КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1331
УДК 004.056.5:004.94:336.74

Мартинюк Ігор Петрович
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
місце роботи: Державний торговельно-економічний університет, Київ, Україна
ORCID:0009-0005-2815-1104
i.p.martyniuk@gmail.com

Десятко Альона Миколаївна
PhD, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
місце роботи: Державний торговельно-економічний університет, Київ, Україна
ORCID:0000-0002-2284-3418
desyatko@gmail.com

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РЕСУРСІВ СТОРІН АТАКИ 51% У БЛОКЧЕЙН-СИСТЕМАХ

Анотація. Актуальність досліджень проблематики атак 51% на блокчейн-системи продовжує зростати в умовах швидкого розвитку криптовалютних технологій та зростання їх популярності серед користувачів. Ці атаки, як показав аналіз публікацій за темою дослідження, є однією з найсерйозніших загроз для цілісності блокчейнів, особливо в системах із низьким хешрейтом, де ризик компрометації значно вищий. Проведене дослідження не лише підтверджує серйозність цієї проблеми, а й надає початкову версію програмного інструментарію для аналізу та розроблення ефективних стратегій захисту. У статті увагу акцентовано на використанні сучасних інформаційних систем і технологій (ІСТ) для імітаційного моделювання, що дасть змогу глибше аналізувати механізми таких атак. У межах подальших досліджень передбачається створення більш деталізованого обчислювального модуля на базі теорії ігор, який стане частиною інтелектуальної інформаційної системи, що може бути інтегрована в інфраструктуру криптовалютних бірж (КВБ), забезпечуючи моніторинг і раннє попередження про потенційні атаки 51%. Використання теорії ігор у цьому контексті дає можливість моделювати поведінку різних учасників мережі, допомагаючи розробити надійніші захисні стратегії. Важливо, що застосування імітаційного моделювання надає можливість досліджувати різні сценарії атак і реакцій на них, що є ключем до формування комплексного підходу до захисту блокчейн-систем, оскільки за допомогою ІСТ можна аналізувати великі обсяги даних та аномалії, які можуть передувати атакам, що значно підвищує рівень захищеності КВБ. Реалізація цих напрямів досліджень дасть змогу суттєво розширити розуміння механізмів атак 51% та розробити ефективніші способи захисту блокчейн-систем, що відкриває низку перспективних напрямів для подальшого вивчення проблематики атак 51%, зокрема вдосконалення алгоритмів консенсусу, розроблення адаптивних систем захисту та впровадження нових технологій, таких як штучний інтелект для автоматичного реагування на загрози, що врешті сприятиме створенню стійкіших і безпечніших криптовалютних екосистем.

Ключові слова: цифрові валюти; криптовалютні біржі; атака 51%; низький хешрейт; теорія ігор; стратегії сторін; імітаційне моделювання.

ВСТУП

Атаки 51% є однією з найзначніших загроз для безпеки блокчейнів, особливо тих, що мають низький хешрейт [1-6]. Ці атаки, коли зловмисник або група зловмисників контролюють понад половину обчислювальних потужностей мережі, можуть призвести до фальсифікації транзакцій і втрати довіри до системи. В умовах зростання популярності цифрових валют (ЦВ) [7-16] необхідність розроблення надійних методів захисту від подібних атак стає особливо актуальною. Зростання інтересу до ЦВ та збільшення кількості учасників у цій сфері створюють нові виклики для забезпечення безпеки блокчейн-технологій. Атаки 51% не лише загрожують цілісності транзакцій, а й ставлять під сумнів саму ідею децентралізації, на якій ґрунтуються блокчейн-системи. Тож важливість вивчення цього явища важко переоцінити. Це дослідження спрямоване на вивчення динаміки взаємодії між захисниками та

зловмисниками в процесі атак 51% з метою виявлення можливих стратегій, здатних підвищити стійкість блокчейн-систем. У межах такого підходу особливу увагу приділено імітаційному моделюванню, яке дає змогу створити реалістичні сценарії взаємодії сторін і проаналізувати різні стратегії захисту та нападу. Використання імітаційного моделювання в цій галузі відкриває нові горизонти для розуміння механізмів атак і розроблення ефективніших заходів захисту. За допомогою сучасних інформаційних технологій (ІТ) можна проводити глибокий аналіз поведінки учасників мережі, що сприятиме точнішому прогнозуванню атакувальних дій і розробленню адаптивних систем безпеки. Як результат, отримані висновки можуть стати основою для створення стійкіших і захищеніших блокчейн-систем, здатних протистояти загрозам, пов'язаним з атаками 51%.

