

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ПРИВАТНИХ КЛЮЧІВ У СУЧАСНИХ КРИПТОГАМАНЦЯХ

Вінницький національний технічний університет

Анотація

У роботі розглядається проблема безпечного зберігання та управління приватними ключами як критичного елементу функціонування сучасних криптогаманців. Проведено аналіз архітектурних особливостей реалізації програмних та апаратних рішень, досліджено алгоритми генерації ентропії, стандарти деривації ключів та методи шифрування даних. Окрема увага приділена порівнянню ефективності традиційних методів захисту з новітніми підходами, такими як технологія багатосторонніх обчислень (MPC) та використання захищених елементів (Secure Element) для протидії кіберзагрозам.

Ключові слова: криптографічний захист, криптогаманець, приватний ключ, TRNG, блокчейн, ієрархічна детермінація, Seed-фраза, апаратний гаманець, MPC, абстракція облікового запису.

Abstract

The paper examines the problem of secure storage and management of private keys as a critical element of the functioning of modern crypto wallets. The author analyzes the architectural features of the implementation of software and hardware solutions, investigates entropy generation algorithms, key derivation standards, and data encryption methods. Special attention is paid to comparing the effectiveness of traditional protection methods with the latest approaches, such as multi-party computation (MPC) technology and the use of secure elements (Secure Element) to counter cyber threats.

Keywords: cryptographic protection, crypto wallet, private key, TRNG, blockchain, hierarchical determination, Seed phrase, hardware wallet, MPC, account abstraction.

Вступ

Поняття «приватний ключ» у контексті цифрової економіки набуло виняткового значення з моменту появи та стрімкого поширення технології блокчейн. Цей криптографічний елемент став фундаментом для сучасних криптогаманців, забезпечуючи користувачам повний контроль над активами, автентифікацію транзакцій та цифрову незалежність. Сучасні криптогаманці еволюціонували від простих сховищ даних до інструментів, що суттєво впливають на фінансовий стан користувачів. Захист криптографічних ключів став запорукою безпеки у децентралізованих системах і головним бар'єром проти несанкціонованого доступу. Тут важливо підкреслити не тільки технічне, але й стратегічне значення захисту ключів, адже надійність їхньої реалізації є визначальним фактором стійкості активів в умовах постійно зростаючих кіберзагроз.

Результати дослідження

Поява сучасних криптогаманців відбулася на тлі стрімкого зростання секторів децентралізованих фінансів DeFi та NFT (2020–2021 рр.), коли просте зберігання монет перестало бути єдиною функцією. Користувачі, зокрема інвестори та розробники, потребували інструментів для взаємодії зі смарт-контрактами, що змінило архітектуру додатків [1]. Після цього гаманець став інтерфейсом Web3, який сучасні платформи використовують для авторизації, перетворившись на «пункт керування» цифровою особистістю [2].

Вперше поняття «криптогаманця» трансформувалося з програми для ключів у браузер децентралізованого інтернету. Фактично, це складний програмно-апаратний комплекс, що містить модулі аналізу транзакцій, захист від фішингу та інтеграцію з різними блокчейнами. Саме такими, мультифункціональними та захищеними, побачили хакери нові цілі для атак. В одному з технічних звітів, експерт з кібербезпеки намагався пояснити, чому неможливо зламати гаманець з технологією MPC (багатосторонніх обчислень), хоча зловмисники перехопили частину даних. «Просто математична фортеця якась», – сказав аналітик, коментуючи розділення ключа на фрагменти між різними пристроями [3]. Окрім MPC, безпека сучасних гаманців базується на системі криптографічних протоколів. Перший рубіж – це генерація ентропії. На відміну від вразливих програмних генераторів (PRNG), сучасні стандарти вимагають використання апаратних TRNG (True Random Number Generator), що збирають шум із фізичних процесів мікросхем для створення ідеально випадкового 256-бітного числа [4]. Другий рубіж – це алгоритми цифрового підпису. Окрім класичного ECDSA на кривій secp256k1, впроваджуються підписи Шнорра (BIP-340), які дозволяють агрегувати кілька підписів в один, підвищуючи приватність (Taproot) [5]. Третій рубіж – ієрархічна детермінація (HD Wallets). Згідно зі стандартом BIP-32, із одного «майстер-зерна» (Master Seed) розгортається нескінченне дерево ключів. Використовуючи шляхи деривації (Derivation Paths, наприклад $m/44'/60'/0'/0/0$), гаманець генерує унікальні адреси для кожної транзакції, унеможливаючи відстеження загального балансу за однією адресою [6]. Четвертий рубіж – захист даних у стані спокою (Data-at-Rest). Ключовий файл шифрується симетричним алгоритмом AES-256-GCM, а для захисту пароля користувача застосовується функція PBKDF2 (RFC 2898) з використанням HMAC-SHA512 та 2048 ітераціями хешування, що робить атаки перебором (Rainbow Tables) економічно недоцільними [7]. Сучасні гаманці діють в складних умовах: постійні атаки методів соціальної інженерії, «сліпий підпис» транзакцій та зловмисні смарт-контракти. Попри це, вони продовжують виконувати захисні функції, демонструючи впровадження симуляції транзакцій перед їх підписанням. Однією з найважливіших подій став крах централізованих бірж (наприклад, FTX) у листопаді 2022 р., що підірвав довіру до зберігання коштів у третіх осіб. У криптоспільноті це стало символом необхідності «повернення до коренів» – некастодіальних гаманців. Того ж періоду ринок висунув користувачам ультиматум – навчитися керувати власними ключами або втратити все. Інвестори вибрали навчання та апаратні рішення. Унаслідок масового відтоку коштів з бірж, мільйони доларів перейшли на Ledger, Trezor та SafePal. Користувачі продовжили контролювати свої активи особисто. Наступна «ротація» технологій відбулася з впровадженням Абстракції Облікового Запису (Account Abstraction). Тепер замість складних Seed-фраз прийшли «розумні акаунти», які дозволяють відновлювати доступ через довірених осіб або біометрію. До боротьби за безпеку долучилися технології Secure Enclave у смартфонах, які одразу перетворили мобільні пристрої схожі до апаратних гаманців [8]. Вважається, що боротьба між зручністю та безпекою тривала роками, але зараз знайдено баланс. Офіційним трендом визнано гібридні моделі захисту. Проте, чималий сегмент «холодного зберігання» (Cold Storage) все ще залишається найнадійнішим форпостом. Хакери перебувають у розпачі від безсилля, оскільки нездатні дистанційно зламати пристрій, який фізично відключений від мережі та вимагає натискання механічної кнопки для підтвердження. У критичних ситуаціях, коли інтерфейс гаманця недоступний або телефон втрачено, спрацьовує механізм сумісності стандартів (BIP-39/BIP-44). Власник бере свою мнемонічну фразу та, ігноруючи блокування конкретного софту чи санкції, він вводить код у будь-який інший сумісний додаток і миттєво відновлює доступ до капіталу [9]. Концепція «Self-Custody» (самостійне зберігання) є основою сучасної криптоекономіки та символом незалежності від банківської системи, важливою сторінкою цифрової еволюції [10].

