https://doi.org/10.31891/2219-9365-2026-85-26
УДК 004.056:004.75

ГРИГОР'ЄВ Костянтин
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0003-1316-4354
prizma2098@gmail.com
ПАВЛЕНКО Володимир
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0002-3958-0415
pavlenko.v@i.ua

СИСТЕМА ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТРАНЗАКЦІЙ З ДАНИМИ З ВИКОРИСТАННЯМ ПРОТОКОЛІВ НУЛЬОВОГО РОЗГОЛОШЕННЯ

У статті розглянуто проблему забезпечення конфіденційності транзакцій з даними в сучасних розподілених інформаційних системах, зокрема у блокчейн-мережах, фінансових платформах та міжорганізаційних транзакційних середовищах. Показано, що традиційні криптографічні механізми, орієнтовані на шифрування каналів або збережених даних, не дозволяють одночасно забезпечити публічну верифікованість транзакцій і приховування їхнього внутрішнього змісту. У роботі запропоновано системний підхід до забезпечення конфіденційності транзакцій на основі протоколів нульового розголошення знань zk-SNARKs та zk-STARKs.

Розроблено архітектуру системи забезпечення конфіденційності транзакцій, у якій визначено модель транзакції з відокремленням відкритих параметрів і прихованих даних, а також визначено механізм формування та верифікації криптографічних доказів коректності без розкриття чутливої інформації. Запропоновано узагальнену модель транзакції з нульовим розголошенням, що дозволяє підтверджувати виконання заданих обмежень на основі формально перевірюваних доказів. Проаналізовано особливості використання протоколів zk-SNARKs та zk-STARKs у складі системи, виконано їх порівняльний аналіз з урахуванням розміру доказів, обчислювальних витрат, вимог до ініціалізації та криптографічної стійкості. Показано, що інтеграція обох протоколів у єдину архітектурну модель забезпечує адаптивність системи до різних транзакційних сценаріїв і вимог середовища виконання. Отримані результати підтверджують, що запропонована система перевершує наявні підходи за рівнем конфіденційності, верифікованості та гнучкості інтеграції, створюючи передумови для її практичного застосування у розподілених транзакційних системах.

Ключові слова: конфіденційність транзакцій, нульове розголошення знань, zk-SNARKs, zk-STARKs, розподілені системи, криптографічна верифікація.

HRYHORIEV Kostiantyn, PAVLENKO Volodymyr
Open International University of Human Development Ukraine

SYSTEM FOR ENSURING CONFIDENTIALITY OF DATA TRANSACTIONS USING ZERO DISCLOSURE PROTOCOLS

The paper addresses the problem of ensuring transaction data confidentiality in modern distributed information systems, including blockchain networks, financial platforms, and inter-organizational transaction environments. It is shown that traditional cryptographic mechanisms focused on channel encryption or data storage protection do not provide a balance between public transaction verifiability and concealment of internal transaction semantics. To overcome this limitation, a system-based approach to transaction confidentiality using zero-knowledge proof protocols zk-SNARKs and zk-STARKs is proposed.

An architecture of a transaction confidentiality assurance system is developed, within which a formal transaction model is defined by separating public parameters from private data. A mechanism for generating and verifying cryptographic proofs of transaction correctness without disclosing sensitive information is described. A generalized zero-knowledge transaction model is introduced, enabling verification of predefined constraints based on formally provable cryptographic evidence. The characteristics of zk-SNARKs and zk-STARKs are analyzed in the context of the proposed system, and a comparative evaluation is performed considering proof size, computational costs, initialization requirements, and cryptographic resilience.

The study demonstrates that integrating both protocols within a unified architectural framework enables adaptive selection of proof mechanisms depending on transaction characteristics and execution environment constraints. The obtained results confirm that the proposed system outperforms existing solutions in terms of confidentiality level, verification reliability, and architectural flexibility. The proposed approach provides a practical foundation for deploying zero-knowledge-based confidentiality mechanisms in real-world distributed transaction processing systems.

