КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1244
УДК 004.056:336.71:519.72

Шиленко Ігор Сергійович
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID:0009-0005-9007-7443
ihor.shylenko@knu.ua

Наконечний Володимир Сергійович
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, м. Київ, Україна
ORCID:0000-0002-0247-5400
volodym.nakonechnyi@knu.ua

ПРОГАЛИНИ МЕТОДІВ МІНІМІЗАЦІЇ КІБЕРБЕЗПЕКОВИХ РИЗИКІВ ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ФІНАНСОВИХ СИСТЕМАХ ДЕРЖАВ

Анотація. У статті представлено результати систематичного огляду наукової літератури за період 2020-2026 років у сфері кібербезпеки криптовалютних систем та їх інтеграції у державну фінансову інфраструктуру. Дослідження виконано згідно з методологією PRISMA 2020. Аналіз проведено у трьох тематичних кластерах: архітектури безпеки цифрових валют центральних банків (CBDC); вразливості інтеграційних шлюзів між традиційними платіжними системами (SWIFT, ISO 20022) та блокчейн-мережами; методи машинного навчання для виявлення аномальних транзакцій. Розглянуто роль методів пояснюваного штучного інтелекту (XAI) та графових нейронних мереж для виявлення відмивання коштів. На основі систематизації відібраних публікацій ідентифіковано три взаємопов'язані дослідницькі прогалини у площині інтеграції технологій: відсутність ML-методів виявлення аномалій, адаптованих специфічно до KYC-верифікованого permissioned середовища CBDC, де транзакційні патерни принципово відрізняються від псевдонімних публічних блокчейнів; відсутність формальної моделі загроз для шлюзу між державною CBDC-інфраструктурою та легасі-системами (SWIFT, ISO 20022); відсутність інтегрованих рішень, що поєднують ML-моніторинг аномалій з протокольною підтримкою FATF Travel Rule у єдиній державній платіжній системі. Запропоновано концептуальний підхід до закриття цих прогалин, що передбачає поетапну реалізацію: розробку методології вибору ML-моделі, побудову формальної моделі загроз для шлюзу та створення Docker-based прототипу системи моніторингу. Результати дослідження є науковою основою для подальшого створення прикладного програмно-технічного рішення з кіберзахисту державної фінансової системи України, зокрема в контексті проєкту е-гривні Національного банку України.

Ключові слова: кібербезпека; криптовалюти; CBDC; виявлення аномалій; машинне навчання; FATF Travel Rule; систематичний огляд; фінансова система; е-гривня; пояснюваний штучний інтелект.

ВСТУП

Постановка проблеми. Стрімка цифровізація глобальної фінансової системи, прискорена технологіями розподіленого реєстру (DLT) та зростанням ринку криптовалют до понад 2,5 трлн доларів США у 2024 році, поставила перед державами нові виклики у сфері фінансової безпеки [1]. Понад 130 країн світу перебувають на різних стадіях розробки або впровадження цифрових валют центральних банків (CBDC) – від пілотних проєктів (цифровий євро, e-CNY) до повноцінних операційних систем (eNaira у Нігерії, Sand Dollar на Багамах). У контексті даного дослідження під «інтеграцією криптовалют у державну фінансову систему» розуміється передусім архітектура CBDC (на прикладі е-гривні Національного банку України), яка поєднує криптографічні примітиви та технології розподіленого реєстру з регульованим permissioned-середовищем; питання щодо публічних децентралізованих криптовалют (Bitcoin, Ethereum) розглядаються лише в обсязі, необхідному для аналізу їх вразливостей як джерел загроз для CBDC-інфраструктури.

Інтеграція криптоактивів у традиційну державну фінансову інфраструктуру створює новий клас кіберзагроз. На відміну від традиційних банківських систем, блокчейн-мережі функціонують за принципово іншими архітектурними та криптографічними принципами, що унеможливлює пряме застосування класичних механізмів безпеки. Хоча 3,1 млрд доларів втрат, зафіксованих у 2022-2023 роках на крос-чейн мостах [2], припадають переважно на децентралізовані (DeFi) протоколи, архітектурна природа цих вразливостей – компрометація ключів валідаторів, маніпуляція оракулами, race conditions у міжланцюговій передачі повідомлень – становить пряму загрозу для шлюзів інтеграції permissioned-мереж CBDC з традиційними платіжними системами. Саме ці класи атак, перенесені на інтерфейс CBDC з мережею SWIFT (формати повідомлень MT та MX на основі стандарту ISO 20022), формують найкритичнішу зону ризику для державних фінансових систем. Водночас обсяг незаконних транзакцій у криптосфері склав 22,2 млрд доларів у 2023 році, що, попри тенденцію до зниження порівняно з 31,5 млрд у 2022-му, свідчить про значне відставання технічних засобів захисту від нормативно-регуляторних вимог [1].

Для України, де Національний банк розробляє концепцію е-гривні, а криптовалютний ринок законодавчо легалізований з 2022 року, питання кібербезпеки цифрових активів набуває стратегічного значення. Ситуацію посилює функціонування критичної фінансової інфраструктури в умовах збройного конфлікту: цілеспрямовані атаки на банківський сектор у 2022-2026 рр. демонструють недостатність традиційних підходів до захисту. Впровадження е-гривні в такому середовищі вимагає превентивного вирішення технічних проблем безпеки, які складають предмет даного дослідження.

