УДК 004.056.55 DOI: 10.31673/2786-8362.2025.029079

Поляков Д.А.; Шикула О.М., д.ф.-м.н.

БЛОКЧЕЙН НА ОСНОВІ ШИФРУВАННЯ ДАНИХ І МЕХАНІЗМИ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ВЕЛИКИХ ДАНИХ

Poliakov D.A., Shykula O.M. Blockchain-based encryption mechanisms for big data confidentiality. This paper provides a comprehensive analysis of the potential of blockchain technology to ensure the confidentiality of big data in modern information systems. Blockchain is examined as an innovative decentralized technology that, due to its architecture and built-in cryptographic mechanisms, provides a high level of data security, resilience to cyberattacks, and transparency of information processing. The study explores the main encryption methods used in blockchain — symmetric, asymmetric, and hashing — providing a comparative analysis of their advantages and limitations and their roles in secure storage and transmission. Special attention is paid to anonymization and pseudonymization techniques. The paper further examines confidential blockchains (Monero, ZCash) that leverage ring signatures and Confidential Transactions, as well as Zero-Knowledge Proofs (ZKP), which enable verification without disclosure. Real-world applications are presented across healthcare (Guardtime, MedRec), finance (privacy-oriented cryptocurrencies), e-government (Estonian registries), and IoT (smart-home scenarios). The discussion highlights the key challenges of blockchain adoption – scalability, computational and energy costs, and regulatory constraints, including tensions between immutability and data erasure requirements. The article outlines future directions: enhanced consensus algorithms, second-layer protocols, advanced smart contracts, and hybrid models.

Keywords: blockchain, big data, encryption, confidentiality, anonymization, pseudonymization, zero-knowledge proofs, Monero, ZCash

Поляков Д.А., Шикула О.М. Блокчейн на основі шифрування даних і механізми збереження конфіденційності великих даних. У даній статті здійснено ґрунтовний аналіз можливостей застосування блокчейн-технології для збереження конфіденційності великих даних у сучасних інформаційних системах. Блокчейн розглядається як інноваційна децентралізована технологія, яка завдяки своїй архітектурі та вбудованим криптографічним механізмам забезпечує високий рівень безпеки даних, стійкість до кібератак та прозорість процесів обробки інформації. У роботі детально досліджено основні методи шифрування, що застосовуються в блокчейні: симетричне, асиметричне та хешування. Проведено їх порівняльний аналіз із зазначенням ключових переваг та обмежень, а також висвітлено роль кожного методу у побудові систем безпечного зберігання та передавання даних. Особливу увагу приділено методам анонімізації та псевдонімізації, які забезпечують приватність у великих масивах даних. У статті розглянуто сучасні інструменти конфіденційних блокчейнів (Monero, ZCash), що використовують кільцеві підписи, технологію «Confidential Transactions» та механізми приховування деталей транзакцій. Також детально проаналізовано технологію доказів з нульовим розкриттям (Zero-Knowledge Proofs, ZKP), яка надає можливість підтвердження достовірності інформації без розкриття самих даних. Механізми оцінено у контексті реальних сценаріїв використання для захисту персональних даних у сфері медицини, фінансів, електронного урядування та IoT. Наведено практичні приклади: системи Guardtime та MedRec у медицині; транзакції з анонімністю в Monero та ZCash; застосування у державних реєстрах Естонії; інтеграція у «розумні будинки» для захисту IoT-пристроїв. Крім того, окреслено ключові виклики впровадження блокчейну: масштабованість, обчислювальні витрати, енергозатратність та правові бар'єри, включно з колізіями між незмінністю реєстру та вимогами до видалення даних. Окреслено перспективи розвитку: удосконалення алгоритмів консенсусу, протоколи другого рівня, застосування удосконалених смарт-контрактів та гібридних моделей.

Ключові слова: блокчейн, великі дані, шифрування, конфіденційність, анонімізація, псевдонімізація, Zero-Knowledge Proofs, Monero, ZCash

Вступ

Стрімке зростання обсягів даних, що обробляються організаціями, супроводжується підвищенням ризиків несанкціонованого доступу, витоків та маніпулювання інформацією. Централізовані моделі зберігання уразливі до одиничних точок відмови та зловмисних впливів. Децентралізована архітектура блокчейну пропонує альтернативу з підвищеною стійкістю, а криптографічні механізми забезпечують конфіденційність, цілісність і контрольований доступ до даних.

