УДК 004.056.55:004.738.5
DOI https://doi.org/10.32689/maup.it.2025.2.16

Ігор МАРТИНЮК
аспірант,
Державний торговельно-економічний університет,
i.p.martyniuk @gmail.com
***ORCID:** 0009-0005-2815-1104*

Альона ДЕСЯТКО
доктор філософії в галузі «Комп'ютерні науки», доцент,
завідувач кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет, desyatko@gmail.com
***ORCID:** 0000-0002-2284-3418*

ЗАГРОЗА АТАКИ 51 % ДЛЯ НИЗЬКОХЕШРЕЙТОВИХ ЦИФРОВИХ ВАЛЮТ

Анотація. *Атаки 51 % являють собою серйозну загрозу для безпеки блокчейнів, особливо для цифрових валют (ЦВ) з низьким хешрейтом, що робить їх уразливими до маніпуляцій і втрати довіри з боку користувачів.*

Мета. *Дослідження загроз атаки 51 % у блокчейнах із низьким хешрейтом, зокрема для ЦВ і криптовалютних бірж (КВБ), з метою розробки ефективних стратегій протидії з використанням інтелектуальних інформаційних систем (ІІС) і теорії ігор.*

Методологія. *Проведений у межах статті огляд і аналіз попередніх досліджень показав, що ця загроза потребує комплексного підходу до захисту. У статті обґрунтовано застосування теорії ігор як інструменту аналізу стратегій обох сторін, що може значно поліпшити розуміння динаміки взаємодії між захисниками і зловмисниками, що в перспективі дасть змогу розробити більш ефективні проактивні заходи захисту ЦВ і КВБ, включно з використанням потенціалу ІІС.*

Наукова новизна. *ІІС можуть включати модуль оцінки стратегій сторін протистояння атакам, а також фінансових ресурсів сторін протистояння, що допоможе прогнозувати можливості реалізації атак 51 % або, навпаки, ефективно протидіяти їм. Показано, що жоден із методів захисту не є універсальним, тому комбінування різних підходів є критично необхідним для створення стійких рішень, здатних ефективно реагувати на нові загрози, як для ЦВ, так і для КВБ.*

Висновки. *Майбутні дослідження мають зосередитися на розробці та тестуванні нових ігрових моделей для обчислювального ядра ІІС, які інтегруватимуть наявні підходи та враховуватимуть еволюцію методів атак і захисту в криптовалютних системах, що дасть змогу не лише підвищити рівень безпеки, а й забезпечити довіру користувачів до цифрових валют, що, в свою чергу, є важливим для їхнього успішного впровадження та використання у фінансових системах.*

Ключові слова: *цифрові валюти, криптовалютні біржі, атака 51 %, низький хешрейт, теорії ігор, стратегія сторін.*

Ihor MARTYNIUK, Alona DESIATKO. THREAT OF 51 % ATTACK FOR LOW-HASHRATE CRYPTOCURRENCIES

Abstract. *51 % attacks pose a serious threat to the security of blockchains, especially for digital currencies (DCs) with a low hash rate, which makes them vulnerable to manipulation and loss of trust by users.*

Purpose. *Research into the threats of 51 % attacks in blockchains with low hashrate, in particular for CCs and cryptocurrency exchanges (CCEs), with the aim of developing effective countermeasure strategies using intelligent information systems (IIS) and game theory.*

Methodology. *The review and analysis of previous research conducted within the article showed that this threat requires a comprehensive approach to protection. The article substantiates the use of game theory as a tool for analyzing the strategies of both parties, which can significantly improve the understanding of the dynamics of interaction between defenders and attackers, which in the future will allow developing more effective proactive measures to protect DCs and cryptocurrency exchanges (CEs), including using the potential of intelligent information systems (IIS).*

Scientific novelty. *IIS may include a module for assessing the strategies of the parties to resist attacks, as well as the financial resources of the parties to the confrontation, which will help predict the possibility of implementing 51 % attacks or, conversely, effectively counteract them. It is shown that none of the protection methods is universal, therefore, combining different approaches is critically necessary to create sustainable solutions that can effectively respond to new threats, both for DCs and CEs.*