Аналіз останніх досліджень і публікацій. Незважаючи на зростаючу кількість публікацій у суміжних галузях, відсутній систематичний аналіз технічних кіберризиків, специфічних для інтеграції криптоактивів у державну фінансову систему. Більшість наявних досліджень зосереджена або на загальних аспектах безпеки блокчейну, або на регуляторних питаннях, залишаючи поза увагою конкретні технічні прогалини на стику традиційних платіжних систем і блокчейн-інфраструктури. Дослідження вразливостей крос-чейн мостів [2] обмежуються блокчейн-блокчейн інтерфейсами без розгляду шлюзів до легасі-систем; огляди безпеки CBDC, своєю чергою, зосереджені на архітектурних рішеннях окремих національних проєктів, але не охоплюють інтеграційного боку. Окремі прориви у машинному навчанні для виявлення аномалій та графових нейронних мережах для AML продемонстрували високу точність на публічних псевдонімних блокчейнах, проте їх адаптація до KYC-верифікованого permissioned-середовища CBDC залишається невирішеним питанням. Регуляторний контекст FATF Travel Rule та існуючі прототипи compliance-систем (CODE на Corda) також не інтегровані з ML-моніторингом аномалій у єдиній архітектурі. Детальний аналіз відповідних робіт за тематичними кластерами (архітектури CBDC, ML-методи, регуляторні рішення) представлено у розділі результатів дослідження.

Мета статті. Провести систематичний огляд наукової літератури 2020–2025 років щодо методів мінімізації кібербезпекових ризиків використання криптовалют у державній фінансовій системі та ідентифікувати актуальні дослідницькі прогалини для подальшого наукового пошуку. Завдання дослідження: (1) систематизувати наукові публікації за темою згідно з методологією PRISMA 2020; (2) проаналізувати наявні підходи у трьох тематичних кластерах – архітектури CBDC, ML-методи виявлення аномалій, регуляторно-протокольні рішення; (3) ідентифікувати дослідницькі прогалини; (4) сформулювати напрями подальшої наукової роботи з прив'язкою до контексту проєкту е-гривні.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для забезпечення відтворюваності та наукової строгості огляду застосовано методологію PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [3]. Пошук наукових публікацій здійснювався у базах даних Scopus, Web of Science, IEEE Xplore, ACM Digital Library та Consensus (Semantic Scholar / ArXiv) за такими ключовими запитами: "CBDC security" AND "cybersecurity"; "cryptocurrency anomaly detection" AND "machine learning"; "blockchain gateway" AND "attack" AND "financial"; "FATF travel rule" AND "cryptocurrency" AND "monitoring"; "cross-chain bridge" AND "vulnerability" AND "state financial".

Часовий діапазон пошуку: 2020-2025 роки. Критерії включення: рецензовані статті та препринти, що містять емпіричні або теоретичні результати щодо технічних аспектів безпеки крипто-фінансових систем; роботи англійською або українською мовами. Критерії виключення: суто регуляторні або економічні дослідження без технічного компоненту; роботи до 2020 року; дублікати; публікації у виданнях, не індексованих у Scopus або Web of Science.

Первинний пошук виявив 847 результатів. Після видалення дублікатів та первинного скринінгу за назвою й анотацією відібрано 112 публікацій. Повнотекстовий аналіз дозволив включити до фінального корпусу 47 статей, які безпосередньо стосуються предмету дослідження (рис. 1).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

За результатами аналізу відібрані публікації розподілено на три тематичні кластери відповідно до ключових аспектів досліджуваної проблеми. Розглянуто також два додаткові міждисциплінарні напрями: пояснюваний штучний інтелект (XAI) та графові нейронні мережі (GNN), що мають критичне значення для контексту державного фінансового моніторингу.

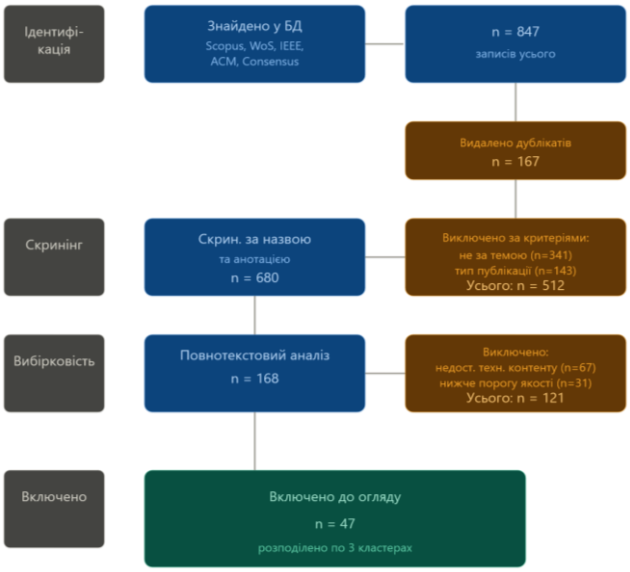

Рис. 1. Діаграма процесу відбору публікацій (PRISMA 2020)

