10. Zhao T., Perez-Felkner L. Perceived abilities or academic interests? Longitudinal high school science and mathematics effects on postsecondary STEM outcomes by gender and race. *International Journal of STEM Education*. 2022. Vol. 9, № 1. URL: https://doi.org/10.1186/s40594-022-00356-w (дата звернення: 12.03.2026).

11. Kusumawati A., Rizal M., Wiharso T. A. Toward Inclusive and Interdisciplinary Applied Mathematics in the Digital Age. *Jurnal Sains MIPA Indonesia*. 2025. Vol. 1, № 1. С. 14–27. URL: https://doi.org/10.61978/jsmi.v1i1.550 (дата звернення: 13.03.2026).

УДК 004.056:336.74

КРИПТОВАЛЮТИ ТА МАТЕМАТИКА: ЩО СТОЇТЬ ЗА ЦИФРОВИМИ ГРОШАМИ?

К. О. Родюк, А. В. Луценко

Анотація. У статті розглянуто математичні принципи функціювання криптовалют як цифрових грошей. Проаналізовано роль криптографічних хеш-функцій, цифрового підпису, еліптичних кривих, дерева Меркла та ймовірнісних алгоритмів узгодження, що забезпечують формування довіри без участі центрального посередника. Показано, що стійкість криптовалютних систем базується не на вірі в код, а на конкретних математичних властивостях, а саме незворотності хешування, складності задач. Описано переваги та обмеження таких систем з позиції безпеки, енерговитрат.

Ключові слова: криптовалюта, хеш-функція, цифрові гроші.

Вступ. Криптовалюти стали помітним явищем цифрової економіки. Вони продемонстрували можливість передавання вартості в мережі без центрального банку та платіжного процесора. Прийняття суспільством криптовалют часто зводиться до коливань курсу, інвестиційного ринку. Такий підхід показує те, що криптовалюта є не лише фінансовим інструментом, а й математично організованою системою, у якій довіра замінюється набором перевірених правил.

Актуальність теми полягає в тому, що математика забезпечує цілісність і послідовність записів у розподіленому реєстрі. Без сучасної криптографії, теорії ймовірностей та дискретної математики криптовалюти не мали б розв'язати ключову проблему цифрових грошей, а саме проблему подвійного витрачання, тобто несанкціонованого повторного використання одного й того самого цифрового активу. У сучасних дослідженнях розглядаються безпека дерева Меркла, роль еліптичних кривих у цифровому підписі, а також математичні моделі формування блоків.

Метою роботи є з'ясування того, які математичні принципи лежать в основі криптовалют і як вони забезпечують захист транзакцій, збереження історії операцій та узгодження стану мережі без єдиного центру керування.

Основна частина. Основною частиною більшості криптовлют є блокчейн, послідовний ланцюг блоків, у яких записуються підтверджені транзакції. Кожен блок пов'язаний із попереднім через хеш його заголовка, а всередині самого блока транзакції організуються у дерево Меркла. Така структура означає, що навіть незначна зміна хоча б одного запису призводить до зміни хешу транзакції, потім проміжних вузлів дерева і, зрештою, кореня Меркла та заголовка блока. Через це блокчейн не є простою базою даних: це структура, у якій цілісність підтримується ланцюжком математично пов'язаних значень [1; 2].

Хеш-функція – це алгоритм, що відображає повідомлення довільної довжини у бітовий рядок фіксованої довжини. З позицій криптографії важливими є три її властивості: стійкість до пошуку прообразу, стійкість до другого прообразу та колізійна стійкість. У криптовалютних системах це означає, що за готовим хешем практично неможливо відновити початкові дані, а знайти два різні повідомлення з однаковим значенням хешу є обчислювально неприйнятно складно. Внаслідок цього хеш перетворюється на короткий «відбиток» транзакції або блока, за яким можна швидко перевірити, чи було щось змінено після запису [3].

Для підтвердження права власності на цифрові активи використовується не хешування саме по собі, а цифровий підпис. Відповідно до сучасного стандарту цифрового підпису, підпис дає змогу виявляти несанкціоновану модифікацію даних, автентифікувати підписувача та забезпечувати неможливість правдоподібного заперечення факту підписання. У практиці криптовалют це означає, що власник приватного ключа може сформувати підпис для транзак-

ції, а будь-який інший вузол мережі здатний перевірити його коректність за відкритим ключем, не отримуючи доступу до секрету.