Аналіз останніх досліджень. У фундаментальній праці S. Nakamoto закладено базові засади ланцюга блоків і механізмів консенсусу. Подальші дослідження зосереджені на приватності та керуванні доступом до даних: Zyskind, Nathan, Pentland запропонували децентралізовані моделі керування приватністю; Miers та колеги представили протокол Zerocoin; Ben-Sasson та ін. – Zerocash із застосуванням доказів з нульовим розкриттям; Wood описав універсальну платформу смарт-контрактів Ethereum. Ряд робіт присвячено правовим аспектам взаємодії з GDPR, масштабованості (шарінг, rollups) та інтеграції з існуючими IT-ландшафтами.

Метою роботи є систематизація підходів до забезпечення конфіденційності великих даних засобами блокчейну та оцінювання їхньої практичної придатності. Для досягнення мети визначено задачі: (1) порівняти криптографічні методи, що застосовуються в блокчейні; (2) узагальнити технології приватності (конфіденційні блокчейни, ZKP, позаланцюгове зберігання з ончейн-керуванням доступом); (3) проаналізувати прикладні сценарії в охороні здоров’я, фінансах, державному секторі та IoT; (4) визначити виклики масштабованості, витрат і регуляторних вимог; (5) окреслити напрями подальшого розвитку.

Виклад основного матеріалу дослідження

Криптографічні методи захисту даних у блокчейні. Ядром конфіденційності та цілісності в блокчейні є криптографія. Симетричне шифрування забезпечує високу продуктивність для захищеного зберігання позаланцюгових об’єктів та каналів зв’язку. Асиметричне шифрування (пара публічний/приватний ключ) використовується для автентифікації, цифрового підпису, обміну ключами та керування доступом. Хешування гарантує незмінність та верифікаційність блоків і транзакцій, будуючи криптографічні зв’язки ланцюга.

Таблиця 1

Методи захисту даних блокчейну

Метод	Опис	Переваги	Обмеження
Симетричне шифрування	Один спільний ключ для шифрування та дешифрування	Висока швидкодія; простота реалізації	Ризики розповсюдження/втрати ключа
Асиметричне шифрування	Пара ключів: публічний (шифрування), приватний (доступ)	Висока безпека; підтримка підписів	Більші обчислювальні витрати
Хешування	Одностороннє перетворення даних у фіксовану довжину	Цілісність, незмінність, швидка перевірка	Неможливість дешифрування первинних даних

Технології конфіденційності: від анонімізації до ZKP. Для великих даних критичними є анонімізація та псевдонімізація, що мінімізують ідентифікаційні ризики. У блокчейні додатково застосовують конфіденційні реєстри (Monero, ZCash), де використовуються кільцеві підписи, адреси зі схованими ключами та приховані суми (Confidential Transactions). Докази з нульовим розкриттям дозволяють верифікувати твердження без розкриття вхідних даних, що створює базу для приватних транзакцій та селективного розкриття.

Прикладні сценарії. Охорона здоров’я: пацієнт-центричні схеми доступу дозволяють власнику записів керувати наданням прав лікарям і страховим компаніям; журнал доступів незмінно фіксується у реєстрі. Фінанси: приватні криптовалюти забезпечують конфіденційність сум і контрагентів; корпоративні мережі застосовують permissioned-підходи для внутрішніх розрахунків. Державний сектор: реєстри власності та актів цивільного стану з ончейн-аудитом підвищують довіру громадян. IoT: у «розумних» будинках криптографічна ідентифікація пристроїв та журналювання подій зменшують ризики підробки та перехоплення даних.

Таблиця 2

Технології конфіденційності блокчейну

Технологія	Приклади	Принцип роботи	Переваги	Недоліки
Конфіденційні блокчейни	Monero, ZCash	Приховують відправника/одержувача та суми (кільцеві підписи, CT)	Висока анонімність транзакцій	Складна інтеграція; регуляторні ризики
Zero-Knowledge Proofs	zk-SNARKs, zk-STARKs	Доказ коректності без розкриття даних	Мінімальне розкриття; масштабована верифікація	Обчислювальні витрати; параметризація
Офчейн з ончейн-доступом	IPFS + смарт-контракти	Дані зберігаються поза ланцюгом, доступ контролює ончейн-логіка	Гнучкість, економія місця	Складність цілісного контролю

Управління згодою та політиками доступу реалізуються смарт-контрактами: атрибутивні схеми дають змогу надавати тимчасові ключі, а селективне розкриття даних відбувається за умовами політик. Це особливо важливо в мультистейкхолдерних системах, де залучені провайдери послуг, користувачі та регулятори.