Архітектури безпеки CBDC та їх вразливості. Цифрові валюти центральних банків стали одним із найактивніших напрямів фінансово-технологічних досліджень. Огляд CBDC-ініціатив різних держав виявляє дві принципово різні архітектурні моделі: централізовану (Китай, Ямайка) та гібридну дворівневу (цифровий євро, Швеція). Кожна модель має власний профіль кіберзагроз. Для централізованих архітектур характерна висока ефективність транзакцій та простота управління ключами, однак вони концентрують ризики у єдиній точці відмови. Гібридні моделі розподіляють операційне навантаження між центральним банком та комерційними посередниками, що ускладнює систему аутентифікації та збільшує поверхню атаки.

Критичною проблемою для CBDC є підтримка офлайн-транзакцій - функціонал, прямо передбачений регуляторною пропозицією Єврокомісії щодо цифрового євро. Дослідження PayOff [4] показує, що жоден з існуючих підходів, включно зі схемами e-cash та рішеннями на основі захищених елементів (Secure Elements), не є повністю відповідним регуляторним вимогам: у разі компрометації SE система позбавлена гарантій і стає вразливою до подвійного витрачання (double-spending) та емісії несанкціонованих платіжних одиниць. Крім того, дослідження UTXO-моделі [5] продемонструвало можливість натівної інтеграції FATF Travel Rule на рівні протоколу транзакцій, з часом верифікації 9 мс при розмірі транзакції 665 байт.

Окремою гілкою досліджень є постквантова загроза CBDC-системам. Дослідження [6] пропонує стратегію міграції CBDC-систем на постквантові алгоритми, обґрунтовуючи, що алгоритм Шора (Shor's algorithm) на достатньо потужному квантовому комп'ютері здатен компрометувати ECDSA-підписи, якими захищені гаманці більшості сучасних CBDC-проєктів. У роботі порівнюються NIST-стандартизовані постквантові алгоритми (CRYSTALS-Dilithium, FALCON, SPHINCS+) і пропонує стратегію апгрейду публічної інфраструктури ключів CBDC, проте окремі виклики (зокрема для офлайн-режиму та довгострокової криптографічної гнучкості) залишаються предметом подальших досліджень.

Вразливості крос-чейн мостів та інтеграційних шлюзів. Інтеграція блокчейн-мереж із традиційною фінансовою інфраструктурою реалізується через крос-чейн мости та API-шлюзи. Масштабне дослідження SoK [2], що охопило 212 документів і 58 академічних статей, систематизувало 45 типів вразливостей таких систем та проаналізувало 18 резонансних хакерських інцидентів. Ключовий висновок: 65,8% вкрадених коштів ($2,9 млрд із $3,1 млрд загальних втрат) походять із проєктів, захищених permissioned-мережами посередників із незахищеними криптографічними операціями з

ключами. Атака на Axie Infinity Ronin Bridge ($600 млн) є найбільшим задокументованим інцидентом і стала наслідком компрометації валідаторних ключів [2].

Серед конкретних технічних векторів атак виділяються: підміна oracle-даних (маніпуляція ціновими сигналами), повторні атаки (replay attacks) через некоректну обробку nonce, уразливості смарт-контрактів-мостів (reentrancy, integer overflow) та компрометація вузлів-валідаторів. Окремий клас становлять атаки соціальної інженерії на адміністраторів valid-set, що були використані як вектор у більшості великих інцидентів 2022-2023 рр.

Існуючі дослідження, однак, зосереджені переважно на атаках між блокчейн-мережами або на захисті традиційних міжбанківських систем окремо. Зокрема, дослідження інтероперабельності CBDC з традиційними платіжними системами (SWIFT, ISO 20022) перебувають переважно у регуляторно-юридичній площині [7] та не охоплюють специфіки інтеграції з блокчейн-інфраструктурою. Вразливості шлюзів між CBDC-системою та легасі-інфраструктурою (SWIFT MT/MX, ISO 20022) залишаються практично не дослідженими. У відкритих джерелах відсутня формальна модель загроз для такого шлюзу, яка б враховувала специфіку державного RTGS (Real-Time Gross Settlement) та регуляторні вимоги до транзакційної остаточності.

ML-методи виявлення аномальних транзакцій у криптомережах. Виявлення шахрайства та відмивання коштів у криптовалютних мережах за допомогою методів машинного навчання є найбільш розвиненим напрямом серед публікацій, відібраних для аналізу. Таблиця 1 узагальнює характеристики ключових підходів.

Проведений аналіз виявив декілька системних тенденцій. По-перше, більшість досліджень оперує відкритими датасетами Bitcoin (Elliptic Dataset) або Ethereum, що не відображають специфіку транзакційних патернів CBDC-систем із регульованим доступом та ідентифікацією учасників. По-друге, ансамблеві методи демонструють найвищу точність, але вимагають якісно анотованих навчальних даних (з експертно проставленими мітками легітимності транзакцій), що проблематично для новостворюваних CBDC-систем із відсутньою базою інцидентів. По-третє, жодне з розглянутих досліджень не адаптовано до вимог пояснюваності (XAI), обов'язкової для державних систем фінансового моніторингу.

