УДК 004.02
DOI https://doi.org/10.32782/2663-5941/2024.1.1/24

Корнійчук О.В.
Державний університет «Житомирська політехніка»

Граф М.С.
Державний університет «Житомирська політехніка»

МЕТОДИ ТА АЛГОРИТМИ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ НА ПРИКЛАДІ ПОБУДОВИ МАЙДАНЧИКУ ДЛЯ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ

Ця стаття присвячена дослідженню методів та алгоритмів забезпечення конфіденційності у децентралізованих системах, з особливим акцентом на розробку платформи для державних закупівель на основі технології блокчейн. У світлі актуальності теми конфіденційності даних у децентралізованих мережах, особливо у сфері державних закупівель, автори провели всебічний аналіз існуючих криптографічних методів, таких як міксування, кільцеві підписи, схеми зобов'язань, гомоморфне приховування та докази з нульовим розкриттям інформації, з метою виявлення їхньої ефективності у забезпеченні приватності особистості користувача та захисту даних.

Основна увага була зосереджена на неінтерактивних доказах з нульовим розкриттям інформації та гомоморфному шифруванні, які виявилися ключовими в контексті реалізації приватності та конфіденційності в блокчейн-платформах для державних закупівель. Автори розкривають важливість встановлення балансу між прозорістю операцій, ефективністю обробки транзакцій та забезпеченням належного рівня конфіденційності даних, враховуючи вимоги, такі як GDPR. Підкреслюється, що використання сучасних криптографічних методів може забезпечити необхідний рівень приватності без втрати переваг децентралізації, що є ключовим для успішної інтеграції блокчейн-технологій у сферу державних закупівель.

Дослідження акцентує увагу на значній ролі різних криптографічних методів у розв'язанні викликів, пов'язаних із забезпеченням конфіденційності в блокчейн-системах, особливо у контексті державних закупівель, де вимоги до прозорості та конфіденційності є одночасно високими. Висвітлюються можливості та обмеження кожного з аналізованих методів, надаючи чітке розуміння того, як кожен з них може бути використаний для досягнення оптимального балансу між безпекою та ефективністю в державних закупівлях. Такий підхід дозволяє забезпечити комплексне вирішення проблеми конфіденційності у децентралізованих системах, відкриваючи нові перспективи для розвитку блокчейн-технологій у державному секторі.

Ключові слова: *блокчейн, державні закупівлі, електронні майданчики, методи збереження конфіденційності, Zero-Knowledge Proof, шифрування.*

Постановка проблеми. Застосування децентралізованих мереж було завжди досить складною задачею, разом з тим однією з найперспективніших технологій наразі є блокчейн. Концепт, який був запропонований у 2008 році Сатосі Накамото через революційну публікацію про Біткоїн, швидко став однією з найперспективніших технологій сучасності. Його основні переваги, такі як децентралізація, резистентність даних та прозорість, відкрили широкі можливості для різноманітних сфер застосування – від криптовалют до системи смарт-контрактів. Однак, разом з ростом популярності та розширенням можливостей блокчейну, постали його обмеження та виклики. Одним з ключових викликів є питання конфіденційності даних, що стає особливо значущим у контексті використання блокчейну в будь яких системах, особливо державних, таких як публічних закупівлях.

Блокчейни за своєю природою поділяються на закриті та відкриті системи. Закриті для задач, в яких відкритість даних є одним з пріоритетів, не підходять за своєю сутністю [1]. Саме публічні блокчейни є прозорими та відкритими реєстрами, що, з одного боку, забезпечують надійність та прозорість угод, але з іншого – викликають питання захисту приватності інформації. Подібні проблеми з конфіденційністю ставлять під сумнів можливість широкого впровадження блокчейну в сферах, де чутливість даних є критичною, зокрема в державних закупівлях.

