Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)
https://doi.org/10.36930/40350513
Article received 24.09.2025
Article accepted 31.10.2025
UDC 004.[75+056.5]
Correspondence author: H. S. Yelisieieva hanna.s.yelisieieva@lpnu.ua

Г. С. Єлісєєва
Національний університет "Львівська політехніка", м. Львів, Україна

МОДЕЛЬ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ТРАНЗАКЦІЙ У БЛОКЧЕЙН-МЕРЕЖАХ ІЗ ДИНАМІЧНИМ УПРАВЛІННЯМ ПРАВАМИ ДОСТУПУ

Виявлено істотні обмеження сучасних підходів до захисту конфіденційності транзакцій у блокчейн-мережах, зокрема – недостатню гнучкість управління правами доступу до транзакцій в разі зміни ролей користувачів, етапів бізнес-процесу чи нормативних умов. Встановлено доцільність застосування гібридної моделі, що поєднує атрибутивне шифрування даних ABE (англ. *Attribute-Based Encryption* – шифрування на підставі атрибутів) із смарт-контрактною авторизацією, здатною автоматично змінювати політики доступу до даних протягом життєвого циклу документа без участі централізованого адміністратора. З'ясовано, що інтеграція ABE у блокчейн-середовище дає змогу відокремити криптографічний захист вмісту від логіки керування політиками доступу до даних, забезпечуючи децентралізованість, прозорий аудит і відтворюваність рішень доступу. Оцінено вплив параметрів шифрування даних, розміру множини атрибутів доступу і частоти оновлення політики доступу до даних на продуктивність транзакцій у приватному тестовому середовищі Ethereum (Solidity 0.8.20, CharmCrypto). Встановлено, що додаткові накладні витрати залишаються в межах прийнятних регламентів для систем електронного документообігу. Охарактеризовано закономірності масштабування системи: збільшення кількості користувачів і ролей зумовлює лінійне зростання тривалості оновлення політики доступу до даних за збереження локальності криптографічних операцій і стабільності пропускної здатності мережі. Оцінено вплив мережевих затримок, варіативності складності транзакцій та нестабільності тривалості формування блоків. Показано, що їхній ефект нівелюється повторними вимірюваннями, нормалізацією серій і використанням подієвих тригерів у смарт-контрактах. Сформульовано практичні рекомендації для впровадження системи: профілювання атрибутів доступу і життєвих циклів документів, ведення журналів подій для трасування рішень, застосування політик доступу до мінімальних привілеїв і регламентів зміни ролей. Доведено, що поєднання атрибутивного шифрування даних і смарт-контрактів забезпечує контекстно-залежне, кероване розкриття інформації та підвищує рівень її приватності без втрати прозорості, відтворюваності й довіри до децентралізованих процесів. Отримані результати підтверджують практичну доцільність розробленої моделі для державних і корпоративних систем, де критичною є не тільки безпека, а й відтворюваність політики доступу до даних в часі.

Ключові слова: електронний документообіг; криптографічна політика доступу до даних; шифрування на підставі атрибутів доступу; смарт-контрактна авторизація; подієве журналювання; децентралізовані реєстри.

Вступ / Introduction

У сучасному світі електронний документообіг є ключовим елементом цифрової трансформації державного сектору. Забезпечення конфіденційності транзакцій у таких системах залишається складним завданням, особливо в децентралізованих середовищах, побудованих на технології блокчейн. Традиційні централізовані системи управління доступом RBAC (англ. *Role-Based Access Control* – керування доступом на основі ролей) та IBAC (англ. *Identity-Based Access Control* – керування доступом на основі ідентичності користувача) не забезпечують достатньої гнучкості у випадках, коли відсутній єдиний адміністратор, а роль користувача може змінюватися залежно від контексту взаємодії.

У світовій науковій літературі досліджують низку підходів до захисту конфіденційності транзакцій у блокчейн-мережах, зокрема – використання технологій Zero-Knowledge Proofs, Federated Blockchain Security та Homomorphic Encryption. Проте, більшість із них зосереджуються на захисті вмісту транзакцій, а не на гнучкому управлінні правами доступу до транзакцій, що залишається відкритою проблемою.