Таблиця 1

Порівняльний аналіз ML-методів виявлення аномалій у крипто-транзакціях (2023-2025)

Метод/Модель	Датасет	Accuracy,%	F1-score, %	Обмеження
Ensemble Stacking (DT+NB+KNN+RF) [8]	Bitcoin (ADASYN-TL)	97	97	Потребує анотованих даних (з готовими мітками класів)
XGBoost + SHAP (Hard Voting) [9]	Ethereum	99	99	Чутливий до дисбалансу класів
DBSCAN (unsupervised) [10]	6 криптовалют	79,7 (precision)	–	Висока залежність від ε (epsilon) – параметра радіусу пошуку сусідніх точок
Isolation Forest + k-means	Bitcoin Network	92,9	–	Великий FPR на реальних даних
DP-GCAE (Graph Neural Network) [11]	Ethereum (phishing)	+37,7% F1 vs baseline	–	Висока обчислювальна складність
SVM + Relief feature selection	Bitcoin (QICAR 2024)	91,1	–	Не тестувався на CBDC-даних

Джерело: складено автором за результатами огляду [8-11].

Графові нейронні мережі та пояснюваний ШІ як перспективні напрями. Окремий клас методів - графові нейронні мережі (GNN) – демонструють найвищу ефективність у виявленні організованих схем відмивання коштів завдяки здатності враховувати топологічні характеристики транзакційного графу. Аналіз досліджень на датасеті Elliptic свідчить про послідовне покращення F1-score завдяки таким архітектурам. Подальші дослідження розвивають цей напрям шляхом інтеграції темпоральних компонентів та розділеного навчання представлень для покращення стійкості до евазивних патернів.

Паралельно зростає роль методів пояснюваного штучного інтелекту (Explainable AI, XAI) у фінансовому моніторингу. Це зумовлено регуляторними вимогами Закону про штучний інтелект ЄС (AI

Act), що класифікує системи фінансового моніторингу як "високоризикові" та вимагає прозорості рішень. У літературі XAI-у-фінансах сфера AML-моніторингу залишається менш дослідженою порівняно з суміжними напрямами, такими як кредитний скоринг. Серед методів пояснення домінують SHAP (від англ. SHapley Additive exPlanations – пояснення на основі значень Шеплі з кооперативної теорії ігор), LIME (Local Interpretable Model-agnostic Explanations – локальні модельно-незалежні інтерпретовані пояснення) та візуалізації важливості ознак. Гібридні моделі XAI + Federated Learning [12] забезпечують одночасно прозорість та конфіденційність – патерн, безпосередньо застосовний до CBDC-моніторингу. Однак жодне з досліджених рішень не поєднує XAI з контекстом криптовалютного або CBDC-моніторингу.

Регуляторний контекст: реалізація FATF Travel Rule. Окрему категорію проблем становить технічна реалізація вимог FATF Рекомендації 16 (Travel Rule), що зобов'язує постачальників послуг віртуальних активів (VASP) передавати ідентифікаційні дані відправника та одержувача при транзакціях понад встановлений поріг (зазвичай 1000 USD/EUR) [13]. Аналіз 205 юрисдикцій станом на 2025 рік свідчить, що відповідне законодавство прийняли лише 85 країн, а застосовують на практиці – лише 35.

Технічні рішення для автоматичного виконання Travel Rule у режимі реального часу залишаються незрілими: існуючі протоколи (OpenVASP, TravelRule Protocol, TRISA) не є взаємосумісними між собою, що породжує "проблему світанку" (sunrise problem) [13] та регуляторний арбітраж. Академічні прототипи compliance-систем зосереджені на обміні ідентифікаційними даними між VASP, але не інтегруються з ML-моніторингом підозрілих транзакцій. Для нових CBDC-систем існує унікальна архітектурна можливість вбудувати AML/CFT-compliance (відповідність вимогам протидії відмиванню коштів та фінансуванню тероризму) безпосередньо на рівні протоколу транзакцій, проте конкретних технічних реалізацій з прив'язкою до CBDC-специфіки у відкритих наукових джерелах не запропоновано.

Дослідницькі прогалини: ідентифікація та характеристика. На основі проведеного аналізу ідентифіковано три взаємопов'язані дослідницькі прогалини (research gaps), що формують напрями подальшої наукової роботи (табл. 2). Кожна з прогалин має комплексний характер та потребує окремого методологічного підходу для свого закриття. Структура наведеної нижче таблиці систематизує для кожної прогалини декілька ключових аспектів: опис існуючих часткових рішень з проаналізованої літератури, конкретизацію того, що залишається невирішеним у науковому полі, а також оцінку потенційних наслідків невчасного закриття цих прогалин для подальшого розвитку CBDC-систем та їх впровадження у державні фінансові інфраструктури. Такий формат подання дозволяє зіставити три прогалини між собою за єдиним критерієм та окреслити пріоритетність їх вирішення в межах подальшої дослідницької програми.