У державних закупівлях прозорість та швидкість прийняття рішень є фундаментальними, але

забезпечення конфіденційності даних не менш важливе. Захист особистих даних та відповідність загальному регламенту захисту даних, прийнятому в межах законодавства Європейського союзу (англ. General Data Protection Regulation або GDPR), ставлять перед блокчейном нові завдання. Вирішення цих задач вимагає комплексного підходу, який поєднує технологічні інновації та юридичну відповідність. Це включає інтеграцію передових криптографічних методів та розробку архітектурних рішень, які можуть гарантувати конфіденційність без втрати переваг децентралізації.

Отже, розробка блокчейн-платформи для державних закупівель, яка балансує між прозорістю, швидкістю обробки транзакцій та конфіденційністю, є надзвичайно важливою та актуальною. Це створює потенційний напрямок для дослідження, що об'єднує в собі технологічні інновації та відповідність сучасним вимогам захисту даних.

Аналіз останніх досліджень та публікацій, на які спираються автори. Задачу забезпечення приватності поділяють на дві основних категорії, що зображені на рисунку 1 – це забезпечення приватності особистості користувача, щоб не було можливості встановити взаємозв'язок між користувачем та транзакцією, яку він зробив, та збереження приватності самих даних задля запобігання розкриття їх третім особам, що не мають мати доступу до них.

В рамках статті було проаналізовано 6 статей і вибрано дві для детального огляду, серед яких «Privacy-preserving solutions for Blockchain: review and challenges» [3] та «A Survey on Privacy Vulnerabilities in Permissionless Blockchains» [4], автори яких детально наводять приклади алгоритмів та методів, які застосовуються для цих задач. Серед алгоримів, які займаються забезпеченням конфіденційності особистості користувача можна виділити наступні категорії:

1. Міксування (Mixing);
2. Кільцевий підпис (Ring Signatures);
3. Схеми зобов'язань (Commitment schemes);
4. Гомоморфне приховування (Homomorphic hiding);
5. Докази з нульовим розкриттям інформації (Zero-Knowledge Proofs).

В свою чергу алгоритми, що покликані захистити дані складаються з наступного списку:

1. Диференціальна конфіденційність (Differential Privacy);
2. Докази з нульовим розкриттям інформації (Zero-Knowledge Proofs);
3. Гомоморфне приховування (Homomorphic hiding).

Чітко видно, що деякі категорії алгоритмів повторюються між собою, це пов'язано з тим, що деякі алгоритми незважаючи на свою категорію однаково добре підходять для обидвох задач або використовують різні алгоритми однієї і тієї самої категорії. Водночас для вирішення задач з побудови майданчика для державних закупівель важливим є обидва типи задач, оскільки потрібно

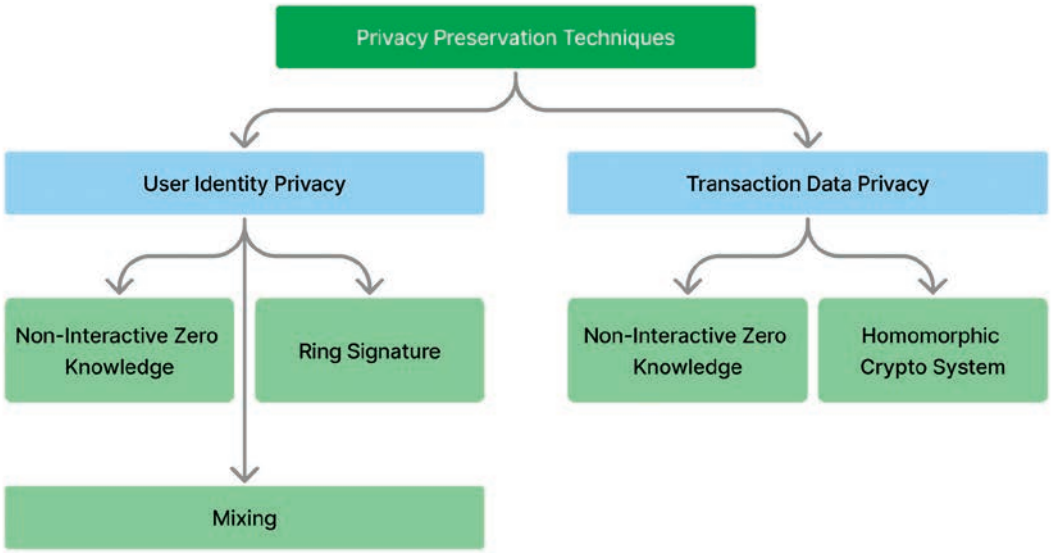

Рис. 1. Умовний поділ алгоритмів на ті, що забезпечують приватність користувача та даних користувача

