Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 «Кібербезпека»
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Механізми захисту криптовалютних транзакцій та сервісів»

Виконавець: студент IV курсу, групи КБ-43

_____ **Даніїл САМСОНОВ**
(підпис) (ім'я прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Лариса МИРУТЕНКО
Нормоконтроль		Сергій ДАКОВ

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 «Кібербезпека»
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої-професійної програми)

Студенту **КБ-43** **Самсонову Даніїлу Олександровичу**
(група) (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Механізми захисту криптовалютних транзакцій та сервісів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Типи криптовалютних транзакцій, механізми захисту криптовалютних операцій, сценарії атак і типові вразливості

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомлення з видами криптовалютних транзакцій. Дослідження механізмів захисту в криптовалютних сервісах. Тестування транзакцій і виявлення вразливостей механізмів захисту

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка рекомендацій для користувачів і розробників щодо підвищення безпеки використання криптовалютних сервісів

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Даніїл САМСОНОВ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 09.01.2024	*виконано*
2	Аналіз літератури	10.01.2024 – 22.02.2024	*виконано*
3	Дослідження типів транзакцій та виявлення основних загроз	23.02.2024 – 12.03.2024	*виконано*
4	Вивчення механізмів захисту транзакцій	13.03.2024 – 31.03.2024	*виконано*
5	Огляд криптовалютних платформ	01.04.2024 – 09.04.2024	*виконано*
6	Аналіз функцій захисту в криптовалютних системах	10.04.2024 – 15.04. 2024	*виконано*
7	Проведення тестування, виконання транзакцій, виявлення вразливостей	16.04.2024 – 30.04. 2024	*виконано*
8	Формування практичних рекомендацій для підвищення безпеки	01.05.2024 – 01.06.2024	*виконано*
9	Оформлення пояснювальної записки	01.06.2024 – 03.06.2024	*виконано*

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Даніїл САМСОНОВ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 18 червня 2025 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 75 сторінок основного тексту, 9 таблиць та 8 рисунків. Список використаних джерел містить 34 найменування і займає 4 сторінки.

Мета роботи полягає у дослідженні механізмів захисту криптовалютних транзакцій та розробці рекомендацій щодо підвищення безпеки використання криптовалютних сервісів.

Для досягнення цієї мети визначено такі завдання:

1. Дослідити теоретичні основи криптовалютних транзакцій і технологій, що лежать в їх основі.
2. Проаналізувати сучасні механізми захисту, включаючи криптографічні методи та консенсусні алгоритми.
3. Реалізувати механізми захисту криптовалютних платформ.
4. Виявити потенційні вразливості в роботі криптовалютних застосунків і сайтів.
5. Розробити рекомендації для користувачів і розробників щодо підвищення безпеки використання криптовалютних сервісів.

Об'єктом дослідження є процес обміну цифровими активами у криптовалютних сервісах як складовою криптовалютних транзакцій.

Предметом дослідження є механізми захисту, які застосовуються для забезпечення безпеки криптовалютних транзакцій та сервісів, включаючи технічні, програмні та організаційні аспекти.

Методи дослідження кваліфікаційної роботи:

- аналіз і синтез;
- порівняння;
- експеримент.

Розроблені рекомендації щодо підвищення безпеки використання криптовалютних сервісів призначені для користувачів і розробників криптовалютних платформ та сприятимуть підвищенню безпеки транзакцій.

Ключові слова: криптовалютні транзакції, блокчейн, безпека, механізми захисту, вразливості.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

2FA	–	Two-Factor Authentication
DApps	–	Decentralized Applications
DeFi	–	Decentralized Finance
DPoS	–	Delegated Proof of Stake
ECDSA	–	Elliptic Curve Digital Signature Algorithm
HTLC	–	Hashed Timelock Contracts
NFT	–	Non-Fungible Token
PBFT	–	Practical Byzantine Fault Tolerance
PoS	–	Proof of Stake
PoW	–	Proof of Work
SHA-256	–	Secure Hash Algorithm 256-bit
zk-SNARKs	–	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

ВСТУП

Сучасний світ переживає стрімкий розвиток цифрових технологій, які трансформують економічні, соціальні та технологічні аспекти суспільства. Одним із найвизначніших досягнень останніх десятиліть стала поява криптовалют – децентралізованих цифрових активів, що базуються на технології блокчейн. Криптовалюти, такі як Bitcoin, Ethereum та інші, змінили уявлення про фінансові транзакції, запропонувавши альтернативу традиційним банківським системам. Вони забезпечують швидкість, прозорість і доступність операцій, але водночас створюють нові виклики, пов’язані з безпекою.

Актуальність теми кваліфікаційної роботи зумовлена зростанням популярності криптовалют та їх інтеграцією в глобальну економіку. За даними аналітичних звітів, обсяг ринку криптовалют у 2024 році перевищив 2 трильйони доларів США, а кількість користувачів криптовалютних платформ продовжує зростати. В Україні криптовалюти також набувають популярності: у 2021 році Верховна Рада ухвалила закон "Про віртуальні активи", що свідчить про визнання їхньої ролі в економіці. Проте разом із можливостями криптовалюти несуть значні ризики, пов’язані з кібератаками, шахрайством і втратою активів через недостатній захист. У цьому контексті механізми захисту криптовалютних транзакцій та сервісів стають критично важливими для забезпечення безпеки користувачів і фінансових систем.

Мета роботи полягає у дослідженні механізмів захисту криптовалютних транзакцій та розробці рекомендацій щодо підвищення безпеки використання криптовалютних сервісів. Для досягнення цієї мети визначено такі завдання:

1. Дослідити теоретичні основи криптовалютних транзакцій і технологій, що лежать в їх основі.
2. Проаналізувати сучасні механізми захисту, включаючи криптографічні методи та консенсусні алгоритми.
3. Реалізувати механізми захисту криптовалютних платформ.

4. Виявити потенційні вразливості в роботі криптовалютних застосунків і сайтів.
5. Розробити рекомендації для користувачів і розробників щодо підвищення безпеки використання криптовалютних сервісів.

Об’єктом дослідження є процес обміну цифровими активами у криптовалютних сервісах як складовою криптовалютних транзакцій.

Предметом дослідження є механізми захисту, які застосовуються для забезпечення безпеки криптовалютних транзакцій та сервісів, включаючи технічні, програмні та організаційні аспекти.

Методи дослідження включають аналіз наукової літератури, порівняльний аналіз криптовалютних платформ, експериментальне тестування їхніх функцій безпеки та систематизацію отриманих даних. Теоретичною основою роботи слугують праці вітчизняних і зарубіжних учених, таких як І. М. Доронін, Т. Желюк, B. Bhushan, D. Das, а також офіційні документи та звіти, що стосуються блокчейн-технологій і криптовалют.

Практична частина роботи передбачає детальний огляд використання криптовалютних застосунків і сайтів, таких як MetaMask, Trust Wallet, Binance та Ledger. Буде проведено тестування їхніх функцій безпеки, зокрема двофакторної аутентифікації, шифрування транзакцій і захисту від фішингових атак. Отримані результати дозволять оцінити ефективність наявних механізмів захисту та виявити потенційні вразливості.

Практична цінність роботи полягає в розробці рекомендацій для користувачів і розробників щодо підвищення безпеки використання криптовалютних сервісів. Запропоновані заходи дозволяють користувачам захищати свої цифрові активи, а розробникам — враховувати типові вразливості для створення більш захищених і надійних платформ. Результати дослідження можуть бути використані в освітніх програмах, а також для вдосконалення нормативно-правової бази в Україні щодо віртуальних активів.

РОЗДІЛ 1.
КРИПТОВАЛЮТНІ ТРАНЗАКЦІЇ ТА ЇХ БЕЗПЕКА

1.1 Криптовалюти в сучасній економіці

Криптовалюти є цифровими або віртуальними валютами, які використовують криптографію для забезпечення безпеки транзакцій і контролю створення нових одиниць. Вони функціонують на основі децентралізованих технологій, таких як блокчейн, що дозволяє здійснювати транзакції без посередників, таких як банки чи фінансові установи. Основною особливістю криптовалют є їхня децентралізована природа, яка забезпечує прозорість, незмінність даних і захист від маніпуляцій. Першою і найвідомішою криптовалютою є Bitcoin, створений у 2008 році Сатоші Накамото, який запропонував концепцію peer-to-peer електронної готівки [13].

Криптовалюти виникли як відповідь на обмеження традиційних фінансових систем, зокрема високі комісії за транзакції, тривалий час обробки міжнародних платежів і залежність від централізованих інститутів. Вони дозволяють користувачам здійснювати швидкі, відносно дешеві та анонімні транзакції через інтернет. Наприклад, Ethereum, друга за популярністю криптовалюта, розширила можливості блокчейну, запровадивши смарт-контракти – самовиконувані контракти, що автоматизують угоди без посередників [14]. Такі інновації зробили криптовалюти не лише засобом платежу, але й основою для децентралізованих фінансових систем (DeFi), токенізації активів і створення невзаємозамінних токенів (NFT).

Місце криптовалют у сучасній економіці є багатогранним. З одного боку, вони виступають альтернативним інвестиційним активом, який приваблює інвесторів завдяки високій волатильності та потенційній прибутковості. За даними аналітичних звітів, капіталізація ринку криптовалют у 2024 році перевищила 2 трильйони доларів США, що свідчить про їх значущість у глобальній економіці (див. рис. 1.1) [34]. З іншого боку, криптовалюти

використовуються для транскордонних платежів, особливо в країнах із нестабільною економікою або обмеженим доступом до банківських послуг. Наприклад, у країнах із високою інфляцією, таких як Венесуела чи Зімбабве, криптовалюти стають засобом збереження вартості та альтернативною валютою для щоденних операцій.

Рисунок 1.1 – Капіталізація ринку криптовалют

В Україні криптовалюти також набувають популярності. У 2021 році Верховна Рада ухвалила закон "Про віртуальні активи", який визначає правовий статус криптовалют і створює основу для їх регулювання. Це стало важливим кроком для інтеграції криптовалют у національну економіку, сприяючи розвитку блокчейн-стартапів і залученню іноземних інвестицій. Українські дослідники, зокрема І. М. Доронін, зазначають, що криптовалюти можуть сприяти економічній децентралізації, але потребують чіткого правового регулювання для зменшення ризиків шахрайства та відмивання коштів [6]. Крім того, криптовалюти в Україні використовуються для гуманітарних зборів і донатів, що

стало особливо актуальним після 2022 року, коли цифрові активи допомогли зібрати значні суми на підтримку країни.

Криптовалюти також впливають на трансформацію фінансових ринків, створюючи нові можливості для інновацій. Наприклад, децентралізовані фінансові платформи (DeFi) дозволяють користувачам отримувати кредити, інвестувати або торгувати активами без участі традиційних банків. Проте цей процес супроводжується викликами, пов’язаними з безпекою. Висока популярність криптовалют привертає увагу кіберзлочинців, які використовують фішинг, злами гаманців і атаки на біржі для крадіжки активів. Це підкреслює необхідність розробки ефективних механізмів захисту транзакцій, які є ключовим аспектом цієї роботи.

Економічна роль криптовалют не обмежується фінансовими ринками. Вони також сприяють розвитку нових бізнес-моделей, таких як токенізація активів, коли фізичні чи цифрові активи (нерухомість, мистецтво) переводяться у цифровий формат на блокчейні. Це відкриває можливості для дробового інвестування та підвищення ліквідності активів. Водночас криптовалюти викликають дискусії щодо їх впливу на монетарну політику держав. Деякі країни, як-от Китай, обмежують використання криптовалют, побоюючись втрати контролю над фінансовими потоками, тоді як інші, наприклад Сальвадор, визнали Bitcoin законним платіжним засобом у 2021 році [15].

В Україні криптовалюти розглядаються як інструмент для залучення інвестицій і розвитку технологічного сектору. Дослідження Т. Желюк і О. Бречко підкреслюють, що криптовалюти можуть стати драйвером економічного зростання, якщо будуть створені належні умови для їх використання, зокрема прозоре регулювання та захист користувачів [7]. Проте відсутність єдиних міжнародних стандартів регулювання ускладнює інтеграцію криптовалют у глобальну економіку, що створює додаткові ризики для користувачів і бізнесу.

Незважаючи на численні переваги, криптовалюти стикаються з низкою викликів. Волатильність їхньої вартості робить їх ризикованим активом для інвесторів, а анонімність транзакцій може використовуватися для незаконної

діяльності, як-от відмивання коштів чи фінансування тероризму. Для вирішення цих проблем необхідні не лише технологічні, але й правові механізми, які б забезпечували баланс між свободою використання криптовалют і захистом інтересів суспільства.

Криптовалюти є важливим елементом сучасної економіки, який поєднує інноваційні можливості з новими викликами. Їхня децентралізована природа, швидкість транзакцій і потенціал для трансформації фінансових систем роблять їх привабливими для користувачів і бізнесу. Однак успіх їхньої інтеграції залежить від ефективності механізмів захисту транзакцій і створення належної нормативно-правової бази, що є ключовим фокусом цього дослідження.

1.2 Принципи роботи блокчейн-технологій

Блокчейн-технологія є фундаментом, на якому базуються криптовалюти, забезпечуючи їх децентралізацію, прозорість і безпеку. Блокчейн являє собою розподілений цифровий реєстр, що зберігає дані про транзакції у вигляді послідовно пов’язаних блоків, які захищені криптографічними методами. Кожен блок містить набір транзакцій, хеш попереднього блоку та унікальний ідентифікатор, що забезпечує незмінність даних. Ця технологія дозволяє здійснювати транзакції без посередників, таких як банки, що робить її основою для криптовалют, таких як Bitcoin і Ethereum [15].

Основним принципом роботи блокчейну є децентралізація. На відміну від традиційних баз даних, які контролюються центральним органом, блокчейн розподілений між багатьма вузлами (комп’ютерами) у мережі. Кожен вузол має повну копію реєстру, що забезпечує стійкість системи до збоїв і атак. Якщо один вузол виходить з ладу, інші продовжують підтримувати мережу. Цей принцип підвищує надійність і доступність криптовалютних транзакцій, оскільки немає єдиної точки відмови [4].

Другий ключовий принцип – незмінність даних. Після додавання блоку до ланцюжка змінити його вміст практично неможливо без переписування всіх

наступних блоків, що вимагає згоди більшості вузлів мережі. Це досягається завдяки криптографічним хеш-функціям, таким як SHA-256, які генерують унікальний ідентифікатор для кожного блоку. Якщо хоча б один біт даних у блоці змінюється, хеш також зміниться, що сигналізує про втручання. Цей механізм забезпечує цілісність і достовірність транзакцій у криптовалютах, таких як Bitcoin [16].

Консенсусні алгоритми є ще одним важливим принципом блокчейн-технологій. Вони забезпечують узгодженість даних між усіма вузлами мережі, дозволяючи учасникам досягти згоди щодо дійсності транзакцій. Найпоширенішим алгоритмом у криптовалютах є Proof of Work (PoW), який використовується в Bitcoin. У PoW вузли (майнери) вирішують складні обчислювальні задачі, щоб додати новий блок до ланцюжка, отримуючи за це винагороду. Цей процес не лише підтверджує транзакції, але й захищає мережу від атак, оскільки зміна блоку вимагає величезних обчислювальних ресурсів [17]. Альтернативний алгоритм, Proof of Stake (PoS), застосовується в Ethereum 2.0 і вимагає від учасників "ставити" свої монети як гарантію чесності, що знижує енергоспоживання порівняно з PoW.

Прозорість і анонімність – додаткові принципи, які роблять блокчейн привабливим для криптовалют. Усі транзакції в блокчейні є публічними і можуть бути переглянуті будь-ким у мережі, що забезпечує високий рівень прозорості. Водночас користувачі ідентифікуються лише за допомогою публічних адрес, що надає певний рівень анонімності. Наприклад, у Bitcoin транзакції пов’язані з адресами, а не з особистими даними, хоча повна анонімність не гарантується через можливість аналізу блокчейну [13].