Перевага цифрового підпису в криптовалюті полягає у тому, що він розділяє публічний і приватний контроль. Користувач може відкрито повідомляти адресу або похідний від відкритого ключа і водночас не розкривати секретний ключ, необхідний для створення підпису. У Bitcoin транзакція містить дані, які дають змогу мережі перевірити коректність витрачання виходів, а відкритий ключ та перевірки стають частиною математично формалізованого правила витрачання коштів [1; 4].

З еліптичними кривими пов'язана і важлива для криптовалют проблема співвідношення між криптостійкістю, швидкодією та розміром ключів. Для криптографії на основі задачі дискретного логарифмування підкреслюють, що коректний вибір параметрів кривої є самостійною умовою безпеки, а не лише технічною деталлю реалізації. У криптовалютних протоколах математична надійність визначається не тільки типом алгоритму, а й вибором конкретної групи, базової точки, порядку підгрупи та процедурою перевірки підпису [5].

Особливе значення займає математика еліптичних кривих. Сучасні схеми на їх основі забезпечують високий рівень криптостійкості за менших розмірів ключів, ніж традиційні асиметричні підходи, що робить їх ефективними для розподілених систем із великою кількістю перевірок. Безпека таких схем спирається на складність задачі дискретного логарифмування на еліптичних кривих. На практиці це означає, що відкритий ключ можна обчислити з приватного, але зворотне відновлення приватного ключа за відкритим у прийнятний час вважається нереалістичним [6].

Ще однією важливою математичною конструкцією є дерево Меркла. Воно дає змогу не лише зберігати великий набір транзакцій у стислому вигляді, а й ефективно доводити включення окремої транзакції до конкретного блока без повного перегляду всього його вмісту [1; 2]. Сучасні дослідження підкреслюють, що безпека дерева Меркла напряму залежить від властивостей базової хеш-функції та від ймовірності кореневих колізій, які теоретично можуть порушити достовірність перевірки. Навіть допоміжні на перший погляд елементи блокчейну мають чітке математичне навантаження [7].

Також треба розглянути механізм консенсусу. У класичних криптовалютах на кшталт Bitcoin історично ключову роль відіграє доказ виконаної роботи – Proof of Work. Його математична суть полягає в тому, що майнер має знайти таке значення змінної частини заголовка блока, за якого хеш цього заголовка буде меншим або рівним за встановлений пороговий рівень складності. Оскільки вихід криптографічної хеш-функції поводиться як псевдовипадкове число, успіх окремої спроби є ймовірнісною подією. Зменшення цільового порога зменшує ймовірність успіху однієї спроби та збільшує середню кількість обчислень, необхідних для знаходження коректного блоку [1; 2].

Тут проявляється роль теорії ймовірностей. Якщо шанс успіху однієї перевірки дуже малий, то мережа в середньому потребує великої кількості незалежних спроб. Це перетворює атаку на історію транзакцій на задачу з надзвичайно великими обчислювальними витратами. У документації Bitcoin прямо підкреслюється, що зміна даних у старому блоці потребує перерахунку цього блоку і всіх наступних, а отже, вартість фальсифікації зростає з кожним новим доданим блоком. Інакше кажучи, незмінність реєстру досягається не абсолютною забороною, а економічно та математично невигідною складністю підробки [2].

Після включення транзакції до блоку кожен наступний блок збільшує глибину її розміщення в ланцюгу, а разом із нею – і сумарну кількість роботи, яку потрібно повторити потенційному порушнику для переписування історії. У спрощеній перевірці платежів клієнт може не зберігати весь блокчейн, а перевіряти наявність транзакції через гілку дерева Меркла та оцінювати глибину блоку як наближену міру безпеки [2].

Проте математична надійність не означає абсолютної досконалості. Дослідження блокчейн-систем показують, що зі зростанням навантаження виникають проблеми масштабованості: збільшуються час підтвердження, затримки поширення блоків і ймовірність розгалужень мережі. До того ж класичний Proof of Work вимагає значних енерговитрат, тому в науковій

літературі активно аналізуються альтернативні моделі консенсусу, зокрема Proof of Stake та Proof-of-Useful-Work. Математика криптовалют розвивається у відповідь на нові вимоги до безпеки, швидкодії та практичної корисності [8].

