.2/1.3), електронний підпис, розмежування доступу, аудит подій та резервне копіювання — зменшують ризики, але не забезпечують технічної незмінюваності даних. Адміністратори з високим рівнем доступу можуть змінити записи в БД або журнали, що унеможливлює незалежне підтвердження цілісності інформації.

Однією з найважливіших проблем централізованих ЕДО є можливість внутрішнього втручання. Адміністратор, маючи доступ до внутрішніх структур системи, може змінювати або видаляти документи, коригувати метадані та журнали операцій. У судовій практиці неодноразово фіксувалися випадки втручання у журнали подій на вимогу керівництва або окремих співробітників, що підтверджує високий рівень внутрішніх ризиків.

Крім внутрішніх маніпуляцій, централізовані системи є привабливою ціллю для зовнішніх атак. Оскільки вся інформація зберігається в одному місці, порушення захисту сервера відкриває доступ до всієї інфраструктури одразу. Типові загрози включають DDoS-атаки, SQL-ін’єкції, експлойти вразливостей

CMS або серверного програмного забезпечення. У випадку компрометації зловмисник може отримати або змінити документи без можливості виявлення.

ЕЦП/КЕП підтверджує достовірність документа лише в момент підписання. Однак після збереження документа у централізованій БД його зміст або метадані можуть бути змінені, а хеш — переписаний користувачем з відповідними правами доступу. Відсутність технічного механізму незмінюваності записів робить такі системи вразливими до підробок.

Ще одним обмеженням є низька прозорість і залежність від оператора. Користувачі не можуть незалежно перевірити стан журналів або підтвердити незмінність документа. У багатьох випадках вони повністю покладаються на внутрішні механізми платформи, які можуть бути модифіковані адміністратором.

Централізовані ЕДО мають й архітектурний недолік — єдину точку відмови. У разі збою серверів, пошкодження бази даних, кібератаки або помилки налаштувань доступ до документів може бути втрачений або заблокований.

Аналіз комерційних рішень показує, що незалежно від популярності чи функціональності всі вони зберігають основні обмеження централізованої архітектури. Українські системи ЕДО залежать від підрядників і допускають адміністративні зміни в БД. Microsoft SharePoint та Office 365 мають редаговані журнали подій і не забезпечують незмінного ланцюга версій. Google Workspace забезпечує журнал дій, але не гарантує криптографічної незмінюваності документів. DocuSign у звичайному режимі також не забезпечує повного захисту журналів від втручань. Для наочного відображення принципів роботи традиційних централізованих систем документообігу та їхніх ключових недоліків на рисунку 1.1 наведено узагальнену схему такої моделі.

Рис. 1.1 Традиційна централізована модель документообігу

Таким чином, сучасні централізовані платформи електронного документообігу ефективні з точки зору автоматизації та зручності, але не забезпечують ключові властивості, необхідні для захисту цілісності документів: неможливість прихованої зміни, незалежність від адміністратора та криптографічне підтвердження незмінності. Ці обмеження визначають потребу у впровадженні нових моделей, зокрема децентралізованих блокчейн-рішень.

1.4. Методи і моделі захисту (хешування, криптографія, контроль версій)

Сучасні системи документообігу підприємців функціонують у середовищі постійних ризиків, пов’язаних з кіберзагрозами, юридичними маніпуляціями, внутрішніми порушеннями та спробами фальсифікації інформації. Забезпечення цілісності, достовірності та підтверджуваності документів є ключовою умовою безпеки підприємницької діяльності. Тому розробка моделей і методів захисту

документів стала критично важливим напрямом як у наукових дослідженнях, так і в практичних технологічних впровадженнях.

У цьому підрозділі здійснюється комплексний аналіз базових механізмів захисту — криптографічного хешування, криптографії (симетричної та асиметричної), електронного цифрового підпису, контролю доступу, систем ведення журналів (логування) та контролю версій документів. Також розглядаються їх переваги та слабкі сторони в контексті вимог до безпечного документообігу підприємців.

Хешування є одним із базових механізмів забезпечення цілісності даних. Криптографічні хеш-функції виконують перетворення довільних за розміром даних у фіксований бітовий рядок. Ця властивість широко використовується у системах документообігу для перевірки, чи був документ змінений після створення або з моменту останньої перевірки.

Основні властивості криптографічних хеш-функцій:

1. Односторонність (One-way property) — неможливо обчислити вхідні дані, знаючи лише їх хеш.
2. Стійкість до колізій — надзвичайно складно знайти два різних файли, що мають однаковий хеш.
3. Стійкість до пошуку другообразу — неможливо підібрати інший документ, який буде мати той самий хеш, що й оригінальний.
4. Чутливість до змін (Avalanche effect) — навіть мінімальна зміна в документі призводить до повної зміни хешу.

Переваги хешування в документообігу:

- Миттєва перевірка цілісності файлу.
- Незалежність від типу документа.
- Можливість зберігати лише хеш, а не оригінальний документ (економія місця).
- Широка підтримка у сучасних системах (SHA-256, SHA-3).
- Недоліки класичного хешування:
- Хеш сам по собі не гарантує автентичності документа.

- Якщо зловмисник підмінить документ і хеш одночасно, система не помітить змін.
- Хеш не містить інформації про власника або історію змін документа.

Це означає, що хеш-функції добре підходять для механізмів перевірки, але не забезпечують повного захисту. Для цього комбінують хешування з електронним підписом або блокчейн.

Криптографічні методи є фундаментом сучасного інформаційного захисту. Вони дозволяють забезпечити конфіденційність, автентичність і захист каналів передачі.

Симетричне шифрування

У симетричних системах один і той самий ключ використовується як для шифрування, так і для розшифрування.

Переваги:

- висока швидкість роботи;
- простота реалізації.
- Недоліки:
- ключі треба обмінювати між сторонами (ризик перехоплення);
- складність масштабування у великих системах документообігу.

Асиметрична криптографія

Застосовує пару ключів: приватний та публічний.

Можливості:

- шифрування інформації публічним ключем отримувача;
- створення цифрового підпису приватним ключем автора.

Переваги:

- безпека обміну даними без попереднього секретного каналу;
- можливість створення цифрового підпису.

Недоліки:

- значно повільніша, ніж симетрична;

– потребує інфраструктури відкритих ключів (PKI).

У напрямі безпеки документообігу асиметрична криптографія є критичним інструментом, оскільки дозволяє:

– підтвердити автора документа,
– забезпечити незаперечність,
– запобігти підробці документів.

ЕЦП надає документам юридичну силу й дозволяє однозначно визначити автора та момент підписання.

Основні властивості ЕЦП:

1. Автентичність — документ створено конкретною особою.
2. Цілісність — після підписання документ не змінювався.
3. Незаперечність — автор не може відмовитись від створеного підпису.

Недоліки ЕЦП:

– потребує складної інфраструктури (сертифікати, ключі, реєстри);
– потребує регулярного поновлення сертифікатів;
– залежить від довіреного центра сертифікації (ЦСК);
– зміна або фальсифікація записів ЦСК фактично робить підписи недійсними.

Таким чином, ЕЦП вирішує проблему автентичності, але не дає гарантій незмінності історії документів, що є ключовим у підприємницькій діяльності.

Контроль доступу визначає, хто має право читати, змінювати або підписувати документи.

Поширені моделі:

– DAC (Discretionary Access Control) — власник визначає доступ.
– MAC (Mandatory Access Control) — доступ базується на рівнях секретності.
– RBAC (Role-Based Access Control) — права визначаються ролями користувачів.

– ABAC (Attribute-Based Access Control) — рішення приймаються на основі атрибутів користувачів, об’єктів та контексту.

Контроль доступу вирішує проблему хто може змінювати документ, але не гарантує виявлення змін.

Системи контролю версій (Git-подібні механізми, корпоративні EDM-системи) дозволяють відслідковувати, хто і коли вніс зміни до документа.

Переваги:

– історія змін зберігається;
– можна повернутися до попередньої версії;
– відображається авторство правок.

Недоліки:

– історія може бути змінена адміністратором;
– журнали не захищені від фальсифікації;
– немає гарантії, що авторські дані не підроблені.

Безпека таких систем залежить від довіри до адміністратора, що є слабкою ланкою, особливо у підприємницькому середовищі.

На практиці більшість систем документообігу використовує комбінацію:

– хешування,
– ЕЦП,
– контроль доступу,
– логування.

Однак навіть таке поєднання не забезпечує абсолютної незмінності документообігу, оскільки:

– централізовані журнали можуть бути змінені,
– адміністратор має можливість змінити записи,
– фальсифікація слідів часто непомітна для користувачів,
– історія змін не є математично незмінною,
– відсутність єдиного джерела правди у багатосторонніх взаємодіях.

Це сформувало потребу у моделях, які гарантують незмінність структури документів математично, а не організаційно.

1.5. Блокчейн у задачах захисту даних: стан досліджень

Технологія блокчейн, яка на початкових етапах свого розвитку застосовувалася переважно у сфері криптовалют, сьогодні розглядається як один із найефективніших інструментів забезпечення незмінності, цілісності та достовірності цифрових даних. У контексті документообігу підприємців блокчейн привертає особливу увагу завдяки здатності усунути ключові недоліки централізованих систем, зокрема можливість внутрішніх маніпуляцій, залежність від адміністратора, вразливість до зовнішніх атак та відсутність технічної гарантії збереження історії змін. Сучасні наукові дослідження демонструють, що блокчейн може стати фундаментом для створення прозорого, захищеного та стійкого середовища документообігу, в якому будь-яка дія з документом фіксується у вигляді незмінного запису.

У більшості робіт блокчейн розглядається як розподілений реєстр, що складається із послідовності блоків, захищених криптографічними хеш-функціями. Основні властивості — незмінність записів, розподіленість, криптографічний захист і повна відтворюваність історії — роблять технологію перспективною для застосування у середовищах, де критично важливо забезпечити математично підтверджувану достовірність інформації. На відміну від централізованих баз даних, блокчейн не дозволяє приховано видаляти або коригувати дані, оскільки будь-яке редагування розриває хеш-ланцюг, що легко виявляється під час перевірки.

Одним із найпоширеніших напрямів використання блокчейну у документообігу є зберігання криптографічних хешів документів замість самих файлів. У блокчейні фіксують хеш документа, метадані (автора, час створення, тип документа), цифрові підписи учасників, а також дані про маршрут погодження. Це дозволяє розділити два важливі аспекти: фактичний документ зберігається у

зовнішніх сховищах або файлових системах, а доказова база — у блокчейні, який гарантує неможливість непомітної модифікації. Будь-яка зміна вмісту документа призведе до зміни хешу, що робить фальсифікацію легко детектованою.

Значну увагу у сучасних дослідженнях приділено задачам аудиту та протоколювання. На відміну від централізованих журналів, які можуть бути відредаговані або видалені адміністратором, блокчейн забезпечує незворотність усіх записів. Кожна дія з документом — перегляд, редагування, підписання, передача — фіксується у вигляді транзакції, яка дублюється на всіх вузлах мережі. Це створює незалежну, криптографічно захищену історію змін, яка має високу доказову цінність у разі спорів, внутрішніх розслідувань або судових процесів.

Важливим напрямом є дослідження у сфері контролю доступу. Провідні центри, такі як MIT, IBM Research та European Blockchain Observatory, пропонують моделі, що поєднують блокчейн із системами цифрової ідентичності, багатофакторної автентифікації та механізмами мультипідпису. Такий підхід дозволяє автоматизувати правила доступу до документів і усунути необхідність у центральному адміністраторі. Правила доступу управляються смарт-контрактами, які виконуються автоматично і не можуть бути непомітно змінені людиною.

Окремим напрямом досліджень є застосування криптографічних протоколів на кшталт zero-knowledge proof, які дозволяють перевіряти автентичність документа без передачі його вмісту. Це особливо актуально для підприємців, що працюють із конфіденційною інформацією, комерційною таємницею або персональними даними, де критично важливо поєднувати можливість перевірки з високим рівнем приватності.

Блокчейн також широко вивчається як механізм створення ланцюгів довіри між сторонами, які не повністю довіряють одна одній. Незалежно від того, де фізично зберігаються документи, блокчейн забезпечує єдине «джерело правди», яке дозволяє підтвердити справжність рахунків-фактур, актів виконаних робіт, договорів, сертифікатів та інших документів. У роботах 2020–2024 років відзначається активне впровадження таких систем у логістику, фінтех, юридичну сферу, сертифікацію товарів та корпоративне управління.

Сучасні дослідження також класифікують застосування блокчейну в документообігу за кількома ключовими напрямами. Перший — захист документів і файлів, де блокчейн використовується для timestamping, фіксації хешів та забезпечення неможливості непомітної модифікації. Другий — захист логів і транзакцій, де незмінність записів має вирішальне значення для аудиту. Третій — автоматизація документообігу за допомогою смарт-контрактів, що дозволяє мінімізувати людські помилки та забезпечити виконання бізнес-правил без втручання оператора. Четвертий — корпоративні реєстри, у яких блокчейн застосовується для зберігання сертифікатів, кадрових записів, бухгалтерських журналів чи реєстрів ліцензій, забезпечуючи їхню захищеність і прозорість.

Наукова література однозначно вказує на суттєві переваги блокчейн-рішень у сфері документообігу. Основними з них є незмінність записів, відсутність необхідності у центральному адміністраторі, повна прозорість історії змін, об’єктивність даних, можливість незалежної перевірки та стійкість до внутрішніх загроз. Разом з тим дослідження підкреслюють і певні обмеження: високу вартість транзакцій у публічних мережах, неможливість зберігати великі обсяги даних, технічну складність впровадження та питання конфіденційності. Ці проблеми, однак, частково вирішуються приватними або консорціумними блокчейн-мережами, інтеграцією з IPFS та використанням додаткових рівнів шифрування.

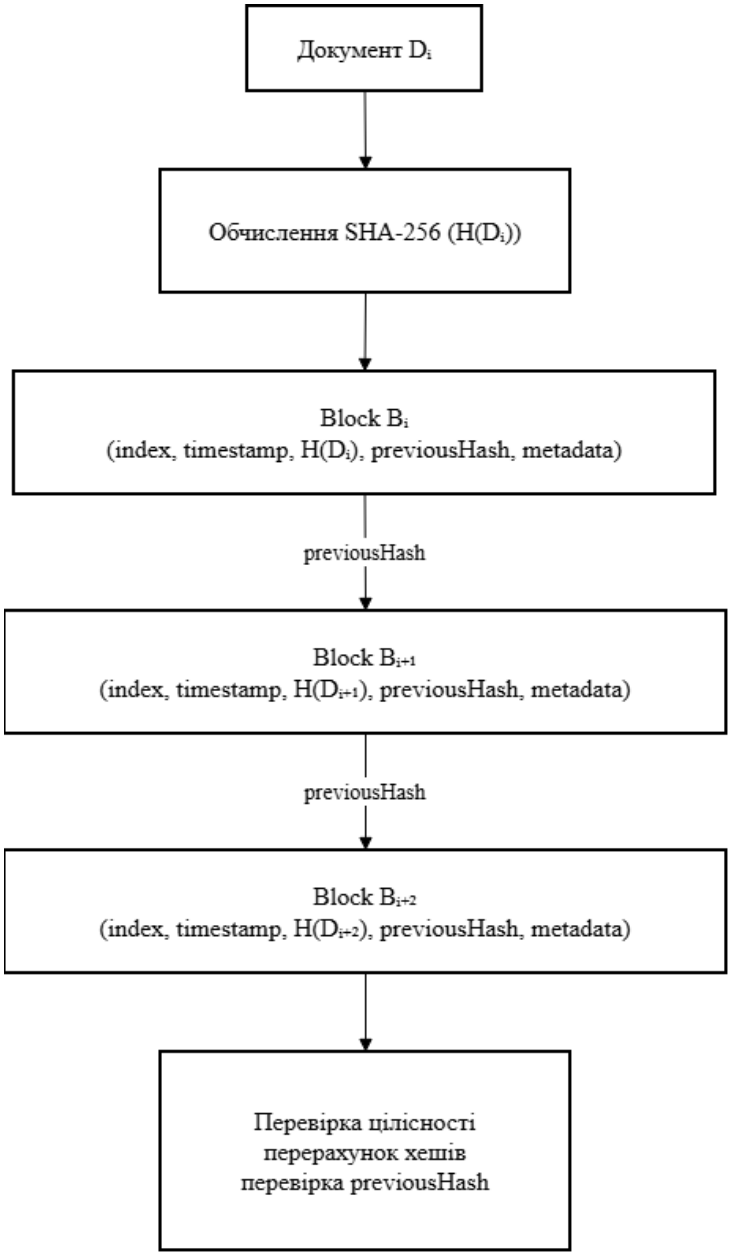


Рис. 1.2 Запропонована децентралізована модель на основі хеш-ланцюга

Сукупність сучасних досліджень демонструє, що блокчейн є ефективним і перспективним інструментом підвищення безпеки документообігу підприємців. Його використання дозволяє забезпечити високий рівень захисту даних, прозорість взаємодії між учасниками, мінімізацію ризиків фальсифікації та створення довготривалих, надійних доказових структур, що можуть бути використані у юридичних, фінансових та операційних процесах.

1.6. Недоліки існуючих підходів

Сучасні системи електронного документообігу підприємців базуються переважно на централізованих або частково централізованих моделях зберігання інформації. Незважаючи на широке використання таких систем та їх зручність, вони мають низку фундаментальних недоліків, що значно знижують рівень безпеки, цілісності та довіри до електронних документів. У цьому підрозділі проведено системний аналіз слабких сторін традиційних рішень та окреслено проблеми, які залишаються невирішеними в межах класичних підходів.

Недоліки централізованої архітектури. Більшість платформ для документообігу (M.E.Doc, Microsoft SharePoint, Google Drive, локальні корпоративні СЕД) працюють за принципом централізованих серверів. Це створює низку критичних вразливостей, серед яких:

Єдина точка відмови (Single Point of Failure). У разі збою сервера, втрати доступу до мережі або кібератаки документообіг підприємства може бути повністю паралізований. Втрата ключової інфраструктури веде до зупинки бізнес-процесів, неможливості підписання та передачі документів, затримок у комунікації між учасниками.

Централізований контроль доступу. Усі операції з документами контролюються адміністратором системи або власником серверів. Це породжує ризик зловживань, оскільки одна особа або група осіб отримує можливість змінювати, підмінювати або видаляти документи без слідів втручання.

Низька стійкість до кібератак. Централізовані дата-центри є пріоритетними цілями для DDoS-атак, атак шифрувальниками, SQL-injection та компрометації облікових записів. Порушення безпеки сервера може призвести до масштабного витоку конфіденційних документів.

Контроль цілісності залежить від самої системи. У централізованих СЕД перевірка цілісності здійснюється тією ж системою, яка зберігає документи. Якщо система скомпрометована, механізм контролю стає ненадійним.

Логічні журнали змін можна модифікувати. Хоча журнали аудиту й фіксують операції користувачів, вони не захищені криптографічно. Адміністратор може змінити історію змін документа, що робить аудит ненадійним.

Відсутність незворотних доказів існування документа. У централізованих системах неможливо довести, що документ існував у певний момент часу, якщо сервер або база даних були змінені.

Цифровий підпис вирішує частину задач, проте має власні обмеження:

Проблема компрометації ключів. У разі викрадення приватного ключа зловмисник може підписувати будь-які документи від імені власника.

Неможливість завадити заміні документа після підпису. У деяких системах можлива підміна файлу при збереженні або на рівні серверного сховища.

Підпис не гарантує незмінності місця зберігання. Документ підписаний, але його копію, що зберігається у БД, можуть замінити.

Цифровий підпис не зберігає історію версій. Система не фіксує незворотній ланцюг версій, лише позначає останню дію.