Таблиця 2

Ідентифіковані дослідницькі прогалини та їх характеристика

№	Прогалина	Наявні часткові рішення	Що відсутнє	Наслідки
G 1	Окремі ML-фреймворки CBDC-моніторингу існують [14], проте не охоплюють інтегрованої методології з пояснюваністю (SHAP/LIME) та real-time обробкою <500 мс	Ансамблі та GNN на Elliptic [8-11]; XAI у банкінгу [12]; CBDC-фреймворки [14]	Методологія вибору моделі для CBDC з критеріями XAI та real-time обробки	Неефективний моніторинг у держ. системі
G 2	STRIDE-моделювання CBDC [15] та security framework для SWIFT/ISO 20022 [16] існують роздільно; інтегрована модель загроз для шлюзу між цими системами та верифікований стенд атак – відсутні	SoK cross-chain [2]; STRIDE для CBDC [15]; SWIFT/ISO 20022 framework [16]; CBDC interop [7]	Attack surface taxonomy + верифікований стенд атак на шлюзовий рівень	Критичні вразливості держ. систем
G 3	Існують концепції інтеграції Travel Rule з ML-технологіями (STRISA [17]), однак відкритого, відтворюваного прототипу для KYC-bound CBDC-середовища у науковій літературі немає	STRISA [17]; UTXO-модель [5]; compliance-протоколи (TRISA, OpenVASP)	Програмно-технічний прототип з інтеграцією у CBDC-ноду	Неможливість виконання AML-вимог

Джерело: складено автором.

Прогалина G1: ML-методи без адаптації до CBDC-контексту. Існуючі методи виявлення аномалій у крипто-транзакціях демонструють високу точність на тестових датасетах (97-99% F1-score для ансамблевих методів), а окремі фреймворки моніторингу CBDC уже з'являються в літературі [14]. Однак ці підходи мають низку обмежень для повноцінного застосування в державних CBDC-системах. По-перше, всі існуючі моделі навчаються на публічних, псевдонімних блокчейн-мережах, де учасники транзакцій не ідентифіковані – тоді як у CBDC-системах кожен гаманець прив'язаний до верифікованої особи (KYC). По-друге, жоден із розглянутих підходів не задовольняє вимогам пояснюваності (XAI), обов'язковим для фінансових регуляторів та Закону про ШІ ЄС. По-третє, відсутня методологія вибору оптимальної ML-моделі залежно від характеристик конкретної CBDC-системи. Закриття прогалини потребує: (а) характеристики розподілу транзакцій у KYC-середовищі; (б) інтеграції SHAP/LIME-пояснень з латентністю менше 500 мс; (в) бенчмарку на синтетичних CBDC-датасетах. Зважаючи на закритість реальних транзакційних даних CBDC, емпіричне закриття даної прогалини у майбутньому потребуватиме генерації синтетичних датасетів із застосуванням методів агентного моделювання (Agent-Based Modeling) або генеративних змагальних мереж (GAN), навчених на патернах публічних блокчейнів з накладанням KYC-обмежень.

Прогалина G2: Вразливості шлюзу CBDC – традиційна інфраструктура. Існуючі роботи розглядають окремі складові цієї проблеми: STRIDE-моделювання загроз для блокчейн-CBDC ідентифікувало 39 класів атак [15], a security framework для inter-bank data transfer у мережі SWIFT з ISO 20022 обґрунтовано в [16]. Дослідження інтероперабельності CBDC у роботі [7] аналізує моделі IMF XC, BIS Universal Ledger та SWIFT-сумісну архітектуру з точки зору правового регулювання для України. Однак інтегрованої моделі загроз саме для шлюзу між CBDC-системою та легасі-інфраструктурою (SWIFT MT/MX, Система електронних платежів НБУ), що поєднує attack surface taxonomy обох систем у єдиній DFD-моделі, у відкритих наукових джерелах не запропоновано. Це особливо критично з огляду на те, що саме такий шлюз є вузловою точкою будь-якої національної CBDC-реалізації. Відсутність формальної attack surface taxonomy не дозволяє ані оцінити поточний рівень ризику, ані визначити пріоритети захисту. Закриття прогалини потребує побудови формальної DFD-моделі шлюзу, застосування методології STRIDE/PASTA для перерахунку загроз та створення контейнеризованого тестового середовища для емпіричної валідації векторів атак.

Прогалина G3: Технічна реалізація FATF Travel Rule. Попри законодавчі зобов'язання більшості країн щодо впровадження FATF Рекомендації 16, технічні рішення для автоматичного виконання Travel Rule у реальному часі залишаються незрілими. Ситуацію ускладнює sunrise problem – відсутність взаємної сумісності між різними постачальниками технічних рішень. Окремі академічні архітектури вже інтегрують Travel Rule з ML-технологіями: STRISA [17] поєднує TRISA-сумісний обмін даними VASP зі смарт-контрактною enforcement-моделлю та автоматизованими ML-механізмами. Однак ця та подібні системи реалізовані як закриті прототипи, що ускладнює їх відтворення та валідацію у незалежних дослідженнях. Для нових CBDC-систем, що лише проєктуються, відкритого, відтворюваного референс-прототипу з прив'язкою до KYC-bound permissioned-архітектури у науковій літературі не запропоновано. Закриття прогалини передбачає створення референс-прототипу: симульована CBDC-нода (Hyperledger Fabric або Ganache) + Python ML-сервіс + модуль перевірки FATF + Grafana-дашборд, повністю контейнеризовані через Docker Compose. Найновіші роботи 2026 року [18] вказують на проблему екстремального дефіциту анотованих даних у крипто-мережах та пропонують ML-підходи з retrieval-grounded контекстом і path-level поясненнями, що особливо релевантно для KYC-bound CBDC-середовища, де анотовані приклади доступні лише обмежено.