Огляди сучасних алгоритмів Proof-of-Useful-Work показують, що замінити «марну» обчислювальну роботу на корисну можна лише за умови збереження трьох властивостей: складності передбачення, простоти перевірки результату і неможливості дешевого повторного використання вже виконаних обчислень. Класичні криптовалютні схеми спираються на задачі, пов'язані з дискретним логарифмуванням, тоді як нові стандарти NIST уже включають постквантові підходи, зокрема ML-DSA. Це не означає негайної втрати працездатності наявних криптовалют, але показує, що математична основа цифрових грошей не стоять на місті, з розвитком обчислювальної техніки змінюються і класи задач, на яких будується практична довіра. Тому перспективні криптовалютні системи мають враховувати не лише сучасну, а й майбутню модель криптографічної стійкості [9].

Ще одним фундаментальним рівнем математики криптовалют є арифметика самих транзакцій. У моделі Bitcoin кожна транзакція складається зі входів і виходів, а коректність платежу перевіряється через зв'язок нового запису з уже наявними невитраченими виходами попередніх транзакцій. Мережа контролює не «баланс рахунку» у звичайному банківському сенсі, а допустимість перетворення одних наборів числово і криптографічно описаних прав на інші. Сума вхідних значень має покривати суму вихідних значень і комісію, а кожен вхід повинен бути підкріплений коректним доказом права витрачання [1].

Не менш важливою є роль випадковості. У криптографічних підписах і в консенсусних процедурах випадкові або псевдовипадкові значення не є другорядним технічним елементом, а входять до самого доказу безпеки. Стандарти цифрового підпису окремо регламентують параметри й процедури, від яких залежить неможливість відновлення секретного ключа зі спостережуваних підписів. Це означає, що стійкість системи визначається не лише складністю базової задачі, а й коректністю вибору допоміжних змінних, розподілів та процедур генерації [7].

За цифровими грошима стоїть поєднання кількох математичних рівнів. На рівні криптографії працюють хеш-функції та цифрові підписи на рівні структур даних. Це дерево Меркла і зв'язування блоків, на рівні теорії ймовірностей, це статистична керованість процесу пошуку блока на рівні алгоритмів, це правила консенсусу, що змушують незалежні вузли приймати одну й ту саму історію операцій. Саме взаємодія цих рівнів робить криптовалюту не просто цифровим записом, а стійкою децентралізованою системою обліку вартості.

Дерево Меркла демонструє, як математична економність безпосередньо впливає на масштабованість. Для того, щоб переконатися, що окрема транзакція входить до блоку, не потрібно повторно передавати весь набір транзакцій: достатньо лише самої транзакції та ланцюжка проміжних хешів до кореня дерева. Через це обсяг доказу зростає не лінійно, а значно повільніше, ніж кількість записів у блоці.

У системах типу Bitcoin окремого значення набуває і математичний механізм коригування складності майнінгу. Якщо сукупна обчислювальна потужність мережі зростає або зменшується, протокол змінює цільову складність так, щоб середній інтервал між блоками залишався близьким до заданого значення – це приклад вбудованого зворотного зв'язку, у якому протокол реагує на статистику попередніх блоків. Отже, стабільність випуску нових блоків досягається не зовнішнім адмініструванням, а автоматичним математичним правилом [2].

Математика пояснює межі анонімності криптовалют. Хоча система не вимагає обов'язкового розкриття особи, самі транзакції утворюють відкритий граф зв'язків між адресами, входами і виходами. Рекомендації розробників Bitcoin прямо вказують, що повторне використання відкритих ключів або адрес погіршує приватність користувача. Через це криптовалюта є математичним механізмом, який захищає справжність і цілісність записів, але не гарантує абсолютної непомітності учасника без додаткових протоколів конфіденційності [3].

Також важливо розуміти, що «цифрові гроші» у вигляді криптовалют не існують як окремі файли чи монети в традиційному сенсі. У мережі фактично існує система записів про допустимі переходи прав на активи. Транзакція спирається на попередні невитрачені виходи, формує нові виходи й підписується власником відповідного ключа. Тобто в основі криптова-

лют лежить не предмет, а правило: хто, коли і за яких математично перевірюваних умов може змінити стан розподіленого реєстру [1].