Постановка проблеми. Незважаючи на широке визнання фахівцями серйозності загроз, пов'язаних з атаками 51%, про що свідчать численні наукові публікації з цієї тематики, недостатньо уваги приділяється детальному аналізу стратегій обох сторін і взаємодії їхніх ресурсів. Складність проблеми полягає в тому, що атаки такого типу потребують значних обчислювальних потужностей і фінансових вкладень сторін, що робить їх реалізацію економічно витратною для зловмисників. Однак за недостатнього захисту з боку учасників мережі можливе виникнення ситуації, у якій зловмисник зможе не лише здійснити атаку, а й ефективно маніпулювати блокчейном, підриваючи довіру користувачів, що власне й зумовило релевантність цього дослідження.

Аналіз останніх досліджень і публікацій. У праці [1] проаналізовано поведінку майнерів у мережах, що зазнали атак 51%, та запропоновано індикатори аномальної концентрації хешрейту. Автори [2] розглядають задачу виявлення атаки 51% як окремий випадок загальної проблеми безпеки блокчейну, а в роботах [3, 4] наведено узагальнений огляд механізмів реалізації таких атак у мережі Bitcoin. Стохастичний аналіз двофазного доказу виконання роботи як засобу запобігання атаці 51% виконано в [5]; у праці [6] методами обробки природної мови досліджено сприйняття таких атак спільнотою користувачів криптовалют, а в [17] – вплив спільноти на курс ЦВ на прикладі порівняння Dogecoin і Litecoin.

Розглянемо окремо дослідження, присвячені інституційному та економічному контексту обігу ЦВ. Так, у [7, 8] розглянуто питання впровадження цифрових валют центральних банків, що засвідчує зростання масштабів застосування блокчейн-технологій, а в [9] проаналізовано динаміку дохідності криптовалют, які зазнали атак, де самі економічні наслідки компрометації мережі. Ці роботи підтверджують, що успішна атака 51% має технічний й фінансовий вплив.

Значна частина публікацій присвячена засобам протидії. У [10] запропоновано підходи до проєктування нових блокчейн-архітектур, у [11] виконано оцінювання механізмів консенсусу та безпеки щодо стійкості до атаки 51%, у [13] і [15] обґрунтовано гібридні схеми PoW-PoS, у [14] – архітектурне рішення для захисту IoT-мереж на основі PoW, а в [16] – схему з урахуванням історично зваженої інформації. Прикладний огляд наслідків атак для користувачів наведено в [12].

Мета статті. Мета дослідження полягає в розробленні кібернетичної імітаційної моделі, що ґрунтується на принципах теорії ігор і реалізована алгоритмічною мовою Python, що дасть змогу оцінювати стратегії взаємодії між захисниками та зловмисниками під час атак 51%. Методи комп'ютерного моделювання, використані у статті, передбачають також аналіз впливу фінансових та обчислювальних ресурсів обох сторін на ймовірність успішної реалізації атаки, а також вивчення можливостей оптимізації ресурсів захисника для підвищення стійкості мережі.

МЕТОДИКА ДОСЛІДЖЕННЯ

У роботі застосовано кібернетичну імітаційну модель, реалізовану алгоритмічною мовою Python, для аналізу стратегій взаємодії між захисниками та зловмисниками під час реалізації атак 51%. Модель враховує як фінансові, так і обчислювальні ресурси сторін, що дає змогу провести аналіз імовірності успішної реалізації атаки.

Імітаційне моделювання надає можливість досліджувати різні сценарії взаємодії, оцінювати стратегії обох сторін і виявляти оптимальні шляхи для захисника в умовах обмежених ресурсів, насамперед фінансових. Модель включає динамічні компоненти, що дають змогу врахувати змінювані умови, такі як коливання хешрейту та фінансових вкладень, що додає елемент реалістичності до процесу симуляції.