вирішити не тільки задачу приховування деталей пропозиції на умовному тендері, а також захистити дані самого замовника, тобто користувача.

Метою статті є проведення аналізу найбільш вживаних алгоритмів та методів забезпечення конфіденційності особистості користувача та його даних в децентралізованих мережах.

Викладення основного матеріалу. В рамках побудови системи для проведення державних закупівель необхідно чітко розуміти які дані і яким чином потрібно захистити. Питання конфіденційності наразі є критично важливим не тільки для створення конкретної системи, а для масового впровадження до побудови систем децентралізованого підходу, що допоможе суттєво підвищити інші показники [5]. Саме тому для вирішення цих задач існує велика множина алгоритмів, кожен з яких має свій підхід для забезпечення конфіденційності. Розглянемо їх більш детально.

Міксування – це методи, що використовуються для анонімізації різних послуг із множинами користувачів. Започатковані у 1981 році для анонімізації електронної пошти, ці методи базуються на групуванні всіх повідомлень від різних користувачів, їх затримці, а потім пересиланні одночасно або в випадковому порядку. Це робить неможливим кореляцію між дією користувача щодо створення повідомлення і його рухом у мережі. Однак, ця техніка не допомагає вирішити проблему персональної інформації, яка може бути в повідомленні.

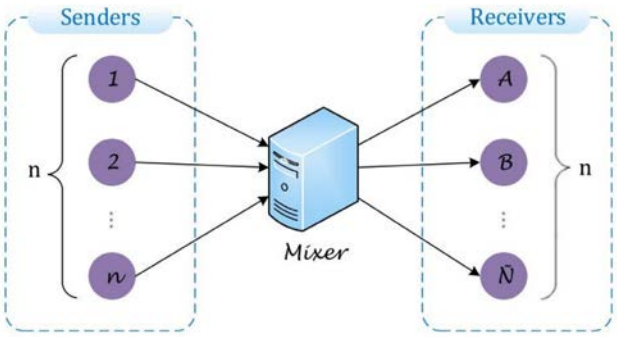

Рис. 2. Архітектура міксувального сервісу [6]

Централізоване міксування використовує веб сайти для анонімізації транзакцій, де користувачі обмінюються транзакціями з метою приховування зв'язків між вхідними та вихідними операціями. Хоча ці веб-сайти пропонують послуги міксування за плату, вони мають низку обмежень, таких як вразливість до атак відмови в обслуговуванні (англ. distributed denial-of-service або DDOS), оскільки централізований міксер залишається однією точкою збою. Це стає перешкодою для розподіленої природи блокчейн-мережі, де централізація служб міксування суперечить базовому принципу децентралізації.

На противагу централізованому міксуванню, децентралізоване міксування пропонує підхід, що дозволяє групі недовірених користувачів публікувати свої повідомлення одночасно та анонімно без потреби в посередництві третьої сторони. Це виключає необхідність плати за міксування та знижує ризик DDOS-атак.

Однак, незважаючи на переваги міксувальних служб у забезпеченні анонімності ідентичності, вони мають власні проблеми. Користувачі міксувальних служб зіштовхуються з високою затримкою очікування, оскільки їм потрібно чекати, поки інші учасники створять свої транзакції, щоб приховати зв'язки між вхідними та вихідними операціями. Це веде до затримок у завершенні транзакцій. Крім того, більшість міксувальних серверів – це веб-сайти або інше програмне забезпечення третіх сторін, що робить їх ненадійними в контексті усунення проблем конфіденційності в блокчейн-мережах. Існує також ризик зловмисного використання міксувальних служб, оскільки сервер має інформацію про всі вхідні та вихідні пари, і приватність в цьому випадку залежить від чесності посередника. Крім того, міксувальні служби зазвичай вимагають оплати за приховування ідентичності користувачів.