Conclusion. *Future research should focus on the development and testing of new game models for the computational core of the IIS, which will integrate existing approaches and take into account the evolution of attack and protection methods in cryptocurrency systems, which will not only increase the level of security, but also ensure user trust in digital currencies, which, in turn, is important for their successful implementation and use in financial systems.*

Key words: *digital currencies, cryptocurrency exchanges, 51 % attack, low hash rate, game theory, strategy of opposing parties.*

Вступ. Останніми роками на тлі популярності Bitcoin, Binance Coin (BNB), тощо, спостерігається значне зростання інтересу й до інших цифрових валют (ЦВ) та криптовалютних систем, що зумовлено їхнім потенціалом у галузі децентралізованих фінансів. Однак разом із цим зростанням виникає низка загроз, здатних підірвати безпеку та стабільність криптовалютних систем. Однією з актуальних є загроза атаки 51 %, яка є ризиком, пов'язаним із концентрацією обчислювальної потужності в руках одного або декількох учасників мережі, а в умовах низького хешрейту ця загроза набуває особливої значущості, оскільки мінімальні ресурси, необхідні для здійснення подібної атаки, стають доступними для значної кількості зловмисників. Зауважимо, що як було показано в низці досліджень, зокрема, в [1–3], ЦВ з низьким хешрейтом являють собою легшу мішень для атак 51 %. У низці джерел до таких валют можна, наприклад, віднести Chia (XCH), Cardano (ADA), Algorand (ALGO), PancakeSwap (CAKE) [2–4].

Як було показано в [2–4] низький хешрейт може бути небезпечним для ЦВ, оскільки він робить мережу більш вразливою до атак, зокрема атаки 51 %, оскільки зловмисник може отримати контроль над більш ніж 50 % хешрейту і почати маніпулювати блокчейном, наприклад, проводити подвійні витрати. А крім того, низький хешрейт може призвести до збільшення часу підтвердження транзакцій, що ускладнить використання ЦВ для платежів, оскільки користувачі можуть чекати довше, ніж зазвичай, для підтвердження своїх транзакцій, а якщо хешрейт падає, це також може спричинити занепокоєння серед користувачів та інвесторів, і призведе до зниження інтересу до ЦВ і, як наслідок, до падіння її вартості.

Зауважимо, що багато країн розглядають можливість запровадження власних ЦВ, відомих як центральні банки цифрових валют (CBDC) [5; 6]. І ці нові ЦВ можуть зіткнутися з аналогічними загрозами, включно з ризиком атаки 51 %, оскільки на початкових етапах впровадження CBDC можуть мати відносно низький хешрейт, особливо якщо їхні мережі будуть не повністю завантажені або використані обмеженим числом учасників. Багато CBDC розробляються з акцентом на централізоване управління, що може знизити рівень децентралізації і зробити систему більш вразливою для атак, а крім того, CBDC можуть використовувати нові технології, які ще не пройшли достатнього тестування на безпеку, що може породити уразливості перед атаками. Отже, зловмисники можуть побачити в атаках на CBDC можливість отримати економічну вигоду, особливо якщо такі ЦВ будуть пов'язані з великими фінансовими системами.

Таким чином, на підставі вищесказаного, можна констатувати, що актуальність досліджень у цій галузі зумовлена не тільки зростаючими інвестиціями в ЦВ, а й необхідністю розроблення ефективних механізмів захисту від атак, здатних завдати шкоди як користувачам, так і інфраструктурі криптовалютних бірж (КВБ). Сучасні інтелектуальні інформаційні системи (ІІС), засновані на алгоритмах машинного навчання (МН) і аналітики даних, можуть істотно підвищити рівень захисту ЦВ, даючи змогу не тільки виявляти аномалії в поведінці мережі, а й передбачати можливі атаки, зокрема атаку 51 %, що відкриває нові горизонти для гарантування безпеки у сфері блокчейн-технологій.