Keywords: transaction confidentiality, zero-knowledge proofs, zk-SNARKs, zk-STARKs, distributed systems, cryptographic verification.

Стаття надійшла до редакції / Received 06.12.2025
Прийнята до друку / Accepted 19.01.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні інформаційно-комунікаційні системи характеризуються стрімким зростанням обсягів транзакцій з даними, які обробляються у розподілених середовищах, зокрема у фінансових платформах,

блокчейн-мережах, системах електронної комерції, міжорганізаційних облікових системах та кіберфізичних інфраструктурах. У таких системах транзакції часто містять чутливі відомості про учасників, структуру операцій, обсяги ресурсів або логіку взаємодії, що створює суттєві ризики порушення конфіденційності у разі перехоплення, аналізу або кореляції переданих даних [1]. Традиційні криптографічні механізми, зокрема симетричне та асиметричне шифрування, орієнтовані переважно на захист каналів зв'язку або збережених даних, однак не забезпечують приховування семантики транзакцій під час їх перевірки, аудиту чи консенсусної обробки у відкритих або напіввідкритих системах [2, 3].

Особливої актуальності проблема конфіденційності набуває в умовах використання децентралізованих реєстрів і публічних обчислювальних платформ, де коректність транзакцій повинна перевірятись для всіх учасників, але без розкриття внутрішнього змісту самих даних [4]. Це породжує суперечність між вимогами прозорості, верифікованості та довіри, з одного боку, і необхідністю обмеження доступу до чутливої інформації – з іншого. Наявні підходи до анонімізації, маскування або агрегування даних не гарантують криптографічно доведеної стійкості та часто є вразливими до повторної ідентифікації або побічного аналізу [5].

У цьому контексті протоколи нульового розголошення знань, зокрема zk-SNARKs та zk-STARKs, розглядаються як перспективний інструмент побудови систем, у яких можливе доведення коректності транзакцій без розкриття їхнього змісту [6]. Застосування таких протоколів дозволяє формувати нову парадигму обробки транзакційних даних, де перевірка виконання правил, обмежень або бізнес-логіки здійснюється на основі криптографічних доказів, а не відкритих даних. Разом з тим, практичне впровадження протоколів нульового розголошення пов'язане з низкою наукових і прикладних викликів, серед яких обчислювальна складність генерації доказів, вимоги до пам'яті, затримки верифікації, масштабованість системи та адаптація до різних типів транзакційних моделей.

Наявність зазначених невирішених питань істотно обмежує можливості практичного застосування протоколів zk-SNARKs та zk-STARKs у реальних інформаційних системах, зокрема в середовищах з обмеженими обчислювальними ресурсами або високими вимогами до пропускної здатності. Це зумовлює необхідність розробки системного підходу до побудови механізмів конфіденційності транзакцій, який поєднує формальні властивості протоколів нульового розголошення з практичними вимогами до продуктивності, надійності та інтеграції у сучасні архітектури обробки даних.

Метою дослідження є розробка та обґрунтування системи забезпечення конфіденційності транзакцій з даними на основі протоколів нульового розголошення знань zk-SNARKs та zk-STARKs з урахуванням вимог до верифікованості, ефективності та практичної реалізовності у розподілених інформаційних системах.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Розвиток криптографічних протоколів нульового розголошення знань став предметом активних наукових досліджень у зв'язку з поширенням децентралізованих обчислювальних платформ і зростанням вимог до конфіденційності транзакційних даних. Перші фундаментальні роботи у цій галузі були зосереджені на теоретичних засадах zero-knowledge proof та визначення властивостей повноти, коректності й нульового розголошення, що створило основу для подальшого переходу від інтерактивних до неінтерактивних протоколів доведення [7, 8]. Подальший розвиток досліджень привів до появи zk-SNARKs як класу компактних неінтерактивних доказів з коротким розміром та швидкою верифікацією, що зробило їх придатними для використання у блокчейн-системах і розподілених реєстрах [9].