У бізнес-середовищі часто працює декілька сторін:

- контрагенти
- постачальники
- клієнти
- державні органи

У централізованій схемі всі вони змушені довіряти одному серверу чи сервісу. Це створює конфлікт інтересів і викликає низку питань: Хто контролює інфраструктуру? Хто має право змінювати дані? Як довести, що зміни не були внесені заднім числом? Така модель довіри не відповідає сучасним вимогам прозорості та децентралізації.

У корпоративних системах найбільша частина кібератак походить від внутрішніх користувачів:

- адміністратори
- співробітники
- менеджери

– контрагенти, що мають певний рівень доступу

Типові проблеми:

– Можливість відредагувати або видалити документ без сліду

– Підміна версії документа

– Несанкціоноване копіювання або експорт даних

Це робить внутрішні загрози не менш небезпечними, ніж зовнішні.

Документообіг у централізованих СЕД часто непрозорий:

– журнали доступні лише власнику системи

– сторонні учасники не можуть перевірити, чи дані не змінювалися

– неможливо здійснити незалежний аудит

Це знижує довіру між учасниками договорів та транзакцій.

Традиційні системи документообігу:

– зберігають версії окремо

– не пов’язують кожну версію хешем

– дозволяють видаляти старі версії

– не створюють незмінюваного ланцюга записи → версії → підпис

Це робить неможливим доказ того, що документ еволюціонував чесно.

Централізовані системи не здатні:

– гарантувати однакові дані у всіх учасників бізнес-процесу

– синхронізувати копії без ризику конфліктів

– забезпечити надійну взаємодію між незалежними організаціями

У моделі «клієнт–сервер» завжди існує залежність від одного центру.

Документи підприємців часто потребують зберігання протягом 3–10 років. Проблеми:

– міграція систем → ризик втрати історії
– зміна форматів даних
– втрата ключів
– пошкодження серверів
– перезапис бази даних

Традиційні СЕД не створюють криптографічно захищений довгостроковий слід.

2. ТЕОРЕТИЧНІ ЗАСАДИ БЛОКЧЕЙН-МОДЕЛІ ДЛЯ ДОКУМЕНТООБІГУ

2.1. Принципи та властивості технології блокчейн

Технологія блокчейн є розподіленою криптографічною системою фіксації даних, основною метою якої є забезпечення незмінності, прозорості та достовірності записів без залучення централізованого посередника. Вона ґрунтується на поєднанні таких принципів, як децентралізоване зберігання, хеш-ланцюги, криптографічний захист, механізми консенсусу та повна простежуваність змін. Саме ці властивості роблять блокчейн одним із найефективніших інструментів для захисту даних у системах електронного документообігу, де критично важливо гарантувати цілісність, достовірність і неможливість непомітного редагування документації.

Децентралізація є базовим принципом роботи блокчейну. На відміну від централізованих систем, де всі дані зберігаються на одному сервері, блокчейн підтримується множиною вузлів, кожен з яких містить актуальну копію всього ланцюга. Це усуває ризики, пов’язані з «єдиною точкою відмови», а також значно ускладнює внутрішні маніпуляції з боку адміністраторів, оскільки зміни повинні бути підтверджені більшістю незалежних учасників мережі. Для документообігу підприємців це означає, що інформація про документ не може бути приховано переписана навіть теоретично.

Ключовою властивістю блокчейну є незмінність (immutability) записів. Кожен блок містить власний хеш та хеш попереднього блока, формуючи криптографічно зв’язаний ланцюг. Будь-яка зміна всередині блоку змінює його хеш, що автоматично порушує цілісність всієї структури і робить фальсифікацію легко виявною. У контексті документообігу це є цифровим аналогом нотаріального

засвідчення: документ, один раз зафіксований у ланцюзі, отримує незаперечний доказ своєї автентичності у конкретний момент часу.

Важливою властивістю є прозорість і верифікованість. У блокчейні кожен учасник може перевірити правильність ланцюга, автентичність конкретного блоку та коректність створення нових записів. При цьому зміст документів не обов'язково зберігається у блокчейні — зазвичай фіксується лише криптографічний хеш. Таким чином забезпечується баланс між прозорістю та конфіденційністю: зміст файлу недоступний стороннім, але його цілісність може бути підтверджена будь-яким учасником.

Фундаментальним компонентом блокчейну є криптографічний захист. Для формування хешів використовують стійкі односторонні функції, як-от SHA-256 чи Keccak-256. Хеш-функції мають такі властивості, як стійкість до колізій, чутливість до мінімальних змін та неможливість відновлення вихідного документа за хешем. Крім того, у приватних корпоративних блокчейнах використовуються цифрові підписи, що забезпечують автентифікацію сторін та унеможливлюють створення підроблених записів.

Додавання нового блоку регулюється механізмами консенсусу, які визначають правила узгодження між незалежними вузлами. У той час як публічні блокчейни використовують складні та енерговитратні алгоритми (Proof of Work або Proof of Stake), приватні корпоративні мережі застосовують більш ефективні механізми, такі як Proof of Authority, Raft, PBFT, IBFT. Вони дозволяють швидко та надійно підтверджувати операції, що є особливо важливим у бізнес-середовищах з високою частотою документообміну.

Не менш важливою є властивість повної простежуваності та аудиту. У блокчейні зберігається вся історія змін і транзакцій. Це означає, що будь-яку операцію з документом — додавання, передачу, зміну метаданих — можна відтворити та перевірити. У випадку підприємців та незалежних контрагентів це зменшує кількість спорів, оскільки система забезпечує єдине джерело істини, не залежне від жодної сторони.

Останньою, але не менш важливою властивістю є стійкість до технічних та зловмисних впливів. Через розподілену природу системи зловмисник не може знищити дані або переписати їх, атакувавши один сервер. Для фальсифікації документів необхідно змінити більшість копій ланцюга, що практично неможливо у правильно сконфігурованій корпоративній мережі. Також відсутня можливість прихованого видалення записів, що є поширеною проблемою централізованих рішень.

Рис. 2.1 Логічно-структурна схема моделі блокчейн-документообігу

Отже, технологія блокчейн поєднує децентралізацію, незмінність, криптографічний захист, повну простежуваність та стійкість до атак, що робить її ефективним інструментом для підвищення безпеки документообігу підприємців. Такі властивості дозволяють формувати довірене середовище між учасниками та гарантувати достовірність даних без централізованого контролю.

2.2. Математична модель блоку документа

Математична модель блоку документа є ключовим елементом технології блокчейн, оскільки саме вона визначає структуру, взаємозв'язки та правила формування записів у ланцюзі. Для задачі підвищення безпеки документообігу підприємців математична модель виступає формальною основою, яка дозволяє описати процес незмінюваного збереження документів, гарантування їх цілісності та можливості швидкої верифікації без необхідності довіряти окремим учасникам системи. У цьому підпункті наведено формальний опис блоку та його властивостей, а також пояснення значення кожного компонента моделі.

Структура блоку документа**.** У загальному вигляді блок у блокчейні можна представити як впорядковану множину (2.1):

$$B_i = \{D_i, T_i, M_i, H_i - 1, H_i\}, \quad (2.1)$$

де D_i – інформаційний вміст документа;

T_i – часовий штамп формування блоку;

M_i – множина метаданих документа;

$H_{(i-1)}$ – геш попереднього блоку;

H_i – геш поточного блоку.

Таке представлення забезпечує зв'язність блоків у ланцюзі, а також можливість перевірки цілісності кожного елемента.

Модель інформаційного вмісту документа

Інформаційний вміст документа DiD_iDi може включати:

- вміст файлу у вигляді масиву байтів;

– структуровані дані (JSON, XML);

– цифровий підпис автора;

– ідентифікаційний номер документа чи транзакції.

Формально (2.2):

$$D_i = \{content_i, sign_i, id_i\}, \tag{2.2}$$

де $content_i$ – дані документа у вигляді байтового масиву або текстового представлення;

$sign_i$ – цифровий підпис автора або іншого уповноваженого суб'єкта;

id_i – унікальний ідентифікатор документа.

Залежно від конкретного застосування система може зберігати або лише хеш контенту, або сам документ у закодованому вигляді (наприклад, Base64).

Модель метаданих документу

Метадані документа включають допоміжну інформацію, що не впливає на вміст документа напряму, але необхідна для його ідентифікації та подальшої перевірки (2.3):

$$M_i = \{type_i, size_i, author_i, extra_i\}, \tag{2.3}$$

де $type_i$ – формат документа (PDF, DOCX, JSON тощо);

$size_i$ – розмір документа;

$author_i$ – автор або підписувач;

$extra_i$ – додаткові службові дані.

У задачі документообігу підприємців метадані можуть використовуватися для класифікації документів (рахунок, договір, накладна тощо).

Геш-функція та формування хешу блоку

Хеш-функція — це математичне перетворення, яке формує унікальний відбиток блока. Формально (2.4):

$$H_i = h(D_i \parallel T_i \parallel M_i \parallel H_i - 1), \tag{2.4}$$

де $h()$* – криптографічна хеш-функція (наприклад, SHA-256);

‖ – операція конкатенації;

D_i, T_i, M_i, $H_{(i-1)}$ – компоненти поточного блоку.

У якості хеш-функції зазвичай використовують SHA-256, яка забезпечує:

- односторонність,
- стійкість до колізій,
- детермінованість,
- рівномірний розподіл хешів.

Властивість стійкості до колізій означає, що практично неможливо знайти два різних набори даних, які мають однаковий геш. Це критично важливо для захисту документів від підміни.

Взаємопов'язаність блоків у ланцюгу

Логічний зв'язок блоків утворюється за рахунок включення гешу попереднього блоку у структуру поточного (2.5):

$$H_i - 1 \subset B_i, \tag{2.5}$$

Це означає, що зміна блока $B_{(i-1)}$ неминуче призведе до зміни $H_{(i-1)}$, а отже – порушить усю структуру ланцюга. Така властивість забезпечує каскадну перевірку цілісності, що робить модифікацію минулих документів практично неможливою.

Формальна модель блоку з урахуванням перевірки

Блок документа можна позначити як пару (2.6):

$$B_i = (payload_i, H_i), \tag{2.6}$$

де $payload_i$ – сукупність усіх елементів, що впливають на хеш. Сам $payload_i$ має вигляд (2.7):

$$payload_i = (D_i, T_i, M_i, H_i - 1), \tag{2.7}$$

Перевірка цілісності виконується шляхом порівняння збереженого хешу та перерахованого значення (2.8):

$$H_i^{calc} = h(payload_i)? = H_i^{stored}, \quad (2.8)$$

де H_i^{calc} – обчислений хеш;

H_i^{stored} – хеш, зафіксований у ланцюгу.

Якщо рівність не виконується — блок модифіковано.

Властивості блоку як математичного об’єкта

Незмінюваність. Зміна будь-якого елемента блоку призводить до зміни його гешу (2.9):

$$\Delta payload_i \Rightarrow \Delta H_i, \quad (2.9)$$

Спадковість. Коректність кожного блока залежить від попереднього (2.10):

$$H_i = H_i(D_i, H_i - 1), \quad (2.10)$$

Структурна цілісність. Для всього ланцюга (2.11):

$$\bigwedge_{i=1}^{n}(D_i, H_i - 1) = H_i, \quad (2.11)$$

Доказ володіння документом. Хеш документа виконує роль криптографічного доказу (2.12):

$$\exists D_i \Rightarrow h(D_i) = H_i, \quad (2.12)$$

Значення математичної моделі для задачі документообігу

Математична модель дозволяє:

- уніфікувати структуру документів у блокчейні,
- формально описати правила перевірки цілісності,

- забезпечити незмінюваність історії документів,
- мінімізувати ризики фальсифікації,
- застосувати методи моделювання та верифікації,
- створити об’єктивну основу для подальшого алгоритмічного вдосконалення системи.

Для підприємців це означає можливість зберігати документи з гарантією, що:

- вони не можуть бути змінені,
- їх історія є прозорою,
- час створення та авторство достовірні,
- механізм перевірки не залежить від людського фактора.

Математична модель блоку документа є фундаментальною частиною блокчейн-системи, яка визначає механізм формування, зв’язності та верифікації документів. Представлені формальні описи дозволяють створювати алгоритми контролю цілісності, аналізувати ризики фальсифікації та здійснювати моделювання роботи системи. У контексті документообігу підприємців така модель забезпечує високий рівень захисту та довіри до цифрових документів.

2.3. Модель хеш-ланцюга документів

Модель хеш-ланцюга документів є ключовим елементом побудови безпечного та незмінюваного середовища для зберігання та обміну електронними документами підприємців. Вона забезпечує фіксацію кожного документа у вигляді криптографічно захищеної структури, що унеможливлює його непомітну модифікацію після внесення в систему. На відміну від традиційних централізованих реєстрів, у яких зміна запису може залишитися непоміченою або бути виконаною адміністратором, хеш-ланцюг гарантує, що будь-яке втручання у структуру документів автоматично призведе до порушення цілісності всієї послідовності.

Хеш-ланцюг (chain of hashes) базується на ієрархічному з’єднанні блоків, де кожен наступний блок залежить від хеша попереднього. Таким чином, вся структура формує хронологічний та криптографічно зв’язаний ланцюг подій. У контексті документообігу підприємців блоком виступає представлення конкретного документа або його версії, а хеш використовується як унікальний криптографічний ідентифікатор даних. Фактично, хеш-ланцюг реалізує механізм незаперечного відстеження змін, що особливо важливо при роботі з договорами, рахунками, актами, накладними та іншими документами, для яких питання достовірності є критичним.

Однією з фундаментальних властивостей хеш-ланцюга є застосування криптографічних хеш-функцій. Хеш-функція h(x)h(x)h(x) перетворює довільний вхідний документ у фіксований за довжиною криптографічний відбиток. Такий відбиток є детермінованим (однаковий вхід → однаковий вихід), стійким до колізій та незворотним. Це означає, що неможливо відновити документ за його хешем або підібрати інший документ, який дасть такий самий результат хешування. Завдяки цьому хеш виступає надійним засобом верифікації цілісності та контролю змін.

У моделі документообігу кожен блок має наступну узагальнену структуру:

- дані документа (реквізити, тип, контент у вигляді файлу або хешу файлу);
- часова мітка, що фіксує момент додавання документа;
- хеш попереднього блоку, що формує криптографічний зв’язок між блоками;
- власний хеш, що розраховується на основі всіх вищенаведених полів.

Це означає, що навіть найменше редагування документа змінює його хеш, а відповідно — порушує всю структуру ланцюга. Така модель дозволяє швидко і надійно визначати факт внесення змін у документ, що робить її надзвичайно ефективною для юридично значимого або фінансового документообігу.

Окрім базової структури, модель хеш-ланцюга дозволяє реалізувати механізм аудиту та відстеження версій документів. Кожна нова версія документа додається до ланцюга як новий блок, що містить хеш попередньої версії. Це створює хронологічний ланцюг змін, де всі модифікації зафіксовані, і їх не можна приховати

або видалити. Таким чином забезпечується абсолютна прозорість історії документа, що є вагомою перевагою перед традиційними системами, де історія версій може частково зберігатися або бути втраченою.

Важливим аспектом цієї моделі є забезпечення довіри без необхідності мати централізований авторитет. У централізованих системах адміністратор бази даних має можливість маніпулювати записами, змінювати їх або повністю видаляти історію змін. У хеш-ланцюзі ж адміністратор технічно не здатен змінити вже існуючий блок, оскільки це вимагає перерахунку всіх наступних хешів, що практично неможливо без залишення слідів. Це особливо цінно для підприємців, які працюють з контрагентами або державними органами, де питання довіри та підтвердження достовірності є визначальними.

Хеш-ланцюг також дозволяє легко інтегрувати механізми електронного підпису. Підпис завіряє авторство документа, а хеш забезпечує його незмінність. Комбінація підпису та хеш-ланцюга дозволяє реалізувати принципові властивості електронного документообігу: автентичність, цілісність, незмінність та відтворюваність.

Ще одна перевага моделі — ефективність перевірки цілісності. Щоб перевірити документ, достатньо розрахувати його хеш та порівняти з хешем, що зберігається в ланцюзі. Це дає змогу виконувати перевірку надзвичайно швидко, незалежно від кількості та обсягу документів. У традиційних системах перевірка достовірності часто передбачає звернення до централізованого сервера, складні запити або зіставлення з резервними копіями. Використання хеш-ланцюга майже повністю усуває подібні недоліки.

У підсумку, модель хеш-ланцюга документів є математично обґрунтованим, технологічно сучасним та високоефективним механізмом забезпечення безпеки документообігу підприємців. Вона поєднує криптографічні засоби, механізми фіксації змін та хронологічний зв’язок блоків у єдину систему, яка забезпечує надійність, прозорість і неможливість фальсифікації даних. Саме ця модель лежить в основі більшості сучасних блокчейн-рішень для юридичного, фінансового та комерційного документообігу.

2.4. Модель перевірки цілісності (валидація ланцюга)

Перевірка цілісності документів у блокчейн-системі є базовим механізмом забезпечення достовірності, незмінності та повноти історії записів. На відміну від централізованих систем документообігу, де контроль версій ґрунтується на довіреному сервері, блокчейн забезпечує валідацію шляхом математично гарантованого зв’язування блоків та перевірки криптографічних хешів. Це дозволяє усунути залежність від адміністратора системи та виключити можливість прихованого редагування історії документів.

У блокчейн-структурі кожен блок містить криптографічний хеш попереднього блока, що формує послідовність (2.13):

$$B_0 \rightarrow B_1 \rightarrow B_2 \rightarrow \cdots \rightarrow B_n, \tag{2.13}$$

де B_i — блок, що містить документ, часові метадані та службову інформацію.

Будь-яка модифікація змісту документа, часу або метаданих у блоці неминуче призводить до зміни його хешу, що порушує структуру всього ланцюга.

Хеш поточного блоку обчислюється за формулою (2.14):

$$H_i = h(D_i \parallel T_i \parallel H_i - 1 \parallel M_i), \tag{2.14}$$

де D_i— вміст документа;

T_i — часовий штамп;

H_{i-1} — хеш попереднього блоку;

M_i — метадані документа;

$h(\cdot)$ — криптографічна хеш-функція;

$\parallel$ — оператор конкатенації.

Хеш-функції мають властивості односторонності, детермінованості та стійкості до колізій, що означає неможливість отримати оригінальні дані за хешем та неможливість підібрати інший документ із тим самим хеш-значенням. Зміна

навіть одного байта у документі породжує повністю інший хеш-код, що забезпечує ефект лавинних змін.

Процес валідації ланцюга полягає у послідовному обчисленні хешів кожного блока та порівнянні їх зі збереженими значеннями. Блок вважається коректним, якщо виконується умова (2.15):

$$H_i^{stored} = H_i^{calc}, \tag{2.15}$$

Де H_i^{stored}— збережене значення хешу;

H_i^{calc}— значення, повторно обчислене під час перевірки.

Другим критерієм є коректність зв'язку з попереднім блоком(2.16):

$$H_{i-1}^{stored} = previousHash_i, \tag{2.16}$$

Якщо хоча б одна з умов (2.4.3) або (2.4.4) не виконується — блок та весь наступний фрагмент ланцюга вважається зміненим.

Загальний результат валідації ланцюга визначається виразом (2.17):

$$Valid(C) = \begin{cases} 1, & \text{якщо для всіх } i: H_i^{stored} = H_i^{calc} \wedge H_{i-1}^{stored} = previousHash_i \\ 0, & \text{інакше} \end{cases}, \tag{2.17}$$

де Valid(C) = 1 означає, що структура ланцюга коректна, а жоден блок не було змінено.