Актуальність дослідження зумовлена потребою у створенні моделі, яка дає змогу динамічно змінювати політику доступу до даних без централізованого контролю. Одним із перспективних підходів є застосування атрибутивного шифрування даних ABE (англ. *Attribute-Based Encryption*), яке забезпечує криптографічне розмежування доступу до даних на підставі атрибутів доступу користувачів. Водночас, статичні політики доступу до даних не враховують змін контексту або ролей користувачів під час виконання бізнес-процесів. Тому запропоновано об'єднати ABE та смарт-контракти для реалізації динамічного управління правами доступу до транзакцій у блокчейн-середовищі, що дасть змогу автоматично оновлювати політики доступу до даних залежно від подій життєвого циклу документа.

Об'єкт дослідження – захист конфіденційності транзакцій у блокчейн-мережах.

Інформація про автора:
Єлісєєва Ганна Сергіївна, д-р філософії, ст. викладач, кафедра безпеки інформаційних технологій.
Email: hanna.s.yelisieieva@lpnu.ua; https://orcid.org/0009-0009-5555-2703
Цитування за ДСТУ: Єлісєєва Г. С. Модель захисту конфіденційності транзакцій у блокчейн-мережах із динамічним управлінням правами доступу. Науковий вісник НЛТУ України. 2025, т. 35, № 5. С. 116–121.
Citation APA: Yelisieieva, H. S. (2025). Model for transaction privacy protection in blockchain networks with dynamic access control management. *Scientific Bulletin of UNFU*, 35(5), 116–121. https://doi.org/10.36930/40350513

Предмет дослідження – методи динамічного управління правами доступу до транзакцій на підставі атрибутивного шифрування даних і смарт-контрактів, що дасть змогу визначити рівень підвищення їхньої безпеки та зниження ризику несанкціонованого доступу.

Мета роботи – розробити гібридну модель захисту конфіденційності транзакцій у блокчейн-системах електронного документообігу, яка забезпечить динамічне управління правами доступу до них без централізованого адміністратора.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати сучасні підходи до захисту конфіденційності транзакцій у блокчейн-середовищах, що дасть змогу виявити переваги та обмеження наявних рішень і обґрунтувати необхідність поєднання криптографічних і смарт-контрактних механізмів;
- розробити архітектуру моделі динамічного управління правами доступу до транзакцій, що забезпечить автоматизоване оновлення політики доступу до даних без участі централізованого адміністратора;
- оцінити ефективність інтеграції атрибутивного шифрування даних і смарт-контрактів у системах електронного документообігу, що дасть змогу визначити рівень підвищення їхньої безпеки та зниження ризику несанкціонованого доступу;
- експериментально перевірити вплив параметрів моделі на продуктивність транзакцій, що дасть змогу оцінити масштабованість системи та баланс між рівнем захисту й обчислювальними витратами.

Аналіз останніх досліджень та публікацій. Проблематика забезпечення конфіденційності транзакцій у блокчейн-мережах є предметом активних досліджень у світовій науковій літературі, починаючи від роботи [11], у якій сформульовано принципи децентралізованого обліку без довіреного посередника. Хоча ця модель усунула потребу в централізованій перевірці транзакцій, вона, водночас, створила складнощі у розбудові політики доступу до даних і захисту чутливих даних.

У подальших роботах [3, 4] узагальнено архітектурні виклики блокчейну, зокрема – обмеженість масштабування та відсутність ефективних механізмів управління конфіденційністю транзакцій. Розвиток технологій ZKP (англ. *Zero-Knowledge Proofs*) у працях [1, 3] відкрив нові можливості для проведення анонімних транзакцій, однак не вирішив питання динамічного контролю доступу до них й породив значні обчислювальні витрати.

Одним із напрямів вирішення цієї проблеми є гомоморфне шифрування даних, яке дає змогу виконувати обчислення над зашифрованими даними [6]. Проте, як зазначено у роботі [15], значна обчислювальна складність цього методу робить його малопридатним для систем із великою кількістю транзакцій, особливо державного рівня.