У цій статті ми проведемо аналіз попередніх досліджень і наукових публікацій щодо загроз, пов'язаних із реалізацією атаки 51 % на ЦВ із низьким хешрейтом, і розглянемо можливості використання сучасних ШІС для розроблення проактивних заходів протидії цим загрозам.

Постановка проблеми. Актуальність дослідження загроз, пов'язаних з атакою 51 % на ЦВ з низьким хешрейтом, зумовлена збільшенням інтересу до ЦВ та їхньою інтеграцією у фінансові системи. Однак деякі ЦВ, володіючи обмеженими ресурсами, стають уразливими для атак, які можуть призвести до значних втрат як для користувачів, так і для інфраструктури. Незважаючи на наявність низки теоретичних досліджень, багато аспектів безпеки ЦВ залишаються недостатньо вивченими, а наявні підходи до захисту ЦВ і КВБ часто не враховують специфічних ризиків, пов'язаних із низьким хешрейтом, що, відповідно, породжує потребу в глибшому аналізі, який дасть змогу виявити вразливості та визначити ефективні заходи протидії. І в зв'язку з цим, розвиток сучасних ІІС може надати нові можливості для аналізу загроз, що посприяє створенню більш стійких і безпечних ЦВ. І важливим кроком на шляху розв'язання зазначеної проблеми є систематизація наявних знань та виявлення напрямів для подальших досліджень у цій галузі.

Мета дослідження. Метою цього аналітичного дослідження є систематизація та критичний аналіз наявних наукових публікацій, присвячених загрозам атаки 51 % на ЦВ з низьким хешрейтом, а також оцінювання потенціалу сучасних ШІС для розроблення проактивних заходів протидії подібним загрозам. Дослідження спрямоване на виявлення ключових вразливостей, що існують у межах цієї проблематики, і визначення напрямів для розв'язання низки конкретних завдань у сфері забезпечення безпеки ЦВ.

Методика дослідження. У роботі застосовано аналітичну методику, що включає огляд і систематизацію наявних наукових публікацій, статей, дисертацій та інших досліджень, присвячених загрозам

атаки 51 % для ЦВ. Основними етапами методики є систематичний пошук актуальних наукових публікацій у спеціалізованих базах даних і наукових журналах, присвячених проблематиці безпеки ЦВ, а також критичний аналіз обраних публікацій з метою виявлення основних тем, підходів і результатів, що стосуються загроз атаки 51 %, а також оцінки застосовуваних методів захисту. Крім того, виконано порівняння різних підходів і рішень, представлених у літературі, для виявлення найефективніших стратегій протидії загрозам реалізації атаки 51 % і виявлено недостатньо вивчені аспекти та напрямки для подальших досліджень, що може сприяти поліпшенню безпеки ЦВ.

Результати дослідження. У світлі вищевикладеного, завдання протидії атакам 51 % на ЦВ з низьким хешрейтом є відносно новим і перебуває на стадії активного дослідження. Останніми роками спостерігається зростання кількості наукових публікацій, присвячених цій проблематиці, що свідчить про зростаючий інтерес до питань безпеки ЦВ і необхідних заходів захисту. Таким чином, подальший аналіз наявних публікацій дасть змогу виявити ключові підходи та напрямки для подальших досліджень у цій галузі.

Так, у [1] розглядається загроза «51 % атаки» на блокчейни, коли одна група майнерів контролює більше половини обчислювальної потужності мережі, при цьому автори проводять дослідження поведінки майнерів, щоб зрозуміти, як такі атаки можуть бути здійснені та які чинники впливають на їхню ймовірність.

У [2] автори розглядають безпеку блокчейнів з фокусом на виявлення атак 51 %. У роботі подано аналіз вразливостей блокчейн-систем і обговорено методи виявлення та запобігання таким атакам. Автори наводять приклади, що ілюструють наслідки атак 51 %, пропонуючи підходи для поліпшення захисту блокчейнів від подібних загроз і акцентуючи увагу на важливості моніторингу та оцінки безпеки блокчейн-мереж.