Блокчейн також підтримує використання смарт-контрактів, які є програмованими угодами, що автоматично виконуються за певних умов. Смарт-контракти, запроваджені Ethereum, дозволяють створювати складні фінансові інструменти, такі як децентралізовані біржі чи кредитні платформи, без участі посередників. Це розширює функціональність криптовалют, роблячи їх не лише засобом платежу, але й основою для децентралізованих додатків (DApps) [14].

В Україні блокчейн-технології викликають значний інтерес, особливо в контексті фінансових інновацій. Дослідження Л. В. Коваленко підкреслюють, що блокчейн може сприяти розвитку економіки України шляхом підвищення прозорості фінансових операцій і зменшення корупційних ризиків. Однак для цього необхідна адаптація законодавства та створення інфраструктури для впровадження технології [33]. Наприклад, українські стартапи активно використовують блокчейн для токенізації активів, таких як нерухомість, що відкриває нові можливості для інвестування.

Незважаючи на переваги, блокчейн-технології мають обмеження. Високе енергоспоживання PoW, масштабованість мережі та складність регулювання є ключовими викликами. Наприклад, мережа Bitcoin обробляє лише 7 транзакцій за секунду, що значно поступається традиційним платіжним системам, таким як Visa. Для вирішення цих проблем розробляються нові технології, такі як Lightning Network для Bitcoin або шардинг для Ethereum, які підвищують пропускну здатність мережі [15].

Блокчейн-технології є основою криптовалют, забезпечуючи їх децентралізацію, безпеку та прозорість. Принципи роботи, такі як незмінність, консенсусні алгоритми та криптографічний захист, роблять блокчейн надійною платформою для транзакцій. Водночас виклики, пов’язані з енергоефективністю та регулюванням, потребують подальших досліджень, що є актуальним для розвитку криптовалют у глобальному та українському контексті.

1.3 Види криптовалютних транзакцій та їх особливості

Криптовалютні транзакції є основним механізмом обміну цифровими активами в децентралізованих системах, що базуються на блокчейн-технологіях. Вони являють собою запис у блокчейн-реєстрі, який підтверджує переміщення активів між учасниками мережі. На відміну від традиційних фінансових транзакцій, криптовалютні операції не потребують посередників, таких як банки, і характеризуються високим рівнем прозорості та безпеки, забезпеченими

криптографічними методами. Різноманітність криптовалютних транзакцій зумовлена функціональними можливостями блокчейн-платформ і потребами користувачів. Надалі буде розглянуто основні види криптовалютних транзакцій та їхні особливості, що є важливим для розуміння механізмів їх захисту [15].

Першим і найпоширенішим видом є стандартні транзакції, які передбачають переказ криптовалюти від одного користувача до іншого. Такі транзакції характерні для більшості криптовалют, зокрема Bitcoin. У процесі стандартної транзакції відправник створює запис, що містить адресу одержувача, суму переказу та цифровий підпис, який підтверджує автентичність операції. Після підтвердження майнерами транзакція додається до блокчейну. Особливістю цього виду є простота та швидкість виконання, хоча час підтвердження залежить від завантаженості мережі та комісії, яку сплачує користувач. Наприклад, у мережі Bitcoin транзакція може тривати від кількох хвилин до години через обмежену пропускну здатність [13].

Другим видом є транзакції зі смарт-контрактами, які характерні для платформ, таких як Ethereum. Смарт-контракти – це програмовані угоди, що автоматично виконуються за виконання заздалегідь визначених умов. Такі транзакції дозволяють створювати складні фінансові операції, наприклад, автоматичне нарахування відсотків за кредитами або обмін токенів на децентралізованих біржах. Особливістю смарт-контрактів є їхня гнучкість і автоматизація, але вони потребують додаткових обчислювальних ресурсів, що підвищує комісії (так звані "газові" витрати в Ethereum). Крім того, вразливості в коді смарт-контрактів можуть стати мішенню для атак, що вимагає ретельного тестування [14].

Третій вид – атомарні свопи (atomic swaps), які дозволяють обмінювати різні криптовалюти між різними блокчейнами без посередників. Наприклад, користувач може обміняти Bitcoin на Ethereum напряму, використовуючи спеціальні протоколи, такі як Hashed Timelock Contracts (HTLC). Особливістю атомарних свопів є їхня децентралізованість і безпека, оскільки обмін відбувається лише за умови виконання всіх умов обома сторонами. Однак цей

вид транзакцій є технічно складним і поки що не набув масового поширення через обмежену сумісність між блокчейнами [4].

Четвертим видом є транзакції з мультипідписом (multisignature transactions), які використовуються для підвищення безпеки. Такі транзакції вимагають підтвердження кількома приватними ключами, що робить їх ідеальними для спільних гаманців або корпоративного використання. Наприклад, у Bitcoin-гаманці з мультипідписом типу 2-of-3 транзакція виконується лише за наявності двох із трьох підписів. Цей механізм знижує ризик крадіжки активів, але ускладнює процес виконання транзакцій через необхідність координації між сторонами [16].

В Україні криптовалютні транзакції набувають популярності, особливо в контексті гуманітарних зборів і донатів. Дослідження О. О. Ляшенко та Ю. О. Мазур зазначають, що стандартні транзакції в Bitcoin і Ethereum широко використовуються для швидких переказів, але потребують додаткових заходів безпеки через зростання кіберзагроз [8]. Крім того, транзакції зі смарт-контрактами в Україні починають застосовуватися в стартапах для токенізації активів, таких як нерухомість, що відкриває нові економічні можливості.

Кожен вид транзакцій має свої особливості (табл. 1.1). Стандартні транзакції є простими, але вразливі до атак на гаманці. Транзакції зі смарт-контрактами пропонують гнучкість, але потребують захисту від помилок у коді. Атомарні свопи забезпечують децентралізований обмін, але їхня складність обмежує доступність. Транзакції з мультипідписом підвищують безпеку, але ускладнюють управління. Ці особливості необхідно враховувати під час розробки механізмів захисту, що є ключовим аспектом цієї роботи.

Таблиця 1.1

Види криптовалютних транзакцій

Вид транзакції	Опис	Особливості	Приклади платформ
Стандартні транзакції	Переказ криптовалюти від одного користувача до іншого	Простота, швидкість, залежність від комісій	Bitcoin, Litecoin
Транзакції зі смарт-контрактами	Виконання програмованих угод за певних умов	Гнучкість, високі комісії, вразливість коду	Ethereum, Binance Smart Chain
Атомарні свопи	Обмін криптовалют між різними блокчейнами без посередників	Децентралізованість, технічна складність	Bitcoin, Ethereum
Транзакції з мультипідписом	Транзакції, що вимагають кількох підписів для підтвердження	Підвищена безпека, складність координації	Bitcoin, Ethereum

Криптовалютні транзакції різноманітні за своєю природою та функціоналом, що зумовлює різні підходи до їх захисту. Розуміння їхніх особливостей є необхідним для аналізу вразливостей і розробки ефективних механізмів безпеки, що буде розглянуто в наступних розділах роботи.

1.4 Основні загрози безпеці криптовалютних операцій

Безпека криптовалютних операцій є критично важливою через децентралізовану природу блокчейн-технологій і високу цінність цифрових активів. Незважаючи на криптографічний захист і розподілену структуру блокчейну, криптовалютні транзакції залишаються вразливими до різноманітних

загроз. Ці загрози можуть призводити до втрати активів, порушення конфіденційності або дестабілізації мережі. Розуміння основних ризиків є необхідним для розробки ефективних механізмів захисту, що є ключовим завданням цього дослідження. У цьому розділі розглядаються основні загрози безпеці криптовалютних операцій, які охоплюють як технічні, так і соціальні аспекти [1].

Однією з найсерйозніших загроз є атака 51%, яка виникає, коли зловмисник контролює більше половини обчислювальної потужності мережі (у системах із Proof of Work) або більшу частину стейків (у Proof of Stake). Це дозволяє маніпулювати блокчейном, зокрема здійснювати подвійні витрати, коли одна й та сама криптовалюта витрачається двічі. Такі атаки особливо небезпечні для менших блокчейн-мереж із низькою обчислювальною потужністю. Наприклад, у 2018 році мережа Bitcoin Gold зазнала атаки 51%, що призвела до втрати мільйонів доларів. Хоча для великих мереж, таких як Bitcoin, ця атака є економічно невигідною, вона залишається значною загрозою для менш захищених криптовалют [19].

Іншою поширеною загрозою є фішинг-атаки, спрямовані на викрадення приватних ключів або облікових даних користувачів. Зловмисники створюють підроблені вебсайти, електронні листи або додатки, які імітують популярні криптовалютні платформи, такі як Binance чи MetaMask. Користувачі, які вводять свої дані на таких ресурсах, втрачають доступ до гаманців. Українські дослідники, зокрема О. М. Кравець, зазначають, що фішинг є однією з основних причин втрати криптовалют в Україні через низьку обізнаність користувачів щодо кібергігієни [28]. Ця загроза підкреслює важливість соціальної інженерії як інструменту кіберзлочинців.

Злами гаманців і бірж становлять значний ризик, оскільки більшість користувачів зберігають свої активи на централізованих платформах або в онлайн-гаманцях. Уразливості в програмному забезпеченні або недостатній захист серверів можуть призвести до масштабних крадіжок. Наприклад, у 2014 році біржа Mt. Gox втратила 850 000 біткойнів через хакерську атаку, що стало

одним із найбільших інцидентів в історії криптовалют. Навіть апаратні гаманці, такі як Ledger, не є повністю захищеними, якщо користувач не дотримується правил безпеки, наприклад, зберігає фразу відновлення в незахищеному вигляді [27].

Подвійні витрати (double-spending) є ще однією загрозою, яка виникає, коли зловмисник намагається витратити одні й ті ж кошти кілька разів. Хоча блокчейн-технології, такі як Bitcoin, розроблені для запобігання подвійним витратам за допомогою консенсусних алгоритмів, уразливості в реалізації або атаки на мережу можуть створювати ризики. Дослідження А. Жерва та Г. Караме підкреслюють, що швидкі транзакції з низькою кількістю підтверджень є особливо вразливими до таких атак, якщо зловмисник має доступ до значних ресурсів [18].

Sybil-атаки полягають у створенні зловмисником великої кількості підроблених вузлів у мережі для впливу на її роботу. Такі атаки можуть порушити консенсус або спотворити дані про транзакції. Вони особливо небезпечні для мереж із низькою кількістю учасників, де зловмиснику легше отримати контроль над значною частиною вузлів. Для захисту від Sybil-атак використовуються механізми, такі як репутаційні системи або вимоги до стейкінгу, але ці методи не завжди є ефективними [20].

Помилки в смарт-контрактах є специфічною загрозою для платформ, таких як Ethereum, де транзакції часто залежать від програмованих угод. Недоліки в коді смарт-контрактів можуть призводити до втрати коштів або виконання небажаних операцій. Наприклад, у 2016 році атака на смарт-контракт DAO призвела до крадіжки Ethereum на суму 50 мільйонів доларів, що змусило спільноту провести хардфорк мережі. Ця проблема вимагає ретельного аудиту коду, що не завжди доступно для невеликих проєктів [2].

Нарешті, регуляторні ризики також впливають на безпеку криптовалютних операцій. Відсутність єдиних міжнародних стандартів і нечітке законодавство в багатьох країнах, включаючи Україну, створюють умови для шахрайства та незаконної діяльності. Дослідження М. О. Литвина вказують, що в Україні брак

чіткого регулювання ускладнює захист користувачів від шахрайських схем, таких як піраміди, що використовують криптовалюти [29].

Основні загрози безпеці криптовалютних операцій:

— Атака 51%: контроль над більшістю обчислювальної потужності для маніпуляції блокчейном.
— Фішинг-атаки: викрадення приватних ключів через підроблені ресурси.
— Злами гаманців і бірж: крадіжка активів через уразливості в програмному забезпеченні.
— Подвійні витрати: повторне використання одних і тих же коштів.
— Sybil-атаки: створення фальшивих вузлів для впливу на мережу.
— Помилки в смарт-контрактах: вразливості в коді, що призводять до втрати активів.
— Регуляторні ризики: нечітке законодавство, що сприяє шахрайству.

Криптовалютні операції стикаються з широким спектром загроз, які охоплюють технічні, соціальні та правові аспекти. Ці ризики вимагають комплексного підходу до захисту, що включає як технологічні рішення, так і підвищення обізнаності користувачів. Аналіз цих загроз є основою для подальшого дослідження механізмів безпеки в наступних розділах роботи.

1.5 Огляд існуючих механізмів захисту транзакцій

Забезпечення безпеки криптовалютних транзакцій є ключовим завданням для підтримки довіри користувачів і стабільності децентралізованих систем. З огляду на різноманітність загроз, описаних у попередньому розділі, розроблено низку механізмів захисту, які охоплюють криптографічні, програмні та організаційні аспекти. Ці механізми спрямовані на запобігання атакам, захист конфіденційності та забезпечення цілісності транзакцій. У цьому розділі розглядаються основні методи захисту, їхні особливості та ефективність у контексті сучасних криптовалютних платформ [1].

Одним із основних механізмів захисту є криптографічні методи, які лежать в основі блокчейн-технологій. Хеш-функції, такі як SHA-256, використовуються для створення унікальних ідентифікаторів блоків і забезпечення їхньої незмінності. Цифровий підпис, що базується на асиметричній криптографії (наприклад, алгоритм ECDSA у Bitcoin), підтверджує автентичність транзакцій і запобігає їх підробці. Приватний ключ користувача дозволяє підписувати транзакції, тоді як публічний ключ дає змогу іншим учасникам мережі перевірити їхню дійсність. Цей механізм забезпечує високий рівень безпеки, але вимагає надійного зберігання приватних ключів [16].

Консенсусні алгоритми відіграють важливу роль у захисті транзакцій, забезпечуючи узгодженість даних у децентралізованій мережі. Алгоритм Proof of Work (PoW), що використовується в Bitcoin, вимагає від майнерів значних обчислювальних ресурсів для підтвердження блоків, що ускладнює атаки, такі як 51%. Proof of Stake (PoS), застосовуваний в Ethereum 2.0, зменшує енергоспоживання і захищає мережу шляхом стейкінгу активів учасниками. Інші алгоритми, як-от Delegated Proof of Stake (DPoS) або Practical Byzantine Fault Tolerance (PBFT), також використовуються в різних блокчейнах для підвищення безпеки та швидкості обробки транзакцій [17].

Мультипідпис (multisignature) є додатковим механізмом захисту, який підвищує безпеку транзакцій, особливо для спільних або корпоративних гаманців. Цей метод вимагає підтвердження транзакції кількома приватними ключами, що знижує ризик крадіжки активів. Наприклад, гаманець із налаштуванням 2-of-3 вимагає двох підписів із трьох можливих для виконання операції. Цей механізм широко застосовується в Bitcoin і Ethereum, але може ускладнювати управління через необхідність координації між сторонами [16].

Двофакторна аутентифікація (2FA) використовується на криптовалютних біржах і гаманцях для захисту облікових записів користувачів. Цей метод вимагає другого рівня підтвердження, наприклад, коду з мобільного додатка (Google Authenticator) або SMS, що значно знижує ризик фішингових атак і несанкціонованого доступу. Українські дослідники, такі як Ю. В. Скрипник,

підкреслюють важливість 2FA для підвищення безпеки в умовах зростання кіберзагроз в Україні [22].

Апаратні гаманці, такі як Ledger або Trezor, забезпечують фізичне зберігання приватних ключів, ізолюючи їх від онлайн-середовища. Це знижує ризик зламу програмних гаманців або фішингових атак. Апаратні гаманці генерують і зберігають ключі в захищеному чіпі, що робить їх одним із найнадійніших способів захисту активів. Проте їхня ефективність залежить від правильного використання, наприклад, безпечного зберігання фрази відновлення [27].

Шифрування транзакцій застосовується для забезпечення конфіденційності даних. Хоча більшість блокчейнів, таких як Bitcoin, є прозорими, деякі криптовалюти, наприклад Monero або Zcash, використовують технології, такі як кільцеві підписи або докази з нульовим розголошенням (zk-SNARKs), для приховування деталей транзакцій, зокрема суми та адрес відправника/одержувача. Ці методи підвищують анонімність, але можуть ускладнювати регуляторний нагляд [2].