Проведення державних закупівель має певні строки і кінцеві дати, саме тому недолік у вигляді недетермінованого часу завершення транзакцій може суттєво вплинути на їх результати.

Ring Signature або Кільцевий підпис. Кільцеві підписи в криптографії є одним із різновидів підписів, які використовуються для досягнення анонімності в блокчейнах. Цей метод був вперше представлений у 2001 році Рональдом Ривестом. Основна ідея кільцевого підпису полягає в тому, що користувач обирає групу учасників для створення кільця, включаючи себе. Кожен учасник у кільці має публічний ключ. Один з користувачів підписує повідомлення своїм приватним ключем та публічними ключами всіх інших учасників. Вузол, що верифікує, знає, що один з членів підписав повідомлення, але не може визначити, хто саме це зробив, таким чином досягаючи анонімності.

Механізм роботи кільцевого підпису можна порівняти з підписом на чеку спільного банківського рахунку, де всі учасники підписують транзакцію своїми публічними ключами разом із приватним ключем ініціатора. Після того, як кожен

учасник кільця підписав транзакцію, вона подається на перевірку та верифікацію.

Основні переваги кільцевих підписів включають неможливість підробки та анонімність. Анонімність поділяється на такі властивості, як невідстежуваність та невстановлюваність. Невстановлюваність означає, що верифікатор не може визначити зв'язок між двома транзакціями, а невідстежуваність – що підписувача не можна ідентифікувати. Ці властивості призвели до розвитку декількох протоколів забезпечення приватності на основі кільцевих підписів, які широко використовуються в блокчейн-мережах.

Однак існують і певні проблеми з кільцевими підписами. Наприклад, великий розмір кільця означає збільшення кількості учасників, що може підвищити ризик деанонімізації. Транзакції з кільцевим підписом великі за розміром, що може становити проблему для масштабування блокчейнів через потребу у більшому обсязі пам'яті для зберігання записів усієї блокчейн-мережі. В рамках системи тендерів кількість учасників обмежена певним числом, що вцілому нівелює ризик деанонімізації шляхом створення через великий розмір кільця.

Протоколи доказу нульового розкриття. Протоколи доказу нульового розкриття (англ. Zero-Knowledge Proof або ZKP), запроваджені у 1980-х роках, стали однією з найбільш широко використовуваних криптографічних технік для забезпечення передачі активів через розподілену мережу блокчейну на основі peer-to-peer мережі з покращеним рівнем конфіденційності. Метою доказів нульового розкриття є підтвердження справжності транзакції без надання верифікатору будь-яких даних про транзакцію [7]. Концепція полягає в тому, що засвідчувач має сформулювати формальний доказ, щоб довести істинність певного твердження, не надаючи верифікатору жодної додаткової та корисної інформації. Варіант ZKP, відомий як non-interactive zero-knowledge proof, широко використовується у блокчейнах, оскільки він виключає необхідність взаємодії між засвідчувачем та верифікатором, замість цього вимагаючи лише одного повідомлення, яке має бути відправлене від засвідчувача до верифікатора. Важливо зазначити, що не всі схеми ZKP є не взаємодіючими.

Більшість протоколів ZKP, які є в літературі, є взаємодіючими (interactive), що означає що засвідчувач має відповідати на різні повідомлення, які надсилає верифікатор, що призводить до багаторазових раундів спілкування. Однак для блокчейнів та інших технологій розподіленого реєстру бажано уникати спілкування, оскільки вузли верифікації не можуть належним чином домовитися про те, як обирати ці повідомлення, через те, що в багатьох конструкціях їх потрібно обирати випадково, тоді як алгоритм верифікації має бути детермінованим для досягнення консенсусу або це зробить складність комунікації системи дуже слабкою. Ця властивість робить non-interactive ZKP придатними для анонімної та розподіленої верифікації повідомлень у блокчейнах.