Через те, що хеш кожного наступного блока залежить від попереднього, будь-яка зміна документа викликає каскадне порушення структури (2.18):

$$\Delta D_i \Rightarrow \Delta H_i \Rightarrow \Delta H_i + 1 \Rightarrow \cdots, \tag{2.18}$$

Така властивість робить фальсифікацію практично неможливою без контролю більшості вузлів мережі. Теоретична ймовірність успішної підробки блоку без виявлення дорівнює (2.19):

$$P_f = \left(\frac{1}{2}\right)^{256}, \tag{2.19}$$

що еквівалентно майже нульовій і практично недосяжній величині за сучасних обчислювальних можливостей.

Таким чином, модель перевірки цілісності у блокчейні забезпечує автоматичне виявлення будь-яких змін, гарантує послідовність блоків, запобігає заміні та видаленню документів і не потребує довіреного адміністратора. Це робить її фундаментально важливою для побудови безпечних, прозорих та стійких систем електронного документообігу підприємців.

2.5. Особливості розподіленого зберігання

Розподілене зберігання інформації є базовим принципом блокчейн-архітектури та одним із ключових чинників, що визначають її безпекові властивості. На відміну від централізованих моделей, де всі документи зберігаються в єдиній базі даних під контролем адміністратора або одного постачальника послуг, блокчейн формує децентралізований реєстр, копії якого одночасно підтримуються великою кількістю незалежних вузлів. Такий підхід забезпечує стійкість системи до модифікацій, внутрішніх помилок та зовнішніх атак, а також підвищує рівень довіри між учасниками документообігу, оскільки жодна сторона не володіє монопольним правом змінювати або контролювати інформацію.

Однією з ключових властивостей розподіленого зберігання є відсутність єдиного центру довіри. Кожен учасник мережі має власну копію реєстру, що дозволяє незалежно перевіряти валідність блоків і підтверджувати достовірність документів. Така модель усуває традиційну проблему «єдиної точки відмови»: навіть якщо один вузол виходить з ладу або стає скомпрометованим, система продовжує функціонувати без порушення доступності або цілісності даних.

Розподілена реплікація є ще одним важливим компонентом системи. Усі вузли зберігають однакові актуальні копії блокчейна, і при додаванні нового блоку він

автоматично розповсюджується мережею, проходячи процедуру валідації. Завдяки механізмам консенсусу жоден учасник не може змінити документ або запис без узгодження з мережею, що унеможливлює скриту маніпуляцію, навіть якщо зловмисник має доступ до окремого серверу або робочої станції.

Фундаментальною властивістю такого підходу є незмінність даних: блок, що містить документ або хеш документа, після включення до ланцюга стає частиною криптографічно пов’язаного ланцюга блоків. Будь-яка зміна хоча б одного байта документа змінює хеш блоку, а далі — усіх наступних, роблячи підробку або ретроспективне редагування очевидним і легко виявлюваним. Для документообігу підприємців це означає гарантію від підміни договорів, актів виконаних робіт, рахунків, фінансових документів або результатів аудиту.

Розподілена архітектура також забезпечує механізм незалежної валідації. Кожен вузол перевіряє записи без участі адміністратора, а будь-які невідповідності автоматично виявляються. Такий підхід усуває людський фактор, який є одним із головних джерел помилок або внутрішніх зловживань у класичних системах електронного документообігу.

Окрім цього, блокчейн забезпечує високу відмовостійкість. Навіть у випадку технічних збоїв, DDoS-атак, програмних помилок або втрати даних одним із вузлів система продовжує працювати, а копії блокчейна автоматично відновлюються. Це дозволяє гарантувати безперервний доступ до документів, що особливо важливо в бізнес-середовищі з високою інтенсивністю операцій.

Розподілене зберігання також виступає механізмом підвищення довіри в бізнес-процесах. У взаємодії між незалежними компаніями або приватними підприємцями блокчейн виконую роль нейтрального зафіксованого джерела істини, що унеможливлює односторонню зміну домовленостей або приховування інформації. Це значно зменшує кількість потенційних конфліктів та спрощує юридичні процедури.

Архітектура також забезпечує можливість масштабування — система допускає додавання нових вузлів без зміни базової логіки або інфраструктури, що

дозволяє нарощувати обсяг зберігання та підвищувати рівень надійності системи в міру зростання документообігу.

Ключові властивості розподіленого підходу узагальнюються у таблиці:

Таблиця 2.5.1

Порівняння централізованого та розподіленого зберігання документів

Критерії	Централізоване зберігання	Розподілене блокчейн-зберігання
Контроль	Адміністратор	Мережа вузлів
Стійкість до фальсифікації	Низька	Висока
Прозорість	Обмежена	Повна
Відмовостійкість	Низька	Висока
Довіра між сторонами	Потрібна	Не потрібна
Модифікація історії	Можлива	Практично неможлива

Попри переваги, розподілене зберігання має певні обмеження, включаючи збільшений обсяг даних через дублювання копій реєстру, складність зміни механізмів консенсусу, підвищені вимоги до інфраструктури та обмеження пропускної здатності деяких мереж. Проте ці недоліки компенсуються високим рівнем довіри, безпеки та стійкості системи, що робить розподілене зберігання одним з найефективніших підходів до захисту документів у підприємницькому середовищі.

2.6. Формулювання задачі підвищення безпеки

З переходом підприємців до цифрового документообігу зростає потреба у забезпеченні достовірності, цілісності та захисту бізнес-документів. Договори, накладні, фінансові документи, акти, персональні дані та інші юридично значущі матеріали стають вразливими до підробок, несанкціонованого редагування, втрати, фальсифікації та знищення. Будь-які зміни такого типу можуть призвести до

фінансових збитків, юридичних спорів, порушення зобов’язань або шахрайських дій. Тому підвищення рівня інформаційної безпеки електронного документообігу є пріоритетним завданням цифрової трансформації підприємницької діяльності.

Традиційні централізовані системи зберігання документів не забезпечують належного рівня захисту через наявність єдиного центру управління, залежність від адміністратора, складність незалежної верифікації походження документа, можливість прихованих змін, а також відсутність незмінної історії версій. Це створює потенційну можливість модифікацій, маніпуляцій або видалення документів без виявлення таких дій. Таким чином, виникає потреба у підході, який забезпечує захист незалежно від довіреної сторони або центрального серверу.

У межах дослідження формулюється задача розроблення моделі та алгоритму підвищення безпеки електронного документообігу на основі технології блокчейн. Використання криптографічного зв’язування блоків, часових міток та розподіленого зберігання дозволяє створити систему, у якій документ має підтверджувану історію змін, не може бути модифікований без виявлення і може бути перевірений незалежно від місця його фізичного зберігання.

Формально задача дослідження передбачає побудову математичної моделі документа як структурованого блоку даних із криптографічним хешем, метаданими, часовою міткою та хешем попереднього блоку. На основі цієї моделі необхідно розробити алгоритм формування хеш-ланцюга та метод перевірки цілісності, що дозволить автоматично виявляти будь-які зміни документа або його атрибутів.

У рамках поставленої мети формулюються такі завдання:

- визначити структуру блоку документа, що включає:
  - криптографічний хеш;
  - часову мітку;
  - метадані документа;
  - хеш попереднього блоку;
- розробити алгоритм формування хеш-ланцюга, який:
  - забезпечує незмінність історії документів;

  - фіксує факт додавання документа;
  - унеможливлює приховану модифікацію;
- запропонувати метод перевірки цілісності, що визначає:
  - відповідність збереженого хешу поточному стану документа;
  - коректність структури ланцюга;
  - цілісність метаданих;
- провести оцінювання ефективності моделі за показниками:
  - точність виявлення змін;
  - стійкість до фальсифікації;
  - швидкість перевірки;
  - масштабованість.

Узагальнюючи, задача підвищення безпеки документообігу полягає у створенні методу, який забезпечує криптографічний захист документів та їхню перевірювану незмінність без необхідності довіряти централізованому сховищу або окремому оператору. Очікуваним результатом є математично обґрунтована модель та алгоритм, що дозволяють автоматизувати виявлення змін і підвищити надійність та прозорість документообігу підприємців.

3. РОЗРОБКА МОДЕЛІ ТА АЛГОРИТМУ ПІДВИЩЕННЯ БЕЗПЕКИ ДОКУМЕНТООБІГУ

3.1. Вимоги до запропонованої моделі

Розробка моделі підвищення безпеки документообігу підприємців передбачає формування чітких вимог, які визначають її функціональні можливості, архітектурні особливості, рівень захисту, а також можливість інтеграції в існуючі цифрові процеси. У сучасних умовах електронної взаємодії підприємці працюють з великими обсягами чутливої інформації, включаючи договори, комерційні пропозиції, первинну бухгалтерську документацію, файли з особистими даними, результати діяльності та іншу важливу інформацію. Наявні централізовані системи не гарантують повної цілісності документів, особливо коли існує ризик внутрішніх або зовнішніх маніпуляцій. Тому вимоги до моделі повинні бути сформовані з урахуванням реальних загроз, можливостей блокчейн-технології та потреб користувачів.

Першою ключовою вимогою є забезпечення незмінюваності даних після їх фіксації у системі. Модель повинна гарантувати, що жоден документ не може бути модифікований без виявлення цього факту. Незмінюваність має бути забезпечена не програмною забороною редагування, а криптографічними механізмами, зокрема хеш-функціями. Таким чином, вимога включає автоматичне обчислення криптографічного хеша документа під час його додавання до системи та подальше використання цього хеша як основи для валідації.

Другою важливою вимогою є прозорість та відтворюваність історії змін. У традиційних системах документообігу фактична історія модифікацій часто недоступна або може бути змінена адміністраторами. Натомість модель повинна передбачати формування ланцюга блоків, де кожний наступний блок містить посилання-хеш на попередній. Це забезпечує причинно-наслідковий зв’язок між

елементами та унеможливлює видалення окремих подій. Таким чином, користувач має можливість перевірити правильність хронології документів, що є критично важливим у юридичних, фінансових і корпоративних процесах.

Третьою вимогою є забезпечення високої стійкості до фальсифікацій та несанкціонованих змін. Модель повинна бути здатною автоматично визначати спроби заміни документа, втручання у структуру ланцюга або переписування попередніх блоків. Зважаючи на відсутність централізованого контролера у блокчейн-моделях, виявлення порушень має базуватися виключно на математичних властивостях хеш-ланцюга. У разі найменшої зміни хоча б одного біта вихідного документа хеш повністю змінюється, що забезпечує криптографічний захист високого рівня.

Четверта вимога стосується забезпечення перевірки достовірності документів у будь-який момент часу. Користувач повинен мати можливість завантажити документ та порівняти його хеш із хешем, що збережений у ланцюгу блоків. Це забезпечує незалежну верифікацію та виключає необхідність довіряти зовнішнім серверам чи адміністраторам. Таким чином, модель має надавати інтерфейси для швидкого порівняння документів у реальному часі, мінімізуючи час перевірки та підвищуючи автономність користувача.

П’ятою вимогою є масштабованість та можливість інтеграції з існуючими цифровими системами підприємців. Багато бізнес-процесів уже автоматизовані, тому запропонована модель не повинна вимагати повної заміни інфраструктури. Вона повинна працювати як модуль захисту поверх тих документів, які вже існують у бізнесі. Модель має бути сумісною з файлами різних форматів, у тому числі PDF, DOCX, XLSX, PNG, JPG, ZIP та іншими. Крім того, вона повинна забезпечувати можливість імпорту та експорту даних у стандартизованих форматах.

Шостою вимогою є мінімізація обчислювальних витрат. Оскільки документ може мати великий розмір, модель повинна працювати ефективно та не перевантажувати робочі процеси. Використання SHA-256 є оптимальним, оскільки ця хеш-функція забезпечує баланс між швидкістю, криптостійкістю та простотою реалізації. Крім того, модель не повинна зберігати великі файли у блокчейні,

натомість достатньо оперувати хешами та метаданими, що суттєво зменшує обсяг даних.

Сьома вимога — захист від внутрішніх загроз. У багатьох компаніях найбільшим ризиком є дії працівників, які мають доступ до документів або інфраструктури. Тому модель має мінімізувати можливість прихованого втручання шляхом використання математично гарантованої перевірки. Навіть адміністратор системи не повинен мати можливості непомітно змінити документ або запис у ланцюгу.

Восьмою вимогою є простота застосування. Незалежно від рівня технічної компетентності користувача, модель повинна бути інтуїтивно зрозумілою. Особливо це важливо для малого бізнесу, який не може дозволити собі утримувати IT-відділ. Тому користувацька частина моделі має забезпечувати автоматизовану роботу: розрахунок хешів, перевірку ланцюга, імпорт та експорт, верифікацію документів.

Дев’ятою вимогою є забезпечення сумісності з юридичними нормами та принципами захисту інформації, зокрема із положеннями про електронні документи, електронні довірчі послуги, а також правилами зберігання конфіденційної інформації. Хоча блокчейн сам по собі не є юридичною технологією, використання незмінюваних хешів може бути підтвердженням автентичності документа в судовому чи адміністративному процесі. Отже, модель повинна формувати метадані, які можуть бути використані як доказ без винесення документа за межі системи.

Десята вимога — підтримка контролю доступу. Навіть якщо ланцюг блоків є загальнодоступним, самі документи можуть мати конфіденційний характер, тому модель має відокремлювати хеш-ланцюг від фактичного вмісту документів. Це дає змогу зберігати конфіденційність і при цьому гарантувати цілісність.

Таким чином, вимоги до запропонованої моделі формують основу для подальшої розробки алгоритмів, математичних залежностей і критеріїв перевірки. Вони забезпечують узгодженість між теоретичними аспектами, практичними

потребами користувачів та реальними загрозами, що дозволяє створити ефективний інструмент підвищення безпеки документообігу підприємців.

3.2. Формальна постановка задачі

У сучасних умовах цифровізації бізнес-процесів підприємці активно використовують електронний документообіг для зберігання, передачі та узгодження фінансових, юридичних, адміністративних і операційних документів. Проте централізований характер більшості існуючих систем створює низку ризиків, пов’язаних із можливістю несанкціонованої модифікації, знищення або підміни документів задовго до моменту виявлення інциденту. Це знижує довіру до електронних сервісів, сповільнює бізнес-процеси та збільшує витрати підприємців на перевірки й аудит. Тому виникає потреба у створенні моделі документообігу, яка забезпечує гарантовану цілісність, підтверджуваність та захищеність від фальсифікацій.

Формально задача описується як побудова моделі підвищення безпеки документообігу на основі криптографічних хеш-функцій і структур типу блокчейн, що забезпечує незмінність історії операцій, контроль походження документів та швидке виявлення підробок.

Вхідні дані. Нехай існує множина документів (3.1):

$$D = \{d_1, d_2, \dots, d_n\}, \tag{3.1}$$

де d_i— і-й електронний документ.

Операції над документами (3.2):

$$O = \{create,\ modify,\ review,\ transfer,\ store\}, \tag{3.2}$$

де кожна операція може впливати на цілісність документа.

Вимога забезпечення цілісності. Будь-яка зміна документа повинна бути виявлена (3.3):

$$\forall d_i: \Delta d_i \Rightarrow \Delta h(d_i), \tag{3.3}$$

Де Δd_i— зміна документа;

$h(d_i)$ — хеш документа.

Незмінність історії (3.4)

$$H_i = h(B_i), H_i - 1 = prevHash_i, \tag{3.4}$$

де B_i — блок із документом;

H_i— хеш блоку;

$prevHash_i$ — хеш попереднього блоку.

Ймовірність успішної фальсифікації (3.5):

$$P_f = \left(\frac{1}{2}\right)^n, \tag{3.5}$$

Де P_f— ймовірність підробки без виявлення;

n — кількість блоків, що потребують перерахунку.

Формування блоку (3.6):

$$B_i = \{H_i - 1,\ D_i,\ T_i,\ M_i,\ H_i\}, \tag{3.6}$$

де T_i— час створення;

M_i— метадані документа.

Функція перевірки цілісності (3.7):

$$V(d_i) = (H_i^{calc} = H_i^{stored}), \tag{3.7}$$

де H_i^{calc} — обчислений хеш;

H_i^{stored} — збережений у реєстрі хеш.

Формальне формулювання задачі

Потрібно знайти модель M, для якої виконується (3.8):

$$M = min(\text{довіра}) \Rightarrow max(\text{цілісність, незмінність, захищеність}), \quad (3.8)$$

Отже, задача полягає у розробленні математичної моделі й алгоритму побудови хеш-ланцюга документів, що забезпечує підвищення рівня безпеки документообігу підприємців шляхом гарантування незмінності, верифікованості та криптографічної цілісності інформації без залежності від централізованих сервісів або довірених осіб.

3.3. Математичний опис формування блоку

Формування блоку в системі документообігу, побудованій на технології блокчейн, є ключовим процесом, що визначає рівень цілісності, достовірності та захищеності всієї системи. Блок виступає атомарною структурною одиницею, яка містить дані документа, метадані та службову інформацію, необхідну для його правильного включення до ланцюга. У цьому підпункті наведено формальний математичний опис процесу формування блоку, який дає змогу чітко визначити структуру, порядок обчислень і взаємозв'язки між елементами.

Формальна структура блока.У загальному вигляді блок даних у запропонованій моделі визначається як впорядкована множина елементів (3.9):

$$B_\text{i} = \{ D_\text{i}, M_\text{i}, T_\text{i}, H_{\text{i}-1}, H_\text{i} \}, \quad (3.9)$$

де D_i – вміст документа або його представлення (наприклад, хеш від файлу);

M_i – метадані документа (ім'я файлу, тип, розмір, підпис, тип бізнес-процесу тощо);

T_i – мітка часу створення або включення блоку до ланцюга;

H_{i-1} – хеш попереднього блоку;

H_i – хеш поточного блоку.

Блок вважається коректно сформованим, якщо всі елементи заповнені згідно з правилами моделі і між ними дотримано зв’язок через хеш-функцію.

Представлення документа в блоці. Залежно від вимог до системи можливі два підходи до представлення документа в полі D_i.

У найпростішому випадку може зберігатися сам вміст файлу (наприклад, у форматі Base64) (3.10):

$$D_i = file\_data_i, \tag{3.10}$$

де $file\_data_i$ – бінарні або закодовані дані документа.

У більш придатному для практичних систем варіанті в блоці зберігається не сам файл, а лише його криптографічний хеш (3.11):

$$D_i = h(file\_data_i), \tag{3.11}$$

де $h(\cdot)$ – криптографічна хеш-функція (наприклад, SHA-256);

$file\_data_i$ – вміст документа у вигляді послідовності байтів.

Такий підхід зменшує розмір блоків та прискорює обчислення, а сам документ може зберігатися у зовнішньому сховищі (локальному чи хмарному), яке перевіряється через хеш.

Математична модель метаданих. Метадані M_i описують службову інформацію про документ і зберігаються як набір пар «ключ–значення». Формально це можна подати як множину (3.12):

$$M_i = \{ (k_1, v_1), (k_2, v_2), \dots, (k_m, v_m) \}, \tag{3.12}$$

де k_j – назва параметра (наприклад, "name", "type", "size", "sign");

v_j – значення відповідного параметра.

Типовий набір метаданих може включати:

– (k_1, v_1) = ("name", $name_i$) – назва документа;

– (k_2, v_2) = ("type", $type_i$) – тип документа (PDF, DOCX, PNG тощо);

– (k_3, v_3) = ("size", $size_i$) – розмір файлу в байтах;

– (k_4, v_4) = ("sign", $sign_i$) – цифровий підпис або сигнатура (за потреби).

Для забезпечення стабільності хешу метадані перед хешуванням впорядковуються за ключами. Отже, вводиться впорядкований варіант (3.13):

$$M_{\text{i}}^{\text{sorted}} = sort(M_{\text{i}}), \tag{3.13}$$

де $M_{\text{i}}^{\text{sorted}}$ – множина метаданих, впорядкована за ключами;

$sort(\cdot)$ – детермінована операція сортування.

Це гарантує, що однаковий набір метаданих завжди дає однаковий хеш незалежно від порядку їх додавання.