Обмеження застосованої методики дослідження. Важливо зазначити, що застосування імітаційного підходу в такій постановці задачі потребує ретельного калібрування параметрів моделі для досягнення адекватних результатів. Необхідність урахування складних взаємодій і непередбачуваності поведінки учасників може обмежити точність отриманих висновків, що підкреслює потребу в подальших дослідженнях і верифікації отриманих даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Основні аспекти моделі прийнято такими, див. рис. 1. На першому етапі визначаємо учасників гри. Це, відповідно, захисник ЦВ, наприклад розробники та користувачі, які прагнуть зберегти безпеку мережі. Друга сторона – це атакувальник, тобто зловмисник, який володіє більш ніж 50% обчислювальних потужностей мережі. Сторони, відповідно, можуть дотримуватися певних стратегій, див. табл. 1.

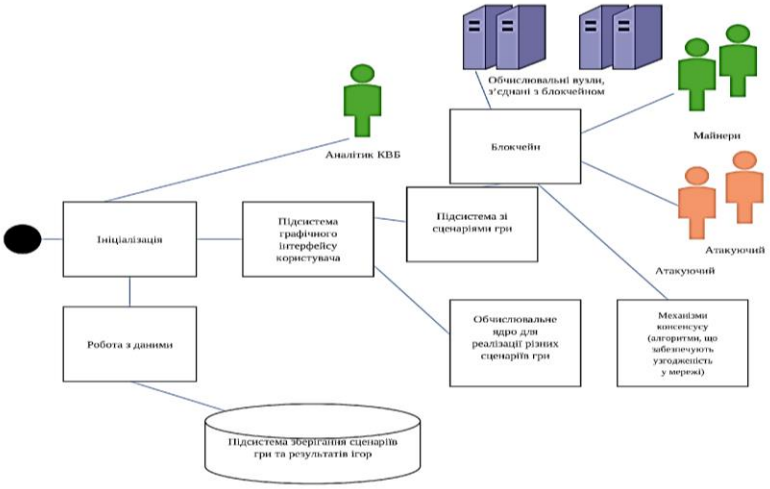

Рис. 1. Загальна архітектура інтелектуальної системи для моделювання сценаріїв атак 51%

Таблиця 1

Стратегії сторін гри

Учасники	Приклади стратегій сторін гри
Захисник	Може обирати між збільшенням хешрейту (наприклад, за рахунок об'єднання потужностей), зміною алгоритму консенсусу або запровадженням нових заходів безпеки. Фінансування заходів для тимчасового відключення мережі в разі загрози атаки 51% з метою запобігання фінансовим збиткам. Вкладення коштів у розподіл майнінгових вузлів для запобігання концентрації обчислювальних потужностей. Створення резервного фонду для покриття фінансових втрат і відновлювальних робіт після атак.
Атакувальник	Може вирішувати, чи варто інвестувати у збільшення хешрейту, чи маніпулювати ланцюгом блоків, щоб підірвати довіру користувачів. Фінансування заохочень або підкупу майнерів для тимчасового переведення їх на бік атакувальника. Використання вразливих КВБ, коли фінансові витрати спрямовуються на організацію атак через КВБ з низьким рівнем захисту для маніпуляцій з курсом ЦВ. Вкладення ресурсів у розроблення стратегій, що використовують уразливості в протоколах або програмному забезпеченні мережі блокчейн.

Зауважимо, що аналіз стратегій сторін в ігровій моделі є винятково важливим, оскільки стратегії захисника й атакувальника під час атак 51% у будь-якому разі потребуватимуть значних фінансових вкладень. А аналіз, подібний до того, результати якого систематизовано в табл. 1, дасть змогу оцінити, наскільки ефективно кожна сторона використовує свої ресурси для досягнення мети, що, наприклад, є критичним в умовах обмежених фінансових ресурсів і, відповідно, допомагає сторонам краще розподіляти бюджети та обирати рентабельніші стратегії. Крім того, інформація про концептуальні стратегії сторін гри та їх вплив на динаміку гри дає змогу прогнозувати можливі результати в розроблюваній імітаційній моделі, оскільки в кібернетичному ігровому моделюванні кожна стратегія змінює хід гри, і детальний аналіз покаже, які стратегії можуть привести до виграшу або програшу сторін.

Ігрова модель пропонує безліч варіантів дій для кожної сторони, отже, детальний аналіз стратегій дасть змогу вже на першому етапі виявити оптимальні рішення, які мінімізують ризики й втрати за максимального досягнення мети – чи то захист від атаки 51%, чи то успішна реалізація такої атаки. Вважаємо, що аналіз стратегій, подібний до наведеного вище в табл. 1, допоможе надалі, під час детального математичного опису гри на основі теорії ігор, зрозуміти, як розподіляються сили між сторонами, оскільки якщо одна сторона має значну перевагу в певних стратегіях, це може призвести до нестійкої рівноваги, що потребує коригування дій іншої сторони. Зауважимо, що в реальних умовах атаки й захист відбуваються динамічно та можуть змінюватися в часі, відповідно, аналіз стратегій у моделі дасть змогу враховувати ці зміни й коригувати дії залежно від поточної ситуації на ринку ЦВ і доступних фінансових ресурсів сторін.