Гнучкішим підходом є атрибутивне шифрування даних ABE (англ. *Attribute-Based Encryption*), запропоноване у роботі [2] і розвинене в роботі [12] у схемі CP-ABE, що дає змогу власнику даних самостійно визначати політики доступу до даних. Подальші дослідження, як у праці [21], підтвердили практичність цього підходу, але наголосили на його статичності.

У контексті блокчейну в роботах [8, 23] показано, що смарт-контракти можуть забезпечити децентралізоване виконання логіки доступу. Втім, без додаткових криптографічних механізмів ці рішення не гарантують конфіденційності самого вмісту транзакцій.

Публікації [9, 23] демонструють спроби поєднати атрибутивне шифрування даних зі смарт-контрактами, проте здебільшого зосереджуються на завданнях ідентифікації користувачів або розмежування ролей, а не на автоматичному оновленні політики доступу до даних упродовж життєвого циклу документа.

Отже, попри значний прогрес у криптографічних механізмах та децентралізованих моделях управління правами доступу до даних, завдання поєднання гнучкого динамічного контролю доступу з повною конфіденційністю транзакцій залишається невирішеним. Це визначає актуальність розроблення гібридної моделі, яка інтегрує атрибутивне шифрування даних і смарт-контракти в єдину архітектуру захисту даних для блокчейн-середовищ.

Матеріали та методи дослідження. Матеріалами для проведення дослідження стали наукові публікації, в яких розглянуто проблеми забезпечення конфіденційності транзакцій у блокчейн-мережах, роботу криптографічних систем із розмежування доступу та впровадження атрибутивного шифрування даних ABE (англ. *Attribute-Based Encryption*) у децентралізованих середовищах. Проаналізовано понад 50 джерел, серед яких праці з теорії розподілених систем, статті міжнародних видань з кібербезпеки, результати попередніх досліджень щодо смарт-контрактів і політики доступу до даних, а також нормативно-правові акти у сфері захисту інформації. Емпіричними матеріалами були експериментальні дані, отримані в процесі моделювання транзакцій у тестовому середовищі приватного блокчейну Ethereum (версія 1.12.2) з використанням бібліотеки Charm-Crypto та смарт-контрактів, реалізованих мовою Solidity (версія 0.8.20).

Результати дослідження та їх обговорення / Research results and their discussion

Для досягнення поставленої мети використано комплекс теоретичних, емпіричних і прогностичних методів дослідження.

До теоретичних методів належать критичний аналіз і систематизація наукових праць, що стосуються криптографічного захисту даних і динамічного управління доступом; узагальнення відомих підходів до поєднання шифрування даних і смарт-контрактів; формалізація моделі динамічного управління політиками доступу до даних у вигляді архітектурної схеми.

До емпіричних методів належать моделювання процесів шифрування даних, їх розшифрування, розроблення та оновлення політики доступу до даних в умовах тестової блокчейн-мережі. Під час експериментів здійснювали вимірювання затримки транзакцій, обсягів службових даних і частоти оновлення політики доступу до даних. Для оброблення експериментальних результатів застосовано методи статистичного аналізу, усереднення вибірок і нормалізації показників.

Прогностичні методи містили процедуру оцінювання масштабованості розробленої моделі, прогнозування зміни її ефективності за збільшення кількості користувачів, атрибутів доступу і транзакцій, а також визначення балансу між рівнем конфіденційності транзакцій та обчислювальними витратами.

Комплексне застосування наведених методів дало змогу розробити обґрунтовану гібридну модель захисту конфіденційності транзакцій із динамічним управлін-

ням правами доступу до транзакцій, що забезпечує кероване розкриття інформації у децентралізованому середовищі без участі централізованого адміністратора.

Архітектура гібридної моделі. Запропонована гібридна модель передбачає поєднання механізмів атрибутивного шифрування даних ABE (англ. *Attribute-Based Encryption*) зі смарт-контрактами для реалізації динамічного управління правами доступу до транзакцій у блокчейн-середовищі. Основною ідеєю є розмежування функцій між криптографічним рівнем, що відповідає за захист змісту даних, і рівнем керування політики доступу до даних, який реалізується у вигляді смарт-контрактів.