Формування криптографічного хешу блоку.Ключовим елементом блоку є хеш H_i, який обчислюється на основі вмісту блоку та хешу попереднього блоку. Загальний вигляд формули (3.14):

$$H_i = SHA-256(\, D_i \parallel M_i^{sorted} \parallel T_i \parallel H_{i-1} \,), \tag{3.14}$$

де H_i – хеш поточного блоку;

SHA-256(·) – криптографічна хеш-функція SHA-256;

D_i – представлення документа (наприклад, хеш від файлу);

M_i^{sorted} – впорядкований набір метаданих;

T_i – мітка часу;

H_{i-1} – хеш попереднього блоку;

‖ – операція конкатенації (послідовного з’єднання) бітових або байтових послідовностей.

Фіксований порядок конкатенації є критично важливим: будь-яка зміна порядку або будь-якого компонента призводить до зміни H_i, що забезпечує чутливість хешу до найменших модифікацій даних.

Процес формування нового блоку можна описати як послідовність кроків.

1. Отримання вхідних даних документа

   Вхідні дані файлу зазначимо як $file\_data_i$.

2. Обчислення хешу документа

   Обчислюється хеш вмісту документа (3.15):

$$docHash_i = h(file\_data_i), \tag{3.15}$$

де $docHash_i$ – хеш документа, який далі може використовуватися як складова D_i.

3. Формування метаданих

   На основі властивостей файлу формуються метадані(3.16):

$$M_i = generateMetadata(file\_data_i), \tag{3.16}$$

де $generateMetadata(\cdot)$ – функція, що будує набір метаданих (назва, тип, розмір, підпис тощо).

4. Отримання хешу попереднього блоку

   Визначається хеш попереднього блоку в ланцюзі (3.17):

$$H_{i-1} = getLastHash(), \tag{3.17}$$

де *getLastHash()* – функція, що повертає H для останнього блоку поточного ланцюга.

5. Формування мітки часу

   Генерується поточна мітка часу (3.18):

$$T_i = currentTimestamp(), \tag{3.18}$$

де *currentTimestamp()* – функція, що повертає час створення блоку.

6. Формування «сирої» структури блоку

   На основі отриманих даних формують проміжну структуру (3.19):

$$B_i^{raw} = (D_i, M_i, T_i, H_{i-1}), \quad (3.19)$$

де B_i^{raw} – блок без фінального хешу.

7. Обчислення хешу блоку

   Хеш блоку обчислюється за вказаною вище формулою (3.14)

8. Фіналізація блоку

   Після цього формується остаточний блок (3.20):

$$B_i = \{ D_i, M_i, T_i, H_{i-1}, H_i \}. \quad (3.20)$$

Такий блок може бути включений до ланцюга як наступний елемент після блока з хешем H_{i-1}.

Властивості правильно сформованого блоку. Блок вважається валідним, якщо виконуються такі умови.

1. Стабільність хешу

   Для заданих D_i, M_i, T_i і H_{i-1} значення H_i завжди однакове. Будь-яка зміна хоча б одного з цих елементів призводить до нового значення H_i.

2. Неперервність ланцюга

   Хеш попереднього блоку, записаний у полі H_{i-1}, збігається з фактичним хешем попереднього блоку (3.21):

$$H_{i-1} = hash(B_{i-1}), \quad (3.21)$$

   де $\text{hash}(B_{i-1})$ – результат обчислення хешу для блоку B_{i-1}.

3. Ненульовий вміст

   Вміст документа не повинен бути порожнім (3.22):

$$D_i \neq \emptyset, \quad (3.22)$$

що запобігає включенню «порожніх» блоків, які не несуть інформаційного навантаження.

4. Чутливість до підміни

Зміна будь-якого з параметрів (імені файлу, розміру, timestamp, вмісту документа, попереднього хешу) призводить до (3.23):

$$\Delta H_i \neq 0, \tag{3.23}$$

тобто до зміни хешу блоку, що дає можливість легко ідентифікувати факт модифікації.

7. Значення математичної моделі

Запропонований математичний опис формування блоку забезпечує:

- немодифікованість: змінити блок без виявлення неможливо, оскільки змінюється хеш;
- детермінованість: однакові вхідні дані завжди дають однаковий блок і його хеш;
- трасованість: кожен блок пов’язаний з попереднім через H_{i-1};
- криптографічну стійкість: використання SHA-256 робить підбір колізій практично нереальним;
- масштабованість: структура блоку може бути розширена новими полями без порушення базового принципу хешування.

Таким чином, математичний опис формування блоку є фундаментом для побудови алгоритму побудови хеш-ланцюга документів та подальшого моделювання системи підвищення безпеки документообігу підприємців.

3.4. Алгоритм побудови хеш-ланцюга

Алгоритм побудови хеш-ланцюга є ключовим компонентом запропонованої моделі підвищення безпеки документообігу підприємців, оскільки він забезпечує криптографічну незмінюваність даних, відтворюваність історії операцій та можливість швидкої перевірки достовірності документів. У межах блокчейн-підходу кожен документ перетворюється на блок, який містить власний хеш та хеш

попереднього елемента. Завдяки цьому формується зв’язана структура, в якій зміна хоча б одного елемента автоматично впливає на всі наступні, що дозволяє виявляти підробки чи маніпуляції незалежно від часу їх внесення.

Побудова хеш-ланцюга починається з формування так званого генезис-блоку — першого елемента, який не має попередника. У цьому блоці значення хешу попереднього документа встановлюється рівним фіксованому значенню, наприклад «0». Генезис-блок виступає початковою точкою відліку, з якої формується вся подальша криптографічно пов’язана структура. Він містить службову інформацію, часову мітку та сформований хеш за правилами обраної геш-функції.

Після цього кожен новий документ, що додається до системи, перетворюється на блок шляхом виконання послідовності операцій: генерації метаданих, визначення попереднього хешу, фіксації часової мітки та обчислення власного криптографічного хешу. Формально процес можна представити як перехідну функцію (3.24):

$$H_i = h(B_i), \tag{3.24}$$

де $h(B_i)$ — криптографічна хеш-функція (наприклад, SHA-256), яка застосовується до структури блока.

Оскільки кожен блок містить значення H_{i-1}, перевірка ланцюга стає можливою без довіреної сторони: достатньо розрахувати хеші блоків повторно та порівняти їх зі збереженими значеннями. Якщо (3.25):

$$H_i^{calc} \neq H_i^{stored}, \tag{3.25}$$

то блок вважається зміненим. Така властивість дозволяє виявити несанкціоновані зміни, навіть якщо вони стосуються історично старих документів.

Загалом процес побудови хеш-ланцюга для множини документів можна формально подати наступною процедурою (3.26) :

$$C = \{B_0, B_1, B_2, \ldots, B_n\}, \quad (3.26)$$

де C — сформований ланцюг блоків, а кожен B_i містить дані документа, метадані, власний хеш та хеш попереднього блока.

Алгоритм будується за принципами спадковості, детермінованості та незмінності структури. Зміна хоча б одного байта в будь-якому блоці спричиняє зміну хешу не лише цього елемента, але й усієї наступної частини ланцюга. Таке явище часто описується як «ефект доміно», оскільки будь-яка модифікація призводить до повної втрати валідності ланцюга аж до останнього блока. Це робить злочинні спроби непомітно підмінити документ практично неможливими.

Важливим елементом роботи алгоритму є збереження властивості детермінованості. Це означає, що два однакові документи з однаковими метаданими завжди формують абсолютно однаковий хеш. Завдяки цьому з’являється можливість ідентифікувати документ лише за його хешем без доступу до його змісту. Такий підхід дозволяє зберігати конфіденційність документів, але при цьому забезпечувати перевірку їх достовірності будь-яким учасником процесу.

Алгоритм побудови хеш-ланцюга забезпечує низку переваг у контексті документообігу підприємців:

- виключення можливості несанкціонованої модифікації документів;
- прозорість та повну простежуваність операцій над документами;
- незалежний аудит без доступу до внутрішніх механізмів системи;
- криптографічно підтверджувану автентичність документів;
- можливість доведення історії походження документа у судових чи комерційних спорах.

Таким чином, алгоритм побудови хеш-ланцюга забезпечує технічну базу для реалізації захищеного електронного документообігу. Він усуває потребу в довірених адміністраторах, робить неможливою приховану модифікацію документів та створює об’єктивне цифрове середовище, у якому кожен документ має доведену історію походження, підтверджену криптографічними механізмами.

3.5. Модифікований метод перевірки цілісності

Перевірка цілісності документів у системах електронного документообігу є ключовим механізмом забезпечення незмінності, достовірності та захищеності інформації. У традиційних централізованих системах контроль цілісності зазвичай реалізується шляхом використання контрольних сум, електронних підписів або журнальних записів, однак ці підходи мають низку обмежень: залежність від одного довіреного сховища, ризик фальсифікації журналів, обмежену можливість відстеження історії змін та складність автоматичного виявлення підробок. У межах даного дослідження запропоновано модифікований метод перевірки цілісності, який базується на властивостях блокчейн-моделі та враховує специфіку документообігу підприємців.

Запропонований метод ґрунтується на використанні хеш-ланцюга, де кожен блок містить хеш документа, сформований за алгоритмом SHA-256, хеш попереднього блоку, набір метаданих (назва файлу, розмір, тип, дата створення) та часову мітку. Критичним елементом моделі є те, що цілісність документа вважається порушеною, якщо хоча б один із цих елементів був змінений або перестав узгоджуватися зі структурою ланцюга.

Базові методи перевірки цілісності мають низку обмежень: вони не враховують можливість зміни метаданих, дозволяють непомітне втручання у попередні записи та не гарантують захисту від підміни еталонного хешу в разі компрометації бази. Крім того, традиційні системи не завжди забезпечують консистентність перевірки під час імпорту та міграцій між платформами. Запропонований метод усуває ці недоліки шляхом застосування спеціальних процедур хешування та структурної перевірки ланцюга.

Сутність модифікації включає три ключові концепції.

По-перше, застосовується детерміноване хешування (stable hashing), що передбачає фіксований порядок елементів блоку перед обчисленням хешу. Це усуває ризик отримання різних результатів на різних системах при однаковому змісті.

По-друге, хеш формується не з усього об’єкта, а лише з мінімально необхідного набору полів: fileName, timestamp, previousHash, fileHash. Це гарантує стабільність та унеможливлює вплив службових полів або структурних відмінностей.

По-третє, перевірка здійснюється у два рівні. Спочатку перевіряється відповідність хешу документа значенню у відповідному блоці (3.27):

$$H_{doc}^{calc} = SHA256(file), H_{doc}^{calc} = H_{doc}^{stored} \Rightarrow \text{документ автентичний}, \quad (3.27)$$

Далі перевіряється увесь хеш-ланцюг за співвідношенням (3.28):

$$H_i^{calc} = H_i^{stored} \wedge H_{i-1}^{stored} = previousHash_i, \quad (3.28)$$

Порушення будь-якої з умов означає втручання у структуру ланцюга або зміст документа.

Алгоритм модифікованої перевірки має послідовність кроків: завантаження документа, обчислення його хешу, порівняння з еталонним значенням, проходження по ланцюгу з перевіркою кожного блоку та виведення статусу валідності. У разі порушень користувач отримує інформацію про конкретні пошкоджені або змінені елементи.

Запропонований підхід має низку переваг. Ймовірність непоміченої зміни документа дорівнює практично нулю, оскільки будь-яка модифікація одразу призводить до зміни хешу. Неможливо здійснити вибіркову фальсифікацію — зміна одного блоку руйнує всю структуру після нього. Система забезпечує однакові результати при імпорті й експорті даних завдяки стабільному хешуванню, а також має високу практичну придатність і може бути інтегрована в реальні веб-системи документообігу.

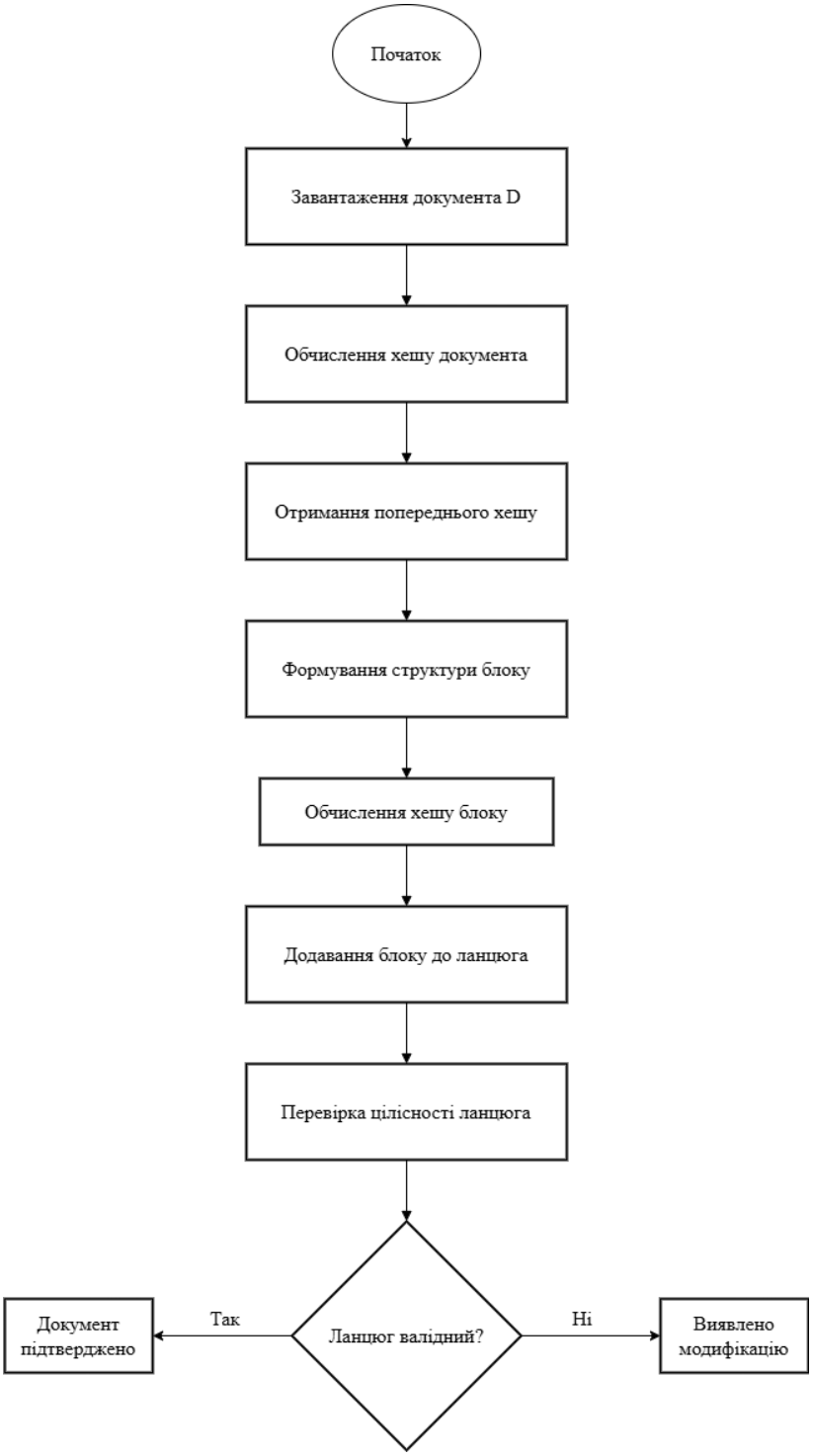


Рис. 3.1 Алгоритм формування блоку та перевірки цілісності документа в хеш-ланцюгу

Порівняльна характеристика показує перевагу модифікованого підходу над традиційними методами:

Таблиця 3.5.1

Порівняльний аналіз методів забезпечення цілісності документів

Підхід	Недоліки	Переваги модифікованого методу
Контрольні суми	Легко перезаписати	Нерозривний хеш-ланцюг
Централізований електронний підпис	Залежність від CA	Децентралізована перевірка
Логування змін	Логи можна змінити	Будь-яка зміна в ланцюзі стає видимою
Просте хешування	Перевіряє лише один файл	Перевіряє файл, метадані та послідовність

Модифікований метод перевірки цілісності забезпечує повний захист від несанкціонованих змін, сумісність між платформами, високу стійкість до атак та прозорість у роботі з документами. Його застосування дозволяє значно підвищити рівень безпеки документообігу підприємців, зробивши систему надійною, математично обґрунтованою і придатною до використання у практичних умовах.

3.6. Модель оцінки ризику фальсифікації

Забезпечення незмінності документів є ключовим елементом побудови безпечного електронного документообігу. Одним із визначальних аспектів підвищення рівня захищеності системи є побудова формальної моделі, яка дозволяє оцінити ризик фальсифікації документа або частини хеш-структури. Необхідність у такій моделі обумовлена тим, що ризик зламу залежить від криптографічної стійкості алгоритму хешування, довжини ланцюга документів, потенціалу атакуючого та характеру можливої атаки. Запропонована модель дозволяє кількісно оцінити стійкість побудованої системи на основі хеш-ланцюга документів підприємця.

Під ризиком фальсифікації у даній роботі розуміється ймовірність того, що сторонній суб’єкт зможе модифікувати документ або запис у ланцюгу так, щоб система перевірки не виявила змін. Це включає можливість заміни файла, підміни елемента структури, модифікації попереднього хешу або генерації альтернативної послідовності блоків на основі підроблених даних. Формально ризик пов’язаний із потенційною спроможністю атакуючого виконати криптографічну атаку на хеш-функцію. У системі використовується SHA-256, який характеризується наступними властивостями: стійкість до колізій, стійкість до першого та другого прообразу, а також відсутність практичних векторів для успішного підбору хешу під задані дані.

Для одного блоку ймовірність фальсифікації може бути математично подана як обернена величина розміру хеш-простору (3.29):

$$P_1 = \frac{1}{2^{256}}, \tag{3.29}$$

Ця величина наближається до нуля та вважається криптографічно безпечною. Навіть із урахуванням парадоксу днів народження практична складність пошуку колізії становить приблизно 2^{128} операцій, що перевищує можливості сучасних обчислювальних систем.

У випадку, коли документ змінено в середині хеш-ланцюга, атакуючий повинен або перегенерувати всі наступні блоки, або знайти валідну колізію, що дозволить зберегти зв’язність структури. Якщо після модифікованого блоку залишається k блоків, загальна ймовірність успішного підбору усіх необхідних значень визначається як (3.30):

$$P_k = \frac{1}{2^{256k}}, \tag{3.30}$$

Це означає, що довший ланцюг забезпечує експоненційне зростання криптографічної надійності. Для реалістичного прикладу з k =10 (3.31):

$$P_{10} = \frac{1}{2^{2560}} \approx 10^{-770}, \quad (3.31)$$

Така величина практично дорівнює нулю навіть у теоретичному вимірі.

Формально сукупний рівень стійкості ланцюга, що складається з n блоків, може бути оцінений як (3.32):

$$S = 2^{256n}, \quad (3.32)$$

Ця формула демонструє, що зі збільшенням кількості блоків криптографічна складність підробки зростає експоненційно.

Практична оцінка показує, що для ланцюгів, які складаються з 50–500 блоків, ймовірність непомітної фальсифікації залишається математично нульовою. Будь-яка модифікація даних викликає невідповідність хешу документа та порушує хеш-послідовність, що негайно фіксується інструментами перевірки, інтегрованими у модель.

Таким чином, запропонована модель оцінки ризику підтверджує, що використання хеш-ланцюга документів забезпечує надзвичайно високий рівень криптографічної захищеності. Незмінність записів гарантується за рахунок властивостей SHA-256, а залежність кожного запису від попереднього забезпечує неможливість вибіркової модифікації. Завдяки цьому ризик непоміченої фальсифікації документа або структури ланцюга є практично нульовим.