Концепція вперше з'явилася у 1985 та призначена для створення протоколів збереження конфіденційності в мережах блокчейнів.

Non-interactive ZKP мають відповідати наступним трьом властивостям:

1. Повнота: все, що є істинним, має доказ.
2. Обґрунтованість: все, що може бути доведено, є істинним.
3. Нульове розкриття: значення відкривається лише коли є доведеним.

Протоколи доказу з нульовим розкриттям мають свої недоліки, такі як складність обчислень, оскільки перевірка та створення доказів може вимагати значних обчислювальних ресурсів, складність реалізації системи та, порівняно з іншими алгоритмами, гірша масштабованість. Але при правильному проектуванні та завчасно визначеними вимогами до системи можна досягти збалансованого використання цих протоколів чим суттєво підвищити безпеку системи в цілому.

Homomorphic hiding або Гомоморфне приховування. Ще одним методом обміну даними та виконання операцій над ними без розкриття приватних значень є гомоморфне шифрування, яке походить від приватного гомоморфізму, запропонованого Рональдом Ривестом у 1978 році. У цьому випадку функція шифрування має певні властивості, що дозволяють виконувати операції над зашифрованим текстом та отримувати зашифрований результат, так само ніби операції були виконані над відкритим текстом, а потім зашифровані за допомогою тієї ж функції шифрування.

Одним з найкращих прикладів гомоморфного приховування є схема шифрування RSA. Задано публічний ключ (e, n) та приватний ключ (d), цілі числа, які відповідають рівностям $n = p \cdot q$, де p та q є простими числами, та $d \cdot e \equiv 1 \bmod \varphi(n)$. Шифрування повідомлення *x* визначається за формулою

$$E(x) \equiv x^e \bmod n, \qquad (1)$$

Тоді множення групи є гомоморфною властивістю шифрування RSA:

$$E(x)\,E(y) = x^e y^e \equiv (xy)^e \bmod n = E(xy), \qquad (2)$$

Гомоморфне приховування є одним із фундаментальних інструментів для створення zk SNARKs та приватних розподілених обчислень загалом, що є схемою доведення-верифікатора, яка використовується у блокчейні.

Ще одне пряме використання гомоморфного шифрування у блокчейні – це пари ключів ECDSA Bitcoin, які мають адитивні та мультиплікативні гомоморфні властивості. Пара ключів (a, A), відповідно приватні та публічні значення, та інша пара (b, B) можуть створити третю дійсну адресу Bitcoin, додавши ключі як (a+b, A+B). Це створює можливість використання адреси (a+b, A+B) заволодівши парою ключів (b, B) та отримавши приватний ключ (A+B). Таким чином, користувач може продати свою адресу іншому, не маючи потреби захищати доставку приватного ключа b, а лише користувач з приватним ключем a зможе використовувати (a+b, A+B).

Схеми зобов'язань. Схеми зобов'язань є фундаментальною концепцією в криптографії та безпечному зв'язку. Вони є аналогічними до цифрового еквіваленту «запечатаних конвертів» і відіграють важливу роль у різних криптографічних протоколах, включаючи безпечне голосування, системи аукціонів та докази з нульовим розкриттям інформації.

Суть схем зобов'язань полягає в тому, що одна сторона (той, хто дає зобов'язання) зобов'язується щодо певного значення, одночасно тримаючи це значення в таємниці від інших. Пізніше, ця сторона може розкрити зобов'язане значення. Процес складається з двох основних етапів: етап зобов'язання, де сторона обіцяє певне значення, не розкриваючи його, і етап розкриття, де це значення стає відомим і може бути перевіреним.

Основні властивості схем зобов'язань включають:

1. Незмінність: після надання зобов'язання, його не можна змінити.