У наукових публікаціях значна увага приділяється питанням криптографічної стійкості zk-SNARKs, зокрема проблемам довірчої ініціалізації, використанню еліптичних кривих і парингових операцій, а також ризикам компрометації початкових параметрів [10]. У відповідь на ці обмеження було запропоновано протоколи zk-STARKs, які базуються на хеш-функціях та алгебраїчних перетвореннях, не потребують довірчої фази налаштування та забезпечують постквантову стійкість [11]. Дослідження у цьому напрямі фокусуються на підвищенні масштабованості та зменшенні обчислювальних витрат, водночас визнаючи збільшення розміру доказів порівняно з zk-SNARKs.

Окремий напрям наукових робіт присвячений застосуванню протоколів нульового розголошення у фінансових транзакціях, системах електронного голосування, анонімних платіжних мережах і корпоративних блокчейн-платформах. У таких публікаціях аналізується можливість приховування ідентичності учасників, значень транзакцій та логіки смарт-контрактів за умови збереження публічної перевірюваності. Водночас результати цих досліджень свідчать про суттєвий компроміс між рівнем конфіденційності та продуктивністю системи, що обмежує використання zk-протоколів у сценаріях з високою інтенсивністю транзакцій. Розглядаються питання інтеграції zk-SNARKs і zk-STARKs у архітектури розподілених систем у вигляді модулів генерації та верифікації доказів, а також їх вплив на затримки обробки транзакцій і споживання ресурсів [12]. Водночас більшість підходів обмежується експериментальними реалізаціями, залишаючи відкритими питання адаптації цих протоколів до реальних умов експлуатації з ресурсними та надійнісними обмеженнями.

Аналіз сучасних досліджень показує, що наявні наукові результати здебільшого зосереджені або на теоретичному вдосконаленні криптографічних протоколів, або на окремих сценаріях їх застосування, без формування цілісної системної моделі забезпечення конфіденційності транзакцій. Недостатньо уваги приділяється комплексному поєднанню властивостей zk-SNARKs та zk-STARKs із вимогами до продуктивності, масштабованості та практичної інтеграції у різнорідні інформаційні системи. Це зумовлює доцільність подальших досліджень, спрямованих на розробку системного підходу до використання протоколів нульового розголошення для захисту транзакційних даних з урахуванням реальних умов експлуатації та сучасних викликів інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Запропонована система забезпечення конфіденційності транзакцій з даними орієнтована на використання протоколів нульового розголошення знань як базового механізму підтвердження коректності операцій без розкриття їхнього внутрішнього змісту. Транзакція в системі розглядається як структурований об'єкт, що містить сукупність прихованих даних, набір обмежень або правил коректності та результат їх виконання, який може бути перевірений незалежними сторонами. Основним призначенням системи є забезпечення криптографічно обґрунтованої конфіденційності транзакцій за умови збереження можливості публічної або напівпублічної верифікації їх коректності.

Ключовим елементом системи є доказ коректності транзакції, який формується на основі протоколів zk-SNARKs або zk-STARKs та підтверджує виконання визначених правил без розкриття самих транзакційних даних. У цьому контексті zk-SNARKs та zk-STARKs виконують роль універсального інструменту криптографічної верифікації, що дозволяє відокремити процес перевірки правильності від доступу до чутливої інформації. Вибір конкретного протоколу у системі визначається вимогами до масштабованості, рівня довіри до початкових параметрів та обчислювальних ресурсів середовища виконання.

Система побудована за модульним принципом, що забезпечує гнучкість її адаптації до різних транзакційних сценаріїв та інформаційних платформ. Взаємодія між компонентами системи організована таким чином, щоб мінімізувати обсяг відкритих даних на кожному етапі обробки транзакції, зберігаючи при цьому можливість формальної перевірки її коректності. Такий підхід дозволяє використовувати систему як у децентралізованих реєстрах, так і в корпоративних або міжорганізаційних середовищах, де існують підвищені вимоги до конфіденційності.

Архітектура системи забезпечення конфіденційності транзакцій включає низку взаємопов'язаних функціональних модулів, кожен з яких відповідає за окремий етап обробки транзакційних даних. Узагальнену структурну схему системи наведено на рис. 1.