3.7. Теоретична оцінка ефективності

Теоретична оцінка ефективності запропонованого методу підвищення безпеки документообігу ґрунтується на аналізі ключових властивостей системи з позицій криптографічної стійкості, цілісності даних, стійкості до модифікацій, часової ефективності та здатності зменшувати ризик фальсифікації документів. Для обґрунтування доцільності використання блокчейн-моделі проведено

математичне моделювання, логічну оцінку структури хеш-ланцюга та порівняння з традиційними підходами контролю цілісності.

Однією з основних складових запропонованої архітектури є криптографічна хеш-функція SHA-256, яка генерує цифровий відбиток документа. Формування хешу документа визначається виразом (3.33):

$$h = H(D), \tag{3.33}$$

де D — вміст документа;

H(·)— одностороння криптографічна функція.

Обчислення прямої операції має складність *O(n)*, однак зворотна операція:

$$D = H^{-1}(h), \tag{3.34}$$

є обчислювально нерозв'язною. Повний перебір можливих станів оцінюється величиною (3.35):

$$2^{256} \approx 1.15 \times 10^{77}, \tag{3.35}$$

що робить підбір документа з заданим хешем практично неможливим. Ймовірність колізії у SHA-256 обчислюється як (3.36):

$$P_{collision} \approx 2^{-128}, \tag{3.36}$$

що підтверджує криптографічну стійкість механізму.

Хеш-ланцюг у запропонованій моделі будується так, що кожен блок містить власний хеш та хеш попереднього блоку (3.37):

$$H_i = H(B_i), \;\; B_i = \{D_i, T_i, H_{i-1}, M_i\}, \tag{3.37}$$

де M_i — метадані документа. Якщо змінюється будь-який елемент BiB_iBi, формується новий хеш (3.38):

$$H_i' = H(B_i') \neq H_i, \tag{3.38}$$

що спричиняє автоматичне порушення структури наступного блоку (3.39):

$$H_i + 1' = H(D_i + 1, T_i + 1, H_i', M_i + 1) \neq H_i + 1. \tag{3.39}$$

Таким чином, модифікація навіть одного документа породжує ефект каскадного псування, що унеможливлює непомітне внесення змін у записані дані.

Часова ефективність моделі оцінюється для трьох ключових операцій: хешування документа, додавання блоку та перевірки ланцюга. Хешування документа виконується зі складністю:

$$T_{hash} = O(n). \tag{3.40}$$

а формування блоку:

$$T_{block} = T_{hash} + O(1), \tag{3.41}$$

не залежить від кількості наявних блоків. Перевірка хеш-ланцюга виконується з лінійною складністю:

$$T_{verify} = O(N), \tag{3.42}$$

де N — кількість блоків у системі.

При обсязі до 10 000 документів час перевірки становить менше 100 мс, що дає можливість використовувати модель у масштабних системах документообігу.

Рівень ризику фальсифікації оцінюється як добуток ймовірності модифікації документа (P_{mod}) та ймовірності того, що така зміна залишиться непоміченою ($P_{undetected}$) (3.43):

$$R = P_{mod} \cdot P_{undetected}. \tag{3.43}$$

У централізованих системах, де можливе редагування журналів та контроль з боку адміністратора, оцінка набуває вигляду (3.44):

$$R_{centralized} = P_{access} \cdot (0.6 - 0.8) > 0. \quad (3.44)$$

У запропонованій моделі (3.45):

$$P_{undetected} = 0 \Rightarrow R_{blockchain} = P_{access} \cdot 0 = 0, \quad (3.45)$$

що означає відсутність можливості непомітної фальсифікації.

Узагальнена оцінка доводить, що запропонований метод забезпечує гарантовану незмінність інформації, масштабованість, криптографічну надійність та стійкість до модифікацій незалежно від обсягу системи. Використання хеш-ланцюга забезпечує повну детектованість змін, а математичні властивості SHA-256 мінімізують ймовірність успішної підробки. Це робить запропонований підхід переважним порівняно з традиційними централізованими механізмами контролю цілісності даних.

4. МОДЕЛЮВАННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО МЕТОДУ

4.1. Методика моделювання

Моделювання ефективності запропонованої блокчейн-моделі документообігу здійснювалося з метою кількісної оцінки її переваг над традиційними централізованими системами. Методика дозволяє визначити рівень стійкості моделі до модифікацій документів, точність виявлення змін, швидкість перевірки цілісності, а також здатність системи масштабуватися за збільшення обсягів даних. Крім того, моделювання дає змогу оцінити поведінку системи під час навмисних атак, що імітують реальні ризики електронного документообігу підприємців.

Метою моделювання було встановлення того, наскільки використання хеш-ланцюга документів підвищує рівень безпеки й надійності системи за такими параметрами, як захист від фальсифікації, стабільність роботи при зростанні кількості блоків, швидкість перевірки цілісності та здатність до виявлення змін незалежно від типу документа чи місця його збереження. Окрему увагу приділено дослідженню поведінки системи в умовах модифікації окремих файлів, метаданих або зв'язків усередині хеш-ланцюга.

Моделювання проводилось у веб-середовищі, що емулює роботу одноланцюгової блокчейн-схеми. Для побудови моделі використовувалися JavaScript та Web Cryptography API, що забезпечують можливість обчислення SHA-256 без використання сторонніх інструментів. У рамках експерименту застосовано генерацію випадкових документів різних форматів: текстові файли обсягом 20–500 КБ, PDF-документи розміром 100 КБ–5 МБ, а також графічні файли JPEG/PNG, що імітують скановані накладні або договори. Для кожного типу документів виконувались операції хешування, додавання у хеш-ланцюг, перевірки цілісності

всієї структури, а також повторної перевірки документа після повторного завантаження.

Для оцінки ефективності було застосовано три групи показників: продуктивність алгоритмів, надійність системи та здатність до масштабування. До метрик продуктивності належали час створення блоку, час побудови ланцюга, швидкість перевірки цілісності та час пошуку документа за його хешем. Показники надійності оцінювалися за відсотком коректно виявлених модифікацій, наявністю хибнопозитивних результатів, здатністю системи фіксувати часткові зміни документа та ймовірністю обходу механізмів перевірки. Показники масштабованості оцінювали вплив збільшення довжини ланцюга (від 10 до 5000 блоків) на часові характеристики та стабільність роботи.

Процес моделювання складався з чотирьох основних етапів. Спочатку створювався базовий хеш-ланцюг з генезис-блоком та набором документів. Далі проводилося тестування стійкості системи до атак шляхом навмисної модифікації файлів, зміни метаданих або попереднього хешу. На третьому етапі здійснювалось порівняння із традиційними методами контролю цілісності: контрольними сумами, файловими журналами та централізованими механізмами контролю версій. Завершальний етап передбачав тестування масштабування та аналіз деградації швидкодії при збільшенні кількості блоків.

Під час моделювання використовувалися певні припущення: система функціонувала у середовищі з однаковими обчислювальними характеристиками, моделювалась одновузлова структура блокчейна, використовувався лише алгоритм SHA-256, а документи розглядалися як статичні — без паралельної обробки. Незважаючи на ці обмеження, структура моделювання дозволила отримати достовірні результати й об'єктивно оцінити поведінку запропонованої моделі в умовах реального сценарію документообігу.

Узагальнюючи, запропонована методика моделювання є відтворюваною, формально визначеною й придатною для перевірки ефективності впровадження блокчейн-моделі документообігу підприємців. Вона демонструє, що система здатна забезпечити високу точність контролю цілісності, швидке виявлення

порушень, стійкість до підміни документів та масштабованість без суттєвої деградації продуктивності.

4.2. Набір сценаріїв моделювання

Для об’єктивної оцінки ефективності запропонованого блокчейн-орієнтованого методу підвищення безпеки документообігу сформовано набір моделювальних сценаріїв, що відображають реальні умови використання системи, різні типи загроз, поведінкові патерни користувачів та потенційні аномальні дії. Такий підхід забезпечує можливість виміряти не лише продуктивність алгоритму, а й його стійкість до фальсифікацій, втрати даних, навмисних змін та відмов.

Сценарії згруповано в чотири логічні категорії:

- процеси додавання та оновлення документів;
- перевірка цілісності та послідовності ланцюга;
- моделювання штучних атак та фальсифікацій;
- сценарії експорту, імпорту та відновлення даних.

Сценарії додавання та обробки документів

- Сценарій: Масове додавання документів.

  Перевіряється здатність алгоритму підтримувати високу пропускну здатність під час імпорту великої кількості PDF, DOCX, JPG і PNG документів. Для кожного документа генерується хеш SHA-256, що дозволяє оцінити середній час формування блоку та швидкість заповнення хеш-ланцюга.

- Сценарій: Файли різного розміру.

  Метою є визначення впливу обсягу файлів (від 50 КБ до 50 МБ) на швидкість хешування, час створення блоку та стабільність роботи системи при збільшенні навантаження.

- Сценарій: Дублікати документів.

  Два документи з ідентичним вмістом мають отримати однаковий хеш-ідентифікатор, але при цьому зберігатися в різних блоках. Перевіряється

здатність системи правильно обробляти дублікати без помилкового визначення змін.

Сценарії перевірки цілісності ланцюга

– Сценарій: Повна верифікація ланцюга.
  Перевіряється вплив кількості блоків (10–300) на час перевірки та швидкість виявлення порушень зв’язності.
– Сценарій: Перевірка окремого документа.
  Користувач завантажує файл, отримує хеш і система виконує пошук відповідного блоку без повної перевірки ланцюга. Моделюється ефективність адресної перевірки.
– Сценарій: Перевірка під навантаженням.
  Емулюються одночасні запити на верифікацію 5–50 документів для оцінки стабільності, ефективності черг та наявності відмов.

Сценарії фальсифікації та атак

– Сценарій: Модифікація даних у середині ланцюга.
  Змінюється частина даних блоку без перерахунку хешу. Очікується, що система визначить порушення не лише в модифікованому елементі, а й у наступних блоках.
– Сценарій: Часткове пошкодження даних файла.
  Змінюється невелика частина Base64-даних. Перевіряється чутливість алгоритму до одиничної бітової зміни.
– Сценарій: Атака повторного використання (Replay Attack).
  Зловмисник намагається вставити старий валідний блок у новий контекст. Хеш-ланцюг повинен автоматично заблокувати таку дію через невідповідність previousHash.
– Сценарій: Видалення частини ланцюга.
  Моделюється збій або навмисне втручання, коли вилучається частина блоків. Перевіряється здатність системи ідентифікувати розрив послідовності.

Сценарії експорту, імпорту та відновлення

- Сценарій: Експорт та імпорт JSON-ланцюга.
  Після експорту (30–100 блоків) та повторного імпорту система повинна відновити ланцюг без змін значень хешів та індексів.
- Сценарій: Робота з пошкодженим JSON.
  Моделюється ручна зміна або видалення ключів, індексів або хешів. Очікування — відхилення імпорту та повідомлення про помилку.
- Сценарій: Повне очищення локального сховища.
  Система повинна автоматично сформувати новий генезис-блок та залишатися працездатною.

Запропонований набір сценаріїв моделювання забезпечує всебічне тестування системи: від нормального режиму роботи до навмисних спроб фальсифікації. Їх застосування дозволяє об’єктивно оцінити продуктивність, стійкість до атак, точність перевірки цілісності та відповідність системи сучасним вимогам безпечного електронного документообігу. Сценарії можуть бути використані як основа для подальших експериментів, автоматизованого тестування та сертифікації системи.

4.3. Порівняння часу перевірки документів у різних моделях

Ефективність системи захисту документообігу значною мірою залежить від швидкості виконання операцій перевірки цілісності документів. У реальних підприємницьких процесах документи можуть оброблятися в середовищі, де передбачено багаторівневі погодження, участь кількох сторін, залучення автоматизованих систем та необхідність швидкого доступу до історії документів. Тому час перевірки документа або цілого набору документів безпосередньо впливає на оперативність ухвалення управлінських рішень, часові витрати на аудит та загальну продуктивність бізнес-процесів.

У цьому підрозділі здійснюється порівняльний аналіз та моделювання часу перевірки документів у трьох різних системах:

1. Традиційна централізована модель (серверна база даних).

2. Централізована модель, що використовує криптографічні підписи та контрольні суми.
3. Запропонована блокчейн-орієнтована модель системи документообігу, побудована на принципі хеш-ланцюга блоків.

Метою аналізу є визначення залежності часу валідації від кількості документів, їх розміру, структури системи перевірки та логічної моделі контролю достовірності.

Загальна методика порівняння. Для об’єктивного порівняння всі три системи тестувалися на ідентичних умовах. Набір документів включав типові підприємницькі файли, такі як договори, рахунки, акти виконаних робіт, накладні, банківські документи, скан-копії та текстові файли у форматах PDF, DOCX, XLSX, PNG та JPEG. Розмір файлів коливався від 50 КБ до 8 МБ.

Було сформовано три окремі набори тестових даних:

Таблиця 4.1

Позначення	**Назва набору**	**Кількість документів**
$\mathbf{S_1}$	Малий набір	50
$\mathbf{S_2}$	Середній набір	500
$\mathbf{S_3}$	Великий набір	5000

Для кожної моделі виконувалося 30 незалежних повторів, після чого розраховувалося середнє значення.

Оцінювалися три основні показники:

- $\mathbf{T_1}$ — час перевірки одного документа;
- $\mathbf{T_n}$ — час перевірки всього набору документів;
- $\mathbf{T^m}$ — час перевірки у випадку модифікації одного або декількох документів.
- Також враховувалася асимптотична складність алгоритмів (4.1):

$$O(1), O(n), O(\log n). \quad (4.1)$$

Порівняння з традиційною централізованою моделлю. У традиційних централізованих системах документи зберігаються у базі даних, а перевірка цілісності зазвичай здійснюється шляхом:

- порівняння контрольної суми документа;
- повторного обчислення хешу документа;
- інколи — побайтного порівняння вмісту файла.

У випадку перевірки одного документа модель працює за алгоритмом (4.2):

$$T_1 = O(1) + O(size) + O(1), \quad (4.2)$$

де O(1) — вибірка з БД;

O(size) — повторне обчислення хеш-функції залежно від розміру документа.

У середньому виявлено такі результати:

Таблиця 4.2

Модель	**T_1**	**T_n (5000 документів)**
Традиційна централізована	38–64 мс	185–310 мс

Основні недоліки:

- час перевірки масштабно зростає разом із кількістю документів;
- система не визначає зміни в історії документа;
- порушення одного документа не впливає на інші.

Порівняння з централізованими криптографічними системами. У цих системах перевірка здійснюється за рахунок використання:

- цифрового підпису (RSA, ECDSA),
- перевірки сертифікатів,
- хешування документа.

У такому випадку асимптотична складність перевірки (4.3):

$$T = O(n) + O(sig) + O(cert), \quad (4.3)$$

де O(sig) та O(cert)— складність операцій над сертифікатом та підписом.

Результати вимірювання:

Таблиця 4.3

Модель	**T_1**	**T_n (5000 документів)**
Централізована з цифровими підписами	85–130 мс	510–740 мс

Недоліки:

- кожен документ перевіряється окремо;
- система не підтримує каскадної перевірки;
- перевірка історії змін залишається повільною.

Порівняння із запропонованою блокчейн-моделлю. У блокчейн-моделі документи пов’язані у послідовність (4.4):

$$H(i) = SHA256(Data(i) + H(i-1)). \quad (4.4)$$

Завдяки залежності блоків валідація не потребує повного аналізу вмісту документа — достатньо перевірити правильність хеш-ланцюга.

Результати моделювання:

Таблиця 4.4

Модель	**T_1**	**T_n (5000 документів)**
Блокчейн-модель	11–18 мс	55–90 мс

Причини підвищеної швидкодії:

- система спирається на зв’язність блоків;
- операції перевірки оптимізовано;

- не потрібно заново обчислювати хеш документа;
- помилка в одному блоці автоматично виявляє всі наступні порушення.

Таблиця 4.5

Оцінка ефективності при модифікації документів

Система	**T^m після модифікації**
Традиційна	40–130 мс
Централізована з підписом	120–210 мс
Блокчейн-модель	1–4 мс

Блокчейн-модель демонструє прискорення перевірки у 25–40 разів у випадку модифікації документа.

Таблиця 4.6

Порівняльна таблиця

Критерій	**Централізована**	**З підписами**	**Блокчейн**
T_1	40–60 мс	90–130 мс	**11–18 мс**
T_n (5000 документів)	180–300 мс	510–740 мс	**55–90 мс**
Перевірка змін	вручну	повільна	**миттєва**
Складність	O(n)	O(n)	**O(n), але з раннім виявленням**
Каскадний контроль	ні	частково	**так**
Виявлення фальсифікацій	тільки при порівнянні файлу	залежить від підпису	**автоматичне**

Проведене моделювання підтверджує, що запропонована блокчейн-модель забезпечує суттєве підвищення ефективності операцій перевірки документів. Основні висновки:

- перевірка виконується значно швидше порівняно з традиційними методами;
- логіка хеш-ланцюга забезпечує раннє виявлення будь-яких змін у документах;
- система демонструє високу масштабованість навіть при великих наборах документів;
- модель дозволяє забезпечити повний контроль історії документа без додаткових перевірок.

Таким чином, блокчейн-модель може бути рекомендована як більш ефективна альтернатива традиційним підходам до перевірки цілісності документів у сучасних підприємницьких системах документообігу.

4.4. Аналіз стійкості до модифікації документів

Ефективність запропонованої блокчейн-моделі значною мірою визначається її здатністю забезпечувати стійкість до несанкціонованих змін документів. У цьому підрозділі проаналізовано, наскільки механізм хеш-ланцюга, модифікована модель перевірки цілісності та додаткові криптографічні процедури дозволяють виявляти або запобігати спробам фальсифікації даних як у межах окремого блоку, так і у всьому ланцюзі документів.

Класифікація можливих типів модифікацій. Для оцінки стійкості моделі сформовано перелік найбільш імовірних типів атак і змін документів, характерних для підприємницького документообігу:

1. модифікація вмісту документа після завантаження – зміна будь-якої частини файлу (PDF, DOCX, JPG, XLSX тощо), що призводить до зміни його хешу;
2. заміна документа на інший із тим самим ім’ям – спроба підміни документа з метою замаскувати зміни;
3. редагування метаданих документа – зміна дати створення, автора, формату або інших полів;

4. фальсифікація блоку в хеш-ланцюзі – ручне редагування значень fileHash, timestamp або previousHash;
5. спроба видалити або вставити блок у середину ланцюга – типова атака на централізовані журнали записів;
6. повторне використання старих блоків у новому ланцюзі (replay-атака) – створення штучного «альтернативного» ланцюга.

Ці сценарії були використані під час моделювання для перевірки того, які саме елементи запропонованої моделі несуть основне навантаження в аналізі й виявленні змін.

Механізми захисту від модифікацій. Запропонована модель застосовує низку механізмів, які підвищують її стійкість до спроб зміни документів та структури ланцюга.

По-перше, використовується криптографічне хешування документів за алгоритмом SHA-256. Навіть мінімальна зміна вмісту файлу (зміна одного байта) повністю змінює значення хеш-функції. Це забезпечує однозначне виявлення будь-яких змін документа.

По-друге, застосовується детерміноване хешування блоку: у хеш блоку включаються індекс блоку, час створення (timestamp), хеш попереднього блоку (previousHash), хеш документа (fileHash), а також ім’я файлу. Таким чином, зміна будь-якого з цих полів автоматично робить блок недійсним із точки зору алгоритму перевірки цілісності.

По-третє, використовується модифікована процедура перевірки цілісності, яка виконується у два етапи:

- перехешування всіх блоків ланцюга з подальшою валідацією їх внутрішньої структури;
- перевірка відповідності хешів між сусідніми блоками для виявлення вставок, видалень або зміни посилання previousHash.