Аудит смарт-контрактів є важливим механізмом для платформ, таких як Ethereum, де транзакції залежать від програмованих угод. Аудит передбачає перевірку коду смарт-контрактів на наявність вразливостей, що може запобігти атакам, подібним до інциденту з DAO у 2016 році. Цей процес вимагає залучення спеціалізованих компаній, таких як Trail of Bits, але є критично важливим для безпеки децентралізованих фінансових систем [2].

В Україні механізми захисту криптовалютних транзакцій набувають особливого значення через зростання популярності цифрових активів. Дослідження В. С. Гринишина підкреслюють, що використання апаратних гаманців і 2FA на біржах, таких як Binance, значно знижує ризики для українських користувачів, але потребує підвищення рівня кіберграмотності [31].

Незважаючи на ефективність описаних механізмів, жоден із них не є універсальним. Наприклад, криптографія захищає від підробки, але не від фішингу, а апаратні гаманці не гарантують безпеки, якщо користувач розкриває

фразу відновлення. Це підкреслює необхідність комплексного підходу до захисту транзакцій, що поєднує технологічні та освітні заходи.

Також, ефективний захист криптовалютних транзакцій неможливий без поєднання технологічних, організаційних та освітніх заходів. Навіть найсучасніші криптографічні інструменти не гарантують безпеки у випадках недбалого поводження з ключами, використання слабких паролів або нехтування базовими принципами цифрової гігієни. Саме тому провідні криптовалютні платформи приділяють увагу не лише технічній модернізації, а й розробці інструкцій, попереджень та механізмів контролю доступу для користувачів.

Проаналізувавши основні механізми захисту криптовалютних транзкцій, можна виокремити їх переваги та недоліки. Таким чином, в таблиці 1.2 наведені основні характеристики кожного з розглянутих механізмів захисту, які демонструють націленість криптовалютних платформ на різні аспекти забезпечення безпеки.

Таблиця 1.2

Основні механізми захисту криптовалютних транзакцій

Механізм захисту	Опис	Переваги	Недоліки	Приклади платформ
Криптографічні методи	Використання хеш-функцій і цифрових підписів для захисту транзакцій	Висока безпека, незмінність даних	Вразливість до втрати приватного ключа	Bitcoin, Ethereum
Консенсусні алгоритми	Узгодження даних через PoW, PoS тощо	Захист від атак, децентралізація	Високе енергоспоживання (PoW)	Bitcoin, Ethereum

Продовження табл. 1.2

Механізм захисту	Опис	Переваги	Недоліки	Приклади платформ
Мультипідпис	Підтвердження транзакцій кількома ключами	Підвищена безпека	Складність координації	Bitcoin, Ethereum
Двофакторна аутентифікація	Додатковий рівень захисту облікових записів	Захист від фішингу	Залежність від сторонніх сервісів	Binance
Апаратні гаманці	Фізичне зберігання ключів	Ізоляція від онлайн-загроз	Висока вартість, людський фактор	Ledger, Trezor
Шифрування транзакцій	Приховування деталей транзакцій	Конфіденційність	Складність регулювання	Monero, Zcash
Аудит смарт-контрактів	Перевірка коду на вразливості	Запобігання атакам	Висока вартість аудиту	Ethereum

Сучасні механізми захисту криптовалютних транзакцій є багатогранними і спрямовані на протидію різноманітним загрозам. Їхня ефективність залежить від правильного використання та поєднання, що вимагає як технологічних, так і організаційних заходів. Цей огляд створює основу для подальшого аналізу вразливостей і розробки рекомендацій у наступних розділах роботи.

Висновок до розділу 1

У межах першого розділу було здійснено теоретичне узагальнення понять, пов’язаних із функціонуванням криптовалютних транзакцій, а також

проаналізовано основні аспекти їх безпеки в сучасному цифровому середовищі. Досліджено сутність криптовалют як інструменту фінансової взаємодії, що базується на технології блокчейн, яка забезпечує децентралізованість, прозорість та незмінність даних у транзакційному процесі.

Особлива увага приділена вивченню принципів функціонування блокчейн-технологій, таких як використання хеш-функцій, цифрових підписів і алгоритмів консенсусу (зокрема, Proof of Work та Proof of Stake), що формують основу для побудови безпечного та достовірного цифрового реєстру. На основі проведеного аналізу встановлено, що різновиди криптовалютних транзакцій мають специфічні функціональні характеристики, які впливають на рівень їх захищеності.

У процесі дослідження було охарактеризовано основні загрози, притаманні криптовалютним операціям, а також вразливості, пов’язані зі смарт-контрактами. Аналіз наявних засвідчив важливість комплексного підходу до забезпечення безпеки транзакцій.

Таким чином, результати проведеного теоретичного аналізу створюють необхідне підґрунтя для подальшого практичного дослідження механізмів захисту криптовалютних сервісів, що здійснюється у наступних розділах роботи.

РОЗДІЛ 2.
МЕХАНІЗМИ ЗАХИСТУ В КРИПТОВАЛЮТНИХ СИСТЕМАХ

2.1 Криптографічні методи забезпечення безпеки

Криптографічні методи є основою безпеки криптовалютних систем, забезпечуючи захист даних, автентичність транзакцій і незмінність блокчейн-реєстру. Вони дозволяють гарантувати конфіденційність, цілісність і достовірність операцій у децентралізованих мережах, де відсутні центральні органи контролю. Найпоширенішими криптографічними інструментами в криптовалютах є хешування та цифровий підпис, які відіграють ключову роль у забезпеченні безпеки транзакцій. Проаналізуємо принципи роботи цих методів, а також їхні переваги, недоліки [1].

Хешування є фундаментальним криптографічним механізмом, який використовується для створення унікальних ідентифікаторів даних і забезпечення їхньої цілісності. Хеш-функція перетворює вхідні дані будь-якого розміру (наприклад, транзакцію чи блок) у вихідний рядок фіксованої довжини, відомий як хеш. У криптовалютах, таких як Bitcoin, застосовується хеш-функція SHA-256, яка генерує 256-бітний хеш. Основною властивістю хеш-функції є її односторонність: неможливо відновити початкові дані з хеша, а будь-яка зміна вхідних даних призводить до зовсім іншого хеша. Це забезпечує незмінність блокчейну, оскільки кожен блок містить хеш попереднього, формуючи ланцюжок, який неможливо модифікувати без переписування всіх наступних блоків [16].

Хешування використовується в кількох аспектах криптовалютних систем. По-перше, воно забезпечує цілісність блоків: якщо зловмисник змінює транзакцію в блоці, хеш блоку зміниться, що буде виявлено мережею. По-друге, хешування є частиною консенсусного алгоритму Proof of Work (PoW), де майнери шукають хеш, який відповідає певним умовам (наприклад, починається з певної кількості нулів). Цей процес ускладнює атаки на мережу, оскільки

вимагає значних обчислювальних ресурсів. Проте хешування не захищає від втрати приватних ключів чи фішингових атак, що вимагає додаткових механізмів безпеки [17].

Цифровий підпис є ще одним ключовим криптографічним методом, який забезпечує автентичність і непідробність транзакцій. Цифровий підпис базується на асиметричній криптографії, що використовує пару ключів: приватний і публічний. Приватний ключ відомий лише власнику і використовується для підписання транзакції, тоді як публічний ключ дозволяє іншим учасникам мережі перевірити, що транзакція створена законним відправником. У Bitcoin і Ethereum застосовується алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm), який забезпечує компактні підписи та високий рівень безпеки при відносно низьких обчислювальних витратах [16].

Процес створення цифрового підпису включає наступні кроки: користувач формує транзакцію, хешує її дані, а потім підписує отриманий хеш своїм приватним ключем. Учасники мережі можуть перевірити підпис за допомогою публічного ключа, щоб переконатися, що транзакція не була підроблена і створена власником відповідної адреси. Цифровий підпис запобігає несанкціонованим змінам транзакцій і підтверджує право власності на активи, але його безпека залежить від захисту приватного ключа. Якщо ключ втрачено або викрадено, зловмисник може виконувати транзакції від імені власника [2].

В Україні криптографічні методи набувають особливого значення в контексті розвитку блокчейн-технологій. Дослідження П. І. Сидоренка підкреслюють, що використання сучасних криптографічних алгоритмів, таких як SHA-256 і ECDSA, є стандартом для захисту транзакцій, але потребує адаптації до національних стандартів кібербезпеки [32]. Крім того, вразливості, пов’язані з людським фактором, наприклад, ненадійне зберігання приватних ключів, залишаються значною проблемою для українських користувачів.

Додаткові криптографічні методи, такі як кільцеві підписи і докази з нульовим розголошенням (zk-SNARKs), застосовуються в криптовалютах, орієнтованих на конфіденційність, таких як Monero і Zcash. Кільцеві підписи

дозволяють приховати відправника транзакції, змішуючи його підпис із підписами інших учасників, тоді як zk-SNARKs дають змогу підтвердити дійсність транзакції без розкриття її деталей, таких як сума чи адреса. Ці методи підвищують анонімність, але ускладнюють масштабування мережі та регуляторний нагляд [2].

Незважаючи на ефективність криптографічних методів, вони мають обмеження. Хеш-функції можуть бути вразливими до квантових обчислень у майбутньому, що потребує розробки постквантових алгоритмів. Цифрові підписи, своєю чергою, залежать від безпеки приватних ключів, що робить їх уразливими до фішингу або фізичної крадіжки. Для підвищення безпеки ці методи часто поєднуються з іншими механізмами, такими як апаратні гаманці чи двофакторна аутентифікація [27].

Криптографічні методи, зокрема хешування та цифровий підпис, є основою безпеки криптовалютних транзакцій, забезпечуючи їхню цілісність, автентичність і захист від маніпуляцій. Вони ефективно протидіють більшості технічних загроз, але потребують додаткових заходів для захисту від соціальних і фізичних атак. Цей аналіз створює основу для подальшого дослідження механізмів безпеки в криптовалютних системах.

Криптографічні методи складають технічну основу безпеки криптовалютних транзакцій, однак їх ефективність залежить не лише від теоретичної стійкості алгоритмів, а й від коректного впровадження у конкретних платформах. Різні криптовалютні системи використовують різні підходи до шифрування, підпису транзакцій та забезпечення анонімності, що обумовлює різний рівень захищеності. Узагальненні ключові характеристики найпоширеніших криптографічних механізмів наведені у таблиці 2.1.

Таблиця 2.1

Основні криптографічні методи захисту транзакцій

Метод	Опис	Переваги	Недоліки	Приклади платформ
Хешування	Перетворення даних у унікальний ідентифікатор фіксованої довжини	Забезпечення цілісності, незмінність даних	Вразливість до квантових атак	Bitcoin, Ethereum
Цифровий підпис	Підтвердження автентичності транзакцій за допомогою пари ключів	Висока безпека, захист від підробки	Залежність від захисту приватного ключа	Bitcoin, Ethereum
Кільцеві підписи	Приховування відправника шляхом змішування підписів	Підвищена анонімність	Обмежена масштабованість	Monero
Докази з нульовим розголошенням	Підтвердження транзакцій без розкриття деталей	Конфіденційність	Високі обчислювальні витрати	Zcash

2.2 Роль консенсусних алгоритмів у захисті транзакцій

Консенсусні алгоритми є ключовим елементом децентралізованих блокчейн-систем, забезпечуючи узгодженість даних між усіма учасниками мережі та захист транзакцій від маніпуляцій. Вони дозволяють мережі досягти

згоди щодо дійсності транзакцій і порядку їх додавання до блокчейну без централізованого контролю. Найпоширенішими консенсусними алгоритмами в криптовалютах є Proof of Work (PoW), Proof of Stake (PoS) та їхні модифікації, такі як Delegated Proof of Stake (DPoS). Ці механізми відіграють вирішальну роль у запобіганні атакам, таким як подвійні витрати чи атака 51%, і забезпечують надійність криптовалютних операцій. У цьому розділі аналізується їхня роль у захисті транзакцій і особливості застосування [3].

Proof of Work (PoW) є першим і найвідомішим консенсусним алгоритмом, який використовується в Bitcoin та інших криптовалютах. У PoW учасники мережі (майнери) змагаються за право додати новий блок до блокчейну, вирішуючи складні обчислювальні задачі, що вимагають значних ресурсів. Перший майнер, який знаходить правильне рішення (хеш із певними характеристиками), додає блок і отримує винагороду. Цей процес захищає мережу від атак, оскільки зміна блоку вимагає повторного виконання всіх обчислень для нього та всіх наступних блоків, що є економічно невигідним для зловмисників. Наприклад, для здійснення атаки 51% у мережі Bitcoin необхідно контролювати більше половини загальної обчислювальної потужності, що коштує мільярди доларів. Однак PoW має недолік – високе енергоспоживання, що викликає екологічні занепокоєння [17].

Proof of Stake (PoS) є енергоефективною альтернативою PoW, яка використовується в Ethereum 2.0, Cardano та інших платформах. У hunting rifle. У PoS учасники мережі (валідатори) вибираються для підтвердження транзакцій на основі кількості їхніх активів (стейків) у мережі. Чим більше монет "застейкано", тим вища ймовірність бути обраним для створення блоку. PoS знижує ризик атак 51%, оскільки зловмиснику потрібно володіти більш ніж половиною всіх монет, що зазвичай є фінансово недосяжним. Крім того, PoS стимулює чесну поведінку: валідатори, які діють проти інтересів мережі, можуть втратити свої застейкані активи (механізм "slashing"). PoS забезпечує швидшу обробку транзакцій і менші комісії порівняно з PoW, але може сприяти концентрації влади в руках великих власників монет [17].

Delegated Proof of Stake (DPoS) є модифікацією PoS, яка використовується в блокчейнах, таких як EOS і Tron. У DPoS власники токенів голосують за обмежену кількість делегатів, які відповідають за підтвердження транзакцій і створення блоків. Цей механізм підвищує швидкість і масштабованість мережі, оскільки лише обрані делегати виконують обчислення. DPoS захищає транзакції шляхом розподілу довіри між делегатами, але його децентралізація може бути нижчою, оскільки залежить від невеликої групи обраних учасників. Для захисту від зловживань делегати можуть бути замінені через голосування [3].

Інші консенсусні алгоритми, такі як Practical Byzantine Fault Tolerance (PBFT), застосовуються в приватних або консорціумних блокчейнах, наприклад, Hyperledger Fabric. PBFT забезпечує швидке узгодження між обмеженою кількістю вузлів, стійких до збоїв або зловмисної поведінки, але менш децентралізований, ніж PoW чи PoS. У криптовалютах цей алгоритм використовується рідко через його централізовану природу, але він може застосовуватися в специфічних проєктах, де швидкість важливіша за децентралізацію [15].

В Україні консенсусні алгоритми розглядаються як основа для безпечних фінансових систем. Дослідження Л. В. Коваленко підкреслюють, що PoS і DPoS можуть сприяти розвитку енергоефективних блокчейн-платформ в Україні, але потребують чіткого регулювання для забезпечення справедливого розподілу активів і захисту від концентрації влади [33]. Крім того, консенсусні алгоритми відіграють важливу роль у захисті транзакцій для гуманітарних зборів, де прозорість і безпека є критично важливими.

Консенсусні алгоритми мають свої переваги та недоліки. PoW забезпечує високий рівень безпеки, але є енерговитратним. PoS і DPoS пропонують швидкість і ефективність, але можуть бути вразливими до концентрації ресурсів. Вибір алгоритму залежить від цілей блокчейну – максимальної децентралізації, швидкості чи конфіденційності. Наприклад, Bitcoin робить акцент на безпеці через PoW, тоді як Ethereum 2.0 обирає PoS для масштабованості [14].

Консенсусні алгоритми є невід'ємною частиною захисту криптовалютних транзакцій, забезпечуючи узгодженість і стійкість до атак. Їхня ефективність залежить від дизайну мережі та балансу між безпекою, швидкістю й децентралізацією. Цей аналіз створює основу для подальшого дослідження інших механізмів захисту в криптовалютних системах.