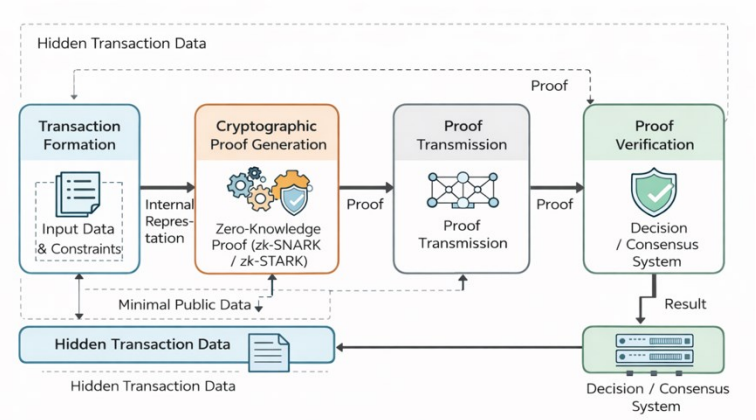

Рис. 1. Загальна архітектурна схема системи забезпечення конфіденційності транзакцій з даними

Модуль формування транзакції здійснює підготовку вхідних даних, визначає набір правил коректності та формує внутрішнє представлення транзакції, яке не підлягає розкриттю зовнішнім учасникам. На основі цього представлення модуль генерації криптографічного доказу створює доказ коректності транзакції відповідно до обраного протоколу zk-SNARKs або zk-STARKs. Сформований доказ передається разом із мінімальним набором відкритих параметрів до модуля верифікації, який здійснює перевірку коректності без доступу до прихованих даних.

Результатом роботи модуля верифікації є рішення щодо прийняття або відхилення транзакції, яке може бути використане системою консенсусу, журналом подій або іншим механізмом фіксації результатів. Така архітектура дозволяє чітко розмежувати обчислювально складні операції генерації доказів та відносно легковагові операції їх перевірки, що є принципово важливим для забезпечення масштабованості та практичної придатності системи.

У межах запропонованої системи транзакція з нульовим розголошенням даних розглядається як впорядкована сукупність відкритих параметрів та прихованих змінних, для яких необхідно довести виконання

заданих умов коректності. Нехай транзакція описується кортежем $T = \langle P, S, C \rangle$, де P – множина відкритих параметрів транзакції, доступних для перевірки всіма учасниками системи, S – множина прихованих даних, що містять чутливу інформацію, а C – множина логічних або арифметичних обмежень, які визначають коректність транзакції. Відкриті параметри можуть включати ідентифікатори, хеші станів або агреговані значення, тоді як приховані дані охоплюють реальні значення транзакцій, внутрішні стани або секретні ключі.

Коректність транзакції визначається виконанням предиката $C(P, S) = 1$, який визначає правила допустимості транзакції. У межах системи не передбачається передача множини S у відкритому вигляді, натомість формується криптографічний доказ π, що підтверджує істинність цього предиката. Таким чином, транзакція у системі подається у вигляді пари $\langle P, \pi \rangle$, де доказ π засвідчує існування таких прихованих даних S, для яких виконуються задані обмеження.

Відображення транзакційних даних у доказ коректності здійснюється за допомогою формальної моделі обчислення, що переводить обмеження C у відповідну арифметичну або логічну форму, придатну для застосування протоколів нульового розголошення. У загальному випадку ця модель може бути подана у вигляді системи рівнянь або схем обчислення, коректність виконання яких підтверджується без розкриття вхідних змінних. Такий підхід забезпечує строгий поділ між семантикою транзакції та механізмом її перевірки, що є принциповим для досягнення конфіденційності.

Формування доказів у запропонованій системі базується на використанні протоколів zk-SNARKs або zk-STARKs, які реалізують неінтерактивне доведення знань із властивістю нульового розголошення. Процес генерації доказу починається з перетворення моделі обмежень транзакції у внутрішнє представлення, придатне для криптографічної обробки. Для zk-SNARKs це представлення, як правило, має вигляд арифметичної схеми або системи ранг-1 обмежень, тоді як для zk-STARKs використовується трасування обчислень із подальшою алгебраїчною апроксимацією. Схема процесу генерації та перевірки доказу наведена на рис. 2.