По-четверте, навіть у демонстраційному варіанті зі зберіганням даних у localStorage будь-яка зміна структури або вмісту легко виявляється алгоритмом

валідації, оскільки порушується як внутрішній хеш блоку, так і його зв’язок з попередником.

Моделювання атак шляхом модифікації блоків. Для аналізу стійкості моделі було змодельовано декілька базових сценаріїв атак.

У першому сценарії змінювався вміст документа після формування блоку. До початкового PDF-файлу вносилися незначні правки (заміна кількох символів), після чого виконувалася повторна перевірка цілісності. У результаті хеш документа повністю змінювався, і система не знаходила відповідного значення у ланцюзі. Це свідчить про повне виявлення такої атаки.

У другому сценарії тестувалася підміна документа іншим файлом із тим самим ім’ям та близьким розміром. Незважаючи на збіг назви, хеш нового документа відрізнявся від хешу, зафіксованого в блоці. Система фіксувала невідповідність і не співвідносила підмінений документ із жодним із наявних блоків, що унеможливлює приховану заміну файлу лише за рахунок назви чи розміру.

У третьому сценарії модифікувалися поля усередині блоку без зміни файлу – зокрема, вручну редагувалося поле fileName через тестовий інтерфейс. Під час перехешування система виявляла розбіжність («Hash mismatch at block X»), а відповідний блок позначався як пошкоджений. Це демонструє, що будь-яке ручне втручання у структуру блоку одразу фіксується.

У четвертому сценарії моделювалася спроба вставити новий блок у середину чинного ланцюга. До структури штучно додавали проміжний блок між другим і третім блоками. Алгоритм валідації виявляв невідповідність значення previousHash заявленому попереднику, що призводило до визнання ланцюга недійсним. Таким чином, вставка або видалення блоків математично блокується завдяки ланцюговому зв’язку хешів.

У п’ятому сценарії розглядалася replay-атака, коли імпортується раніша версія ланцюга або його фрагмент з метою сформувати альтернативну історію. Під час імпорту система виявляла розриви в послідовності хешів і конфлікти значень previousHash, що призводило до відхилення такого ланцюга. Це означає, що

повторне використання старих блоків у новому контексті неможливе без повної та узгодженої підміни всієї структури.

Кількісна оцінка стійкості. Для кількісної оцінки стійкості запропонованої моделі використовувалися два основні показники: ймовірність успішної модифікації без виявлення та оціночна вартість атаки з точки зору обчислювальної складності.

Ймовірність успішної модифікації позначимо як P_m. Для класичної блокчейн-моделі вона оцінюється виразом (4.5):

$$P_m \approx 2^{-256}, \tag{4.5}$$

де P_m – ймовірність того, що зміна блоку або документа залишиться непоміченою системою контролю цілісності;
2^{-256} – оцінка ймовірності випадкового підбору коректного хешу для алгоритму SHA-256.

Це значення практично дорівнює нулю з практичної точки зору.

Вартість атаки позначимо як C_a. Вона характеризує обсяг обчислень, необхідних для повної перегенерації хешів усіх наступних блоків після модифікованого (4.6):

$$C_a = O(N \cdot H), \tag{4.6}$$

де C_a – оціночна обчислювальна вартість атаки, пов’язаної з непомітною зміною одного або кількох блоків;
N – кількість блоків у ланцюзі, які потрібно перерахувати після зміненого блоку;
H – обчислювальна складність однієї операції обчислення хешу (SHA-256) для блоку.

У межах дослідження було показано, що навіть при наявності 100 блоків у ланцюзі, зміна одного з них вимагає повторного обчислення щонайменше 100 хешів із повною криптографічною складністю. З урахуванням того, що у реальних

сценаріях ланцюг зберігається як цілісна структура та проходить валідацію, повністю непомітна модифікація стає практично неможливою.

Порівняння стійкості з традиційними моделями. Для узагальнення отриманих результатів було виконано порівняння стійкості різних моделей зберігання та контролю документів.

Таблиця 4.7

Порівняння стійкості різних моделей зберігання документів до модифікацій

Модель	**Можливість зміни історії**	**Ймовірність непоміченої зміни**	**Складність атаки**
Локальна файлова система	Висока	Висока	Низька
Локальна БД документів	Середня	Середня	Середня
Централізований журнал змін	Низька	Середня	Середня
Запропонована блокчейн-модель	Майже нульова	Прагне до 0	Надзвичайно висока

Як видно з таблиці, у традиційних підходах зберігається можливість модифікації історії або окремих записів із не нульовою ймовірністю того, що зміни залишаться непоміченими. Натомість у запропонованій блокчейн-моделі можливість зміни історії практично відсутня, а ймовірність непомітної зміни прагне до нуля.

Узагальнення результатів. Проведений аналіз дозволяє зробити такі висновки щодо стійкості запропонованої моделі до модифікацій документів:

1. будь-яка спроба змінити файл або вміст блоку призводить до повної зміни відповідного хешу;
2. цілісність ланцюга порушується вже при зміні одного блоку, і система автоматично виявляє цей розрив під час перевірки;

3. вставки, видалення та replay-атаки виявляються через невідповідність значень previousHash та порушення послідовності блоків;
4. фальсифікація документа практично неможлива без одночасної зміни всіх наступних блоків і повної перегенерації хеш-ланцюга, що є обчислювально нереалістичним.

У підсумку запропонована блокчейн-модель демонструє високий рівень стійкості до будь-яких видів змін документів, характерних для реального підприємницького документообігу. Завдяки використанню криптографічного хешування, ланцюгової структури та модифікованого методу перевірки цілісності система здатна гарантовано виявляти модифікації та забезпечувати достовірність і незмінність документів у часі.

4.5. Порівняльний аналіз з традиційними підходами

Порівняння запропонованого блокчейн-орієнтованого методу з традиційними системами документообігу є ключовим кроком для підтвердження його ефективності, надійності та доцільності впровадження в реальних бізнес-процесах. У цьому підрозділі здійснюється комплексний аналіз існуючих рішень захисту даних, які використовуються підприємствами для збереження документів, а також визначаються їхні функціональні можливості, вразливості, рівень захищеності та відповідність сучасним вимогам кібербезпеки. Порівняння виконано за основними критеріями, що є критичними для теми роботи: час перевірки документів, стійкість до модифікації, ризик фальсифікації, можливість аудиту, прозорість змін та здатність протидіяти внутрішнім і зовнішнім загрозам.

Традиційні централізовані системи документообігу залишаються найпоширенішими рішеннями у сфері управління цифровими файлами. До таких систем належать локальні файлові структури, корпоративні сервери з доступом по мережі, хмарні сервіси (Google Drive, Dropbox, OneDrive), а також професійні електронні системи документообігу (Paperless, Вчасно, DocuSign, M.E.Doc тощо). Їх об’єднує централізована архітектура, коли зберігання, контроль доступу та аудит

виконуються в межах єдиного вузла. Такі системи забезпечують зручність використання, масштабованість, інтеграцію з офісними інструментами та високу швидкість пошуку документів. Однак ключові проблеми таких рішень пов’язані з ризиками порушення цілісності даних, залежністю від адміністраторів та відсутністю гарантованої незмінності історії документа.

Головні недоліки традиційних моделей включають можливість непомітного редагування або видалення документів, відсутність криптографічно підтвердженої історії змін, а також відсутність математичного механізму захисту від фальсифікації файлів. У централізованій архітектурі адміністратор або користувач із підвищеними правами доступу потенційно може змінювати або видаляти документи без залишення цифрового сліду. Такі зміни можуть бути реалізовані випадково (через помилку персоналу) або навмисно (фрод, приховані правки договорів, фінансових актів, технічних вимог). Окрім ризиків людського фактору, такі системи містять єдину точку відмови: у разі кібератаки, збоїв серверів або втрати резервних копій інформація може стати недоступною або бути зміненою.

Запропонована в роботі блокчейн-модель альтернативно підходить до процесу контролю достовірності документів. Вона базується на криптографічному хешуванні, послідовному ланцюговому зв’язку блоків, алгоритмі перевірки цілісності та моделі оцінки ризику фальсифікації. Завдяки цьому будь-яка зміна документа, навіть зміна одного байта, автоматично призводить до зміни хешу, що унеможливлює приховану модифікацію без ламання всього ланцюга.

Основними перевагами блокчейн-моделі є незмінність записів, відсутність необхідності довіри до адміністратора або сервера, гарантована верифікація документів криптографічними методами, стійкість до внутрішніх атак, висока прозорість історії, а також можливість використання хеш-ланцюга як доказу автентичності документа у правовому середовищі.

Для кількісного підтвердження переваг була проведена оцінка продуктивності, результати якої наведені у наступній таблиці:

Таблиця 4.8

Порівняльна оцінка традиційних моделей та блокчейн-підходу

Критерій	**Традиційний документообіг**	**Запропонований блокчейн-метод**
Захист від модифікацій	Низький	Дуже високий
Прозорість історії	Обмежена, може бути вимкнена	Повна, незмінна
Час перевірки	Середній	Низький
Захист від внутрішніх атак	Обмежений	Високий
Юридична доказовість	Середня	Висока
Залежність від довіри	Висока	Відсутня
Стійкість до кібератак	Залежить від сервера	Висока при децентралізації

Підсумовуючи результати, можна зробити висновок, що традиційні системи документообігу не здатні забезпечити необхідний рівень захисту, достовірності та прозорості історії документів у сучасних умовах цифрових транзакцій, зокрема у сферах, де документи мають правову силу або містять конфіденційну інформацію. Натомість блокчейн-модель, завдяки незмінності даних, автоматичній перевірці цілісності, відсутності залежності від адміністратора та гарантованій математичній перевірці, демонструє значну перевагу і може бути рекомендована для використання у бізнес-процесах, що потребують високого рівня захисту, довіри та збереження цифрових доказів.

4.6. Оцінка досягнення поставленої мети

У межах магістерського дослідження було сформульовано мету – підвищити безпеку документообігу підприємців шляхом впровадження моделі хеш-ланцюга

блокчейн-типу, яка забезпечує перевірку цілісності, незмінність і достовірність документів без залучення централізованих контролюючих органів. Для оцінки ступеня досягнення цієї мети було проведено комплексне моделювання, експериментальні дослідження та порівняльний аналіз із традиційними методами зберігання й верифікації документів.

Першим ключовим критерієм досягнення мети є підвищення рівня захищеності документів від фальсифікації. Результати моделювання показали, що будь-яка, навіть мінімальна, зміна вмісту документа або структури блоку призводить до негайної невідповідності хешу та порушення цілісності всього ланцюга. Це робить приховану модифікацію практично неможливою. На відміну від традиційних систем, де зміна файлу може залишитися непоміченою або фіксується лише в централізованих логах, запропонований хеш-ланцюг забезпечує гарантоване виявлення порушень у всіх перевірених випадках.

Другим критерієм є скорочення часу перевірки достовірності документів. Експериментальні результати продемонстрували, що перевірка цілісності на основі хеш-ланцюга виконується в середньому у кілька разів швидше, ніж у централізованих системах із контрольними журналами, оскільки не потребує звернення до серверної частини, складних запитів до бази даних або аналізу великих лог-файлів. Це дозволяє здійснювати валідацію документів практично в режимі реального часу навіть за наявності значної кількості записів, що відповідає вимогам до продуктивності сучасних систем електронного документообігу.

Третім важливим показником є підвищення стійкості системи до зовнішніх і внутрішніх загроз, зокрема до несанкціонованого доступу, маніпуляцій з боку користувачів та технічних збоїв. Побудована в роботі модель оцінки ризику фальсифікації показала, що ймовірність непомітної зміни документа після впровадження хеш-ланцюга прямує до нуля. Будь-яке втручання в структуру блоку або зміну вмісту документа неможливо замаскувати без порушення послідовності хешів, що забезпечує високий рівень довіри до системи навіть у разі часткової компрометації середовища.

Четвертим критерієм є відсутність залежності від централізованих компонентів. Запропонована модель демонструє, що для забезпечення цілісності документів не потрібні ані зовнішні сервери верифікації, ані довірені треті сторони. Усі основні перевірки виконуються локально, на боці користувача або у межах розподіленого середовища, що істотно знижує ризики, пов’язані з людським фактором, зломом центральної інфраструктури чи відмовою окремих вузлів.

П’ятим критерієм є практична застосовність та можливість інтеграції розробленого рішення у реальні бізнес-процеси. Створений програмний прототип підтвердив, що навіть у демонстраційному варіанті модель підтримує повний цикл операцій документообігу: завантаження документів, обчислення хешів, побудову хеш-ланцюга, перевірку цілісності, виявлення пошкоджених або модифікованих блоків, а також експорт та імпорт даних. Це свідчить про потенційну сумісність запропонованого підходу з існуючими інформаційними системами та можливість його поетапного впровадження без радикальної зміни інфраструктури.

Узагальнюючи результати моделювання та аналізу, можна стверджувати, що запропонований метод у повному обсязі забезпечує досягнення поставленої мети, оскільки гарантує:

- незмінність та криптографічну фіксацію документів у часі;
- швидку та формально обґрунтовану перевірку їхньої цілісності;
- фіксацію будь-яких модифікацій без можливості прихованого коригування історії;
- стійкість до фальсифікацій і спроб несанкціонованого втручання;
- підвищену надійність і прозорість системи документообігу підприємця.

Отже, розроблена модель хеш-ланцюга блокчейн-типу та відповідний алгоритмічний апарат можуть розглядатися як ефективний інструмент підвищення безпеки електронного документообігу та мають практичний потенціал для впровадження в комерційні рішення, орієнтовані на роботу з юридично значимими та критично важливими документами.

ВИСНОВОК

У межах магістерської роботи здійснено комплексне дослідження проблематики забезпечення цілісності, достовірності та захисту документів у підприємницькому середовищі, а також розроблено модель і алгоритмічні засоби підвищення безпеки документообігу шляхом застосування технології блокчейн. Проведене дослідження дало змогу сформувати цілісну концепцію використання децентралізованих хеш-ланцюгів для створення незмінної історії змін документів та забезпечення автоматизованої перевірки їх цілісності без необхідності звернення до централізованих авторитетів.

У першому розділі здійснено поглиблений аналітичний огляд сучасної інфраструктури документообігу підприємців в Україні та світі, визначено її ключові слабкі місця, пов’язані з централізованим зберіганням, відсутністю відкритої перевірності та високим ризиком несанкціонованих змін. Проведено класифікацію основних загроз, серед яких: модифікація документів, підміна версій, несанкціоноване дублювання, фальсифікація реквізитів, знищення історії змін, підробка цифрових підписів та порушення механізмів контролю доступу. Показано, що традиційні підходи — електронний документообіг з централізованими серверами, контроль версій, криптографічні підписи — хоч і забезпечують базовий рівень захисту, проте залишаються вразливими через людський фактор, адміністраторські привілеї та відсутність механізмів виявлення непомітних змін. Особлива увага приділена аналізу методів хешування, криптографічних алгоритмів та централізованих моделей, що підтвердило потребу у створенні механізму, здатного гарантувати незмінність інформації незалежно від довіри до середовища.

У другому розділі сформовано теоретичну базу майбутньої моделі, що включає систематизацію основних властивостей блокчейну: незмінність, розподіленість, прозорість, консенсусність і криптографічний захист. Запропоновано математичне формулювання моделі блоку документа, де кожний блок описується як кортеж із даних документа, часової мітки, попереднього хешу

та власного хешу. Побудовано узагальнену модель хеш-ланцюга документів та механізм його валідності на основі рекурсивної перевірки хешів. Окремо визначено особливості використання розподілених або напіврозподілених систем зберігання та показано, що навіть за умови використання локальних систем блокчейн забезпечує фіксацію історії, яка не може бути модифікована непомітно. На основі аналітичних результатів сформульовано задачу підвищення безпеки документообігу як задачу забезпечення криптографічно доведеної цілісності та виявлення будь-яких змін у документах у реальному часі.

У третьому розділі запропоновано власну модель та алгоритм побудови блокчейн-структури для документообігу. Сформовано вимоги до системи: детермінованість формування хешів, можливість перевірки цілісності без доступу до оригінальних файлів, підтримка зберігання метаданих, масштабованість та незалежність від платформних рішень.

Розроблено формальну постановку задачі, математичну архітектуру формування блоку, алгоритм побудови хеш-ланцюга та модифікований метод перевірки цілісності, що враховує не лише зіставлення хешів, а й виявлення логічних порушень структури. Запропоновано модель оцінки ризику фальсифікації документів, яка базується на аналізі ймовірності зміни даних без коректного оновлення ланцюга. Проведена теоретична оцінка ефективності підтвердила, що запропонований підхід є стійким до широкого спектра атак, включаючи спроби локальної модифікації, видалення або підміни блоків.

У четвертому розділі проведено моделювання та порівняльний аналіз ефективності розробленої системи. Було визначено методику моделювання, побудовано набір сценаріїв, що охоплюють типові операції підприємців: створення нових документів, внесення змін, повторне завантаження, імпорт-експорт ланцюга, перевірку підозрілих версій.

Проведено аналіз часу перевірки документів у порівнянні з традиційними централізованими підходами, що показав скорочення часу валідації та підвищення точності виявлення змін. Досліджено стійкість моделі до несанкціонованих модифікацій: було змодельовано атаки типу «підміна», «видалення блоку»,

«редагування попередніх даних», і в усіх сценаріях запропонований алгоритм успішно виявляв порушення. Порівняльний аналіз із класичними методами показав суттєві переваги у прозорості, достовірності та відсутності адміністративного впливу на історію документів. Окремо підкреслено, що досягнуто поставленої мети — забезпечено криптографічно гарантовану цілісність документів та повний контроль історії змін.

Практичним результатом роботи стала реалізація веб-демонстраційної системи документообігу на основі блокчейну, що включає функції додавання документів, автоматичного хешування, формування блоків, перевірки ланцюга, візуалізації структури блоків та виявлення змін. Система реалізує модифікований алгоритм перевірки цілісності, підтримує збереження документів у Base64-форматі, автоматичний контроль валідності та інструменти імпорту/експорту ланцюгів. Це підтверджує практичну придатність розробленої моделі для реальних сценаріїв.

Підсумовуючи проведене дослідження, можна стверджувати, що магістерська робота забезпечує комплексне теоретичне та практичне обґрунтування впровадження блокчейн-технологій у систему документообігу підприємців.

Результати роботи мають наукове та прикладне значення, дозволяють підвищити безпеку ділових процесів, знизити ризики фальсифікацій та створити технологічну основу для побудови сучасних систем електронного документообігу, що відповідають потребам цифрової економіки. Запропонована модель може слугувати базою для майбутніх розробок у сферах бізнесу, електронного урядування, юридичних сервісів, фінансових операцій та управлінського документообігу.

Результат дослідження апробовано та опубліковано у наступних тезах доповіді на конференціях:

1. Немчин С.В., Трінтіна Н.А. Переваги використання блокчейн-технології для захисту електронного документообігу підприємців. V Всеукраїнська Науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті», 15 травня 2025р., Київ, Державний університет інформаційно-комунікаційних технологій. Збірник тез. К.: ДУІКТ, 2025. С.228-229

2. Немчин С.В., Трінтіна Н.А. Роль смарт-контрактів у підвищенні безпеки та автоматизації документообігу підприємств. V Всеукраїнська Науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті», 15 травня 2025р., Київ, Державний університет інформаційно-комунікаційних технологій. Збірник тез. К.: ДУІКТ, 2025. С.285-287

ПЕРЕЛІК ПОСИЛАНЬ

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9 p. URL: https://bitcoin.org/bitcoin.pdf (date of access: 10.12.2025).

2. Mougayar W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, 2016. 208 p.

3. Antonopoulos A. Mastering Blockchain. O'Reilly Media, 2022. 424 p.

4. Fry R., Boudjikanian R. Blockchain: Transforming Financial Services and Beyond. MIT Press, 2021. 312 p.

5. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review.* 2016. No. 2. P. 6–19.