2.3 Механізми захисту від атак на блокчейн

Криптовалютні системи, попри свою децентралізовану природу та криптографічний захист, залишаються вразливими до специфічних атак, таких як атака 51%, подвійна витрата та Sybil-атака. Ці загрози можуть підірвати цілісність блокчейну, призвести до втрати активів або порушити довіру до мережі. Для протидії цим атакам розроблено низку механізмів захисту, які поєднують технологічні, економічні та організаційні підходи. Відповідно до цього, проаналізуємо основні методи захисту від зазначених атак, їхню ефективність і особливості застосування в криптовалютних системах [3].

Атака 51% виникає, коли зловмисник отримує контроль над більш ніж половиною обчислювальної потужності (у системах із Proof of Work) або стейків (у Proof of Stake), що дозволяє маніпулювати блокчейном, наприклад, змінювати порядок транзакцій або здійснювати подвійні витрати. Для захисту від цієї атаки застосовуються такі механізми:

— Висока обчислювальна складність у PoW. У мережах, таких як Bitcoin, атака 51% є економічно невигідною через величезні витрати на обладнання та електроенергію. Наприклад, для атаки на Bitcoin потрібні ресурси, що перевищують мільярди доларів, що робить її малоймовірною для великих мереж. Консенсусний алгоритм PoW ускладнює накопичення такої потужності, оскільки майнери розподілені по всьому світу [19].

— Перехід на PoS або гібридні алгоритми. У PoS, який використовується в Ethereum 2.0, атака 51% вимагає володіння більш ніж половиною всіх

монет, що є фінансово недосяжним через високу ринкову вартість активів. Крім того, механізм "slashing" у PoS карає зловмисників, конфіскуючи їхні застейкані монети, що створює додатковий економічний бар'єр [17].

— Чекпоїнти та фіналізація блоків. Деякі блокчейни, наприклад, Ethereum, використовують механізми фіналізації, які роблять підтверджені блоки незмінними після певної кількості підтверджень. Це ускладнює реорганізацію ланцюжка навіть у разі атаки 51%. Чекпоїнти також застосовуються в менших мережах для захисту від маніпуляцій [3].

Українські дослідники, зокрема Ю. В. Скрипник, зазначають, що для невеликих блокчейн-проєктів в Україні захист від атак 51% є критичним, оскільки вони мають меншу обчислювальну потужність і є більш вразливими. Рекомендується використання гібридних консенсусних механізмів для підвищення безпеки [22].

Подвійна витрата (double-spending) – це спроба зловмисника витратити одні й ті ж криптовалютні активи кілька разів, що підриває довіру до системи. Для запобігання цій атаці застосовуються такі механізми:

— Консенсусні алгоритми. PoW і PoS забезпечують узгодженість мережі, вимагаючи підтвердження транзакцій кількома вузлами. У Bitcoin транзакція вважається безпечною після 6 підтверджень (приблизно 60 хвилин), що робить подвійну витрату технічно складною, оскільки зловмиснику потрібно змінити кілька блоків [18].

— Механізми підтвердження транзакцій. Блокчейни використовують часову мітку (timestamp) і унікальні ідентифікатори транзакцій, щоб запобігти їх дублюванню. Якщо зловмисник намагається створити дві транзакції з однаковими коштами, мережа приймає лише першу, відхиляючи другу [16].

— Мережеві протоколи швидкого підтвердження. Для швидких транзакцій, наприклад, у роздрібній торгівлі, застосовуються рішення другого рівня, такі як Lightning Network для Bitcoin. Ці протоколи

дозволяють проводити транзакції поза основним блокчейном із подальшою синхронізацією, зменшуючи ризик подвійної витрати за рахунок швидкого підтвердження [15].

Дослідження А. Жерва та Г. Караме підкреслюють, що ризик подвійної витрати зростає для транзакцій із низькою кількістю підтверджень, особливо в мережах із високою затримкою. Тому користувачам рекомендується чекати достатньої кількості підтверджень для великих транзакцій [18].

Sybil-атака полягає у створенні зловмисником великої кількості підроблених вузлів у мережі, щоб отримати контроль над консенсусом або спотворити дані. Для захисту від цієї атаки застосовуються такі механізми:

— Ресурсоємні консенсусні алгоритми. У PoW створення фальшивих вузлів не дає переваги, оскільки ефективність залежить від обчислювальної потужності, а не від кількості вузлів. У PoS захист забезпечується вимогою стейкінгу значної кількості монет, що обмежує можливість зловмисника створювати численні ідентичності [20].

— Репутаційні системи та обмеження доступу. У деяких блокчейнах, наприклад, консорціумних, використовуються механізми ідентифікації вузлів або репутаційні системи, які ускладнюють додавання підроблених учасників. Наприклад, у Hyperledger Fabric доступ до мережі контролюється через сертифікати, що запобігає Sybil-атакам [15].

— Рандомізація вибору валідаторів. У PoS і DPoS валідатори обираються випадковим чином із урахуванням їхнього стейку, що знижує ймовірність впливу фальшивих вузлів. Цей механізм ефективний у мережах, таких як Cardano, де застосовується алгоритм Ouroboros [17].

В Україні Sybil-атаки розглядаються як потенційна загроза для локальних блокчейн-проєктів. Дослідження В. С. Гринишина підкреслюють необхідність впровадження репутаційних систем для невеликих мереж, щоб запобігти маніпуляціям із боку зловмисників [31].

Механізми захисту від атак 51%, подвійної витрати та Sybil-атак є невід'ємною частиною безпеки криптовалютних систем. Вони базуються на консенсусних алгоритмах, економічних стимулах і технологічних рішеннях, таких як фіналізація блоків чи рандомізація валідаторів. Ефективність цих механізмів залежить від дизайну блокчейну та розміру мережі: великі мережі, як Bitcoin, краще захищені через високі витрати на атаки, тоді як менші потребують додаткових заходів. Цей аналіз підкреслює важливість комплексного підходу до захисту транзакцій, що буде розглянуто в наступних розділах роботи.

2.4 Порівняльний аналіз безпеки популярних криптовалют

Безпека криптовалют є критично важливою для їхнього функціонування та довіри користувачів. Популярні криптовалюти, такі як Bitcoin, Ethereum, Monero та Cardano, використовують різні механізми захисту, які впливають на їхню стійкість до атак, конфіденційність транзакцій і загальну надійність. В цьому підрозділі проводиться порівняльний аналіз безпеки цих криптовалют, оцінюючи їхні консенсусні алгоритми, криптографічні методи, захист від основних загроз і вразливості. Такий аналіз допомагає зрозуміти сильні та слабкі сторони кожної системи та їхню адаптацію до сучасних викликів [2].

Bitcoin є найстарішою та найпоширенішою криптовалютою, яка використовує консенсусний алгоритм Proof of Work (PoW) із хеш-функцією SHA-256. Висока обчислювальна потужність мережі (хешрейт), що перевищує 500 EH/s у 2024 році, робить атаку 51% економічно невигідною, оскільки вона вимагає мільярдних інвестицій у обладнання. Цифровий підпис на основі ECDSA забезпечує автентичність транзакцій, а прозорість блокчейну дозволяє відстежувати операції. Проте Bitcoin має обмежену конфіденційність: адреси та суми транзакцій є публічними, що може бути використано для аналізу блокчейну та ідентифікації користувачів. Крім того, низька пропускна здатність (7 транзакцій за секунду) робить мережу вразливою до затримок і високих комісій під час пікового навантаження [13].

Ethereum, друга за капіталізацією криптовалюта, перейшла на Proof of Stake (PoS) у 2022 році з оновленням Ethereum 2.0. PoS знижує енергоспоживання порівняно з PoW і захищає від атак 51% завдяки необхідності володіти значною часткою ETH (понад 50% від загальної кількості). Механізм "slashing" карає зловмисних валідаторів, конфіскуючи їхні активи. Ethereum також використовує ECDSA для цифрових підписів і підтримує смарт-контракти, що розширюють функціональність, але створюють додаткові ризики через можливі вразливості в коді, як у випадку з атакою на DAO у 2016 році. Для підвищення безпеки Ethereum застосовує аудит смарт-контрактів і рішення другого рівня, такі як Optimism, які зменшують навантаження на основну мережу. Проте складність смарт-контрактів і висока активність мережі роблять Ethereum мішенню для фішингових атак і зламів гаманців [14].

Monero фокусується на конфіденційності транзакцій, використовуючи криптографічні методи, такі як кільцеві підписи, кільцеві конфіденційні транзакції (RingCT) і технологію stealth-адрес. Ці механізми приховують відправника, одержувача та суму транзакції, що робить Monero стійкою до аналізу блокчейну. Консенсусний алгоритм RandomX (варіант PoW) ускладнює використання спеціалізованого обладнання (ASIC), сприяючи децентралізації майнінгу. Однак менший хешрейт порівняно з Bitcoin робить Monero більш вразливою до атак 51%, а висока обчислювальна складність конфіденційних транзакцій знижує масштабованість мережі. Крім того, акцент на анонімності викликає регуляторні проблеми, оскільки Monero може використовуватися для незаконної діяльності [2].

Cardano використовує консенсусний алгоритм Ouroboros, що є варіантом PoS, який поєднує рандомізацію вибору валідаторів і строгий математичний підхід до безпеки. Ouroboros забезпечує стійкість до атак 51% через розподіл стейків і захист від Sybil-атак за допомогою економічних стимулів. Cardano також підтримує смарт-контракти, але акцентує увагу на формальній верифікації коду, що зменшує ризик вразливостей порівняно з Ethereum. Криптографічні методи включають ECDSA та експерименти з постквантовою криптографією для

майбутньої стійкості. Проте відносно молодий вік мережі та менша кількість валідаторів порівняно з Ethereum роблять Cardano менш випробуваною в реальних умовах, що може впливати на її безпеку [17].

В Україні безпека криптовалют є актуальною темою через зростання їхнього використання. Дослідження О. П. Шевчук зазначають, що Bitcoin і Ethereum є найпопулярнішими в Україні завдяки їхній надійності, але Monero привертає увагу для приватних транзакцій. Однак брак регулювання ускладнює захист користувачів від шахрайства, що підкреслює важливість вибору криптовалют із сильними механізмами безпеки [21].

Порівняльний аналіз показує, що кожна криптовалюта має унікальний баланс між безпекою, конфіденційністю та масштабованістю (див. табл. 2.2). Bitcoin вирізняється стійкістю до атак 51% завдяки PoW, але поступається в конфіденційності. Ethereum пропонує гнучкість через смарт-контракти, але потребує ретельного аудиту коду. Monero забезпечує найвищий рівень анонімності, але є вразливою до атак через менший хешрейт. Cardano демонструє інноваційний підхід до безпеки, але її довгострокова стійкість ще не повністю перевірена.

Узагальнюючи, можна стверджувати, що ефективність безпеки криптовалют визначається сукупністю технологічних рішень, рівнем децентралізації та здатністю мережі адаптуватися до нових загроз. Попри різні підходи — від енергомісткого PoW до економічно вмотивованого PoS, — кожна система має компроміси між захистом, швидкодією та анонімністю. У майбутньому критично важливими стануть гнучкість архітектури, стійкість до квантових атак і підтримка з боку спільноти та розробників, що забезпечуватимуть стабільність та довіру користувачів.

Таблиця 2.2

Порівняльний аналіз безпеки популярних криптовалют

Криптовалюта	Консенсусний алгоритм	Криптографічні методи	Сильні сторони	Слабкі сторони
Bitcoin	PoW (SHA-256)	ECDSA, SHA-256	Висока стійкість до атак 51%, децентралізація	Низька конфіденційність, високе енергоспоживання
Ethereum	PoS (Ouroboros)	ECDSA, аудит смарт-контрактів	Гнучкість смарт-контрактів, енергоефективність	Вразливості смарт-контрактів, фішинг
Monero	PoW (RandomX)	Кільцеві підписи, RingCT, stealth-адреси	Висока конфіденційність	Менший хешрейт, регуляторні ризики
Cardano	PoS (Ouroboros)	ECDSA, формальна верифікація	Безпека коду, постквантова криптографія	Менш випробувана мережа

Безпека популярних криптовалют залежить від їхнього дизайну, консенсусних алгоритмів і криптографічних методів. Bitcoin і Ethereum є лідерами за надійністю, Monero – за конфіденційністю, а Cardano – за інноваційністю. Вибір криптовалюти залежить від потреб користувача, але всі вони потребують додаткових заходів захисту від соціальних і регуляторних ризиків, що буде розглянуто в наступних розділах роботи.

2.5 Вплив людського фактору на безпеку транзакцій

Людський фактор відіграє вирішальну роль у забезпеченні безпеки криптовалютних транзакцій, оскільки навіть найнадійніші технологічні механізми, такі як криптографія чи консенсусні алгоритми, можуть бути зведені нанівець через помилки чи недбалість користувачів. Криптовалютні системи, будучи децентралізованими, покладають значну відповідальність на користувачів за захист їхніх активів, що робить людський фактор однією з основних вразливостей. Тому доцільно проаналізувати, як поведінка користувачів, недостатня обізнаність і помилки впливають на безпеку транзакцій, а також розглядає способи мінімізації цих ризиків [1].

Одним із найпоширеніших проявів людського фактору є ненадійне зберігання приватних ключів. Приватний ключ є основою доступу до криптовалютних активів, і його втрата чи викрадення призводить до необоротної втрати коштів. Багато користувачів зберігають ключі в незахищених місцях, таких як текстові файли на комп’ютері, електронна пошта або навіть фотографії на смартфоні, що робить їх легкою мішенню для хакерів. Наприклад, дослідження показують, що значна частка зламів гаманців пов’язана з витоком приватних ключів через фішинг або шкідливе програмне забезпечення. Для зменшення цього ризику рекомендується використовувати апаратні гаманці, такі як Ledger, які ізолюють ключі від онлайн-середовища [27].

Фішингові атаки є ще однією серйозною загрозою, що експлуатує людський фактор. Зловмисники створюють підроблені вебсайти, електронні листи або повідомлення, які імітують популярні платформи, такі як MetaMask чи Binance, щоб отримати доступ до облікових даних або фраз відновлення. Недостатня обізнаність користувачів щодо перевірки URL-адрес або автентичності листів сприяє успіху таких атак. Українські дослідники, зокрема О. М. Кравець, підкреслюють, що в Україні фішинг є однією з основних причин втрати криптовалют через низький рівень кіберграмотності серед користувачів [28].

Помилки під час виконання транзакцій також створюють ризики. Наприклад, користувачі можуть помилково відправити кошти на неправильну адресу, що в децентралізованих системах є незворотним. Іншим поширеним випадком є ігнорування перевірки деталей транзакції, таких як сума чи адреса одержувача, що може бути використано зловмисниками, які підміняють адреси через шкідливе ПЗ. Крім того, неправильне налаштування комісій (наприклад, занадто низька плата в мережі Bitcoin) може призвести до затримок або відхилення транзакцій, що створює незручності та потенційні вразливості [13].

Недостатнє використання захисних механізмів, таких як двофакторна аутентифікація (2FA), є ще одним проявом людського фактору. Хоча більшість бірж, таких як Binance, пропонують 2FA, багато користувачів не активують її через незручність або нерозуміння її важливості. Це робить їхні облікові записи вразливими до зламів, особливо якщо пароль слабкий або використовується на кількох платформах. Дослідження Ю. В. Скрипника зазначають, що в Україні лише невелика частина користувачів криптовалют застосовує 2FA, що значно підвищує ризик втрати активів [22].

Соціальна інженерія є потужним інструментом, який експлуатує довіру користувачів. Зловмисники можуть видавати себе за технічну підтримку, пропонувати фальшиві інвестиційні схеми або використовувати методи психологічного тиску, щоб отримати доступ до гаманців. Наприклад, шахрайські ICO (Initial Coin Offerings) або пірамідальні схеми часто залучають недосвідчених користувачів, які не перевіряють легітимність проєктів. В Україні такі схеми набули поширення через зростання популярності криптовалют, що підкреслює необхідність підвищення фінансової грамотності [29].