На етапі ініціалізації система формує набір атрибутів доступу користувачів (роль, організаційна належність, рівень довіри, стадія процесу тощо), а також публічні та приватні ключі для ABE-схеми. Коли створюється транзакція або документ, його шифрують відповідно до політики доступу до даних у форматі дерева атрибутів доступу до них, визначеної власником даних.

Структурну взаємодію компонент гібридної моделі наведено на рис. 1, де показано взаємозв'язок між рівнем користувачів, криптографічним рівнем, рівнем смарт-контрактів і блокчейн-реєстром.

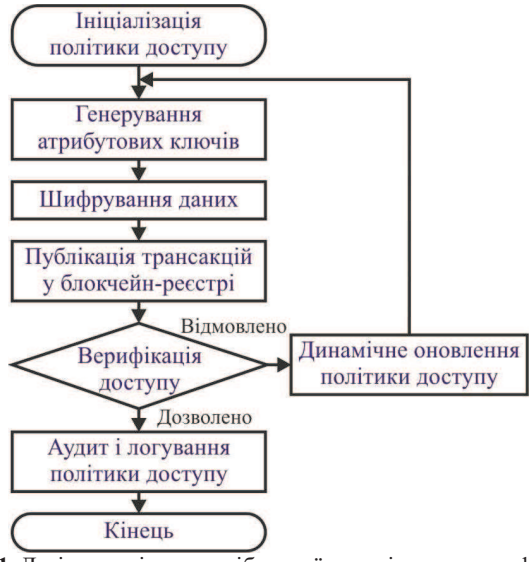

Рис. 1. Логічна архітектура гібридної моделі захисту конфіденційності транзакцій у блокчейн-мережах / Logical architecture of the hybrid model for transaction confidentiality protection in blockchain networks

На рис. 1 подано послідовність етапів функціонування гібридної моделі, що поєднує атрибутивне шифрування даних зі смарт-контрактами. Модель складається із семи основних блоків: ініціалізація політики доступу до даних, генерування атрибутивних ключів, шифрування даних, публікація транзакції у блокчейні, верифікація доступу (умовне розгалуження "дозволено/відмовлено"), динамічне оновлення політики доступу до даних та аудит із журналюванням подій. Така архітектура забезпечує гнучке управління правами доступу до транзакцій й підтримує конфіденційність інформації в умовах децентралізованого середовища.

Смарт-контракт, розміщений у блокчейні, зберігає метадані політики доступу до даних і автоматично змінює її стан у разі подій (підписання, затвердження, зміна ролі). Усі оновлення політики доступу до даних фіксуються у блокчейні, що гарантує аудитованість і неможливість підміни правил доступу. Зміна ролі користувача ініціює подію смарт-контракту, яка автоматично оновлює політику доступу до даних, не вимагаючи централізованого адміністратора.

Послідовність виконання операцій перевірки доступу до даних у системі подано у вигляді алгоритмічної схеми (рис. 2), де визначено основні етапи – ініціалізацію параметрів, шифрування даних, реєстрацію транзакції у блокчейні, перевірку атрибутів доступу користувача через смарт-контракт і розшифрування даних у разі позитивної авторизації.

Рис. 2. Алгоритмічна схема перевірки доступу до даних у гібридній моделі / Algorithmic scheme for data access verification in the hybrid model

Отже, система реалізує гнучке керування конфіденційністю транзакцій з урахуванням контексту процесу та дає змогу автоматично адаптувати політики доступу до даних без участі адміністратора.

Методика проведення дослідження. Для оцінювання ефективності запропонованої моделі було створено експериментальне середовище на підставі тестової блокчейн-мережі Ethereum (версія 1.12.2). Смарт-контракти реалізовано мовою Solidity 0.8.20, а операції атрибутивного шифрування даних виконувались із використанням бібліотеки Charm-Crypto (Python 3.10).