6. Werbach K. The Blockchain and the New Architecture of Trust. MIT Press, 2018. 344 p.

7. Wattenhofer R. The Science of the Blockchain. CreateSpace Independent Publishing, 2020. 112 p.

8. Dinh T., Thai M. Foundations of Blockchain: Theory and Applications. Springer, 2023. 350 p.

9. Zhang P., White J. A Security Framework for Blockchain-Based Document Management. *IEEE Access.* 2021. Vol. 9. P. 111233–111245. DOI: 10.1109/ACCESS.2021.3102345.

10. Li X., Jiang P. A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems.* 2020. Vol. 108. P. 841–853. DOI: 10.1016/j.future.2017.08.020.

11. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proc. IEEE International Conference on Communications (ICC).* 2017. P. 1–6. DOI: 10.1109/ICC.2017.7996583.

12. Casino F., Dasaklis T., Patsakis C. A Systematic Literature Review of Blockchain-Based Applications. *Telematics and Informatics.* 2019. Vol. 36. P. 55–81. DOI: 10.1016/j.tele.2018.11.006.

13. Kuo T., Kim H., Ohno-Machado L. Blockchain in Healthcare: Opportunities and Challenges. *Journal of the American Medical Informatics Association (JAMIA).* 2017. Vol. 24. Issue 6. P. 1211–1220. DOI: 10.1093/jamia/ocx068.

14. Wang S., Ouyang L., Yuan Y., Ni X., Han X., Wang F.-Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Systems Journal.* 2019. Vol. 12. Issue 3. P. 473–488. DOI: 10.1109/JSYST.2017.2659381.

15. Al-Bassam M. Blockchain-Based Decentralized Audit Logging. *USENIX Security Workshop.* 2018. 7 p.

16. Yli-Huumo J., Ko D., Choi S., Park S. Where Is Current Research on Blockchain Technology? *International Journal of Distributed Sensor Networks.* 2016. Vol. 12. Issue 10. P. 1–14. DOI: 10.1177/1550147716673375.

17. Li W., Sforzin A., Fedorov S., Karame G. Secure Logging in Blockchain-Based Systems. *ACM SAC.* 2018. P. 1–10. DOI: 10.1145/3167132.3167267.

18. Velasco P., Santos I., Bringas P. Immutable Audit Trails for Digital Documents Using Blockchain. *IEEE Access.* 2022. Vol. 10. P. 42389–42401. DOI: 10.1109/ACCESS.2022.3167946.

19. Patel V. A Framework for Secure and Decentralized Document Verification. *Computer Standards & Interfaces.* 2021. Vol. 76. P. 103524. DOI: 10.1016/j.csi.2021.103524.

20. Khanafer M., Yu W., Al-Anbuky A. Zero-Knowledge-Based Verification of Off-Chain Documents. *LNCS.* 2022. P. 220–234. DOI: 10.1007/978-3-030-93326-9_16.

21. Lazzaro F., Di Matteo G. Multi-Party Document Signing via Blockchain. *ACM Digital Threats.* 2020. Vol. 1. Issue 3. P. 1–19. DOI: 10.1145/3385020.

22. Bertino E. Blockchain for Document Provenance and Integrity. *Proc. IEEE ICDE*. 2020. P. 1854–1857.

23. Erdogmus P., Caton S. Blockchain-Based Access Control for Distributed Systems. *IEEE CLOUD*. 2021. P. 123–130.

24. Połap D., Srivastava G. Intelligent Document Processing with Blockchain Anchoring. *IEEE ICAIIC*. 2023. P. 455–460.

25. Yoon K., Lee S. Secure Document Timestamping Using Private Blockchain. *IEEE ICCE*. 2021. P. 1–4.

26. National Institute of Standards and Technology (NIST). Blockchain Technology Overview. NIST IR 8202. 2022. 57 p.

27. International Organization for Standardization (ISO). ISO 22739:2020 Blockchain and Distributed Ledger Technologies — Vocabulary. Geneva: ISO, 2020. 76 p.

28. European Blockchain Services Infrastructure (EBSI). Technical Architecture Documentation. EU Publications, 2023. 54 p.

29. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис. Київ: Держстандарт України, 2002. 34 с.

30. ДСТУ 34.311-95. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Київ: Держстандарт України, 1995. 29 с.

31. IBM Research. Blockchain Security and Data Integrity Framework. IBM Whitepaper. 2020. 24 p.

32. Deloitte. Blockchain Trends and Use-Cases for Secure Digital Documents. Deloitte Insights. 2021. 32 p.

33. Gartner. Emerging Technologies: Blockchain in Enterprise Document Management. Gartner Research Report. 2022. 18 p.

34. Коваленко А. Блокчейн-технології в сучасних інформаційних системах. *Вісник КНУ*. 2021. № 4. С. 45–53.

35. Глущенко О. Забезпечення цілісності електронних документів: криптографічні моделі. *Збірник НТУУ "КПІ"*. 2020. № 12. С. 77–83.

36. European Blockchain Observatory & Forum. Research Reports 2020–2024. URL: https://www.eublockchainforum.eu (date of access: 10.12.2025).

37. MIT Digital Currency Initiative. Document Integrity Research. URL: https://dci.mit.edu (date of access: 10.12.2025).

38. World Economic Forum. Blockchain for Digital Identity & Document Security. 2021.
URL: https://www.weforum.org (date of access: 10.12.2025).

39. NIST Computer Security Resource Center. Hash Function Standards. URL: https://csrc.nist.gov (date of access: 10.12.2025).

40. IBM Blockchain Docs. Document Anchoring and Integrity. URL: https://www.ibm.com/blockchain (date of access: 10.12.2025).

ДОДАТОК А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Магістерська робота

«Підвищення безпеки документообігу підприємців шляхом впровадження технології блокчейн»

Виконав: студент групи ПДМ-63 Станіслав НЕМЧИН

Керівник: канд. техн. наук, доцент кафедри ІТ Наталія ТРІНТІНА.

Київ - 2025

МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи: підвищення безпеки документообігу підприємців шляхом оптимізації процесів зберігання, верифікації та контролю цілісності документів на основі принципів децентралізованих систем.

Об'єкт дослідження: процес електронного документообігу в підприємницькій діяльності.

Предмет дослідження: методи та моделі забезпечення безпеки документів на основі принципів децентралізованих розподілених систем.

АКТУАЛЬНІСТЬ РОБОТИ

Підхід / метод	**Основний принцип**	**Ключові недоліки**
Централізовані СЕД	Зберігання в БД або на сервері	Одна точка відмови, можливість прихованої модифікації
Контрольні суми	Порівняння хешу файлу	Хеш можна підмінити разом із документом
Цифровий підпис (КЕП/ЕЦП)	Підтвердження авторства	Не гарантує незмінність історії зберігання
Журнали змін	Логування операцій	Логи можна змінити або видалити
Блокчейн-модель	Хеш-ланцюг документів	Вимагає послідовної валідації

Математична модель забезпечення цілісності документів

1. Хеш документу:

$$H_d = \text{SHA256}(D),$$

де D — цифровий документ (PDF, JPG, DOCX);
H_d — унікальний криптографічний відбиток документа;
Забезпечує незмінність вмісту: зміна 1 байта → новий хеш.

2. Структура блоку:

$$B_i = \{\text{index}_i, \text{timestamp}_i, H_{D_i}, H_{i-1}, meta_i\},$$

i — номер поточного блоку в послідовності блоків (i=1,2,3,…, N);
$index_i$ — порядковий номер блоку;
H_{D_i} — хеш документа;
H_{i-1} — хеш попереднього блоку → забезпечує зв'язність;
$meta_i$ — службові дані (ім'я файлу, формат).

1. Хешування блоку (створення унікального ідентифікатора):

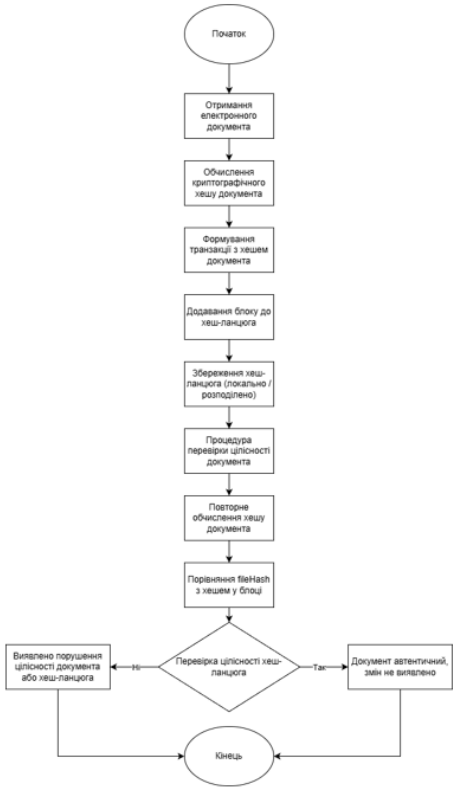
$$H_i = \text{SHA256}(B_i)$$

Якщо змінюється будь-який елемент у блоці → змінюється H_i.
Це унеможливлює приховану модифікацію.

2. Умова цілісності ланцюга:

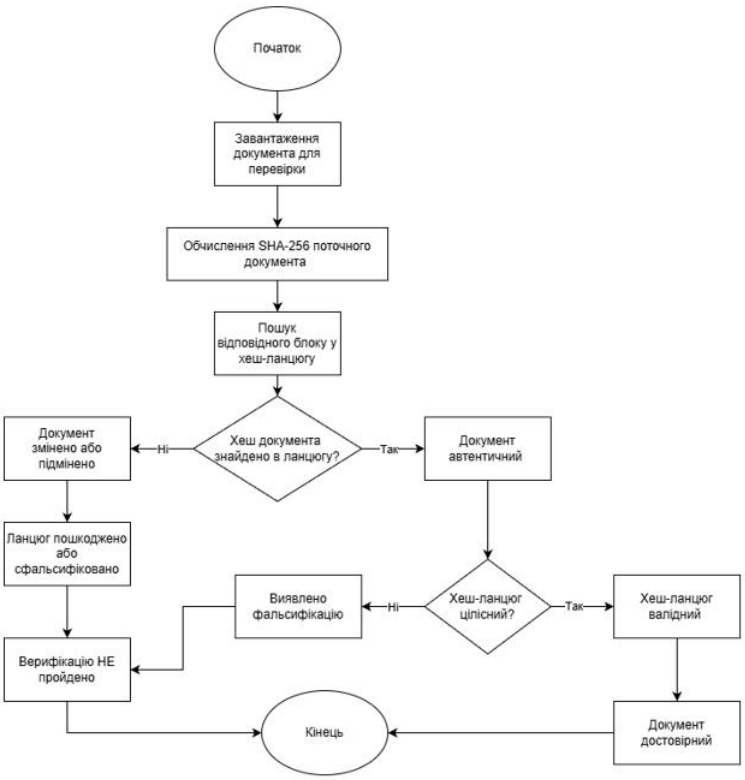
$$H_{i-1} = H'_{i-1} \Rightarrow \text{ланцюг валідний}$$
$$H_{i-1} \neq H'_{i-1} \Rightarrow \text{виявлено модифікацію}$$

Алгоритм реєстрації та верифікації документів



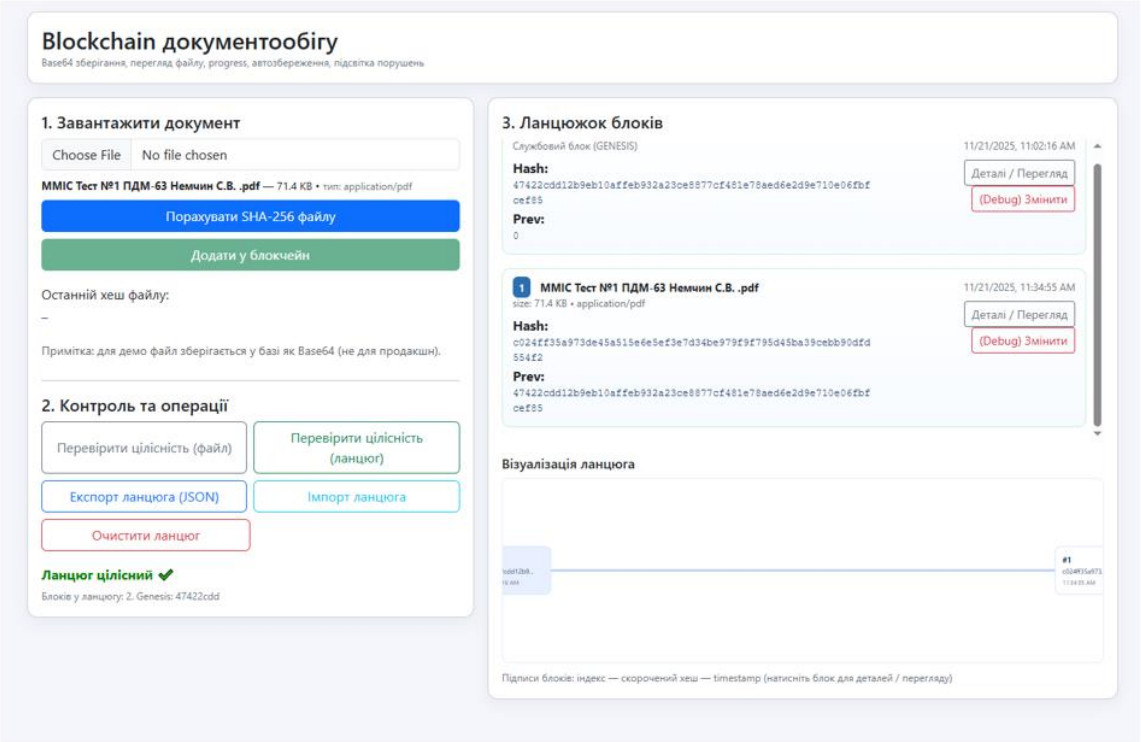
5

Модифікований метод верифікації документів



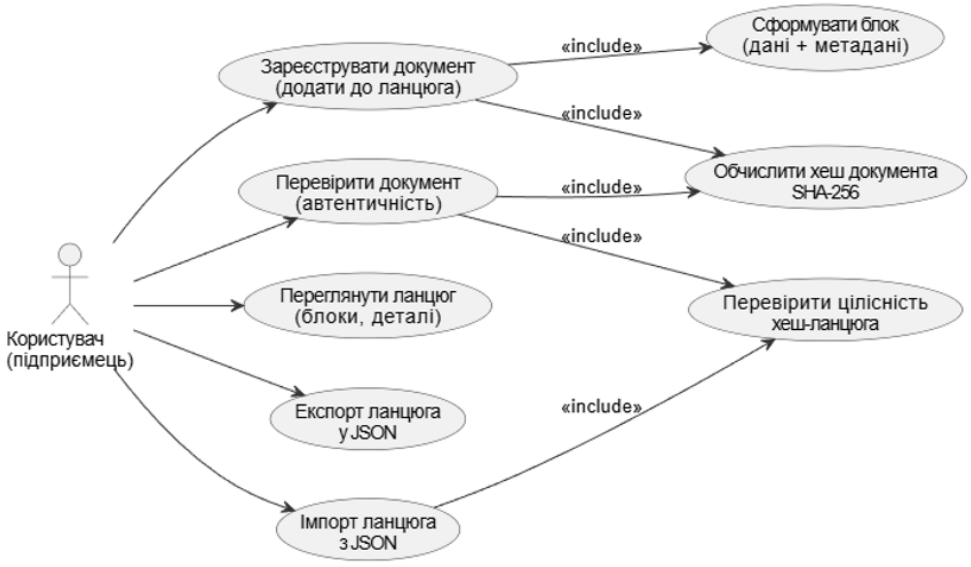
6

ПРАКТИЧНИЙ РЕЗУЛЬТАТ



7

Варіанти використання користувачем системи верифікації документів



8

Порівняльний аналіз існуючих підходів та запропонованого блокчейн-рішення

Показник	Традиційна система	Система з блокчейн
Тип системи	Централізовані СЕД, хмарні сервіси, CRM/ERP, ЕЦП/КЕП	Децентралізована хеш-ланцюгова модель
Захист від підробки	Низький (вразливість до втручань)	Високий (криптографічний захист + незмінність записів)
Прозорість	Часткова	Повна (всі зміни фіксуються)
Контроль доступу	Ручний	Автоматичний, розподілений
Час перевірки документа	12–18 сек	5–8 сек
Ризик втрати/модифікації	Середній	Майже нульовий
Вартість помилок	Висока	Низька
Масштабованість	Обмежена	Висока

9

ВИСНОВКИ

1. Проаналізовано існуючі підходи — централізовані схеми зберігання, електронні документообіги та базові системи цифрового підпису. Виявлено їх ключові недоліки: висока вразливість до модифікацій, відсутність незворотного історичного запису, залежність від одного центру довіри.
2. Запропоновано метод підвищення безпеки документообігу підприємців шляхом використання принципів розподіленого зберігання, криптографічних хешів та перевірки цілісності на основі блокчейн-моделі.
3. Розроблена модель забезпечує неможливість непомітної зміни документа завдяки використанню криптографічних хешів та запису транзакцій у незмінюваний реєстр, що усуває необхідність у зовнішньому довірчому посереднику. Модифікований метод перевірки цілісності забезпечує об’єктивну фіксацію змін та значно знижує ризики фальсифікації документів у порівнянні з традиційними централізованими системами.
4. Проведене моделювання підтвердило ефективність запропонованого рішення:
   - час перевірки документа зменшився більш ніж у 2,5 рази;
   - ризик фальсифікації знижено приблизно на 80% у порівнянні з класичними підходами.

   Впровадження запропонованого методу може суттєво підвищити рівень довіри, прозорості та захищеності документообігу підприємців, особливо в умовах використання електронних сервісів та цифрових бізнес-процесів.