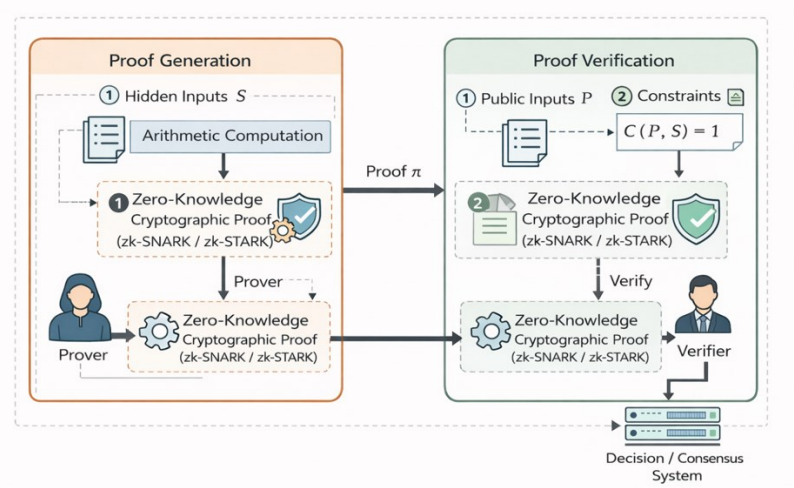

Рис. 2. Процес формування та перевірки доказів у системі

На етапі генерації доказу відправник транзакції, володіючи прихованими даними S та відкритими параметрами P, формує доказ π, який криптографічно зв'язує ці дані з обмеженнями C. Процес верифікації полягає у перевірці доказу π на основі лише відкритих параметрів P без доступу до прихованих змінних. У разі успішної перевірки система отримує гарантію коректності транзакції, не розкриваючи її внутрішнього змісту.

У контексті запропонованої системи відмінності між zk-SNARKs та zk-STARKs проявляються насамперед у вимогах до ініціалізації, обчислювальних витратах та масштабованості. zk-SNARKs забезпечують компактні докази та швидку верифікацію, що є доцільним для середовищ із жорсткими обмеженнями на розмір даних, однак потребують довірчої фази налаштування. zk-STARKs, у свою чергу, не потребують такої фази та ґрунтуються на хеш-функціях, що підвищує криптографічну надійність і постквантову стійкість, але призводить до збільшення розміру доказів.

Інтеграція обох підходів у межах єдиної системи дозволяє адаптувати механізм формування доказів до вимог конкретного транзакційного середовища, забезпечуючи баланс між рівнем конфіденційності, продуктивністю та практичною реалізовністю запропонованого рішення.

У межах запропонованої системи протоколи zk-SNARKs та zk-STARKs розглядаються як альтернативні механізми формування доказів коректності транзакцій, вибір яких визначається вимогами конкретного транзакційного середовища. Для обґрунтування доцільності їх використання виконано порівняльний аналіз основних характеристик цих протоколів з урахуванням архітектури системи забезпечення конфіденційності транзакцій. Узагальнені результати порівняння наведено в табл. 1.

Таблиця 1

Порівняльна характеристика протоколів zk-SNARKs та zk-STARKs у складі системи

Характеристика	zk-SNARKs	zk-STARKs
Розмір доказу	Малий, сталий	Значно більший
Обчислювальні витрати генерації	Високі	Високі
Обчислювальні витрати верифікації	Низькі	Помірні
Необхідність довірчої ініціалізації	Потрібна	Не потрібна
Криптографічна основа	Парингові операції	Хеш-функції
Постквантова стійкість	Обмежена	Висока
Масштабованість	Обмежена	Висока

Проведений аналіз показує, що zk-SNARKs є доцільними для сценаріїв, у яких критичними є компактність доказів та швидкість верифікації, зокрема у системах з обмеженою пропускною здатністю мережі або жорсткими вимогами до затримок. Водночас залежність від довірчої ініціалізації створює додаткові ризики для систем, орієнтованих на відкриті або міжорганізаційні середовища. zk-STARKs, навпаки, забезпечують вищий рівень криптографічної надійності та стійкості до майбутніх атак, що робить їх придатними для довготривалих систем з підвищеними вимогами до безпеки, хоча й за рахунок збільшення розміру доказів і навантаження на мережу.