У межах дослідження змодельовано 50 транзакцій з різною кількістю користувачів (від 10 до 200) та різними наборами атрибутів доступу. Для кожного сценарію фіксувалися такі показники:

- середня тривалість шифрування даних та їх розшифрування;
- тривалість оновлення політики доступу до даних;
- затримка транзакцій за оновлення політики доступу до даних;
- обсяг переданих метаданих і споживання пам'яті смарт-контрактами.

Отримані дані усереднювались за п'ятьма незалежними серіями запусків для зменшення випадкових коливань. Розрахунки виконувались на вузлах з процесорами Intel Core i7-11700 (2,5 GHz), 16 GB RAM, у середовищі Ubuntu 22.04. Для порівняння ефективності системи застосовано базову модель зі статичними політиками доступу до даних, що дало змогу оцінити відносне зростання затримки транзакцій та скорочення обсягу переданих.

Основними джерелами потенційних похибок є затримки мережевої взаємодії між вузлами, варіації складності транзакцій та нестабільність часу блоків у тестовому середовищі. Їхній вплив мінімізовано шляхом повторних вимірювань, нормалізації даних і порівняння результатів між серіями експериментів.

Результати дослідження. Розроблена гібридна модель забезпечення конфіденційності транзакцій у блокчейн-системах продемонструвала узгодженість між криптографічними механізмами та децентралізованою логікою управління політиками доступу до даних.

Під час експериментального моделювання було підтверджено, що поєднання атрибутивного шифрування даних (ABE) зі смарт-контрактами дає змогу динамічно змінювати політики доступу до даних без участі цен-

тралізованого адміністратора, зберігаючи при цьому повну прозорість і аудитованість процесів у розподіленому реєстрі.

Результати моделювання свідчать, що використання смарт-контрактів як механізму контролю політики доступу до даних не призводить до істотного збільшення часу транзакцій, а навпаки – удосконалює оброблення запитів завдяки паралельній перевірці атрибутів доступу. Це дає змогу зменшити кількість дублювань у запитах до реєстру та скоротити обсяг переданих службових метаданих.

Аналіз взаємодії між рівнями системи показав, що атрибутивне шифрування даних ефективно ізолює їхній вміст навіть у разі компрометації окремого вузла або учасника мережі. Завдяки динамічному оновленню політики доступу до даних, кожна зміна статусу користувача (наприклад, підписання документа чи зміна ролі) автоматично тягне за собою оновлення умов доступу до даних, що вилучає нагромадження "застарілих" дозволів.

Використання гібридного підходу також сприяє рівномірному розподілу навантаження між криптографічним модулем і смарт-контрактом. Етапи шифрування даних і їх розшифрування відбуваються локально на стороні користувача, тоді як перевірка політики доступу до даних виконується у мережі, що мінімізує ризик витоку ключів або метаданих.

Криптографічна компонента, заснована на атрибутивному шифруванні, забезпечує відокремлення змісту транзакцій від логіки управління правами доступу, що усуває ризики несанкціонованого аналізу даних навіть у разі компрометації одного з вузлів мережі. Такий розподіл функцій дає змогу досягти балансу між конфіденційністю транзакцій та доступністю інформації, що було одним із ключових недоліків ранніх моделей на базі Zero-Knowledge Proofs.

Водночас, результати моделювання підтвердили, що впровадження смарт-контрактів як засобу контролю політики доступу до даних не спричиняє істотного зростання затримки транзакцій, що узгоджується з висновками роботи [10] щодо можливості оптимізації обчислювальних витрат у гібридних криптосистемах.

Отже, підтверджено наукову та практичну доцільність виконаного дослідження, а його результати створюють підґрунтя для подальшого розроблення державних і корпоративних систем електронного документообігу з підвищеним рівнем конфіденційності транзакцій.

Отримані результати дослідження підтвердили, що запропонована архітектура моделі є придатною для використання у системах електронного документообігу, де вимагається високий рівень довіри, відстежуваності та динамічного оновлення прав доступу до даних. Гібридну модель можна адаптувати для корпоративних середовищ, державних реєстрів та систем із багаторівневою структурою користувачів, забезпечуючи як технічну, так і організаційну безпеку інформаційних потоків.