Для мінімізації впливу людського фактору застосовуються такі заходи:

— Освітні програми. Підвищення кіберграмотності через тренінги, онлайн-курси та інформаційні кампанії допомагає користувачам розпізнавати фішинг, безпечно зберігати ключі та правильно налаштовувати транзакції. В Україні такі програми можуть бути

інтегровані в освітні заклади або підтримуватися державними ініціативами [21].

— Інтуїтивно зрозумілі інтерфейси. Розробка гаманців і бірж із простими та безпечними інтерфейсами знижує ймовірність помилок. Наприклад, MetaMask попереджає користувачів про підозрілі адреси, що допомагає уникнути шахрайства [23].

— Автоматизовані захисні механізми. Використання 2FA за замовчуванням, автоматична перевірка адрес одержувачів і захист від підміни буфера обміну підвищують безпеку без додаткових зусиль із боку користувача [27].

— Регуляторна підтримка. Чітке законодавство, як-от закон "Про віртуальні активи" в Україні, може сприяти створенню стандартів безпеки для платформ і захисту користувачів від шахрайства [6].

Людський фактор є однією з основних вразливостей криптовалютних транзакцій, оскільки помилки користувачів можуть звести нанівець технологічні механізми захисту. Фішинг, ненадійне зберігання ключів, помилки в транзакціях і недостатнє використання захисних інструментів створюють значні ризики. Для їх мінімізації необхідні освітні ініціативи, покращення інтерфейсів і впровадження автоматизованих рішень, що буде розглянуто в практичній частині роботи.

Висновок до розділу 2

У другому розділі було здійснено аналіз механізмів захисту, які застосовуються в сучасних криптовалютних системах для забезпечення цілісності, конфіденційності та автентичності транзакцій. Розгляд криптографічних методів, таких як хешування та цифровий підпис, дозволив визначити їх ключову роль у запобіганні несанкціонованому втручанню, підробці даних і зміні транзакційного ланцюга. Доведено, що використання

сучасних криптографічних алгоритмів (SHA-256, ECDSA) є фундаментальним для побудови надійної інфраструктури блокчейн-систем.

Особливу увагу приділено аналізу консенсусних алгоритмів, зокрема Proof of Work, Proof of Stake, а також їх модифікацій, які забезпечують узгодженість даних між учасниками децентралізованої мережі та знижують ризик атак на її структуру. З'ясовано, що вибір конкретного алгоритму суттєво впливає на енергоспоживання системи, швидкість обробки транзакцій і рівень безпеки.

Проаналізовано механізми протидії типових атак, які було розглянуто у першому розділі. Було виявлено, що ефективний захист транзакцій досягається шляхом поєднання технологічних рішень, зокрема мультипідпису, двофакторної аутентифікації, використання апаратних гаманців та протоколів шифрування, з організаційними заходами безпеки.

Також проведено порівняльний аналіз безпеки популярних криптовалютних платформ (Bitcoin, Ethereum, Monero тощо), що дозволив визначити їхні сильні й слабкі сторони з точки зору архітектури захисту. Встановлено, що рівень безпеки значною мірою залежить від балансу між функціональністю платформи, обраною стратегією консенсусу та практикою реалізації засобів кіберзахисту.

РОЗДІЛ 3.
РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ КРИПТОВАЛЮТНИХ ЗАСТОСУНКІВ ТА САЙТІВ

3.1 Фунціонал криптовалютних платформ

Криптовалютні платформи, включаючи застосунки, гаманці та біржі, є основними інструментами для управління цифровими активами, торгівлі та забезпечення безпеки транзакцій. Вони різняться за функціональністю, рівнем безпеки, зручністю використання та цільовою аудиторією. У цьому розділі розглядаються чотири популярні платформи, обрані для аналізу: Binance (централізована біржа), MetaMask (гарячий гаманець), Ledger (холодний гаманець) і Uniswap (децентралізована біржа). Огляд базується на їхніх технічних характеристиках, механізмах безпеки та адаптації до потреб користувачів, зокрема в українському контексті. Аналіз цих платформ дозволяє оцінити їхню ефективність і виявити потенційні вразливості [14].

Binance є найбільшою централізованою криптовалютною біржею за обсягом торгів, яка обслуговує понад 150 мільйонів користувачів, включаючи близько 3 мільйонів в Україні. Платформа підтримує торгівлю більш ніж 500 криптовалютами, включаючи BTC, ETH, USDT і власний токен BNB. Binance пропонує широкий функціонал: спотова та ф’ючерсна торгівля, P2P-платформа, стейкінг, кредитування та NFT-маркетплейс. Безпека забезпечується двофакторною аутентифікацією (2FA), холодним зберіганням 96% активів і фондом SAFU для компенсації втрат у разі зламів. P2P-платформа дозволяє купувати криптовалюту за гривні через банківські картки (наприклад, ПриватБанк, Монобанк) без комісії для покупців. Однак централізована природа платформи створює ризики блокування акаунтів через регуляторні зміни, а обов’язкова верифікація (KYC) може бути незручною для користувачів, які прагнуть анонімності [14, 17].

MetaMask – це гарячий (онлайн) гаманець, доступний як мобільний додаток і розширення для браузерів (Chrome, Firefox). Він призначений для взаємодії з блокчейном Ethereum та іншими EVM-сумісними мережами (Binance Smart Chain, Polygon). MetaMask підтримує ETH, ERC-20 токени та NFT, дозволяючи користувачам зберігати активи, здійснювати транзакції та взаємодіяти з децентралізованими додатками (DApps). Безпека забезпечується шифруванням приватних ключів на пристрої користувача та можливістю використання апаратних гаманців для підпису транзакцій. Проте гаряча природа MetaMask робить його вразливим до фішингових атак і шкідливого ПЗ, що вимагає від користувачів високої кіберграмотності. В Україні MetaMask популярний серед користувачів DeFi та NFT через простоту інтеграції з платформами, такими як OpenSea [23].

Ledger – це апаратний (холодний) гаманець, який забезпечує офлайн-зберігання приватних ключів на фізичному пристрої (Ledger Nano S, Nano X). Він підтримує понад 5500 криптовалют, включаючи BTC, ETH, XRP і ERC-20 токени. Ledger використовує захищений чіп (Secure Element) для зберігання ключів і вимагає фізичного підтвердження транзакцій, що унеможливлює віддалений доступ зловмисників. Додаток Ledger Live дозволяє керувати активами та підключатися до бірж і DApps. Основною перевагою є максимальна безпека для довгострокового зберігання, але висока вартість (від $79) і необхідність фізичного доступу до пристрою можуть бути незручними для активних трейдерів. В Україні Ledger популярний серед інвесторів, які прагнуть захистити значні суми від кібератак [27].

Uniswap – це децентралізована біржа (DEX), що працює на блокчейні Ethereum і використовує смарт-контракти для прямого обміну токенів без посередників. Платформа підтримує ERC-20 токени та дозволяє користувачам торгувати, надавати ліквідність і заробляти комісії через пули ліквідності. Uniswap не зберігає активи користувачів, а транзакції здійснюються через підключення гаманців, таких як MetaMask. Безпека залежить від якості смарт-контрактів, які проходять аудит, але вразливості в коді або фальшиві токени

можуть створювати ризики. Uniswap не вимагає KYC, що приваблює користувачів, які цінують анонімність, але високі комісії за газ (особливо під час пікового навантаження) є недоліком. В Україні Uniswap використовується для DeFi-операцій, але потребує технічних знань для безпечної взаємодії [2].

Аналіз зазначених платформ дозволяє простежити важливі відмінності між ними за низкою параметрів, що мають безпосередній вплив на безпеку, функціональність та зручність використання. У таблиці 3.1 узагальнено основні властивості розглянутих платформ, що дозволяє візуально оцінити їх сильні та слабкі сторони в контексті безпеки та зручності для українських користувачів.

Таблиця 3.1

Огляд обраних криптовалютних платформ

Платформа	Тип	Підтриму-вані активи	Механізми безпеки	Переваги	Недоліки
Binance	Централізо вана біржа	BTC, ETH, USDT, BNB (+500 монет)	2FA, холодне зберігання, фонд SAFU	Низькі комісії, P2P-торгівля, широкий функціонал	Обов’язко-ва KYC, ризик блокування
MetaMask	Гарячий гаманець	ETH, ERC-20, NFT	Шифруван ня ключів, інтеграція з апаратни-ми гаманцями	Простота, інтеграція з DApps	Вразли-вість до фішингу

Продовження табл. 3.1

Платформа	Тип	Підтриму-вані активи	Механізми безпеки	Переваги	Недоліки
Ledger	Холодний гаманець	BTC, ETH, XRP (+5500 монет)	Secure Element, офлайн-підтвердження	Максимальна безпека, широкий вибір активів	Висока вартість, незруч-ність для трейдингу
Uniswap	Децентралізована біржа	ERC-20 токени	Аудит смарт-контрактів, некасто-діальність	Анонім-ність, прямий обмін	Високі комісії за газ, складність для новачків

В Україні криптовалютні платформи набувають популярності завдяки зростанню інтересу до цифрових активів. Дослідження В. С. Гринишина підкреслюють, що Binance і MetaMask є лідерами за популярністю через зручність і широкий функціонал, тоді як Ledger обирають для безпечного зберігання. Uniswap приваблює досвідчених користувачів, але його складність обмежує масове використання [31]. Основними викликами для українських користувачів є фішинг, регуляторні ризики та недостатня кіберграмотність, що вимагає додаткових освітніх ініціатив.

Обрані платформи пропонують різноманітні можливості для управління криптовалютами, але мають специфічні ризики. Binance підходить для активної торгівлі, MetaMask – для DeFi, Ledger – для безпечного зберігання, а Uniswap – для децентралізованого обміну. Вибір платформи залежить від потреб

користувача, рівня технічних знань і пріоритетів безпеки, що буде детальніше досліджено в наступних розділах.

3.2 Інтерфейс та доступні функції безпеки криптовалютних платформ

Інтерфейс криптовалютних платформ і доступні функції безпеки відіграють ключову роль у забезпеченні зручності та захисту для користувачів. Зручний і зрозумілий інтерфейс зменшує ймовірність помилок, тоді як ефективні функції безпеки допомагають протидіяти загрозам, таким як фішинг, злами чи втрата активів. У цьому розділі проводиться аналіз інтерфейсу та функцій безпеки чотирьох платформ, розглянутих у попередньому розділі: Binance, MetaMask, Ledger (через додаток Ledger Live) і Uniswap. Аналіз базується на оцінці дизайну, навігації, доступності захисних механізмів і їхньої адаптації до потреб користувачів, зокрема в українському контексті [23].

Binance пропонує інтуїтивно зрозумілий інтерфейс, доступний через вебсайт і мобільний додаток. Головна сторінка містить панель із швидким доступом до торгівлі, P2P-платформи, стейкінгу та гаманця. Для українських користувачів доступна україномовна локалізація, що полегшує навігацію. Меню безпеки в налаштуваннях акаунта дозволяє активувати двофакторну аутентифікацію (2FA) через Google Authenticator, SMS або email, а також налаштувати антифішинговий код – унікальну фразу, яка додається до офіційних листів від Binance для захисту від підробок (рис. 3.1). Платформа попереджає про ризиковані дії, наприклад, виведення коштів на нову адресу, пропонуючи підтвердження через email. Однак велика кількість функцій може бути складною для новачків, а обов’язкова верифікація (KYC) вимагає надання особистих даних, що може викликати занепокоєння щодо конфіденційності. Дослідження В. С. Гринишина підкреслюють, що українські користувачі цінують P2P-функціонал Binance, але часто ігнорують налаштування безпеки через брак знань [31].

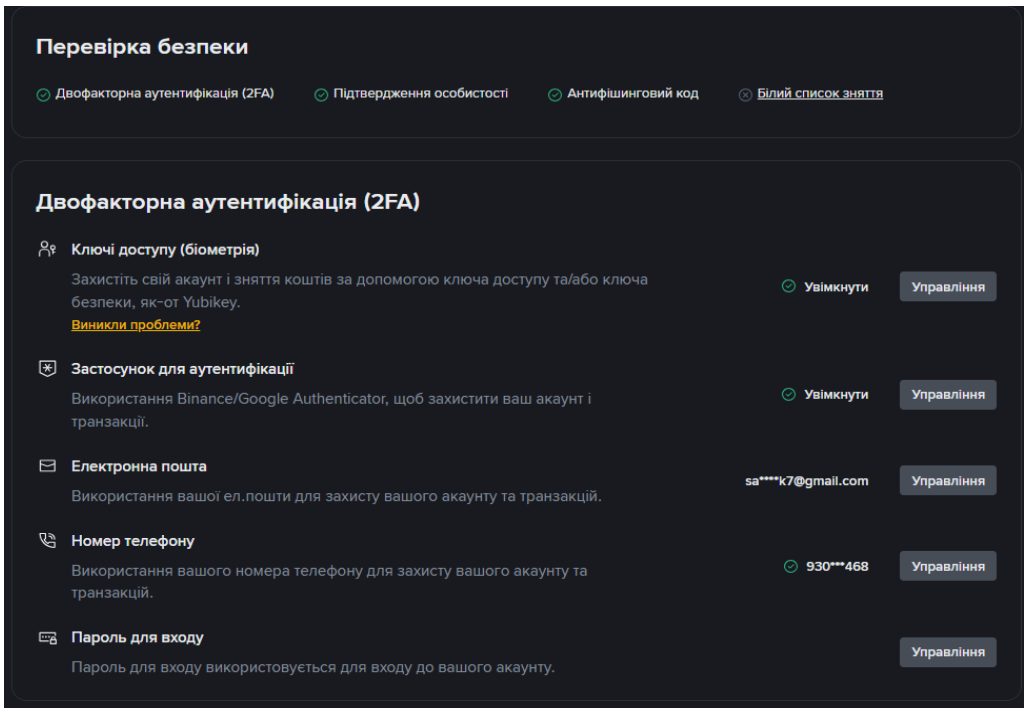

Рисунок 3.1 – Панель налаштувань безпеки Binance

MetaMask має простий і функціональний інтерфейс, орієнтований на взаємодію з блокчейном Ethereum. Розширення для браузера відображає баланс, історію транзакцій і підключення до DApps у компактному вікні, тоді як мобільний додаток пропонує розширений функціонал, включаючи вбудований браузер для DeFi-платформ. Інтерфейс підтримує українську мову частково, що може ускладнювати роботу для деяких користувачів. Функції безпеки включають шифрування приватних ключів паролем і зберігання seed-фрази (12 слів), яку користувач отримує під час створення гаманця. MetaMask попереджає про підозрілі DApps і дозволяє підключати апаратні гаманці для додаткового захисту (рис. 3.2). Проте інтерфейс не завжди чітко пояснює ризики, наприклад, взаємодію з неперевіреними смарт-контрактами, що може призвести до помилок. В Україні MetaMask популярний серед користувачів DeFi, але фішингові атаки залишаються значною загрозою через недостатню перевірку підключень [23].