У [3] розглядається проблема атаки 51 % для мережі Біткойн. Автори надають огляд цієї загрози та описують механізми, які можуть бути використані для її здійснення, а також наслідки, які така атака може мати для мережі та користувачів. Також авторами обговорюються методи захисту та поліпшення безпеки Біткойн-мережі, щоб знизити ризики, пов'язані з цією атакою.

У дисертації [4] досліджується вплив різних атак на ринки ЦВ. Дисертант аналізує, як різні види атак, як-от зломи КВБ і атаки 51 %, впливають на ціни та волатильність ЦВ. У роботі розглядаються також механізми реагування ринків на такі загрози та їхні довгострокові наслідки для інвесторів та екосистеми ЦВ загалом.

У [7] розглядаються особливості атаки 51 %, включно з механізмами її реалізації та потенційними наслідками для блокчейн-систем, при цьому автор аналізує різні аспекти вразливості блокчейнів до цієї атаки, а також пропонує методи для захисту від неї.

У [8] аналізується метод запобігання атаці 51 % на Біткойн з використанням стохастичного аналізу двофазного механізму proof-of-work. Автор аналізує, як цей підхід може поліпшити безпеку мережі, знижуючи ймовірність того, що одна група майнерів зможе контролювати більш ніж половину обчислювальної потужності, а також обговорюються переваги та недоліки запропонованого методу, а також його потенційний вплив на стійкість блокчейна до подібних атак.

У [9] досліджуються сприйняття атак 51 % на ЦВ з алгоритмом proof-of-work у соціальних медіа. Автори застосовують методи обробки природної мови (NLP) для аналізу обговорень і думок користувачів у соціальних мережах, щоб зрозуміти, як ці атаки впливають на суспільне сприйняття і довіру до ЦВ.

У [10] автори сфокусувалися на тому, як атаки, включно з атаками 51 %, впливають на прибутковість ЦВ. Автори аналізують ринкові дані та намагаються зрозуміти, які зміни в цінах відбуваються під час атак, а також виявляють закономірності та фактори, які можуть впливати на реакцію ринку у відповідь на кіберзагрози.

У [11] досліджуються різні аспекти проектування нових блокчейнів. Автори розглядають, як інноваційні підходи можуть бути застосовані для створення більш стійких і ефективних блокчейнів, а також як вони можуть допомогти у вирішенні існуючих проблем, таких як безпека і консенсус.

Робота [12] присвячена оцінці механізмів консенсусу і безпеки блокчейна в розрізі загрози реалізації атаки 51 %. Автори аналізують наявні методи захисту, їхню ефективність і вразливості, пропонуючи рекомендації щодо поліпшення безпеки блокчейнів для запобігання подібних атак.

У [13] обговорюється, що відбувається під час атак 51 % і як вони впливають на мережі блокчейна. Автор пояснює механізми атаки 51 %, її наслідки для користувачів і мережі загалом, а також у висновку сформульовано рекомендації поради щодо мінімізації ризиків, пов'язаних із подібними загрозами.

У [14] представлено інструмент під назвою BlockScope, який призначений для виявлення та дослідження вразливостей, що виникають унаслідок форків блокчейн-проектів. Автори аналізують, як уразливості можуть поширюватися і впливати на безпеку та стабільність форкнутих блокчейнів, пропонуючи методи для їх виявлення та усунення.

Робота [15] аналізує маніпуляції з ЦВ, відомі як «pump and dump». Автори досліджують методи виявлення та аналізу таких маніпуляцій на ринках ЦВ, пропонуючи підходи для захисту інвесторів і підвищення прозорості торгових практик.

У [16] розглядається вплив інтернет-спільноти на ЦВ на прикладі порівняння Dogecoin і Litecoin у Twitter. Автори аналізують, як обговорення і думки користувачів у соціальних мережах можуть впливати на сприйняття і цінність цих ЦВ, досліджуючи динаміку взаємодії інтернет-спільноти з цими проектами.

У [17] представлено ефективний підхід до захисту блокчейнів з алгоритмом proof-of-work від атак 51 % з використанням інформації про минулі блоки. Автори пропонують схему, яка враховує історію майнінгу та обчислювальної потужності, щоб підвищити безпеку мережі та зробити атаки менш імовірними.