На наступному етапі виконується оцінювання ресурсів учасників гри. Вважаємо, що кожна сторона має обмежені фінансові та обчислювальні ресурси, що слід урахувати в моделі, див. табл. 2. Також можна використовувати випадкові змінні для моделювання непередбачуваності результату гри.

На наступному етапі, який передбачає оцінювання результатів взаємодій, модель зможе передбачати різні результати залежно від стратегій гравців. Наприклад, успішна атака знизить довіру до мережі, і навпаки, якщо атаку успішно «відбито», то це зміцнить довіру до ЦВ.

Таблиця 2

Витрати ресурсів на реалізацію своїх стратегій

Учасники	Витрати ресурсів на реалізацію своїх стратегій
Фінансові ресурси	
Захисник	Витрати на обладнання, зокрема закупівля та підтримка обчислювальної потужності (майнінгові установки, сервери тощо). Витрати на електроенергію, включно з вартістю електроенергії для роботи обладнання. Програмне забезпечення та оновлення, включно з ліцензіями на ПЗ, ПЗ для безпеки та ін. Резервні фонди, зокрема наявність запасів на випадок атаки (наприклад, на розроблення нових рішень або компенсації користувачам).
Атакувальник	Витрати на обчислювальну потужність, тобто на купівлю або оренду обладнання для збільшення хешрейту. Витрати на електроенергію, включно з вартістю електроенергії для роботи обладнання. Витрати на маніпуляції, наприклад можливі додаткові витрати на підкуп, організацію атак або поширення дезінформації про стійкість ЦВ. Ризикові витрати, наприклад витрати, пов’язані з невдалими атаками або втратою довіри до свого капіталу.
Обчислювальні ресурси	
Захисник	Захисник (зазвичай це майнери або пули майнінгу) використовує свої обчислювальні потужності для створення нових блоків і підтвердження транзакцій. Відповідно, хешрейт визначає швидкість, з якою вони можуть обробляти дані та додавати їх до блокчейну. Якщо захисник збільшує свій хешрейт, це ускладнює атаки, оскільки зловмиснику необхідно мати понад 50% від загального хешрейту мережі, щоб успішно реалізувати атаку. Захисник може оптимізувати свою інфраструктуру, наприклад використовуючи ефективніше обладнання або алгоритми, щоб підвищити свою продуктивність без значного збільшення витрат. Також деякі захисники можуть зберігати певний обсяг обчислювальних ресурсів у резерві, готових до швидкої активації в разі загрози. Крім того, захисник може об’єднувати свої ресурси з іншими учасниками мережі (наприклад, через пул майнінгу), щоб створити потужніший захист проти атак.
Атакувальник	Атакувальник прагне накопичити понад 50% хешрейту мережі, щоб отримати можливість маніпулювати блокчейном, скасовувати транзакції або реалізовувати подвійні витрати. Для досягнення цієї мети атакувальник може використовувати власне обладнання, орендувати потужності або організувати консорціум інших учасників для збільшення своїх ресурсів. Також атакувальник може обирати час і місце для атаки, ґрунтуючись на оцінюванні обчислювальних ресурсів захисника. Наприклад, він може зачекати, доки захисник

Учасники	Витрати ресурсів на реалізацію своїх стратегій
	знизить свої потужності, щоб реалізувати атаку. Збільшення хешрейту може потребувати значних фінансових вкладень в обладнання та електроенергію, що робить атаки економічно витратними, відповідно, атакувальник має ретельно планувати свої ресурси. Атакувальник може використовувати різні методи для зниження хешрейту захисника, наприклад шляхом створення економічних перешкод, що робить атаку ефективнішою.