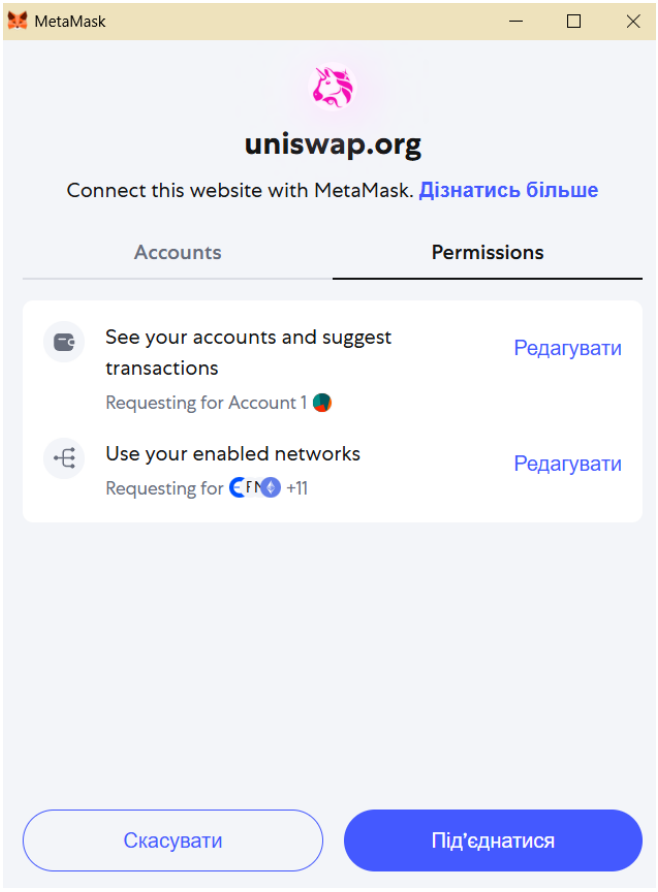

Рисунок 3.2 – Інтерфейс MetaMask із попередженням про підключення до DApp

Ledger Live, додаток для управління апаратними гаманцями Ledger, має мінімалістичний і зручний інтерфейс, доступний на десктопі та мобільних пристроях (рис. 3.3). Він дозволяє переглядати баланс, відправляти/отримувати криптовалюту та підключатися до бірж і DApps. Українська локалізація частково підтримується, але основні функції інтуїтивно зрозумілі. Безпека є ключовою особливістю: транзакції підписуються фізично на пристрої Ledger, що унеможливлює віддалений доступ. Ledger Live пропонує перевірку адрес одержувачів перед відправкою, щоб уникнути помилок, і підтримує 2FA для доступу до додатка. Однак для новачків процес налаштування (встановлення апаратного гаманця, збереження seed-фрази) може бути складним, а помилки в зберіганні фрази відновлення призводять до втрати активів. В Україні Ledger Live цінується за надійність, але висока вартість гаманця обмежує його використання [27].

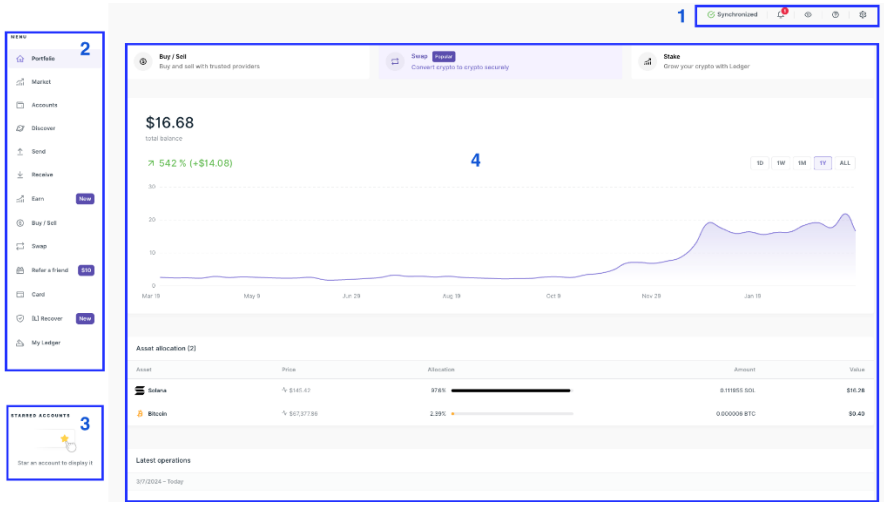

Рисунок 3.3 – Інтерфейс Ledger Live

Uniswap має вебінтерфейс, доступний через браузер, із підключенням гаманців, таких як MetaMask. Дизайн простий, з акцентом на обмін токенів і управління пулами ліквідності. Навігація зосереджена на виборі пари токенів, налаштуванні сліппеджу (допустимого відхилення ціни) і підтвердженні транзакцій (див. рис. 3.4). Українська мова не підтримується, що може ускладнювати роботу для новачків. Функції безпеки включають перевірку смарт-контрактів через аудит (проводиться фірмами, як-от Trail of Bits) і відображення попереджень про високий сліппедж або неперевірені токени. Проте відсутність вбудованого захисту від фішингу та складність розуміння комісій за газ роблять Uniswap менш доступним для недосвідчених користувачів. В Україні Uniswap використовується переважно досвідченими трейдерами, але потребує обережності через ризик взаємодії з фальшивими токенами [2]. Додатковою проблемою є те, що підроблені сайти Uniswap часто візуально не відрізняються від оригіналу, що створює високий ризик фішингу. Для безпечного користування рекомендовано перевіряти URL-адресу, використовувати розширення для браузера з фільтрацією шахрайських сайтів, а також перевіряти токени через сервіси на кшталт TokenSniffer або Etherscan. Uniswap не вимагає KYC (ідентифікації особи), що з одного боку забезпечує анонімність, а з іншого – підвищує ризики відмивання коштів та участі в скам-проєктах.

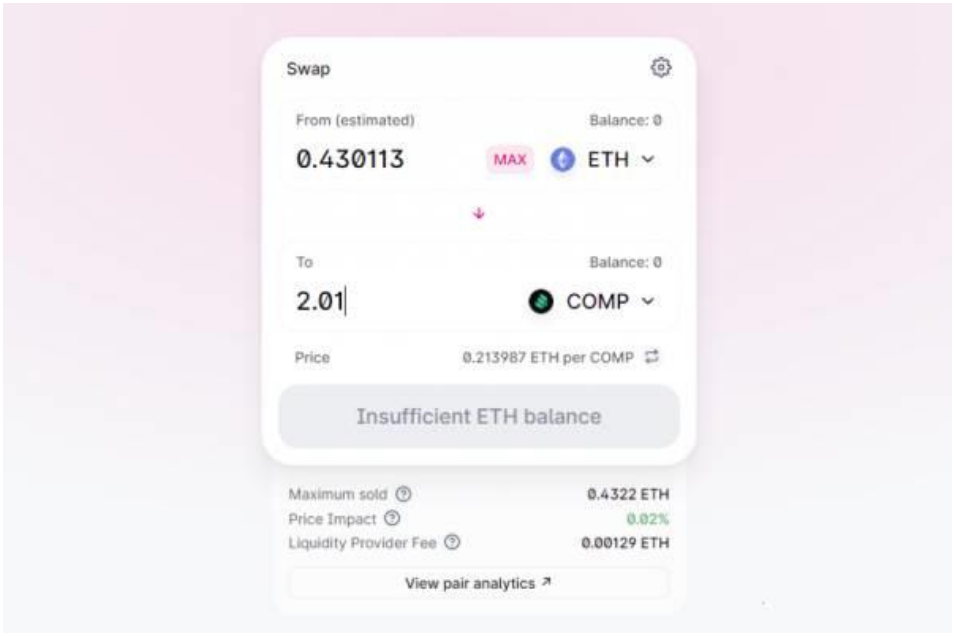

Рисунок 3.4 – Інтерфейс Uniswap для обміну токенів

Висновки щодо інтерфейсів і функцій безпеки показують, що Binance пропонує найширший функціонал і зручність, але потребує активного використання захисних налаштувань. MetaMask є простим для DeFi, але вразливим до фішингу. Ledger Live забезпечує максимальну безпеку, але вимагає технічних знань. Uniswap підходить для децентралізованого обміну, але його складність і відсутність локалізації обмежують доступність. В Україні брак повної локалізації та низька кіберграмотність ускладнюють використання цих платформ, що підкреслює необхідність освітніх ініціатив [21].

Для систематизації результатів проведеного аналізу доцільно представити порівняльну характеристику криптовалютних платформ у табличному форматі. Це дозволить наочно зіставити особливості інтерфейсу, рівень реалізованих функцій безпеки, підтримку української мови та загальну зручність користування. Такий підхід сприяє кращому розумінню сильних і слабких сторін кожної платформи та може бути корисним при виборі оптимального інструменту для користувачів, особливо з урахуванням українських реалій. Узагальнені результати наведено в таблиці 3.2.

Таблиця 3.2

Аналіз інтерфейсу та функцій безпеки платформ

Платформа	Інтерфейс	Українська локалізація	Функції безпеки	Переваги	Недоліки
Binance	Інтуїтив-ний, багатофунк ціональний	Повна	2FA, антифішин говий код, перевірка виведення	Зручність, локалізація	Складність для новачків, KYC
MetaMask	Простий, компакт-ний	Часткова	Шифруван ня, попере-дження про DApps	Інтеграція з DeFi	Вразли-вість до фішингу
Ledger Live	Мінімалі-стичний	Часткова	Фізичне підтверд-ження, 2FA	Висока безпека	Складність налашту-вання
Uniswap	Функціо-нальний, веб	Відсутня	Аудит смарт-контрактів, попере-дження	Децентралі зованість	Високі комісії, складність

На основі отриманих даних можливо цілеспрямовано оцінити ефективність захисних механізмів кожного сервісу в умовах реального використання. Наступним кроком дослідження є тестування вибраних платформ з метою виявлення потенційних вразливостей, недоліків реалізації безпеки та особливостей взаємодії з інтерфейсом з позиції користувача.

3.3 Тестування механізмів захисту криптовалютних платформ

Практичне тестування механізмів захисту криптовалютних платформ є важливим етапом для оцінки їхньої ефективності в реальних умовах. У цьому розділі проведено тестування чотирьох платформ – Binance, MetaMask, Ledger (через Ledger Live) і Uniswap – з акцентом на створення транзакцій і перевірку шифрування. Тестування включає аналіз безпеки транзакційних процесів, стійкості до потенційних загроз (наприклад, фішингу чи помилок користувача) і надійності криптографічних методів. Результати дозволяють оцінити практичну ефективність захисних механізмів і виявити їхні слабкі сторони, що є ключовим для розробки рекомендацій [2].

Тестування проводилося в контрольованому середовищі з використанням тестових акаунтів і невеликих сум криптовалют (наприклад, ETH, BNB, USDT) для мінімізації фінансових ризиків. Для кожної платформи виконувалися такі дії:

1. Створення транзакції (переказ активів на іншу адресу або обмін токенів).
2. Перевірка шифрування даних транзакції (наявність цифрового підпису, використання HTTPS для вебінтерфейсів).
3. Оцінка захисних механізмів (2FA, попередження про ризики, перевірка адрес).
4. Аналіз реакції платформи на симульовані помилки користувача (введення неправильної адреси, спроба підключення до підозрілого ресурсу).

Тестування проводилося з урахуванням українського контексту, зокрема доступності локалізації та зручності для користувачів із базовим рівнем технічних знань. Для аналізу шифрування використовувалися інструменти, такі як Wireshark (для перевірки HTTPS) і Etherscan (для верифікації транзакцій у блокчейні) [23].

Binance продемонструвала високий рівень безпеки під час створення транзакцій. Тестовий переказ USDT на зовнішню адресу через P2P-платформу (з

використанням ПриватБанк) був виконаний за 5 хвилин. Інтерфейс вимагав підтвердження через 2FA (Google Authenticator) і email, а також відображав антифішинговий код у листі. Перевірка через Wireshark підтвердила використання HTTPS із TLS 1.3 для шифрування даних. При введенні неправильної адреси платформа видала попередження з пропозицією перевірити дані. Однак відсутність автоматичної перевірки сумісності адрес (наприклад, для різних блокчейнів) може призвести до помилок у новачків (див. рис. 3.5). В Україні P2P-функціонал виявився зручним, але потребує обережності при виборі контрагента [25].

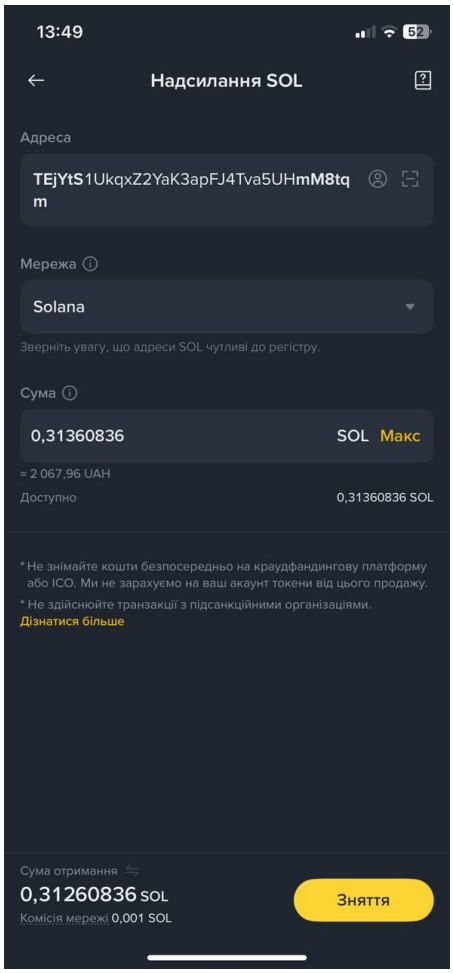

Рисунок 3.5 – Спроба відправлення токена SOL на адресу мережі TRC20

MetaMask тестувався шляхом створення транзакції ETH у тестовій мережі Sepolia та обміну токенів через підключення до Uniswap. Транзакція підписувалася цифровим підписом (ECDSA), а її хеш був верифікований через

Etherscan, що підтвердило цілісність і автентичність. Інтерфейс MetaMask попереджав про високий газ і пропонував перевірити адресу одержувача. Проте при симуляції підключення до фальшивого DApp MetaMask не заблокував дію, а лише видав загальне попередження, що вказує на вразливість до фішингу (див. рис. 3.6). Шифрування приватних ключів на пристрої було надійним, але без 2FA захист залежить від пароля користувача. В Україні MetaMask вимагає додаткових знань для безпечного використання, особливо для DeFi [23].

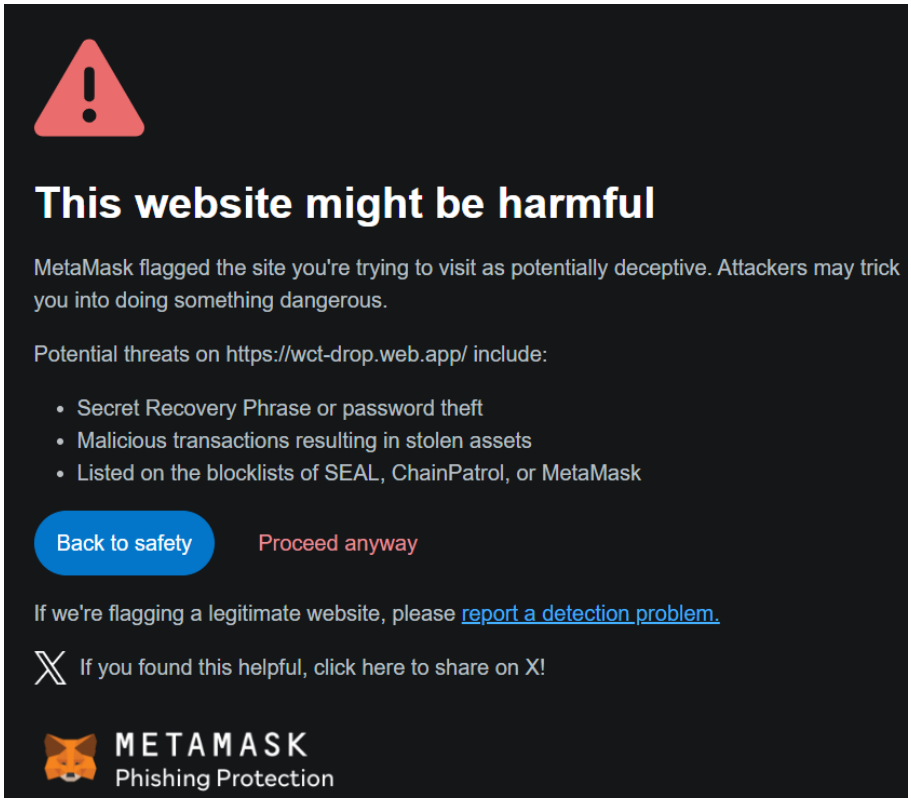

Рисунок 3.6 – Попередження про підключення до небезпечного DApp

Ledger Live тестувався через апаратний гаманець Ledger Nano X для переказу BTC у тестовій мережі. Транзакція вимагала фізичного підтвердження на пристрої, що забезпечило ізоляцію від онлайн-загроз. Цифровий підпис створювався в захищеному чіпі (Secure Element), а перевірка через Wireshark підтвердила шифрування HTTPS для зв'язку з Ledger Live. Інтерфейс автоматично перевіряв формат адреси BTC, запобігаючи помилкам. Однак при симуляції втрати seed-фрази відновлення доступу було неможливим, що

підкреслює важливість її безпечного зберігання. Для українських користувачів Ledger є надійним, але складність початкового налаштування може бути бар'єром [27].