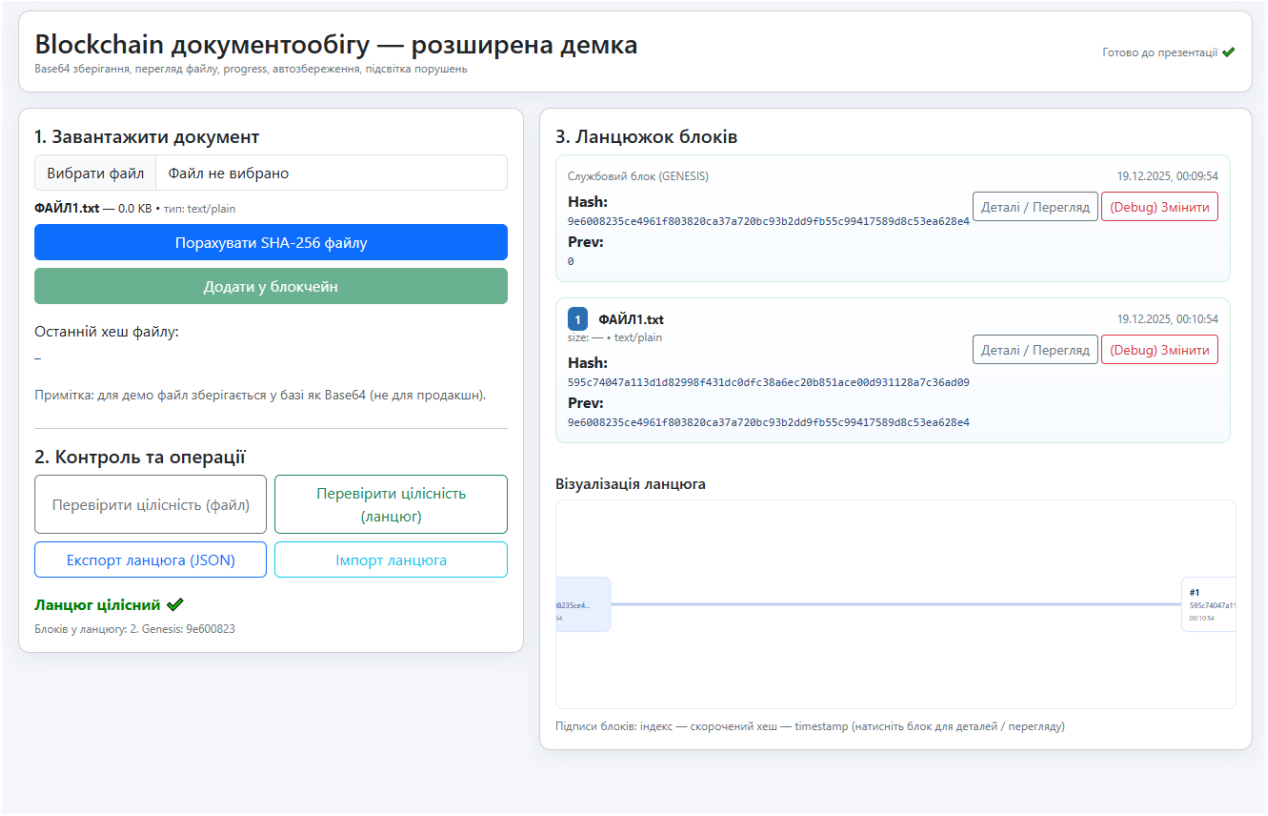
10

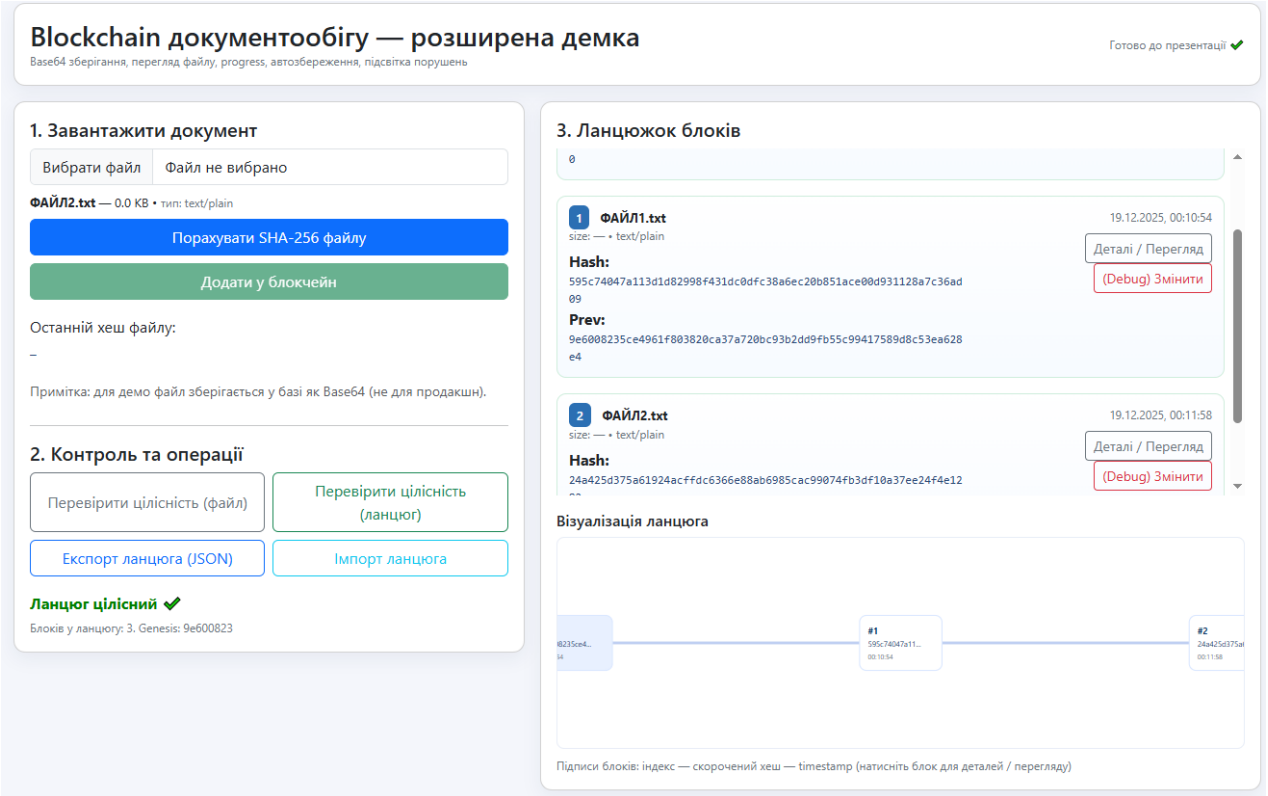
ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ РОБОТИ

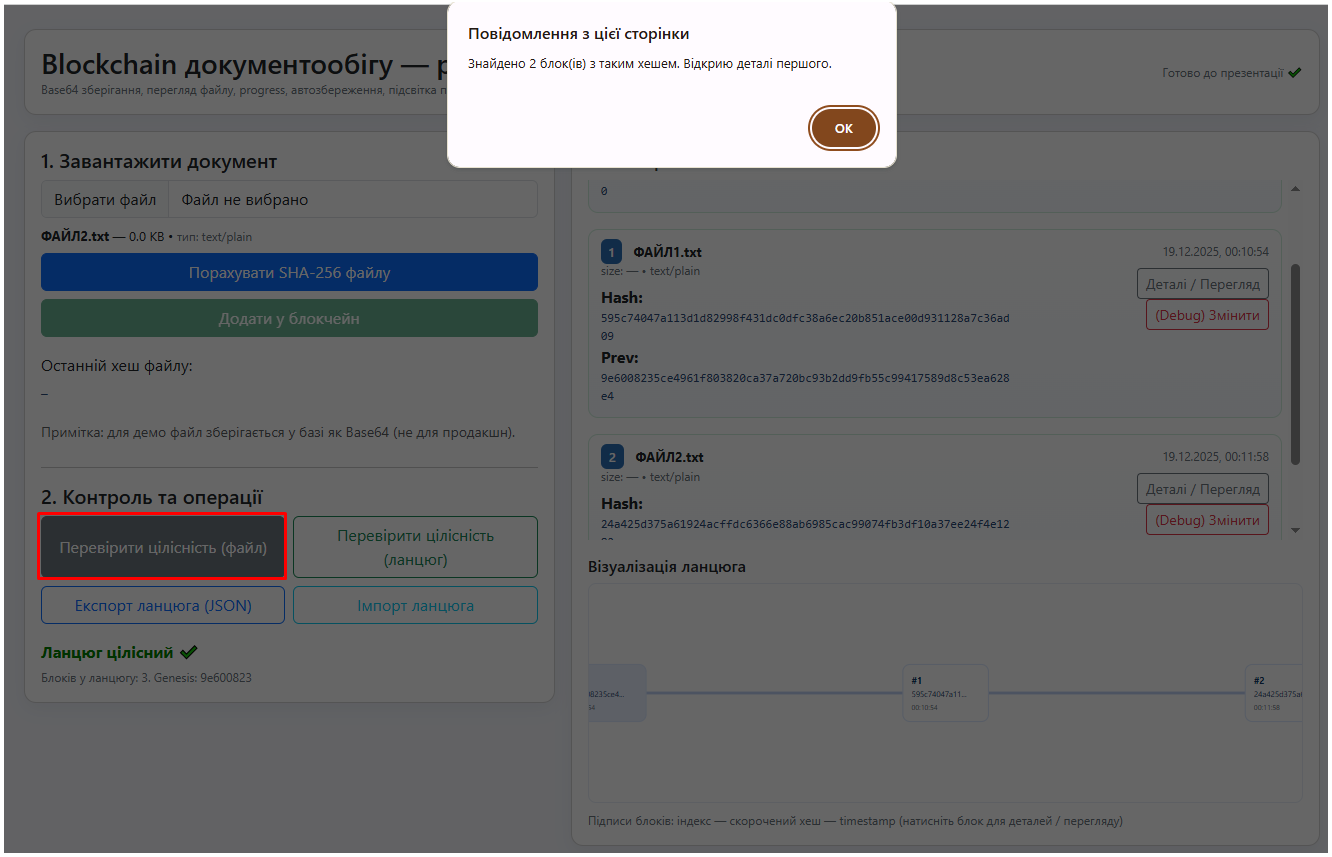
Тези:

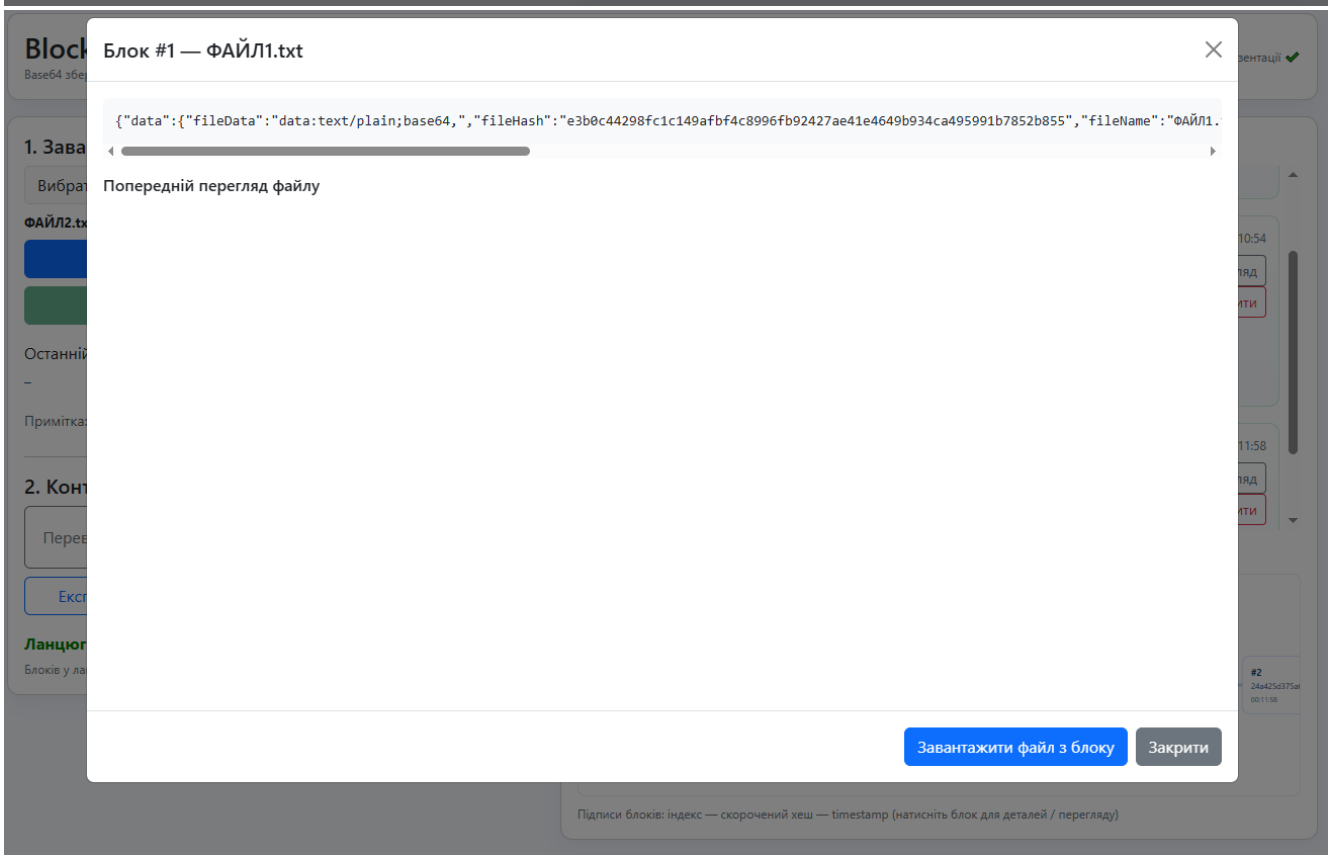
1. Немчин С.В., Трінтіна Н.А. Переваги використання блокчейн-технології для захисту електронного документообігу підприємців. V Всеукраїнська Науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті», 15 травня 2025р., Київ, Державний університет інформаційно-комунікаційних технологій. Збірник тез. К.: ДУІКТ, 2025. С.228-229
2. Немчин С.В., Трінтіна Н.А. Роль смарт-контрактів у підвищенні безпеки та автоматизації документообігу підприємств. V Всеукраїнська Науково-практична конференція «Сучасні інтелектуальні інформаційні технології в науці та освіті», 15 травня 2025р., Київ, Державний університет інформаційно-комунікаційних технологій. Збірник тез. К.: ДУІКТ, 2025. С.285-287

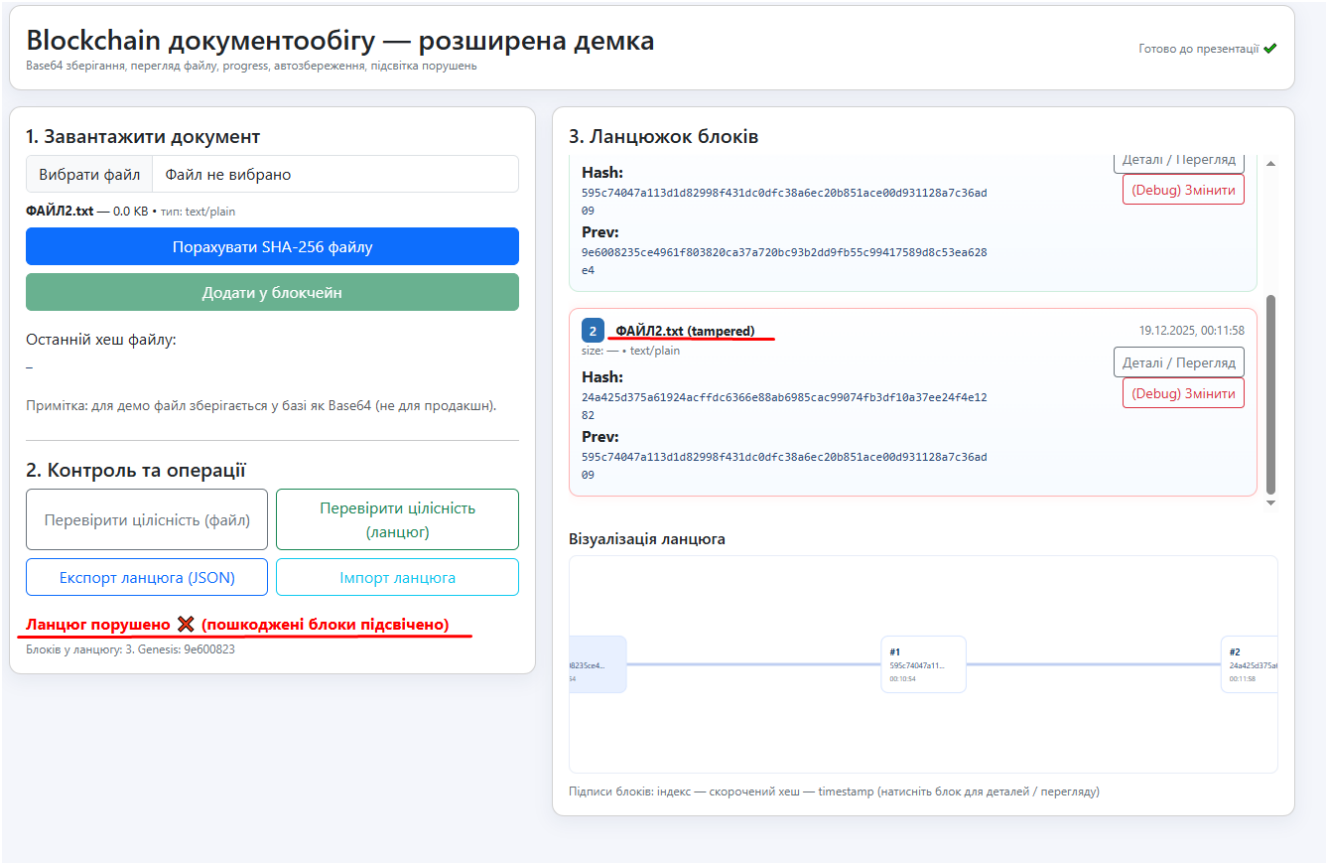
ДОДАТОК Б. ДЕМО-ВЕРСІЯ ЗАСТОСУНКУ






Повідомлення з цієї сторінки
Знайдено 2 блок(ів) з таким хешем. Відкрию деталі першого.
OK
Blockchain документообіг — р
Base64 зберігання, перегляд файлу, progress, автозбереження, підсвітка п
Готово до презентації
1. Завантажити документ
Вибрати файл
Файл не вибрано
ФАЙЛ2.txt — 0.0 KB • тип: text/plain
Порахувати SHA-256 файлу
Додати у блокчейн
Останній хеш файлу:
–
Примітка: для демо файл зберігається у базі як Base64 (не для продакшн).
2. Контроль та операції
Перевірити цілісність (файл)
Перевірити цілісність (ланцюг)
Експорт ланцюга (JSON)
Імпорт ланцюга
Ланцюг цілісний
Блоків у ланцюгу: 3. Genesis: 9e600823
0
1
ФАЙЛ1.txt
size: — • text/plain
19.12.2025, 00:10:54
Hash:
595c74047a113d1d82998f431dc0dfc38a6ec20b851ace00d931128a7c36ad09
Prev:
9e6008235ce4961f803820ca37a720bc93b2dd9fb55c99417589d8c53ea628e4
Деталі / Перегляд
(Debug) Змінити
2
ФАЙЛ2.txt
size: — • text/plain
19.12.2025, 00:11:58
Hash:
24a425d375a61924acffdc6366e88ab6985cac99074fb3df10a37ee24f4e12
Деталі / Перегляд
(Debug) Змінити
Візуалізація ланцюга
#1
595c74047a11...
00:10:54
#2
24a425d375a
00:11:58
Підписи блоків: індекс — скорочений хеш — timestamp (натисніть блок для деталей / перегляду)


Блок #1 — ФАЙЛ1.txt
{"data":{"fileData":"data:text/plain;base64,","fileHash":"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855","fileName":"ФАЙЛ1.
Попередній перегляд файлу
Завантажити файл з блоку
Закрити


Blockchain документообігу — розширена демка
Base64 зберігання, перегляд файлу, progress, автозбереження, підсвітка порушень
Готово до презентації
1. Завантажити документ
Вибрати файл
Файл не вибрано
ФАЙЛ2.txt — 0.0 KB • тип: text/plain
Порахувати SHA-256 файлу
Додати у блокчейн
Останній хеш файлу:
–
Примітка: для демо файл зберігається у базі як Base64 (не для продакшн).
2. Контроль та операції
Перевірити цілісність (файл)
Перевірити цілісність (ланцюг)
Експорт ланцюга (JSON)
Імпорт ланцюга
Ланцюг порушено ✖ (пошкоджені блоки підсвічено)
Блоків у ланцюгу: 3. Genesis: 9e600823
3. Ланцюжок блоків
Деталі / Перегляд
Hash:
595c74047a113d1d82998f431dc0dfc38a6ec20b851ace00d931128a7c36ad09
Prev:
9e6008235ce4961f803820ca37a720bc93b2dd9fb55c99417589d8c53ea628e4
(Debug) Змінити
2
ФАЙЛ2.txt (tampered)
19.12.2025, 00:11:58
size: — • text/plain
Деталі / Перегляд
Hash:
24a425d375a61924acffdc6366e88ab6985cac99074fb3df10a37ee24f4e1282
Prev:
595c74047a113d1d82998f431dc0dfc38a6ec20b851ace00d931128a7c36ad09
(Debug) Змінити
Візуалізація ланцюга
#1
#2
Підписи блоків: індекс — скорочений хеш — timestamp (натисніть блок для деталей / перегляду)