Як середовище для створення імітаційної моделі було обрано VS Code, яке забезпечує високий ступінь гнучкості, зручності та ефективності, що сприяє продуктивнішому розробленню програмного інструментарію для імітаційного моделювання в контексті атак 51% на блокчейн-системи, див. рис. 2. Оскільки VS Code підтримує безліч мов програмування, це інтегроване середовище розроблення може бути легко налаштоване за допомогою розширень, що дасть змогу інтегрувати в проєкт у міру потреби нові бібліотеки та інструменти, необхідні для моделювання й аналізу, включно з бібліотеками для роботи з даними та графікою. Крім того, VS Code має вбудовані інструменти для роботи з Git, що дає змогу зручно керувати версіями коду, відстежувати зміни та спільно працювати над проєктом кільком розробникам.

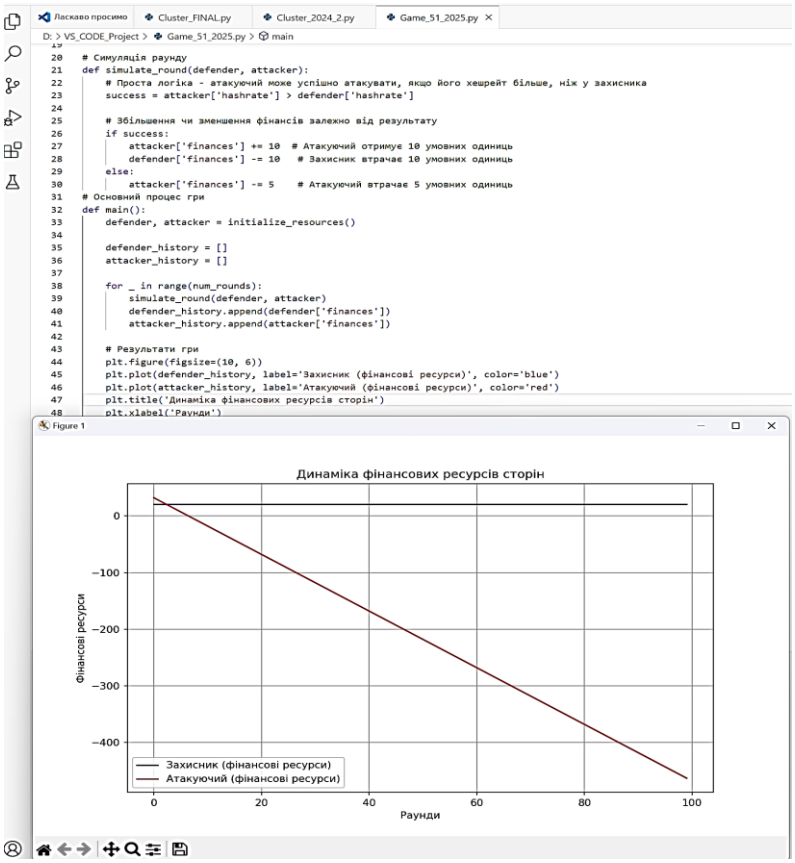

Рис. 2. Приклад реалізації найпростішої гри в заданій постановці (середовище програмування VS Code)

Як видно на рис. 2, кожна сторона гри (захисник і атакувальник) отримує випадкові значення фінансових та обчислювальних ресурсів у діапазоні від 1 до 100. Ці початкові параметри задають вихідні умови для взаємодії сторін і впливають на подальший хід гри. У кожному раунді атакувальник перевіряє, чи може він успішно реалізувати атаку, порівнюючи свій хешрейт із хешрейтом захисника. Якщо хешрейт атакувальника перевищує хешрейт захисника, атака визнається успішною. У разі успішної атаки атакувальник отримує 10 умовних одиниць фінансових ресурсів, що дасть йому змогу нарощувати свої можливості для подальших атак. Водночас захисник втрачає 10 умовних одиниць, що знижує його здатності до захисту. Отже, отриманий графік показує динаміку зміни фінансових ресурсів сторін упродовж 100 раундів. У результаті ми можемо зафіксувати для найпростішої гри таке. Фінансові

ресурси атакувальника можуть збільшуватися за успішних атак, що може призвести до їх домінування в грі. Фінансові ресурси захисника, навпаки, можуть значно коливатися залежно від результатів атак, що ілюструє важливість стійкості та стратегічного планування для захисника. Отже, подібне комп'ютерне моделювання як частина дослідження дає змогу вже на цьому етапі не лише спостерігати за результатами взаємодії сторін, а й проводити аналіз різних сценаріїв, що слугує потужним інструментом для дослідження динаміки ігор, дозволяючи тестувати різні стратегії захисту й атаки. Наприклад, можна варіювати початкові умови (хешрейти та фінансові ресурси) і досліджувати, як ці зміни впливають на ймовірність успіху атак і стабільність мережі, див. рис. 3.