Дисертація [18] присвячена розробці гібридної моделі консенсусу, що об'єднує механізми proof-of-work (PoW) і proof-of-stake (PoS) для захисту криптовалютної системи від атак 51 %. Автор досліджує, як така комбінація може підвищити стійкість мережі до атак, покращуючи безпеку і знижуючи ризики для учасників.

У дисертації [19] розглядаються атаки 51 % на блокчейни та пропонується архітектура рішення для забезпечення безпеки Інтернету речей (IoT) з використанням механізму proof-of-work. Автор досліджує, як можна адаптувати блокчейн-технології для захисту IoT-пристроїв від атак, забезпечуючи безпеку та цілісність даних.

Робота [20] присвячена гібридному підходу для мінімізації ризику атак 51 % на ЦВ. Автори пропонують методи та стратегії, які комбінують різні механізми консенсусу та безпеки, щоб підвищити стійкість криптовалютних систем до таких атак, обговорюючи їхню ефективність та застосування.

У [21] автор аналізує проблеми безпеки, з якими стикаються КВБ, а також розглядає фактори, що сприяють кіберзагрозам, наприклад, такі як уразливості в системах безпеки, соціальна інженерія тощо.

У [22] розглядаються різні ризики, з якими стикаються компанії, що працюють у сфері ЦВ, а також обговорюються фінансові, операційні, технологічні та правові ризики, характерні для криптовалютного бізнесу. Також аналізуються причини виникнення цих ризиків, включно з нестабільністю ринку, змінами в законодавстві та кіберзагрозами.

На підставі виконаного огляду попередніх досліджень сторонніх авторів можна стверджувати, що для ефективної протидії атакам 51 % важливо задіяти потенціал сучасних інтелектуальних інформаційних систем (ІІС), оскільки такі ІІС можуть посприяти розробленню проактивних заходів, спрямованих на виявлення та запобігання атакам на ранніх стадіях, аналізуючи великі обсяги даних про мережеву активність і моделюючи поведінку учасників. Використання ШІС дасть змогу не тільки підвищити безпеку криптовалютних мереж, а й створити більш стійкі механізми консенсусу, що в кінцевому підсумку посилить довіру користувачів до блокчейн-технологій.

Крім того, важливо в таких ІІС задіяти модулі оцінки фінансових ресурсів сторін протистояння, адже для проведення такої атаки зловмиснику знадобляться значні фінансові ресурси для реалізації своїх стратегій з контролю над ЦВ. І якщо ми згадали, що для реалізації атаки 51 % сторонам необхідно задіяти фінансові ресурси, то сторони, відповідно, можуть дотримуватися певних стратегій, причому обидві сторони можуть зазнати як фінансових втрат, так і отримати виграш, якщо обрана стратегія для сторони протистояння виявиться правильною.

Наприклад, зловмисники можуть вкласти значні кошти в обладнання для майнінгу та електроенергію, щоб збільшити свою частку хешрейту. Однак, така стратегія пов'язана з ризиком, оскільки високі витрати на обладнання та можливість невдачі в атаці можуть призвести до фінансових втрат.

Також обидві сторони можуть об'єднувати свої ресурси з іншими майнерами для збільшення шансів на успішну атаку. Такий варіант також пов'язаний з ризиками, оскільки можливий розпад альянсу і поділ прибутку, що може призвести до фінансових втрат для всіх учасників.

Слід згадати й те, що зловмисники (атакуюча сторона) може маніпулювати ринковими цінами ЦВ, створюючи дефіцит або розпускаючи чутки. Однак, ця стратегія теж ризикована, оскільки непередбачувана реакція ринку може призвести до значних збитків для зловмисника.

Атака з виведенням активів:

Сторона захисту щонайменше може інвестувати в дослідження вразливостей блокчейну для виявлення шляхів атаки, хоча ця стратегія і пов'язана з витратами, які можуть не окупитися.