Запропонована система підтримує використання обох протоколів у межах єдиної архітектури, що дозволяє адаптивно обирати механізм формування доказів залежно від характеристик транзакцій, доступних ресурсів та вимог до довіри. Такий підхід забезпечує гнучкість системи та розширює спектр можливих сценаріїв її застосування. Інтеграція системи забезпечення конфіденційності транзакцій у розподілене транзакційне середовище передбачає її використання як логічного надбудовного рівня над існуючими платформами обробки транзакцій. У блокчейн-мережах система може бути застосована для прихованої перевірки коректності транзакцій або виконання умов смарт-контрактів без розкриття внутрішніх параметрів. У такому сценарії у розподілений реєстр записуються лише відкриті параметри транзакції та відповідні докази коректності, тоді як чутливі дані залишаються поза межами публічного доступу.

Взаємодія з вузлами мережі зводиться до стандартної процедури верифікації доказів, що не потребує модифікації механізмів консенсусу або довірених компонентів. Це дозволяє зберегти прозорість і перевірюваність транзакцій на рівні мережі, водночас істотно підвищуючи рівень конфіденційності. У розподілених корпоративних системах або міжорганізаційних платформах запропонований підхід може бути використаний для підтвердження виконання бізнес-правил або регламентів без розкриття внутрішніх даних кожної сторони.

Застосування протоколів нульового розголошення у складі системи позитивно впливає на масштабованість обробки транзакцій, оскільки верифікація доказів виконується незалежно від складності прихованих обчислень. Це дозволяє зменшити обсяг даних, що циркулюють у мережі, та знизити ризики кореляційного аналізу транзакцій, зберігаючи при цьому формальну перевірюваність і довіру між учасниками розподіленого середовища.

Отримані результати дослідження підтверджують доцільність використання протоколів нульового розголошення знань як базового механізму забезпечення конфіденційності транзакцій у розподілених інформаційних системах. Запропонована система визначає процес обробки транзакцій таким чином, що коректність виконання визначених правил підтверджується криптографічним доказом без розкриття чутливих даних, що усуває характерну для традиційних підходів залежність між прозорістю перевірки та рівнем конфіденційності.

Запропонований підхід базується на побудові цілісної архітектурної моделі забезпечення конфіденційності транзакцій, у якій механізми zk-SNARKs та zk-STARKs інтегровані як взаємозамінні компоненти. Це забезпечує адаптацію системи до різних транзакційних моделей і вимог середовища виконання без зміни логіки верифікації, надаючи можливість вибору між компактністю доказів і рівнем криптографічної надійності. Система може застосовуватися у відкритих і напіввідкритих транзакційних середовищах без залучення додаткових довірених сторін, а використання формально перевірюваних доказів знижує ризики компрометації даних та підвищує довіру між учасниками. Відсутність обов’язкової довірчої ініціалізації при використанні zk-STARKs розширює можливості застосування системи в критичних і довготривалих інфраструктурах.

Порівняно з традиційними механізмами захисту транзакцій, що базуються на шифруванні або анонімізації, запропонована система забезпечує вищий рівень верифікованості без втрати конфіденційності. Зменшення обсягу відкритих даних та відокремлення перевірки коректності від доступу до внутрішнього змісту транзакцій знижує ймовірність побічного аналізу та кореляційних атак. Крім того, модульна архітектура системи дозволяє масштабувати обробку транзакцій без суттєвого збільшення навантаження на мережеву інфраструктуру.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі розглянуто проблему забезпечення конфіденційності транзакцій з даними в умовах зростаючої прозорості та відкритості сучасних розподілених інформаційних систем. Показано обмеженість традиційних криптографічних підходів, які не дозволяють поєднати перевірюваність коректності транзакцій із нерозкриттям їхнього внутрішнього змісту. Запропоновано системний підхід до розв'язання цієї проблеми на основі протоколів нульового розголошення знань zk-SNARKs та zk-STARKs.