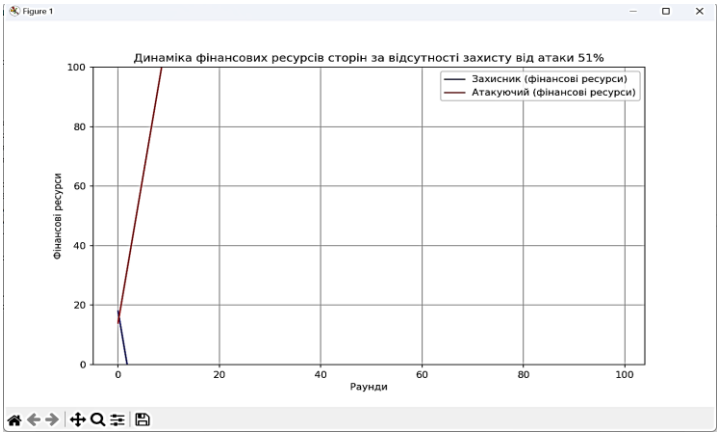

Рис. 3. Результати симуляції для фіксованого хешрейту захисника

На рис. 3 показано ситуацію, коли в захисника встановлено фіксований хешрейт (30), що робить його вразливим до атак 51%, оскільки гіпотетично атакувальник матиме хешрейт від 50 до 100, що завжди дає йому змогу успішно атакувати ЦВ. Тут у кожному раунді атакувальник завжди успішно здійснює атаку, що призводить до постійної втрати фінансових ресурсів захисника та збільшення ресурсів атакувальника. Візуалізацію для розглядуваного сценарію обмежено за віссю Y, щоб краще відобразити динаміку фінансових ресурсів. Отже, за відповідних даних ми за допомогою комп'ютерного моделювання ілюструємо ситуацію, у якій фінансові ресурси захисника стрімко зменшуються за відсутності достатніх ресурсів для захисту від атаки 51%. Атакувальник же нарощуватиме свої фінансові ресурси, що наочно ілюструє наслідки вразливості мережі.

Зауважимо, що за допомогою симуляції можна виявити оптимальні стратегії для захисника, щоб мінімізувати втрати та підвищити ефективність захисту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження не лише підтверджує серйозність загрози атак 51% для блокчейн-систем із низьким хешрейтом, а й надає програмний інструментарій для аналізу та розроблення ефективних стратегій захисту, а також відкриває низку перспективних напрямів для подальшого вивчення проблематики атак 51% на блокчейн-системи. У межах дослідження передбачається створення обчислювального модуля на базі теорії ігор для інтелектуальної інформаційної системи, яка може стати частиною систем криптовалютних бірж для моніторингу та раннього попередження про потенційні атаки 51%. Реалізація цих напрямів досліджень дасть змогу суттєво розширити розуміння механізмів атак 51% і розробити ефективніші способи захисту блокчейн-систем.

Перспективи подальших досліджень. Перспективи подальших досліджень полягають у тому, щоб розширити можливості цієї кібернетичної моделі врахуванням додаткових параметрів і факторів впливу, а також розробити складніші сценарії взаємодії учасників гри. Крім того, видається доцільним проаналізувати на такій кібернетичній моделі ефективність різних стратегій захисту за різних початкових умов та економічну доцільність для атакувальника у проведенні атак 51% з урахуванням витрат і потенційної вигоди.

Окрема подяка Ткачову Віталію Миколайовичу, помічнику ректора з питань інформаційних технологій Харківського національного університету радіоелектроніки, за те, що саме він створив необхідні умови для реалізації цього проєкту. Без його активної позиції на початковому етапі проведення дослідження було б неможливим.