Виклики та обмеження. Масштабованість: публічні мережі обмежені пропускною здатністю та латентністю. Можливі шляхи – шаринг, rollups, канали платежів, а також гібридні архітектури (permissioned ядро + публічний анкеринг). Витрати: верифікація приватних транзакцій та побудова доказів потребують суттєвих обчислень і енергії. Право: вимоги GDPR щодо видалення даних конфліктують із незмінністю – застосовують посилання на офчейн-дані та криптографічне «логічне видалення» (re-encryption, ключове стирання).

Інтеграція: для вбудовування блокчейну в наявну IT-інфраструктуру необхідні конектори, схеми міграції даних і процесні зміни. Людський фактор: успіх залежить від правильної операційної моделі, управління ключами та підготовки персоналу.

Висновки

Блокчейн формує стійку основу для конфіденційності великих даних за рахунок криптографії, незмінності журналів і гнучких схем доступу. Найбільший ефект досягається у поєднанні з офчейн-сховищами, політиками керування згодою та доказами з нульовим розкриттям. Перспективами досліджень є практичні оцінки продуктивності zk-схем у прикладних системах, стандартизація моделей керування доступом і типові правові патерни сумісності з GDPR та нацзаконодавством.

Список використаної літератури:

1. Wright C. S. Bitcoin: a peer-to-peer electronic cash system. *SSRN electronic journal*. 2008. URL: https://doi.org/10.2139/ssrn.3440802.

2. Zyskind G., Nathan O., Pentland A. Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE security and privacy workshops (SPW)*, San Jose, CA, 21–22 May 2015. 2015. URL: https://doi.org/10.1109/spw.2015.27.

3. Zerocoin: anonymous distributed e-cash from bitcoin / I. Miers et al. *2013 IEEE symposium on security and privacy (SP) conference*, Berkeley, CA, 19–22 May 2013. 2013. URL: https://doi.org/10.1109/sp.2013.34.

4. Efficient variant transaction injection protocols and adaptive policy optimisation for decentralised ledger systems / C. F. Chiang et al. *International journal of grid and utility computing*. 2020. Vol. 11, no. 6. P. 847. URL: https://doi.org/10.1504/ijguc.2020.10032064.

5. Zerocash: decentralized anonymous payments from bitcoin / E. Ben Sasson et al. *2014 IEEE symposium on security and privacy (SP)*, San Jose, CA, 18–21 May 2014. 2014. URL: https://doi.org/10.1109/sp.2014.36.

6. Groth J. On the size of pairing-based non-interactive arguments. *Advances in cryptology – EUROCRYPT 2016*. Berlin, Heidelberg, 2016. P. 305–326. URL: https://doi.org/10.1007/978-3-662-49896-5_11.

7. MedRec: using blockchain for medical data access and permission management / A. Azaria et al. *2016 2nd international conference on open and big data (OBD)*, Vienna, Austria, 22–24 August 2016. 2016. URL: https://doi.org/10.1109/obd.2016.11.

8. Underwood S. Blockchain beyond bitcoin. *Communications of the ACM*. 2016. Vol. 59, no. 11. P. 15–17. URL: https://doi.org/10.1145/2994581.

9. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*. 2017. Vol. 41, no. 10. P. 1027–1038. URL: https://doi.org/10.1016/j.telpol.2017.09.003.

10. Gdpr enforcement. *EU general data protection regulation (GDPR), third edition*. 2019. P. 285–297. URL: https://doi.org/10.2307/j.ctvr7fcwb.19.

11. Akeela R., Krawiec-Thayer M. P. Efficient HW/SW partitioning of Halo: FPGA-accelerated recursive proof composition in blockchain. *Microsystem technologies*. 2021. URL: https://doi.org/10.1007/s00542-020-05138-4.

12. Blockchain industry 5.0: next generation smart contract and decentralized application platform / S. B et al. *2022 international conference on innovative computing, intelligent communication and smart electrical systems (ICSES)*, Chennai, India, 15–16 July 2022. 2022. URL: https://doi.org/10.1109/icses55317.2022.9914151.

Автори статті

Поляков Дмитро – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0002-5321-2448

Шикула Олена – доктор фізико-математичних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-7385-2816

Authors of the article

Poliakov Dmytro – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0002-5321-2448

Shykula Olena – Doctor of Sciences (physics and mathematics), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0002-7385-2816