Вважаємо, що для продовження дослідження для розгляду стратегій сторін доцільно задіяти потенціал теорії ігор, оскільки в даній постановці задачі можна виокремити двох основних гравців – захисника, який прагне захистити ЦВ від атаки 51 %, і зловмисника, який намагається реалізувати цю атаку.

Використовуючи теорії ігор, можна під час майбутніх досліджень розробити для обчислювального ядра ІІС математичні моделі, що описують стратегії обох сторін, їхні вибори та потенційні результати, а також оцінювати ризики та вигоди для кожної зі стратегій, аналізуючи, які дії призводять до оптимальних результатів для кожного гравця.

Однак, для ефективної протидії атакам 51 % на блокчейни важливо розглянути різні підходи, які можуть допомогти в розробці стратегій захисту. У (табл. 1) представлено порівняння підходу на основі теорії ігор з іншими методами, включаючи їхні переваги та недоліки.

Таблиця 1

Порівняння різних підходів, їхніх переваг і недоліків для розв'язання задачі аналізу протидії атакам 51 % для низькохешрейтових ЦВ

Підхід для розв'язання задачі	Переваги	Недоліки
Теорія ігор.	Дозволяє моделювати взаємодії двох гравців. Аналізує стратегії та їхні результати. Оцінка ризиків і вигод для обох сторін.	Вимагає складних математичних моделей. Обмежена передбачуваність поведінки гравців.
Аналіз вразливостей.	Дозволяє виявляти слабкі місця в системі. Допомагає розробити конкретні заходи захисту.	Може бути недостатньо актуальним. Не враховує поведінку зловмисників.
Прогностичні моделі (наприклад, машинне навчання).	Забезпечує передбачення на основі великих даних. Дозволяє виявляти аномалії в реальному часі.	Залежність від якості вхідних даних. Може не враховувати нові, невідомі загрози.
Фінансовий аналіз і ризик-менеджмент.	Оцінка витрат і потенційних збитків. Допомагає ухвалювати обґрунтовані рішення на основі фінансових даних.	Може ігнорувати технічні аспекти. Не завжди враховує динаміку загроз.

Джерело: складено авторами на підставі даних літературних джерел [1–10]

Виконаний у таблиці 1 аналіз різних підходів до розв'язання задачі протидії атакам 51 % демонструє, що кожен метод має свої унікальні переваги та обмеження, що додатково наголошує на необхідності комплексного підходу, який поєднує в собі елементи теорії ігор та інші стратегії, щоб забезпечити максимальний захист і стійкість ЦВ і КВБ.

Висновки. Проведений огляд і аналіз попередніх досліджень засвідчив, що атаки 51 % становлять серйозну загрозу для безпеки блокчейнів, особливо для ЦВ із низьким хешрейтом. Обґрунтовано, застосування теорії ігор як інструменту аналізу стратегій обох сторін, що допоможе значно поліпшити розуміння динаміки взаємодії між захисниками та зловмисниками, даючи змогу розробити більш проактивні заходи захисту, зокрема й на основі задіяння потенціалу інтелектуальних інформаційних систем (ІІС), що можуть містити модуль оцінювання стратегій сторін протистояння та їхніх фінансових ресурсів для реалізації атаки 51 % або протидії їй.

Показано, що жоден із методів не є універсальним, тому важливо комбінувати їх для створення стійких рішень, здатних ефективно реагувати на нові загрози для ЦВ і КВБ.

Майбутні дослідження мають зосередитися на розробці та тестуванні нових ігрових моделей для обчислювального ядра ШІС, що інтегрують наявні підходи та враховують еволюцію методів атаки та захисту в криптовалютних системах.

Список використаних джерел:

1. Гонак І. М. Ризики функціонування криптовалютного бізнесу. *Науковий вісник Херсонського державного університету. Серія "Економічні науки"*, 2021. (44), 81–86.

2. Гребельний А. Кіберризики на криптовалютних біржах: причини, наслідки та їх мінімізація. *Modern engineering and innovative technologies*, 2024. (34-01), 106–113.