Дослідження виконано в межах науково-дослідної роботи кафедри комп'ютерного моделювання та інтелектуальних технологій Харківського національного університету радіоелектроніки за темою «Аналіз та захист систем від шкідливого програмного забезпечення».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. IEEE Access, *9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291
2. Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018). Analysis of security in blockchain: Case study in 51%-attack detecting. In 2018 5th International Conference on Dependable Systems and Their Applications (DSA) (pp. 15–24). IEEE. https://doi.org/10.1109/DSA.2018.00015
3. Raju, R. S., Gurung, S., & Rai, P. (2022). An overview of 51% attack over Bitcoin network. In Contemporary issues in communication, cloud and big data analytics: Proceedings of CCB 2020 (pp. 39–55). Springer. https://doi.org/10.1007/978-981-16-4244-9_4
4. Hao, Y. (2022). 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)* (pp. 278–283). IEEE. https://doi.org/10.1109/CVIDLICCEA56201.2022.9825149
5. Bastiaan, M. (2015). Preventing the 51%-attack: A stochastic analysis of two phase proof of work in Bitcoin. In Proceedings of the 22nd Twente Student Conference on *IT*. University of Twente.
6. Baruwa, Z., Bhattacherjee, S., Chandnani, S. R., & Zhu, Z. (2023). Social media perceptions of 51% attacks on proof-of-work cryptocurrencies: A natural language processing approach [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2310.14307
7. Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). Cluster Computing, *26*(4), 2183–2197. https://doi.org/10.1007/s10586-023-03962-7
8. Nabilou, H. (2020). Testing the waters of the Rubicon: The European Central Bank and central bank digital currencies. Journal of Banking Regulation, *21*(4), 299–314. https://doi.org/10.1057/s41261-019-00112-1
9. Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. Blockchain: Research and Applications, *2*(3), Article 100021. https://doi.org/10.1016/j.bcra.2021.100021
10. Kim, S. K., Yeun, C. Y., Damiani, E., & Al-Hammadi, Y. (2019). Various perspectives in new blockchain design by using theory of inventive problem solving. In 2019 IEEE International Conference on Blockchain and Cryptocurrency *(ICBC)*. IEEE.
11. Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, *9*(9), Article 1788. https://doi.org/10.3390/app9091788
12. Taylor, K. (n.d.). What happens in 51% attacks? CoinMarketCap Academy. CoinMarketCap Academy
13. Rahman, A. (2019). A hybrid PoW-PoS implementation against 51% attack in cryptocurrency system [Doctoral dissertation, United International University].
14. Amin, M. R. (2020). 51% attacks on blockchain: A solution architecture for blockchain to secure IoT with proof of work [Bachelor's thesis, International University of Business Agriculture and Technology].
15. Niranjani, V., Kamachi, P. S., Siddhaarth, S., Venkatachalam, B., & Vishal, N. (2022). Hybrid approach to minimize 51% attack in cryptocurrencies. In 2022 8th International Conference on Advanced Computing and Communication Systems *(ICACCS)* (Vol. 1, pp. 2100–2103). IEEE. https://doi.org/10.1109/ICACCS54159.2022.9785056
16. Yang, X., Chen, Y., & Chen, X. (2019). Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 261–265). IEEE. https://doi.org/10.1109/Blockchain.2019.00041
17. Lansiaux, E., Tchagaspanian, N., & Forget, J. (2022). Community impact on a cryptocurrency: Twitter comparison example between Dogecoin and Litecoin. Frontiers in Blockchain, *5*, Article 829865. https://doi.org/10.3389/fbloc.2022.829865

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

Ihor Martyniuk
PhD student, Department of Software Engineering and Cybersecurity
Work place: State University of Trade and Economics, Kyiv, Ukraine
ORCID:0009-0005-2815-1104
i.p.martyniuk@gmail.com

Alona Desiatko
PhD, Associate Professor, Department of Software Engineering and Cybersecurity
Work place: State University of Trade and Economics, Kyiv, Ukraine
ORCID:0000-0002-2284-3418
desyatko@gmail.com

SIMULATION MODELLING OF THE RESOURCES OF THE PARTIES TO A 51% ATTACK IN BLOCKCHAIN SYSTEMS

Abstract. The relevance of research into 51% attacks on blockchain systems continues to grow amid the rapid development of cryptocurrency technologies and their increasing popularity among users. As the analysis of publications on the research topic has shown, such attacks constitute one of the most serious threats to blockchain integrity, especially in systems with a low hashrate, where the risk of compromise is considerably higher. The study conducted not only confirms the severity of this problem but also provides an initial version of a software toolkit for analysing and developing effective protection strategies. The article focuses on the use of modern information systems and technologies (IST) for simulation modelling, which will make it possible to analyse the mechanisms of such attacks in greater depth. Further research envisages the creation of a more detailed computational module based on game theory, which will become part of an intelligent information system that can be integrated into the infrastructure of cryptocurrency exchanges (CEX), providing monitoring and early warning of potential 51% attacks. The use of game theory in this context makes it possible to model the behaviour of various network participants, helping to develop more reliable defensive strategies. Importantly, the application of simulation modelling provides an opportunity to investigate different attack scenarios and responses to them, which is key to forming a comprehensive approach to protecting blockchain systems, since IST makes it possible to analyse large volumes of data and anomalies that may precede attacks, thereby significantly increasing the security level of cryptocurrency exchanges. The implementation of these research directions will substantially expand the understanding of the mechanisms of 51% attacks and enable the development of more effective ways of protecting blockchain systems. This opens up a number of promising areas for further study of 51% attacks, including the improvement of consensus algorithms, the development of adaptive protection systems and the introduction of new technologies, such as artificial intelligence for automated response to threats, ultimately contributing to the creation of more resilient and secure cryptocurrency ecosystems.