Висновки

Сучасний криптогаманець став символом технологічної зрілості та вершиною прикладної криптографії. Інтеграція апаратної генерації ентропії (TRNG), сучасних стандартів цифрового підпису та ієрархічної детермінації ключів, попри зростання складності кіберзагроз, забезпечує математично гарантований рівень безпеки. Це не просто утиліта для переказів, а ешелонована система захисту, що змінила парадигму володіння, поєднала зручність Абстракції Облікового Запису з непорушністю криптографічних алгоритмів. Використання сучасних некастодіальних рішень підкреслює: користувачі здатні ефективно захищати власний капітал, опираючись не на довіру до третіх сторін, а на закони математики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The history and evolution of cryptocurrency wallets. Cointelegraph. URL: <https://cointelegraph.com/learn/articles/the-history-and-evolution-of-cryptocurrency-wallets> (дата звернення: 13.12.2025).
2. Web3-гаманці: повний посібник. URL: <https://www.kraken.com/uk/learn/web3-wallets> (дата звернення: 13.12.2025).
3. What is MPC (Multi-Party Computation)? | Fireblocks. Fireblocks. URL: <https://www.fireblocks.com/what-is-mpc> (дата звернення: 14.12.2025).
4. What is entropy and how does Trezor generate your wallet | Trezor Knowledge Base. Trezor Hardware Wallet (Official) | Bitcoin & Crypto Security. URL: https://trezor.io/guides/trezor-devices/trezor-fundamentals/what-is-entropy-and-how-does-trezor-generate-your-wallet?srsltid=AfmBOoprJz3jvPVqCbuo1_9Xbv8ip_oHYgYK6gjNHVYApoKhltVh9DA&utm (дата звернення: 14.12.2025).
5. Bips/bip-0340.mediawiki at master · bitcoin/bips. GitHub. URL: <https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki> (дата звернення: 14.12.2025).
6. Bips/bip-0032.mediawiki at master · bitcoin/bips. GitHub. URL: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki> (дата звернення: 14.12.2025).
7. bips/bip-0039.mediawiki at master · bitcoin/bips. GitHub. URL: <https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki> (дата звернення: 14.12.2025).
8. Децентралізація: Як вона змінює криптоіндустрію після краху FTX. OKX. URL: <https://www.okx.com/ua/learn/decentralization-crypto-industry-post-ftx> (дата звернення: 15.12.2025).
9. Що таке BIP32, BIP39 та BIP44 у криптовалютних гаманцях?. URL: <https://blog.whitebit.com/what-is-bip-in-crypto-wallets/> (дата звернення: 15.12.2025).
10. What is Non-Custodial Wallet? Definition, Security, How It Works. Cube Exchange | Best Way to Buy Bitcoin, Solana & Dogecoin. URL: <https://www.cube.exchange/uk/what-is/non-custodial-wallet> (дата звернення: 16.12.2025).

Салієва Ольга Володимирівна – доктор філософії за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: saliev8257@vntu.edu.ua

Деркач Євгеній Юрійович – студент групи 3KITC-236, Факультету менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: derkaczena81@gmail.com

Saliieva Olha Volodymyrivna – Doctor of Philosophy in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: saliev8257@vntu.edu.ua

Derkach Evgeniy Yuriyovich – student of group 3KITS-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, e-mail: derkaczena81@gmail.com