Обговорення результатів та позиціонування у літературі. Проведений аналіз виявляє характерні протиріччя: наукова спільнота активно досліджує або загальні аспекти безпеки публічних блокчейнів, або регуляторні питання, залишаючи практично недослідженою технічну специфіку інтеграції криптоактивів у регульовану державну фінансову систему. Особливо показово, що всі три ідентифіковані прогалини виникають у одній і тій самій точці архітектурного рішення – на стику двох різнорідних систем: сучасної блокчейн-інфраструктури та легасі фінансових систем держави. Саме тут концентрується найбільший технічний ризик, і саме тут наукова увага є найменшою.

Ще одним важливим спостереженням є системна упередженість дослідницьких датасетів. Домінування датасету Elliptic (Bitcoin) у дослідженнях ML/GNN створює ризик переоптимізації моделей під специфічний розподіл публічних псевдонімних транзакцій. Для забезпечення наукової валідності результатів у CBDC-контексті критично важливим є створення нових датасетів або адаптація існуючих через техніки domain adaptation.

Окремий вимір проблеми становить інтероперабельність CBDC у міжнародному контексті. Концептуальною основою для побудови захищених національних CBDC-систем виступають загальні принципи механізмів довіри та консенсусу, що забезпечують захист конфіденційних даних у

розподілених системах [19]; ці принципи зберігають свою релевантність і для permissioned-середовищ центральних банків.

У роботі [7] на прикладі України порівняно три моделі трансграничних розрахунків – IMF XC, BIS Universal Ledger та SWIFT-сумісну архітектуру – та обґрунтовано перспективність моделі IMF XC для національної фінансової системи. Цей юридичний аналіз доповнює технічну сторону питання, але не закриває потребу у формальній моделі загроз для безпосереднього інтерфейсу е-гривні з SWIFT/ISO 20022 – що залишається відкритою науковою проблемою. Слід зазначити, що ситуація в Україні є специфічною: воєнний стан підвищує критичність фінансової кіберстійкості. Досвід кібератак на фінансову інфраструктуру (атаки на банки 2022-2026 рр.) демонструє, що традиційні підходи до захисту є недостатніми. Впровадження е-гривні в такому середовищі вимагає превентивного вирішення технічних проблем безпеки, описаних у даній роботі. Це підкреслює практичну значущість запропонованого підходу для національного фінансового сектору в умовах активної цифровізації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За результатами систематичного огляду наукової літератури (47 відібраних публікацій 2020-2026 рр.) отримано такі основні результати:

1. Систематизовано наявні підходи до забезпечення безпеки CBDC-систем та виявлено ключову проблему – відсутність стандартизованих архітектурних рішень для захисту офлайн-транзакцій та постквантової стійкості.

2. Встановлено, що ML-методи виявлення аномалій у крипто-транзакціях, незважаючи на високу точність на публічних блокчейнах (97-99% F1), не є адаптованими для застосування в контексті державного CBDC-моніторингу – через відсутність прив'язки до регуляторних вимог (FATF, AML/KYC) та пояснюваності рішень.

3. Графові нейронні мережі (GNN) демонструють найвищу ефективність у виявленні організованих схем (F1 до 98%), однак їх адаптація до CBDC-контексту з пояснюваністю та real-time обмеженнями залишається відкритою проблемою.

4. Ідентифіковано три критичні дослідницькі прогалини (G1-G3), що визначають напрями подальшої наукової роботи та становлять основу для трьох наступних публікацій у рамках дисертаційного дослідження.

5. Обґрунтовано актуальність розробки програмно-технічного прототипу системи моніторингу крипто-транзакцій, адаптованої до умов функціонування державної фінансової системи України.