Висновки. Математична надійність криптовалюти не означає абсолютної неможливості злому. Система побудована так, щоб вартість атаки, її обчислювальна складність і ймовірність успіху для порушника зростали швидше, ніж очікувана вигода від підміни історії операцій. Через це в блокчейні настільки важливим є поняття ймовірнісної остаточності. Якщо в традиційній базі даних запис може вважатися остаточним після команди сервера, то в криптовалютній довіра до запису зростає поступово, з кожним новим блоком стає менш ймовірним, що альтернативний ланцюг перевищить чесний. У цьому сенсі підтвердження транзакції є не формальною позначкою, а математичною оцінкою ризику. Що глибше транзакція розташована в ланцюгу, то більший обсяг ресурсів потрібно витратити для її скасування, то вищим стає рівень практичної довіри до такого запису.

Окремого значення набуває і зв'язок між математикою та економічною мотивацією учасників мережі. Правила консенсусу самі по собі не існують у відриві від стимулів, вони поєднуються з винагородою за блок, комісіями за транзакції та ризиком втрати витрачених ресурсів у разі невдалої або нечесної поведінки. Безпека криптовалюти формується на перетині дискретної математики, теорії алгоритмів і елементів теорії ігор. Мережа є стійкою доти, доки для більшості вузлів і майнерів або валідаторів чесне дотримання протоколу є раціональнішим, ніж спроба його обійти. Сучасні огляди консенсусних механізмів показують, що різні підходи змінюють саме цей баланс між витратами, пропускною здатністю, енерговитратами та рівнем безпеки. Математика в криптовалютах працює не ізольовано, а як частина ширшої системи, у якій формальна коректність алгоритму має узгоджуватися з поведінкою реальних незалежних учасників.

Ще один важливий аспект полягає в тому, що криптовалютні системи розв'язують задачу перевірки не лише через складність обчислень, а й через ефективну організацію доказів. Тут проявляється роль дерева Меркла. Воно мінімізує обсяг інформації, потрібної для перевірки окремої транзакції, і тим самим знижує вимоги до вузлів, які не зберігають усю історію блокчейну. Це приклад того, як правильно побудована структура даних дає не менший ефект, ніж сильний криптографічний примітив, без скорочення доказів блокчейн був би значно важчим для розповсюдження, перевірки та масштабування. Цінність дерева Меркла полягає не тільки у виявленні змін, а й у тому, що воно забезпечує логарифмічну за своєю природою схему підтвердження включення даних до блоке. Завдяки цьому криптовалюта залишається доступною не лише для повних вузлів, а й для легких клієнтів, що суттєво розширює практичні межі використання таких систем.

Математичні основи криптовалют не усувають усіх обмежень, а лише роблять їх чітко формалізованими. Підвищення безпеки часто пов'язане зі зниженням або зростанням витрат. Чим жорсткіші вимоги до перевірки блоку та до досягнення консенсусу, тим важче забезпечити високу пропускну здатність мережі без втрати децентралізації. У наукових публікаціях блокчейн дедалі частіше розглядається як об'єкт оптимізації, де потрібно шукати компроміс між часом підтвердження, розміром блоку, навантаженням на вузли, затримками поширення інформації і ймовірністю появи конкурентних гілок. Математика в криптовалютах не лише гарантує безпеку, а й задає межі масштабованості, вона показує, які параметри можна змінювати без руйнування системи, а які змінюють саму природу в мережі.

Сьогодні значна частина криптовалют спирається на схеми цифрового підпису, безпека яких пов'язана зі складністю задач на еліптичних кривих. Поява достатньо потужних квантових обчислень у майбутньому теоретично може змінити співвідношення між складністю задачі та можливістю її практичного розв'язання. Нові стандарти вже фіксують альтернативні підходи до цифрового підпису, зокрема постквантові алгоритми на основі ґраток. Для криптовалют це означає, що математичний фундамент цифрових грошей не є раз і назавжди завершеним, він продовжує розвиватися разом із розвитком обчислювальної техніки та криптоаналізу. Відповідь на питання, що стоїть за цифровими грошима, не обмежується блокчейном як технологією, за ним стоїть динамічна система математичних ідей, у якій безпека, ефективність і довіра постійно переосмислюються й уточнюються.

Abstract. This article examines the mathematical principles underlying the functioning of cryptocurrencies as digital money. It analyzes the role of cryptographic hash functions, digital signatures, elliptic curves, Merkle trees, and probabilistic consensus algorithms, which enable the establishment of trust without the involvement of a central intermediary. It is shown that the robustness of cryptocurrency systems is based not on trust in the code, but on specific mathematical properties, namely the irreversibility of hashing and the complexity of computational problems. The advantages and limitations of such systems are described from the perspective of security and energy consumption.