Keywords: digital currencies; cryptocurrency exchanges; 51% attack; low hashrate; game theory; strategies of the parties; simulation modelling.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. IEEE Access, *9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291
2. Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018). Analysis of security in blockchain: Case study in 51%-attack detecting. In 2018 5th International Conference on Dependable Systems and Their Applications (DSA) (pp. 15–24). IEEE. https://doi.org/10.1109/DSA.2018.00015
3. Raju, R. S., Gurung, S., & Rai, P. (2022). An overview of 51% attack over Bitcoin network. In Contemporary issues in communication, cloud and big data analytics: Proceedings of CCB 2020 (pp. 39–55). Springer. https://doi.org/10.1007/978-981-16-4244-9_4
4. Hao, Y. (2022). 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)* (pp. 278–283). IEEE. https://doi.org/10.1109/CVIDLICCEA56201.2022.9825149

5. Bastiaan, M. (2015). Preventing the 51%-attack: A stochastic analysis of two phase proof of work in Bitcoin. In Proceedings of the 22nd Twente Student Conference on *IT*. University of Twente.
6. Baruwa, Z., Bhattacherjee, S., Chandnani, S. R., & Zhu, Z. (2023). Social media perceptions of 51% attacks on proof-of-work cryptocurrencies: A natural language processing approach [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2310.14307
7. Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). Cluster Computing, *26*(4), 2183–2197. https://doi.org/10.1007/s10586-023-03962-7
8. Nabilou, H. (2020). Testing the waters of the Rubicon: The European Central Bank and central bank digital currencies. Journal of Banking Regulation, *21*(4), 299–314. https://doi.org/10.1057/s41261-019-00112-1
9. Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. Blockchain: Research and Applications, *2*(3), Article 100021. https://doi.org/10.1016/j.bcra.2021.100021
10. Kim, S. K., Yeun, C. Y., Damiani, E., & Al-Hammadi, Y. (2019). Various perspectives in new blockchain design by using theory of inventive problem solving. In 2019 IEEE International Conference on Blockchain and Cryptocurrency *(ICBC)*. IEEE.
11. Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, *9*(9), Article 1788. https://doi.org/10.3390/app9091788
12. Taylor, K. (n.d.). What happens in 51% attacks? CoinMarketCap Academy. CoinMarketCap Academy
13. Rahman, A. (2019). A hybrid PoW-PoS implementation against 51% attack in cryptocurrency system [Doctoral dissertation, United International University].
14. Amin, M. R. (2020). 51% attacks on blockchain: A solution architecture for blockchain to secure IoT with proof of work [Bachelor's thesis, International University of Business Agriculture and Technology].
15. Niranjani, V., Kamachi, P. S., Siddhaarth, S., Venkatachalam, B., & Vishal, N. (2022). Hybrid approach to minimize 51% attack in cryptocurrencies. In 2022 8th International Conference on Advanced Computing and Communication Systems *(ICACCS)* (Vol. 1, pp. 2100–2103). IEEE. https://doi.org/10.1109/ICACCS54159.2022.9785056
16. Yang, X., Chen, Y., & Chen, X. (2019). Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 261–265). IEEE. https://doi.org/10.1109/Blockchain.2019.00041
17. Lansiaux, E., Tchagaspanian, N., & Forget, J. (2022). Community impact on a cryptocurrency: Twitter comparison example between Dogecoin and Litecoin. Frontiers in Blockchain, *5*, Article 829865. https://doi.org/10.3389/fbloc.2022.829865

Отримано редакцією журналу / Received: 30.01.26
Прорецензовано / Revised: 09.02.26
Схвалено до друку / Accepted: 24.09.26