Перспективи подальших досліджень: (1) розробка порівняльної методології вибору ML-моделі для CBDC-моніторингу з оцінкою за критеріями точності, XAI-пояснюваності та обчислювальної ефективності (закриття прогалини G1); (2) побудова та тестування формальної моделі загроз для шлюзу CBDC – SWIFT/ISO 20022 (закриття прогалини G2); (3) розробка Docker-based стенду для прототипу системи моніторингу крипто-транзакцій з інтеграцією у симульовану CBDC-ноду та модулем FATF Travel Rule (закриття прогалини G3). Кожен із цих напрямів становитиме предмет окремої наукової публікації у рамках трирічного дисертаційного дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chainalysis. (2024). *The 2024 crypto crime report*. Chainalysis Inc. https://go.chainalysis.com/crypto-crime-report.html
2. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024). SoK: Security and privacy of blockchain interoperability. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 3840-3865). IEEE. https://doi.org/10.1109/SP54263.2024.00255
3. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology, 134,* 178-189. https://doi.org/10.1016/j.jclinepi.2021.03.001
4. Beer, C., Zingg, S., Kostiainen, K., Wüst, K., Capkun, V., & Capkun, S. (2024). *PayOff: A regulated central bank digital currency with private offline payments* (arXiv:2408.06956). arXiv. https://doi.org/10.48550/arXiv.2408.06956
5. Islam, M. M., et al. (2022). A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs. *IEEE Transactions on Services Computing, 16*(4), 2372-2386. https://doi.org/10.1109/TSC.2022.3226120
6. Hupel, L., & Rafiee, M. (2023). *How does post-quantum cryptography affect central bank digital currency?* (arXiv:2308.15787). arXiv. https://doi.org/10.48550/arXiv.2308.15787

7. Kamyshanskyi, V. (2025). Interoperability of CBDC: Optimizing cross-border settlements through the prism of national and international regulation. *Scientific Herald of the National Academy of Internal Affairs, 30*(1), 34-44. https://doi.org/10.63341/naia-herald/1.2025.34
8. Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., & Jamil, M. (2023). A new framework for fraud detection in Bitcoin transactions through ensemble stacking model in smart cities. *IEEE Access, 11*, 90916-90938. https://doi.org/10.1109/ACCESS.2023.3308298
9. Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable AI approach. *Engineering, Technology & Applied Science Research, 14*(1), 12822-12830. https://doi.org/10.48084/ETASR.6641
10. Latif, M. N., Kaplan, M., & Khan, A. I. (2025). Unsupervised machine learning based anomaly detection in high frequency data: Evidence from cryptocurrency market. *Pakistan Journal of Commerce and Social Sciences, 19*(1). https://doi.org/10.64534/commer.2025.511
11. Kang, J., & Buu, S.-J. (2024). Graph anomaly detection with disentangled prototypical autoencoder for phishing scam detection in cryptocurrency transactions. *IEEE Access, 12*. https://doi.org/10.1109/ACCESS.2024.3419152
12. Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *IEEE Access, 12*, 64551-64560. https://doi.org/10.1109/ACCESS.2024.3394528
13. Abdullaeva, S. (2025). FATF standards and the implementation of the Travel Rule in preventing crypto-related money laundering. *Yangi Davr Ilm-Fani: Inson Uchun Innovatsion G'oya va Yechimlar*. https://doi.org/10.47390/ydif-y2025v1i10/n04
14. Malkoochi, R. (2025). Multilayered CBDC fraud detection framework: Securing digital currency ecosystems. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/WJARR.2025.26.2.1841
15. Hans, J., et al. (2023). Blockchain CBDC security threats using STRIDE. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE. https://doi.org/10.1109/BCCA58897.2023.10338905
16. Olajide, O., et al. (2024). Developing a robust security framework for inter-bank data transfer systems in the financial service sector. *International Journal of Scholarly Research in Science and Technology, 5*(1). https://doi.org/10.56781/IJSRST.2024.5.1.0029
17. Tsai, W., et al. (2020). STRISA: A new regulation architecture to enforce Travel Rule. In *Proceedings of the IEEE International Conference on Blockchain*. https://doi.org/10.1007/978-3-030-72725-3_4
18. Na, G., Park, M., Kim, S., Shin, J., & Chai, S. (2026). *Knowledge-integrated representation learning for crypto anomaly detection under extreme label scarcity* (arXiv:2601.12839). arXiv. https://doi.org/10.48550/arXiv.2601.12839
19. Lutsenko, V. V., & Nakonechnyi, V. S. (2025). Decentralized trust and consensus mechanisms for protecting confidential data in distributed systems. *Security of Information Systems and Technologies, 2*(10), 54-60. https://doi.org/10.17721/ISTS.2025.10.54-60

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Ihor Shylenko
PhD candidate, Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0009-0005-9007-7443
ihor.shylenko@knu.ua

Volodymyr Nakonechnyi
Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0000-0002-0247-5400
volodym.nakonechnyi@knu.ua

GAPS IN METHODS FOR MINIMISING CYBERSECURITY RISKS ASSOCIATED WITH THE USE OF CRYPTOCURRENCIES IN NATIONAL FINANCIAL SYSTEMS