3. Amin M. R. 51% Attacks on Blockchain: Architecture of a Solution for a Proof-of-Work Blockchain to Protect IoT. Bachelor's thesis, International University of Business Agriculture and Technology, Dhaka, Bangladesh. 2020.

4. Aponte-Novoa F. A., Orozco A. L. S., Villanueva-Polanco R., Wightman P. The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE access*, 2021. 9, 140549–140564.

5. Baruwa Z., Bhattacherjee S., Chandnani S. R., Zhu Z. Perceptions of Social Media Perceptions of 51% Attacks on Proof-of-Work Cryptocurrencies: A Natural Language Processing Approach. arXiv preprint arXiv:2310.14307. 2023.

6. Bastiaan M. Preventing the 51%-Attack: A Stochastic Analysis of Two-Phase Proof-of-Work in Bitcoin. Access by link. 2015, January. URL: https://fmt.ewi.utwente.nl/media/175.pdf.

7. Hao Y. Research of the 51% Attack Based on Blockchain. In 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA. IEEE. 2022, May. pp. 278–283.

8. Kim S. K., Yeun C. Y., Damiani E., Al-Hammadi Y. Diverse Perspectives in New Blockchain Design Using Inventive Problem Solving Theory. У IEEE International Conference on Blockchain and Cryptocurrency, Seoul, South Korea. 2019, May.

9. La Morgia M., Mei A., Sassi F., Stefa J. Dogecoin on Wall Street: Analyzing and Detecting Cryptocurrency Pump-and-Dump Manipulations. *ACM Transactions on Internet Technology*, 2023. 23(1), 1–28. DOI: 10.1145/356130

10. Lansiaux E., Tchagaspanian N., Forget J. Social Influence on Cryptocurrency: A Comparative Example on Twitter between Dogecoin and Litecoin. *Frontiers in Blockchain*, 2022. 5, 829865. DOI:10.3389/fbloc.2022.829865

11. Lee S. A. Investigating the impact of cyber security attacks on cryptocurrency markets (doctoral dissertation, Macquarie University). 2022.

12. Nabilou H. Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies. Journal of Banking Regulation, 2020. 21(4), 299–314.

13. Niranjani V., Kamachi P. S., Siddharth S., Venkatchalam V., Vishal H. A hybrid approach to minimise 51% attack in cryptocurrencies. In 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS) *IEEE.* 2022, March. Vol. 1, pp. 2100–2103.

14. Rahman A. Implementation of hybrid PoW–PoS to prevent 51% attack in cryptocurrency system (Ph.D. dissertation, United International University). 2019.

15. Raju R. S., Gurung S., Rai P. Огляд атаки 51% в мережі Bitcoin. Contemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020, 2022. 39–55.

16. Ramos S., Pianese F., Leach T., Oliveras E. The Great Crypto Turbulence: Understanding Cryptocurrency Profitability under Attacks. Blockchain: Research and Applications, 2021. 2(3), 100021.

17. Sayeed S., Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied sciences*, 2019. 9(9), 1788. DOI:10.3390/app9091788

18. Sethaput V., Innet S. Blockchain application for central bank digital currencies (CBDC). *Cluster Computing*, 2023. 26(4), 2183–2197.

19. Taylor C. What Happens in a 51% Attack? CoinMarketCap Academy. URL: https://coinmarketcap.com/academy/article/what-happens-in-51-attacks

20. Yang X., Chen Y., Chen X. An Efficient Scheme against 51% Blockchain Attacks in Proof-of-Work Systems with weighted historical information. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 261-265). IEEE.

21. Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018, September). Analysis of security in blockchain: Case study in 51%-attack detecting. In 2018 5th International conference on dependable systems and their applications (DSA). *IEEE.* 2019, July. pp. 15–24.

22. Yi X., Fang Y., Wu D., Jiang L. BlockScope: detection and analysis of common vulnerabilities in forked blockchain projects. 2022. arXiv preprint arXiv:2208.00205.

Дата надходження статті: 23.06.2025
Дата прийняття статті: 01.07.2025
Опубліковано: 23.09.2025