Keywords: Cryptocurrency, hash function, digital money.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Transactions. *Bitcoin Developer Guide.* URL: https://developer.bitcoin.org/devguide/transactions.html
2. Block Chain. *Bitcoin Developer Guide.* URL: https://developer.bitcoin.org/devguide/block_chain.html
3. FIPS 180-4. Secure Hash Standard (SHS). *NIST.* 2015. URL: https://doi.org/10.6028/NIST.FIPS.180-4
4. Vovchak O., Veres Z. Modeling the Block Formation Process in Blockchain and Its Impact on Scalability. *Computer Systems and Networks.* 2024. Vol. 6, № 2. P. 1–14. URL: https://doi.org/10.23939/csn2024.02.001
5. Operating Modes. *Bitcoin Developer Guide.* URL: https://developer.bitcoin.org/devguide/operating_modes.html
6. Elliptic Curve Cryptography: Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey / S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, M. Yousaf. *Computer Science Review.* 2024. Vol. 53. Article 100650. URL: https://doi.org/10.1016/j.cosrev.2024.100650
7. FIPS 186-5. Digital Signature Standard (DSS). *NIST.* 2023. URL: https://doi.org/10.6028/NIST.FIPS.186-5
8. Evaluating the Security of Merkle Trees: An Analysis of Data Falsification Probabilities / O. Kuznetsov, A. Rusnak, A. Yezhov, K. Kuznetsova, D. Kanonik, O. Domin. *Cryptography.* 2024. Vol. 8, № 3. Article 33. URL: https://doi.org/10.3390/cryptography8030033
9. FIPS 204. Module-Lattice-Based Digital Signature Standard. *NIST.* 2024. URL: https://doi.org/10.6028/NIST.FIPS.204

УДК 004.934:004.8

ЗАСТОСУВАННЯ КОНЦЕПЦІЇ MOBILE-FIRST ПІД ЧАС ПРОЄКТУВАННЯ ІНТЕРФЕЙСІВ У СЕРЕДОВИЩІ FIGMA

Д. В. Рихлецька, Н. Р. Веселовська

Анотація. У статті висвітлено концепцію Mobile-First і її вплив на сучасне проєктування користувацьких інтерфейсів (UI) та користувацького досвіду (UX). В умовах зростаючої популярності мобільного вебтрафіка підхід «від мобільного до десктопу» закріпився як індустріальний стандарт, що спонукає дизайнерів опановувати нові методології та інструменти. Особлива увага приділена середовищу Figma – провідній платформі для створення адаптивних макетів. Детально розглянуто функціональні можливості Figma, як-от Auto Layout, системи компонентів, варіанти (Variants), а також застосування 8-піксельної сітки. На основі реального кейсу розробки інтерфейсу розважального вебдодатка «Зодіакальний бандерогусь» демонструється весь процес проєктування – від створення низькодеталізованих вайрфреймів (low-fidelity) до розробки високодеталізованих макетів (high-fidelity) та налаштування інтерактивного прототипу. Результати дослідження підтверджують, що поєднання концепції Mobile-First із сучасним функціоналом Figma дає змогу вести розробку цифрових продуктів із високою продуктивністю. Такі рішення характеризуються ергономічністю, масштабованістю та відповідають найвищим стандартам якості.

Ключові слова: UI/UX дизайн, Mobile-First, Figma, прототипування, мобільні інтерфейси, вебдодаток, Auto Layout.

Вступ. Сучасний розвиток цифрових технологій супроводжується стрімким зростанням важливості мобільних пристроїв. За даними провідних аналітичних агенцій, понад 60 % глобального вебтрафіка тепер генерується саме зі смартфонів, і ця цифра продовжує невпинно збільшуватися. Така тенденція докорінно змінила підходи до проєктування користувацьких інтерфейсів (UI) та досвіду взаємодії (UX). Відповідно до нових умов, у сфері вебдизайну закріпилася методологія Mobile-First, яка сьогодні є визнаним стандартом розробки. Її впровадження потребує не лише нового погляду дизайнера на вирішення задач, але й впевненого володіння сучасними інструментами, серед яких лідером виступає хмарна платформа Figma.

Історично процес створення цифрових інтерфейсів базувався на принципі Desktop-First, тобто насамперед розроблялися повноцінні версії для великих екранів. Даліїх функціонал поступово скорочувався для адаптації до мобільних пристроїв, що часто призводило до перева-