Abstract. This paper presents the results of a systematic literature review covering peer-reviewed publications from 2020 to 2026 on cybersecurity of cryptocurrency systems and their integration into state financial infrastructure, conducted in accordance with the PRISMA 2020 methodology. The analysis is organized around three thematic clusters: security architectures of Central Bank Digital Currencies (CBDC); vulnerabilities of integration gateways between traditional payment systems (SWIFT, ISO 20022) and blockchain networks; and machine learning methods for anomaly detection in cryptocurrency transactions. Additionally, the role of explainable AI (XAI) techniques and graph neural networks for anti-money laundering detection is examined. Based on the systematic synthesis of selected publications, three interrelated research gaps are identified at the intersection of technology domains: the absence of ML anomaly detection methods adapted specifically to the KYC-verified permissioned CBDC environment, where transaction patterns differ fundamentally from pseudonymous public blockchains; the absence of a formal threat model for the integration gateway between state CBDC infrastructure and legacy systems (SWIFT, ISO 20022); and the lack of integrated solutions combining ML-based anomaly monitoring with protocol-level FATF Travel Rule support within a single state payment system. A conceptual approach to addressing these gaps is proposed, comprising a staged implementation strategy: development of an ML model selection methodology, construction of a formal threat model for the gateway, and creation of a Docker-based prototype monitoring system. The research findings establish a scientific foundation for the subsequent development of an applied software and technical solution for cybersecurity protection of the Ukrainian state financial system, particularly in the context of the National Bank of Ukraine e-hryvnia project.

Keywords: cybersecurity; cryptocurrency; CBDC; anomaly detection; machine learning; FATF Travel Rule; systematic review; financial system; e-hryvnia; explainable artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Chainalysis. (2024). *The 2024 crypto crime report*. Chainalysis Inc. https://go.chainalysis.com/crypto-crime-report.html
2. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024). SoK: Security and privacy of blockchain interoperability. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 3840-3865). IEEE. https://doi.org/10.1109/SP54263.2024.00255
3. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology, 134*, 178-189. https://doi.org/10.1016/j.jclinepi.2021.03.001
4. Beer, C., Zingg, S., Kostiainen, K., Wüst, K., Capkun, V., & Capkun, S. (2024). *PayOff: A regulated central bank digital currency with private offline payments* (arXiv:2408.06956). arXiv. https://doi.org/10.48550/arXiv.2408.06956
5. Islam, M. M., et al. (2022). A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs. *IEEE Transactions on Services Computing, 16*(4), 2372-2386. https://doi.org/10.1109/TSC.2022.3226120
6. Hupel, L., & Rafiee, M. (2023). *How does post-quantum cryptography affect central bank digital currency?* (arXiv:2308.15787). arXiv. https://doi.org/10.48550/arXiv.2308.15787

7. Kamyshanskyi, V. (2025). Interoperability of CBDC: Optimizing cross-border settlements through the prism of national and international regulation. *Scientific Herald of the National Academy of Internal Affairs, 30*(1), 34-44. https://doi.org/10.63341/naia-herald/1.2025.34
8. Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., & Jamil, M. (2023). A new framework for fraud detection in Bitcoin transactions through ensemble stacking model in smart cities. *IEEE Access, 11*, 90916-90938. https://doi.org/10.1109/ACCESS.2023.3308298
9. Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable AI approach. *Engineering, Technology & Applied Science Research, 14*(1), 12822-12830. https://doi.org/10.48084/ETASR.6641
10. Latif, M. N., Kaplan, M., & Khan, A. I. (2025). Unsupervised machine learning based anomaly detection in high frequency data: Evidence from cryptocurrency market. *Pakistan Journal of Commerce and Social Sciences, 19*(1). https://doi.org/10.64534/commer.2025.511
11. Kang, J., & Buu, S.-J. (2024). Graph anomaly detection with disentangled prototypical autoencoder for phishing scam detection in cryptocurrency transactions. *IEEE Access, 12*. https://doi.org/10.1109/ACCESS.2024.3419152
12. Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *IEEE Access, 12*, 64551-64560. https://doi.org/10.1109/ACCESS.2024.3394528
13. Abdullaeva, S. (2025). FATF standards and the implementation of the Travel Rule in preventing crypto-related money laundering. *Yangi Davr Ilm-Fani: Inson Uchun Innovatsion G'oya va Yechimlar*. https://doi.org/10.47390/ydif-y2025v1i10/n04
14. Malkoochi, R. (2025). Multilayered CBDC fraud detection framework: Securing digital currency ecosystems. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/WJARR.2025.26.2.1841
15. Hans, J., et al. (2023). Blockchain CBDC security threats using STRIDE. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE. https://doi.org/10.1109/BCCA58897.2023.10338905
16. Olajide, O., et al. (2024). Developing a robust security framework for inter-bank data transfer systems in the financial service sector. *International Journal of Scholarly Research in Science and Technology, 5*(1). https://doi.org/10.56781/IJSRST.2024.5.1.0029
17. Tsai, W., et al. (2020). STRISA: A new regulation architecture to enforce Travel Rule. In *Proceedings of the IEEE International Conference on Blockchain*. https://doi.org/10.1007/978-3-030-72725-3_4
18. Na, G., Park, M., Kim, S., Shin, J., & Chai, S. (2026). *Knowledge-integrated representation learning for crypto anomaly detection under extreme label scarcity* (arXiv:2601.12839). arXiv. https://doi.org/10.48550/arXiv.2601.12839
19. Lutsenko, V. V., & Nakonechnyi, V. S. (2025). Decentralized trust and consensus mechanisms for protecting confidential data in distributed systems. *Security of Information Systems and Technologies, 2*(10), 54-60. https://doi.org/10.17721/ISTS.2025.10.54-60

Отримано редакцією журналу / Received: 19.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 24.09.26