Обговорення результатів дослідження. Отримані результати підтверджують, що динамічне управління правами доступу до транзакцій у блокчейн-мережах можна ефективно реалізувати шляхом інтеграції атрибутивного шифрування даних зі смарт-контрактами. Це узгоджується із сучасними тенденціями розвитку блокчейн-технологій, окресленими у дослідженні [22], де підкреслено необхідність поєднання криптографічних і архітектурних рішень для підвищення конфіденційності транзакцій й масштабованості систем.

Подібні підходи до атрибутно орієнтованого контролю доступу розглянуто у працях [13, 17], однак більшість із них залишаються статичними, не враховуючи змін контексту користувача або подій у бізнес-процесі. Запропонована модель усуває це обмеження завдяки подієвому оновленню політики доступу до даних смарт-контрактами без участі адміністратора.

Історично важливим є напрям обчислень над зашифрованими даними [23], але такі схеми залишаються ресурсомісткими для транзакційних навантажень. Натомість запропонована архітектура розділяє функції криптографічного захисту та перевірки політики доступу до даних, забезпечуючи кероване їх розкриття із мінімальними обчислювальними витратами на рівні ланцюга.

Запропонована архітектура узгоджується з принципами побудови надійних і масштабованих розподілених систем [21] та архітектурними підходами до блокчейн-застосунків [19], але розширює їх за рахунок динамічного механізму реакції на зміни атрибутів доступу користувачів. Це дає змогу зберегти баланс між децентралізованим контролем і гнучкістю політики доступу до даних.

Дослідження [8] доводить ефективність політик адаптації у процесі конфіденційного обміну даними, проте не враховує криптографічної сегментації контенту. У нашій моделі це реалізовано через розподіл логіки доступу (контракт) і шифрування даних (ABE), що підвищує стійкість до компрометації вузлів мережі. Подібний принцип комбінованої ізоляції даних застосовано у роботі [17], але без урахування контекстних залежностей атрибутів доступу до даних, які в нашій роботі реалізуються через динамічні ключі доступу.

Тонке розмежування прав доступу в децентралізованих системах на підставі ABE описано у роботі [10], однак процес оновлення політик доступу до них там переважно ручний і не враховує часової динаміки. У нашому рішенні реалізовано часово- та подієво-залежне оновлення правил, що усуває нагромадження "застарілих" дозволів і знижує ризики за делегування ролей.

Гібридні рішення для державних систем, орієнтовані на приватність [5], зазвичай не забезпечують локального виконання криптографічних операцій. У нашій архітектурі цей недолік усунуто: шифрування даних і їх розшифрування виконуються на стороні користувача, а перевірка політики доступу до даних – у мережі, що підвищує безпечність і масштабованість.

Адаптивне управління доступом у permissioned-мережах розглянуто в роботах [18, 20], проте його ефективність часто спирається на довіру до адміністраторів. У нашій моделі смарт-контракт виконує роль автономного контролера політики доступу до даних, фіксуючи всі зміни в реєстрі, що забезпечує прозорість і аудитованість без централізованого втручання.

Окрім цього, сучасні праці [13, 18] акцентують увагу на самонавчальних системах контролю доступу до даних, де політики доступу до них адаптуються на підставі поведінкових характеристик користувачів. Запропонована архітектура є сумісною з цим підходом і може бути розширена засобами машинного навчання для прогнозування змін політики доступу до даних у режимі реального часу.

Узагальнення проведеного обговорення результатів дослідження показує, що результати, які ми отримали, узгоджуються з актуальними науковими тенденціями,

проте перевершують наявні рішення завдяки комплексному поєднанню атрибутивного шифрування даних і смарт-контрактів у єдиній гібридній архітектурі. Запропонована модель забезпечує динамічне оновлення політики доступу до даних, повну аудитованість подій і збереження децентралізованості без потреби в адміністративному контролі.

Загалом, проведене обговорення результатів дослідження показує, що розглянуті роботи не поєднують подієву динамічність, атрибутивне шифрування даних і автономне оновлення політик доступу до них у межах єдиної гібридної моделі.