У статті розроблено та описано архітектуру системи забезпечення конфіденційності транзакцій, у межах якої визначено модель транзакції з відокремленням відкритих параметрів і прихованих даних, а також визначено механізм формування та верифікації доказів коректності без розкриття чутливої інформації. Проведений аналіз показав, що інтеграція протоколів zk-SNARKs і zk-STARKs у єдину архітектурну модель дозволяє забезпечити гнучкість системи та адаптацію до різних вимог щодо продуктивності, масштабованості й рівня криптографічної надійності.

Отримані результати підтверджують, що запропонована система забезпечує вищий рівень конфіденційності транзакцій порівняно з наявними рішеннями, зберігаючи при цьому формальну верифікованість і прозорість перевірки. Модульна побудова системи та можливість відмови від довірчої ініціалізації створюють передумови для її застосування у відкритих блокчейн-мережах, корпоративних розподілених платформах та міжорганізаційних транзакційних середовищах.

Перспективи подальших досліджень пов'язані з оптимізацією обчислювальних витрат генерації доказів, зменшенням затримок обробки транзакцій та підвищенням енергоефективності системи. Окремий інтерес становить дослідження адаптивних механізмів вибору протоколів нульового розголошення залежно від характеристик транзакцій і стану мережі, а також експериментальна оцінка ефективності запропонованого підходу в реальних розподілених середовищах.

Література

1. Said, D. (2022). A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities. *IEEE Engineering Management Review*, 51(1), 76–107. https://doi.org/10.1109/EMR.2022.3184699
2. Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. *Computers, Materials & Continua*, 78(3). https://doi.org/10.32604/cmc.2024.046782
3. Jimale, M. A., Z'aba, M. R., Kiah, M. L. B. M., Idris, M. Y. I., Jamil, N., Mohamad, M. S., & Rohmad, M. S. (2022). Authenticated encryption schemes: A systematic review. *IEEE Access*, 10, 14739–14766. https://doi.org/10.1109/ACCESS.2022.3146178
4. Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. *Computers*, 13(1), 27. **https://doi.org/10.3390/computers13010027**
5. Aldrich, S. T., & Smith, K. R. (2024). Safeguarding Identity: A Comprehensive Survey of Anonymization Strategies for Behavioral Biometric Data. *European Journals of Emerging Computer Vision and Natural Language Processing*, 1(01), 34–59.
6. Gupta, S. (2025). Zero-Knowledge Proofs for Privacy-Preserving Systems: A Survey Across Blockchain, Identity, and Beyond. *Engineering and Technology Journal*, 10(07), 5755–5761.
7. Bhasker Reddy, M. V., & Duvvi, S. (2024). Blockchain Privacy through Zero-Knowledge Proofs: A Survey of Techniques and Use Cases. *Frontiers in Health Informatics*, 13(3). https://doi.org/10.30699/fhi.v13i3.558
8. Sassi, Z. B., Yaici, C. C., Xiang, J., Salem, O., & Mehaoua, A. (2025). Benchmarking Zero-Knowledge Proof-Based Authentication Protocols. In *2025 IEEE International Symposium on Future Telecommunication Technologies (SOFTT)* (pp. 131–137). IEEE. https://doi.org/10.1109/SOFTT64218.2025.10648577
9. Ballesteros-Rodríguez, A., Sánchez-Alonso, S., & Sicilia-Urbán, M. Á. (2024). Enhancing privacy and integrity in computing services provisioning using blockchain and zk-SNARKs. *IEEE Access*, 12, 117970–117993. https://doi.org/10.1109/ACCESS.2024.3432210
10. Aziz, R., Badr, Y., & Bouzefrane, S. (2025). Enhancing Trust in Central Differential Privacy Using zk-SNARKs and Cryptographic Hashes. In *International Conference on Advanced Information Networking and Applications* (pp. 163–176). Springer. https://doi.org/10.1007/978-3-031-70563-2_14
11. Maidine, K., Ahmed, E. Y., & Trichni, S. (2025). Quantum-resistant identity management via zk-STARKs and decentralized storage. *Ingénierie des Systèmes d'Information*, 30(5), 1297. https://doi.org/10.18280/isi.300517
12. Nassar, S. T., Hamdy, A., & Nagaty, K. (2024). Hybrid zk-STARK and zk-SNARK Framework for Privacy-Preserving Smart Contract Data Feeds. In *2024 International Conference on Computer and Applications (ICCA)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICCA62202.2024.10567894