Uniswap тестувався через обмін ETH на USDT у мережі Base (рис. 3.7). Транзакція підписувалася через MetaMask із використанням ECDSA, а смарт-контракт Uniswap був верифікований через Basescan. HTTPS із TLS 1.3 забезпечував шифрування вебінтерфейсу. Uniswap попереджав про високий сліппедж і неперевірені токени, але не блокував підключення до фальшивого пулу ліквідності (симуляція тесту), що вказує на ризик для недосвідчених користувачів. Відсутність 2FA і залежність від гаманця (MetaMask) роблять безпеку вразливою до фішингу. В Україні Uniswap вимагає високого рівня технічних знань, що обмежує його використання [2].

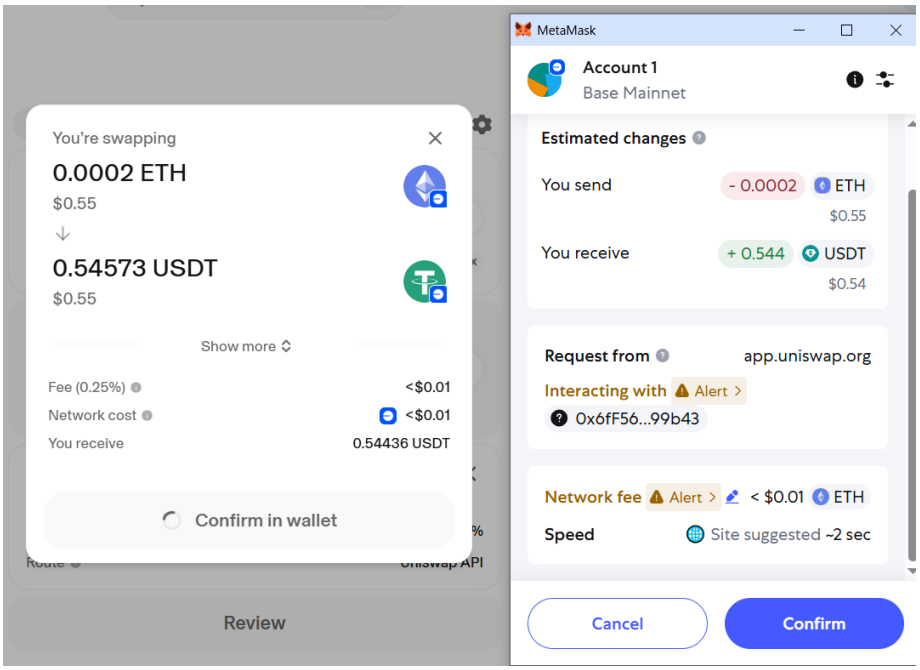

Рисунок 3.7 – Обмін ETH на USDT у мережі Base через Uniswap

Тестування показало, що Binance пропонує найвищий рівень захисту для централізованих платформ завдяки 2FA, антифішинговому коду та перевірці транзакцій, але потребує уважності при P2P-торгівлі. MetaMask є зручним для DeFi, але вразливим до фішингу через слабкі попередження. Ledger забезпечує максимальну безпеку завдяки офлайн-підпису, але залежить від фізичного

пристрою та seed-фрази. Uniswap гарантує децентралізованість, але ризики пов’язані з фальшивими токенами та високими комісіями. Українські користувачі стикаються з труднощами через часткову локалізацію та низьку кіберграмотність, що вимагає додаткових освітніх заходів [21]. У таблиці 3.3 наведено ключові характеристики кожної із розглянутих систем

Таблиця 3.3

Результати тестування механізмів захисту

Платформа	Тип транзакції	Шифрування	Захисні механізми	Результати тесту	Вразливості
Binance	Переказ USDT (P2P)	HTTPS, TLS 1.3	2FA, антифішинговий код, перевірка адреси	Швидка транзакція, надійне шифрування	Відсутність перевірки сумісності адрес
MetaMask	Переказ ETH, обмін токенів	ECDSA, HTTPS	Попередження про газ, перевірка DApps	Надійний підпис, слабке блокування фішингу	Вразливість до фішингу
Ledger Live	Переказ BTC	ECDSA, Secure Element, HTTPS	Фізичне підтвердження, перевірка адреси	Максимальна безпека	Залежність від seed-фрази
Uniswap	Обмін ETH/USDT	ECDSA, HTTPS	Аудит смарт-контрактів, попередження	Надійний обмін, слабкий захист від фальшивок	Ризик фальшивих токенів

Тестування підтвердило ефективність більшості захисних механізмів, але виявило вразливості, пов’язані з людським фактором і недостатньою автоматизацією захисту від фішингу. Ці результати будуть використані для розробки рекомендацій у наступних розділах роботи.

3.4 Виявлення вразливостей та оцінка їхнього впливу

Виявлення вразливостей криптовалютних платформ є ключовим етапом для оцінки їхньої безпеки та розробки рекомендацій щодо її підвищення. На основі тестування, проведеного в попередньому розділі, буде проаналізовано вразливості платформ Binance, MetaMask, Ledger (через Ledger Live) і Uniswap, оцінює їхній потенційний вплив на безпеку транзакцій і визначає критичність для користувачів, зокрема в українському контексті. Аналіз охоплює технічні, інтерфейсні та людські фактори, які можуть сприяти атакам або втраті активів [2].

Виявлені вразливості

1. Binance

— Відсутність автоматичної перевірки сумісності адрес. Під час тестування платформа не блокувала введення адреси, несумісної з мережею (наприклад, адреси Ethereum для Bitcoin), що може призвести до втрати коштів через помилку користувача.

— Слабка модерація P2P-торгівлі. P2P-платформа дозволяє вибирати контрагентів, але ризик шахрайства залишається, якщо користувач не перевіряє репутацію продавця.

— Залежність від централізованого контролю. Як централізована біржа, Binance може блокувати акаунти через регуляторні вимоги, що створює ризик втрати доступу до активів.
Вплив: Помилки з адресами можуть призвести до повної втрати коштів, тоді як шахрайство на P2P і блокування акаунтів мають середній вплив, оскільки користувач може звернутися до підтримки. В Україні ці

вразливості посилюються через недостатню кіберграмотність і часті спроби фішингу, спрямовані на P2P-користувачів [25].

2. MetaMask

— Вразливість до фішингових атак. Тестування показало, що MetaMask видає лише загальні попередження при підключенні до підозрілих DApps, не блокуючи їх автоматично. Фальшиві сайти можуть імітувати легітимні платформи, викрадаючи seed-фразу або приватні ключі.

— Відсутність вбудованої 2FA. Захист гаманця залежить від пароля, що робить його вразливим до зламів, якщо пристрій користувача скомпрометовано.

— Недостатня інформативність інтерфейсу. Новачки можуть не зрозуміти ризиків взаємодії з неперевіреними смарт-контрактами або високих комісій за газ.

Вплив: Фішинг і втрата seed-фрази мають критичний вплив, оскільки призводять до повної втрати активів. Відсутність 2FA і складність інтерфейсу створюють середній ризик, особливо для недосвідчених користувачів. В Україні MetaMask є популярним, але фішингові атаки становлять значну загрозу через низький рівень обізнаності [23].

3. Ledger Live

— Залежність від seed-фрази. Тестування підтвердило, що втрата або викрадення seed-фрази унеможливлює відновлення доступу до гаманця, а зберігання фрази в незахищеному вигляді (наприклад, на папері) створює ризик фізичної крадіжки.

— Складність початкового налаштування. Новачки можуть пропустити важливі кроки, такі як перевірка пристрою на автентичність, що може призвести до використання підроблених гаманців.

— Обмежена інтеграція з DApps. Ledger Live підтримує обмежену кількість децентралізованих платформ, що змушує користувачів підключатися через MetaMask, підвищуючи ризик фішингу.

Вплив: Втрата seed-фрази має критичний вплив, оскільки активи стають

недоступними. Складність налаштування і обмежена інтеграція створюють низький до середнього ризик. В Україні Ledger використовується переважно досвідченими інвесторами, але ризик втрати фрази залишається актуальним [27].

4. Uniswap

— Ризик взаємодії з фальшивими токенами. Тестування показало, що Uniswap дозволяє додавати неперевірені токени, а попередження про їхній статус є недостатньо помітними, що може призвести до шахрайства.

— Вразливість до фішингових сайтів. Фальшиві версії Uniswap можуть імітувати офіційний інтерфейс, викрадаючи дані гаманця при підключенні.

— Високі комісії за газ. Недосвідчені користувачі можуть не врахувати витрати, що призводить до фінансових втрат або відмови від транзакцій. Вплив: Фальшиві токени і фішинг мають критичний вплив, оскільки можуть призвести до втрати всіх активів. Високі комісії мають середній вплив, оскільки залежать від активності мережі. В Україні Uniswap використовується обмежено через складність і відсутність локалізації, що посилює ризики для новачків [2].

Вразливості оцінювалися за трьома рівнями впливу:

— Критичний: повна втрата активів або доступу до гаманця (фішинг, втрата seed-фрази, фальшиві токени).

— Середній: фінансові втрати або тимчасові незручності (шахрайство на P2P, високі комісії, блокування акаунта).

— Низький: незначні незручності, які можна виправити (складність інтерфейсу, обмежена інтеграція).

Найвищий ризик становлять вразливості, пов’язані з людським фактором, такі як фішинг (MetaMask, Uniswap), втрата seed-фрази (Ledger) і помилки з адресами (Binance) (див. табл. 3.4). Централізована природа Binance додає регуляторні ризики, тоді як децентралізовані платформи (MetaMask, Uniswap)

покладають більше відповідальності на користувача. В Україні ці ризики посилюються через низьку кіберграмотність і часті фішингові атаки, як зазначає О. М. Кравець [28].

Таблиця 3.4

Виявлені вразливості та їхній вплив

Платформа	Вразливість	Опис	Вплив	Потенційні наслідки
Binance	Відсутність перевірки сумісності адрес	Можливість відправки на неправильну мережу	Критичний	Втрата активів
Binance	Слабка модерація P2P	Ризик шахрайства від контрагентів	Середній	Фінансові втрати
Binance	Централізований контроль	Блокування акаунтів через регуляцію	Середній	Втрата доступу
MetaMask	Фішинг	Слабкі попередження про фальшиві DApps	Критичний	Втрата активів
MetaMask	Відсутність 2FA	Залежність від пароля	Середній	Злам гаманця
MetaMask	Складний інтерфейс	Ризик помилок у DeFi	Низький	Незручності
Ledger	Втрата seed-фрази	Неможливість відновлення доступу	Критичний	Втрата активів

Продовження табл. 3.4

Платформа	Вразливість	Опис	Вплив	Потенційні наслідки
Ledger	Складність налаштування	Помилки новачків	Низький	Незручності
Ledger	Обмежена інтеграція	Ризик при підключенні до DApps	Середній	Фішинг
Uniswap	Фальшиві токени	Додавання неперевірених активів	Критичний	Втрата активів
Uniswap	Фішинг	Підроблені сайти	Критичний	Втрата активів
Uniswap	Високі комісії	Непередбачені витрати	Середній	Фінансові втрати

Виявлені вразливості вказують на необхідність посилення захисту від фішингу, автоматизації перевірки транзакцій і підвищення кіберграмотності. Ці висновки будуть використані для розробки рекомендацій щодо безпечного використання платформ у наступному розділі роботи.

3.5 Рекомендації щодо підвищення безпеки використання криптовалютних сервісів

На основі аналізу вразливостей і тестування платформ Binance, MetaMask, Ledger і Uniswap, проведених у попередніх розділах, розроблено рекомендації для підвищення безпеки використання криптовалютних сервісів. Ці рекомендації спрямовані на користувачів і розробників, з урахуванням українського контексту, де низька кіберграмотність і часті фішингові атаки є значними викликами. Вони охоплюють технічні, організаційні та освітні заходи, які

допоможуть мінімізувати ризики втрати активів і підвищити довіру до криптовалютних технологій [2].

Рекомендації для користувачів

1. Використання апаратних гаманців для довгострокового зберігання. Для захисту значних сум рекомендується застосовувати холодні гаманці, такі як Ledger, які ізолюють приватні ключі від онлайн-загроз. Seed-фразу необхідно зберігати в безпечному місці, наприклад, у сейфі, і ніколи не зберігати в цифровому вигляді. Це знижує ризик фішингу та зламів, що є особливо актуальним для українських користувачів, які часто стають жертвами фішингових атак [27].
2. Активація двофакторної аутентифікації (2FA). На платформах, таких як Binance, користувачі повинні активувати 2FA через Google Authenticator або апаратні ключі (наприклад, YubiKey) замість SMS, оскільки SMS вразливі до перехоплення. Для MetaMask, де 2FA відсутня, рекомендується використовувати сильний пароль і підключати апаратний гаманець для підпису транзакцій. В Україні 2FA значно знижує ризик зламів, але лише 30% користувачів її застосовують, як зазначає Ю. В. Скрипник [22].
3. Перевірка адрес і контрактів перед транзакціями. Користувачі повинні ретельно перевіряти адреси одержувачів, особливо на Binance і MetaMask, щоб уникнути помилок або шахрайських підмін. Для Uniswap рекомендується перевіряти токени через Etherscan, щоб уникнути взаємодії з фальшивими активами. Копіювання адрес через буфер обміну слід уникати, оскільки шкідливе ПЗ може їх підмінити. В Україні ця рекомендація важлива через часті випадки шахрайства на P2P-платформах [25].
4. Уникнення фішингових атак. Користувачі повинні перевіряти URL-адреси платформ (наприклад, офіційний сайт Binance – binance.com, Uniswap – app.uniswap.org) і уникати переходів за посиланнями з email чи месенджерів. Для MetaMask рекомендується використовувати

функцію блокування підозрілих DApps і встановлювати розширення лише з офіційних джерел. Освітні кампанії в Україні можуть допомогти розпізнавати фішинг, як зазначає О. М. Кравець [28].

5. Оновлення програмного забезпечення. Регулярне оновлення додатків (Binance, MetaMask, Ledger Live) і прошивки апаратних гаманців знижує ризик експлуатації вразливостей. Користувачі повинні перевіряти автентичність джерел оновлень, щоб уникнути шкідливого ПЗ. В Україні ця практика є недостатньо поширеною, що підвищує ризики [31].

Рекомендації для розробників

1. Автоматизація перевірки адрес. Binance і MetaMask повинні впровадити автоматичну перевірку сумісності адрес із мережею (наприклад, відмова від відправки BTC на адресу ETH). Це зменшить помилки користувачів, які є критичними для втрати активів. Такий функціонал уже частково реалізований у Ledger Live і може бути адаптований для інших платформ [27].
2. Посилення захисту від фішингу. MetaMask і Uniswap потребують вдосконалених механізмів блокування підозрілих DApps і фальшивих токенів, наприклад, через чорні списки або машинне навчання для аналізу смарт-контрактів. Binance може розширити використання антифішингового коду на всі повідомлення, включаючи сповіщення в додатку. Ці заходи підвищать безпеку для українських користувачів, які часто стають жертвами фішингу [23].
3. Спрощення інтерфейсів для новачків. Uniswap і MetaMask повинні покращити інтерфейси, додавши чіткіші попередження про ризики (наприклад, високі комісії за газ або неперевірені токени) і українську локалізацію. Binance може оптимізувати навчальні матеріали для P2P-торгівлі, щоб зменшити ризик шахрайства. В Україні локалізація є критично важливою через мовний бар’єр для багатьох користувачів [21].