Отже, внаслідок виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – розроблено гібридну модель захисту конфіденційності транзакцій у блокчейн-системах електронного документообігу, яка поєднує атрибутивне шифрування даних й смарт-контракти, а також забезпечує реалізацію динамічного управління політиками доступу до даних без участі централізованого адміністратора.

Практична значущість результатів дослідження – можливе впровадження розробленої моделі в державних і корпоративних системах електронного документообігу з підвищеним рівнем вимог до конфіденційності транзакцій.

Висновки / Conclusions

Розроблено гібридну модель захисту конфіденційності транзакцій у блокчейн-системах електронного документообігу, яка забезпечує динамічне управління правами доступу до транзакцій без централізованого адміністратора. За результатами проведеного дослідження можна зробити такі основні висновки.

1. Розроблено гібридну модель захисту конфіденційності транзакцій у блокчейн-мережах із динамічним управлінням правами доступу до транзакцій, що поєднує атрибутивне шифрування даних (ABE) та смарт-контракти.
2. Доведено, що запропонована модель забезпечує автоматичне оновлення політики доступу до даних під час зміни ролей користувачів або етапів бізнес-процесу, усуваючи потребу у централізованому адмініструванні.
3. Проведено експериментальне дослідження ефективності моделі, яке показало, що динамічне управління доступом до транзакцій не призводить до істотного зростання їхньої затримки і зменшує обсяг службових даних у мережі.
4. Встановлено, що розподіл функцій між криптографічним модулем і смарт-контрактом забезпечує високий рівень конфіденційності, цілісності даних і стійкість до компрометації окремих вузлів блокчейну.
5. З'ясовано, що гібридний підхід підтримує децентралізованість процесу управління політиками доступу до даних і прозорість перевірки політик доступу до них без участі адміністратора.
6. Підтверджено, що запропоновану архітектуру моделі захисту конфіденційності транзакцій у блокчейн-мережах можна впровадити в корпоративних, державних і фінансових системах електронного документообігу з підвищеними вимогами до конфіденційності даних.
7. Окреслено перспективи етапів подальшого дослідження, які полягають у розширенні моделі засобами машинного навчання для прогнозування змін політики доступу до даних і адаптації системи до поведінкових характеристик користувачів.

References

1. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. 2014 *IEEE Symposium on Security and Privacy* (*SP*), Berkeley, CA, USA, 459–474. https://doi.org/10.1109/SP.2014.36
2. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. 2007 *IEEE Symposium on Security and Privacy* (*SP 07*), *Berkeley, CA, USA*, 321–334. https://doi.org/10.1109/SP.2007.11
3. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short proofs for confidential transactions and more. 2018 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, CA, USA, 315–334. https://doi.org/10.1109/SP.2018.00020
4. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review, 2*, 6–10. URL: https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf
5. Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving e-government system. Wireless Networks, 29, 1005–1015. https://doi.org/10.1007/s11276-018-1883-0
6. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. STOC 09: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* (*STOC*), 169–178. https://doi.org/10.1145/1536414.1536440
7. Hu, V. C., Ferraiolo, D. R., & Kuhn, D. R. (2015). Attribute-based access control. *IEEE Computer, 48*(2), 85–88. https://doi.org/10.1109/MC.2015.33
8. Hu, V. C., Kuhn, D. R., Ferraiolo, D. R., & Voas, J. (2022). Blockchain for Access Control Systems (NIST IR 8403). Gaithersburg, MD: NIST, 1–21. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8403.pdf
9. Kim, H., Park, J., & Kim, J. (2021). Federated blockchain security: Combining distributed learning and decentralized control. *IEEE Access, 9*, 102942–102953. https://doi.org/10.1109/ACCESS.2021.3097004
10. Lu, X., et al. (2021). A Fine-Grained IoT Data Access Control Scheme Combining Attribute-Based Encryption and Blockchain. *Security and Communication Networks*, 2021, article ID 5308206, 13 p. https://doi.org/10.1155/2021/5308206
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, 1–9 p. URL: https://bitcoin.org/bitcoin.pdf
12. Nguyen, T., & Hoang, D. (2021). Policy-driven access management in enterprise blockchain ecosystems. *Future Internet, 13*(4), article ID 95. https://doi.org/10.3390/fi13040095
13. Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management. *IEEE Internet of Things Journal*, *5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239
14. Ouaddah, A., Elkalam, A., & Ouahman, A. A. (2017). FairAccess: a new Blockchain-based access control framework for the IoT. *Security and Communication Networks*, *9*(18), 5943–5964. https://doi.org/10.1002/sec.1748
15. Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation*, 169–180. URL: https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf
16. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. *EUROCRYPT 2005*, 457–473. https://doi.org/10.1007/11426639_27
17. Sylla, T., Mendiboure, L., Chalouf, M. A., & Krief, F. (2021). Blockchain-Based Context-Aware Authorization Management as a Service in IoT. *Sensors*, *21*(22), article ID 7656. https://doi.org/10.3390/s21227656
18. Wang, Y., & Zhao, Q. (2023). Privacy-preserving attribute policies in distributed ledger systems. *Early Access, IEEE Transactions on Dependable and Secure Computing*, *22*(1), 170–183. https://doi.org/10.1109/TDSC.2023.3278931

19. Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. *Cham: Springer*, 307 p. https://doi.org/10.1007/978-3-030-03035-3
20. Zaidi, S. Y. A., Shah, M. A., Khattak, H. A., Maple, C., Rauf, H. T., El-Sherbeeny, A. M., & El-Meligy, M. A. (2021). An attribute-based access control for IoT using blockchain and smart contracts. *Sustainability*, *13*(19), article ID 10556. https://doi.org/10.3390/su131910556
21. Zhang, K., & Jacobsen, H.-A. (2018). Towards dependable, scalable, and pervasive distributed ledgers with blockchains. 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 1337–1346. https://doi.org/10.1109/ICDCS.2018.00134
22. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.10016848
23. Zhonghua, C. (2023). Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing. *The Journal of Supercomputing*, *79*(12), 13734–13756. https://doi.org/10.1007/s11227-023-05517-4

H. S. Yelisieieva

Lviv Polytechnic National University, Lviv, Ukraine

MODEL FOR TRANSACTION PRIVACY PROTECTION IN BLOCKCHAIN NETWORKS WITH DYNAMIC ACCESS CONTROL MANAGEMENT

This study identifies core limitations of privacy-preserving techniques in blockchain networks, notably the lack of flexible, context-aware access control when user roles, process stages, or compliance constraints change. To overcome these constraints, we propose a hybrid privacy model that couples Attribute-Based Encryption (ABE) with smart-contract authorization so that access policies are updated dynamically by on-chain event triggers. The architecture deliberately separates cryptographic content protection from policy-management logic, ensuring decentralization, transparency, and verifiable auditability without a central authority. The methodology comprised (1) designing the logical architecture, (2) implementing Solidity contracts and ABE modules within an Ethereum-based testbed, and (3) evaluating performance under varied encryption parameters, attribute set cardinality, policy-update frequency, and numbers of active users (10–200). Moreover, we executed five independent runs per scenario, normalized results, and analyzed network-delay sensitivity to mitigate random fluctuations. The findings show that transaction latency remains within acceptable thresholds for state and corporate e-document systems; scalability exhibits a near-linear trend in policy-update time as user and role counts grow, while cryptographic operations remain local to clients. Consequently, the integration of smart contracts with cryptographic policy enforcement enables traceable decision-making and event-based logging, producing a transparent audit trail for all access actions and policy transitions. Resource-consumption profiling indicates controllable gas overhead for policy updates and stable throughput under moderate load. As a result, the model supports controlled, context-aware disclosure aligned with least-privilege principles and lifecycle policies. The benefits of this study include a practical framework for deploying hybrid access control in decentralized infrastructures, implementation guidelines for attribute profiling and audit governance, and a roadmap for future optimizations such as multi-authority ABE, selective re-encryption, and improved crypto-blockchain interoperability.

Keywords: data confidentiality; cryptographic data access policy; attribute-based encryption; smart-contract authorization; event-based logging; decentralized infrastructures.