References

1. Said, D. (2022). A survey on information communication technologies in modern demand-side management for smart grids: Challenges, solutions, and opportunities. *IEEE Engineering Management Review*, 51(1), 76–107. https://doi.org/10.1109/EMR.2022.3184699
2. Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. *Computers, Materials & Continua*, 78(3). https://doi.org/10.32604/cmc.2024.046782
3. Jimale, M. A., Z'aba, M. R., Kiah, M. L. B. M., Idris, M. Y. I., Jamil, N., Mohamad, M. S., & Rohmad, M. S. (2022). Authenticated encryption schemes: A systematic review. *IEEE Access*, 10, 14739–14766. https://doi.org/10.1109/ACCESS.2022.3146178
4. Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. *Computers*, 13(1), 27. **https://doi.org/10.3390/computers13010027**
5. Aldrich, S. T., & Smith, K. R. (2024). Safeguarding Identity: A Comprehensive Survey of Anonymization Strategies for Behavioral Biometric Data. *European Journals of Emerging Computer Vision and Natural Language Processing*, 1(01), 34–59.
6. Gupta, S. (2025). Zero-Knowledge Proofs for Privacy-Preserving Systems: A Survey Across Blockchain, Identity, and Beyond. *Engineering and Technology Journal*, 10(07), 5755–5761.
7. Bhasker Reddy, M. V., & Duvvi, S. (2024). Blockchain Privacy through Zero-Knowledge Proofs: A Survey of Techniques and Use Cases. *Frontiers in Health Informatics*, 13(3). https://doi.org/10.30699/fhi.v13i3.558
8. Sassi, Z. B., Yaici, C. C., Xiang, J., Salem, O., & Mehaoua, A. (2025). Benchmarking Zero-Knowledge Proof-Based Authentication Protocols. In *2025 IEEE International Symposium on Future Telecommunication Technologies (SOFTT)* (pp. 131–137). IEEE. https://doi.org/10.1109/SOFTT64218.2025.10648577
9. Ballesteros-Rodríguez, A., Sánchez-Alonso, S., & Sicilia-Urbán, M. Á. (2024). Enhancing privacy and integrity in computing services provisioning using blockchain and zk-SNARKs. *IEEE Access*, 12, 117970–117993. https://doi.org/10.1109/ACCESS.2024.3432210
10. Aziz, R., Badr, Y., & Bouzefrane, S. (2025). Enhancing Trust in Central Differential Privacy Using zk-SNARKs and Cryptographic Hashes. In *International Conference on Advanced Information Networking and Applications* (pp. 163–176). Springer. https://doi.org/10.1007/978-3-031-70563-2_14
11. Maidine, K., Ahmed, E. Y., & Trichni, S. (2025). Quantum-resistant identity management via zk-STARKs and decentralized storage. *Ingénierie des Systèmes d'Information*, 30(5), 1297. https://doi.org/10.18280/isi.300517
12. Nassar, S. T., Hamdy, A., & Nagaty, K. (2024). Hybrid zk-STARK and zk-SNARK Framework for Privacy-Preserving Smart Contract Data Feeds. In *2024 International Conference on Computer and Applications (ICCA)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICCA62202.2024.10567894