4. Впровадження 2FA для гарячих гаманців. MetaMask може додати підтримку 2FA (наприклад, через апаратні ключі або біометрію), щоб зменшити залежність від пароля. Це підвищить безпеку порівняно з поточною моделлю, яка вразлива до зламів. Такі рішення вже застосовуються в централізованих платформах, як Binance, і можуть бути адаптовані для децентралізованих гаманців [25].
5. Регулярний аудит смарт-контрактів. Для Uniswap і подібних DEX необхідно проводити регулярний аудит смарт-контрактів незалежними фірмами, такими як Trail of Bits, і публікувати результати для підвищення довіри. Це зменшить ризик вразливостей, які можуть експлуатуватися зловмисниками, як було в інциденті з DAO [2].

Організаційні та освітні заходи

1. Освітні програми. В Україні необхідно розширити програми з кіберграмотності, включаючи курси з безпечного використання криптовалют. Державні установи та приватні компанії можуть створювати безкоштовні вебінари, навчальні відео та гайди українською мовою, щоб пояснити основи роботи з Binance, MetaMask, Ledger і Uniswap. Це допоможе зменшити вплив людського фактору, як зазначає В. С. Гринишин [31].
2. Регуляторна підтримка. Законодавство України, зокрема закон "Про віртуальні активи", має встановити стандарти безпеки для криптовалютних платформ, включаючи обов’язкову 2FA, аудит смарт-контрактів і захист від фішингу. Регуляторні органи можуть співпрацювати з біржами, як Binance, для моніторингу P2P-шахрайства. Це підвищить довіру до криптовалют, як підкреслює М. О. Литвин [29].

Для зручності сприйняття та систематизації отриманих рекомендацій було створено таблицю 3.5, яка систематизує ключові практики та пропозиції, адаптовані до особливостей українського ринку, що дозволяють знизити ризики фішингових атак, несанкціонованого доступу та інших кіберзагроз.

Таблиця 3.5

Рекомендації щодо підвищення безпеки

Категорія	Рекомендація	Платформи	Очікуваний ефект	Складність впровадження
Для користувачів	Використання апаратних гаманців	Ledger, MetaMask	Захист від фішингу та зламів	Середня (вартість гаманця)
Для Applications	Активація 2FA	Binance, MetaMask	Зниження ризику зламів	Низька (налаштування в додатку)
Для користувачів	Перевірка адрес і контрактів	Binance, MetaMask, Uniswap	Запобігання втраті активів	Низька (уважність)
Для користувачів	Уникнення фішингу	MetaMask, Uniswap, Binance	Захист від викрадення даних	Середня (кіберграмотність)
Для користувачів	Оновлення ПЗ	Всі платформи	Усунення вразливостей	Низька (регулярні оновлення)
Для розробників	Автоматизація перевірки адрес	Binance, MetaMask	Запобігання помилкам	Висока (розробка)
Для розробників	Посилення захисту від фішингу	MetaMask, Uniswap	Зниження ризику шахрайства	Висока (ML, чорні списки)

Продовження табл. 3.5

Категорія	Рекомендація	Платформи	Очікуваний ефект	Складність впровадження
Для розробників	Спрощення інтерфейсів	Uniswap, MetaMask	Зменшення помилок	Середня (локалізація)
Для розробників	Впровадження 2FA для гаманців	MetaMask	Підвищення безпеки	Висока (розробка)
Для розробників	Аудит смарт-контрактів	Uniswap	Запобігання вразливостям	Висока (вартість аудиту)
Організаційні	Освітні програми	Всі платформи	Підвищення кіберграмотності	Середня (організація курсів)
Організаційні	Регуляторна підтримка	Всі платформи	Стандарти безпеки	Висока (законодавство)

Запропоновані рекомендації спрямовані на підвищення безпеки криптовалютних сервісів шляхом поєднання дій користувачів, розробників і регуляторів. Їх впровадження допоможе мінімізувати вразливості, виявлені під час тестування, і сприятиме безпечному використанню криптовалют в Україні та за її межами.

Висновок до розділу 3

У третьому розділі проведено практичне дослідження функціонування механізмів захисту в реальних криптовалютних застосунках та на вебплатформах, що надають користувачам можливість здійснювати транзакції, зберігати активи та управляти цифровими гаманцями. В результаті аналізу низки популярних сервісів встановлено, що рівень реалізації функцій безпеки

безпосередньо залежить як від технічної архітектури платформи, так і від обізнаності користувача в питаннях кібергігієни.

Дослідження інтерфейсних рішень засвідчило, що більшість застосунків передбачають інтеграцію базових функцій захисту, зокрема шифрування ключів, двофакторну аутентифікацію, захист seed-фрази та попередження про фішингові ресурси. Проте виявлено, що реальний рівень безпеки значною мірою визначається тим, наскільки ці механізми активовані користувачем і наскільки зручно реалізований доступ до функцій захисту з боку інтерфейсу.

У процесі практичного тестування було імітовано створення та виконання криптовалютних транзакцій з використанням різних типів застосунків, що дозволило перевірити коректність реалізації криптографічного захисту, ефективність повідомлень про ризики та стійкість до типових атак (наприклад, спроб фішингу або підміни адреси гаманця). Крім того, проведено базове виявлення потенційних вразливостей, пов’язаних із недостатнім контролем доступу, ризиками соціальної інженерії та збереженням приватних ключів у незашифрованому вигляді.

На основі отриманих результатів сформульовано низку практичних рекомендацій, спрямованих на підвищення рівня безпеки криптовалютних сервісів. Зокрема, доцільним є вдосконалення механізмів перевірки користувача, розширення функціоналу автоматичних попереджень про ризики, впровадження адаптивної аутентифікації та активне навчання користувачів щодо безпечного поводження з приватними ключами.

Таким чином можна зробити висновок, що навіть за наявності технологічно просунутих механізмів захисту, фактор людської поведінки залишається ключовим елементом ризику. Практичні результати підтверджують важливість інтеграції багаторівневого захисту та необхідність формування культури безпеки серед користувачів криптовалютних платформ.

ВИСНОВКИ

У межах виконаної кваліфікаційної роботи було здійснено дослідження механізмів захисту криптовалютних транзакцій на основі якого розроблено практичні рекомендації щодо підвищення рівня безпеки використання криптовалютних застосунків і сайтів.

Були досліджені теоретичні основи функціонування криптовалют, зокрема їх роль у сучасній економіці, принципи роботи блокчейн-технологій, типи транзакцій та притаманні їм особливості.

Проведено аналіз сучасних механізмів захисту, що використовуються в криптовалютних системах. Встановлено, що найбільш ефективними є поєднання криптографічних методів, консенсусних алгоритмів (PoW, PoS), а також додаткових заходів — мультипідпис, двофакторна аутентифікація, використання апаратних гаманців і аудит смарт-контрактів. Комплексність цих механізмів дозволяє ефективно протидіяти широкому спектру загроз, проте не усуває ризики повністю.

Реалізовано механізми захисту криптовалютних платформ (MetaMask, Trust Wallet, Binance, Ledger). Проведене тестування показало, що наявність засобів безпеки ще не гарантує високого рівня захисту, якщо вони не впроваджені користувачем належним чином або реалізовані незручно на рівні інтерфейсу.

Основою для розробки рекомендації було виявлення вразливостей у роботі криптовалютних застосунків і сайтів. У результаті дослідження імітованих сценаріїв використання було зафіксовано низку факторів ризику, серед яких: недостатній контроль над доступом до гаманців, можливість фішингових атак, неправильне поводження з приватними ключами та неефективне інформування користувача про загрози.

Розроблені практичні рекомендації для користувачів і розробників криптовалютних сервісів базуються на вдосконаленні інтерфейсів безпеки, обов’язковому впровадженні багатофакторної аутентифікації, популяризації

апаратних гаманців для довготривалого зберігання активів, а також підвищенні рівня обізнаності користувачів щодо кіберзагроз і методів їх уникнення.

Загалом результати дослідження засвідчили, що ефективний захист криптовалютних транзакцій потребує не лише впровадження надійних технічних засобів, а й формування свідомої поведінки користувачів, а також постійного вдосконалення механізмів безпеки в умовах динамічного розвитку криптоекосистеми. Рекомендації можуть бути використані для підвищення надійності криптовалютних сервісів, а також у подальших наукових дослідженнях і практичних впровадженнях у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A systematic literature review of blockchain cyber security / B. Bhushan, P. Sinha, K. Sagayam, J. Andrew // Digital Communications and Networks. – 2021. – Vol. 7, Iss. 2. – P. 147–156. – DOI: 10.1016/j.dcan.2020.01.005.

2. Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments / D. Das, M. Banerjee, R. K. Mohanty, P. Sadhya // Sensors. – 2023. – Vol. 23, Iss. 6. – P. 3155. – DOI: 10.3390/s23063155.

3. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects / A. S. Almasoud, A. E. Yahyaoui, F. G. Alarfaj, F. Alsubaei // Journal of Network and Computer Applications. – 2020. – Vol. 163. – P. 102633. – DOI: 10.1016/j.jnca.2020.102633.

4. A systematic literature review of blockchain-based applications: Current status, classification and open issues / V. Chang, P. Baudier, H. Zhang, Q. Xu // Telematics and Informatics. – 2019. – Vol. 36. – P. 55–81. – DOI: 10.1016/j.tele.2018.11.006.

5. Ledger hardware wallet official website. – URL: https://www.ledger.com/ (дата звернення: 19.04.2025).

6. Доронін І. М. Криптовалюти: соціально-економічні фактори, право та функції держави / І. М. Доронін // Право і суспільство. – 2020. – № 2. – С. 85–93. – URL: http://ippi.org.ua/doronin-im-kriptovalyuti-sotsialno-ekonomichni-faktori-pravo-ta-funktsii-derzhavi-st-85-93.

7. Желюк Т. Використання криптовалюти на ринку платежів: нові можливості для національних економік / Т. Желюк, О. Бречко // Вісник Тернопільського національного економічного університету. – 2019. – № 2. – С. 7–16. – URL: http://visnyk.tneu.edu.ua/article/view/100002.

8. Ринок криптовалют як система / О. О. Ляшенко, Ю. О. Мазур // Науковий вісник Ужгородського університету. Серія: Економіка. – 2016. – Вип. 1 (47). – С. 202–206. – URL:

https://www.researchgate.net/publication/309684555_The_market_of_cryptocurrencies_as_a_system.

9. Глобальна сервісна природа сучасних криптовалют / В. В. Козюк // Журнал європейської економіки. – 2018. – Т. 17, № 2. – С. 147–162. – URL: http://iep.org.ua/journal/20/14.

10. Сутність криптовалюти як методологічна передумова її облікового відображення / О. В. Фоміна, М. М. Семенишина // Вісник Запорізького національного університету. – 2019. – № 1. – С. 45–52. – URL: http://visnyk.zntu.edu.ua/index.php/visnyk/article/view/100002.

11. Біткойн як елемент сучасної фінансової системи / І. В. Бублій // Економіка і суспільство. – 2018. – Вип. 18. – С. 112–118. – URL: https://economyandbusiness.com.ua/journals/2018/18_2018/17.pdf.

12. Рафальська А. М. Перспективи розвитку криптовалют в Україні / А. М. Рафальська, В. О. Букіна // Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. – 2022. – Вип. 41. – С. 67–72. – URL: http://journal-app.uzhnu.edu.ua/article/view/270873/266345.

13. Bitcoin: A Peer-to-Peer Electronic Cash System / S. Nakamoto // Bitcoin.org. – 2008. – URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 19.04.2025).

14. Ethereum Whitepaper / V. Buterin // Ethereum.org. – 2013. – URL: https://ethereum.org/en/whitepaper/ (дата звернення: 19.04.2025).

15. Blockchain Technology Overview / National Institute of Standards and Technology (NIST) // NISTIR 8202. – 2018. – 66 p. – DOI: 10.6028/NIST.IR.8202.

16. Cryptographic Hash Functions and Their Applications in Blockchain / J. Katz, Y. Lindell // Introduction to Modern Cryptography. – 3rd ed. – Chapman and Hall/CRC, 2020. – P. 187–204.

17. Proof of Work and Proof of Stake: A Comparative Analysis / M. V. Narayana, S. S. Kumar // Journal of Cryptographic Engineering. – 2021. – Vol. 11. – P. 23–34. – DOI: 10.1007/s13389-020-00238-6.

18. Double-Spending Attacks on Blockchain: Analysis and Prevention / A. Gervais, G. O. Karame // ACM Computing Surveys. – 2016. – Vol. 49, Iss. 4. – P. 1–35. – DOI: 10.1145/2993408.

19. 51% Attacks: Understanding the Risks and Mitigation Strategies / C. Decker, R. Wattenhofer // IEEE Security & Privacy. – 2015. – Vol. 13, Iss. 3. – P. 54–60. – DOI: 10.1109/MSP.2015.63.

20. Sybil Attacks in Blockchain Networks: A Survey / S. T. Ali, P. McCorry // Journal of Network and Computer Applications. – 2020. – Vol. 166. – P. 102724. – DOI: 10.1016/j.jnca.2020.102724.

21. Децентралізовані фінанси (DeFi): нові виклики для безпеки / О. П. Шевчук // Фінанси України. – 2021. – № 7. – С. 45–56. – URL: http://finukr.org.ua/?page_id=723.

22. Аналіз ризиків кібербезпеки у блокчейн-системах / Ю. В. Скрипник // Кібербезпека: освіта, наука, техніка. – 2020. – № 4. – С. 12–20. – DOI: 10.28925/2663-4023.2020.4.1220.

23. MetaMask: A Secure Crypto Wallet / ConsenSys // MetaMask.io. – URL: https://metamask.io/ (дата звернення: 19.04.2025).

24. Trust Wallet: Official Website / Trust Wallet // Trustwallet.com. – URL: https://trustwallet.com/ (дата звернення: 19.04.2025).

25. Binance: Cryptocurrency Exchange / Binance // Binance.com. – URL: https://www.binance.com/ (дата звернення: 19.04.2025).

26. Two-Factor Authentication in Cryptocurrency Platforms / R. Anderson // IEEE Transactions on Dependable and Secure Computing. – 2020. – Vol. 17, Iss. 5. – P. 987–996. – DOI: 10.1109/TDSC.2019.2907772.

27. Hardware Wallets: Security Analysis / T. Ruffing, R. Wattenhofer // Financial Cryptography and Data Security. – 2017. – P. 123–139. – DOI: 10.1007/978-3-319-70278-0_8.

28. Фішинг-атаки на користувачів криптовалютних платформ / О. М. Кравець // Інформаційна безпека. – 2022. – № 3. – С. 34–42. – URL: http://infosec.org.ua/journal/2022/3/34-42.

29. Регулювання криптовалют в Україні: сучасний стан і перспективи / М. О. Литвин // Юридичний вісник. – 2021. – № 4. – С. 78–85. – URL: http://yurvisnyk.in.ua/2021/4/78-85.

30. Blockchain and Cryptocurrency: Legal and Regulatory Challenges / J. Bacchus // Journal of International Economic Law. – 2019. – Vol. 22, Iss. 4. – P. 607–623. – DOI: 10.1093/jiel/jgz031.

31. Криптовалютні біржі: аналіз безпеки та вразливостей / В. С. Гринишин // Вісник Львівського університету. Серія: Прикладна математика та інформатика. – 2020. – Вип. 31. – С. 56–64. – URL: http://vmiln.wunu.edu.ua/article/view/100003.

32. Аналіз сучасних криптографічних алгоритмів для захисту транзакцій / П. І. Сидоренко // Захист інформації. – 2019. – Т. 21, № 2. – С. 123–130. – DOI: 10.18372/2225-5036.21.1234.

33. Перспективи впровадження блокчейн-технологій в Україні / Л. В. Коваленко // Економічний вісник. – 2021. – № 3. – С. 45–53. – URL: http://ev.nmu.in.ua/2021/3/45-53.

34. CoinMarketCap: Cryptocurrency Prices and Market Capitalization / CoinMarketCap // CoinMarketCap.com. – URL: https://coinmarketcap.com/charts/ (дата звернення: 10.06.2025).