2. Приховування: в зобов'язанні не міститься інформації про фактичне значення до моменту його розкриття.

Ці властивості забезпечують, що зобов'язання може бути використане як надійний спосіб захисту інформації, а також як інструмент для створення довіри в цифрових взаємодіях. Схеми зобов'язань є ключовим елементом у багатьох аспектах криптографічної безпеки і мають широке застосування в сучасних цифрових системах.

Схеми зобов'язань та докази з нульовим розкриттям інформації (ZKP) відіграють взаємопов'язані ролі у криптографії, особливо у контексті державних закупівель. Схеми зобов'язань дозволяють учаснику системи зобов'язатися щодо певного значення, приховуючи його до моменту розкриття. Це важливо для забезпечення надійності та повноти інформації в процесах, де важливим є гарантування правдивості даних, наприклад, у аукціонах або при поданні тендерних пропозицій.

З іншого боку, ZKP дозволяє стороні довести іншій стороні істинність певного твердження без розкриття будь-якої конкретної інформації, крім самого факту істинності твердження. Це особливо корисно у контексті забезпечення конфіденційності та безпеки в системах державних закупівель, де важливо встановити достовірність інформації, не розкриваючи чутливих даних.

У системах державних закупівель схеми зобов'язань можуть використовуватися на етапі подання тендерних пропозицій, де учасники зобов'язуються надати певну інформацію або пропозицію без її розкриття до визначеного моменту. Це дозволяє забезпечити чесність та прозорість процесу тендеру.

ZKP, у свою чергу, можуть використовуватися на етапі верифікації пропозицій, щоб переконатися у їхній відповідності вимогам без необхідності розкриття деталей пропозиції до моменту відбору переможця. Це допомагає забезпечити конфіденційність інформації та захист від недобросовісної конкуренції.

Описані методи, що дозволяють вирішувати проблеми конфіденційності користувача та його даних, мають певні недоліки, серед яких найбільш поширеним є складність обчислень, оскільки для кожного алгоритму та методу необхідно проводити певний об'єм обчислень, на що витрачається час, який має бути детермінований в децентралізованих системах для стабільної роботи. Вирішенням конкретно цього питання є створення окремих допоміжних сервісів, які будуть робити обчислювально роботу, а саму валідацію результатів вже проводити в рамках блокчейну. В рамках аналізу прийшли до висновку, що забезпечення комплексного підходу до безпеки в плані приватності даних можливо досягти шляхом збалансованого використання пари алгоритмів.

Для забезпечення приватності даних пропонується використання протоколів доведення з нульовим доказом через простоту верифікації на блокчейні та доволі високу надійність до взлому. В свою чергу, захист особистості користувача можна реалізувати також через використання кільцевого підпису, що неможливість ідентифікації учасника тендеру.

Висновки та перспективи подальших досліджень. У даному дослідженні розглянуто методи та алгоритми забезпечення конфіденційності в системах державних закупівель. При розгляді особлива увага приділяється можливості побудови платформи для державних закупівель, використовуючи технологію блокчейн. Найбільш детально розглянуто такі криптографічні методи, як Mixing, Ring Signatures, Commitment schemes, Homomorphic hiding, і Zero-Knowledge Proofs. Перераховані методи спрямовані на забезпечення приватності користувачів та захисту їхніх даних. Особлива увага дослідження була зосереджена на невзаємодіючих доказах нульового розкриття та гомоморфному шифруванні, їх застосування в контексті блокчейну для державних закупівель.

Важливим аспектом проєктування систем для проведення державних закупівель є забезпечення балансу між прозорістю, швидкістю обробки транзакцій та конфіденційністю. Це створює унікальні виклики та вимагає ретельного розгляду як технологічних можливостей, так і юридичних вимог, зокрема відповідність загальному регламенту захисту даних (GDPR). Необхідно підкреслити, що ефективність цих методів та алгоритмів можна підвищити шляхом розумного комбінування та планування архітектури з розуміння всіх вимог до системи державних публічних закупівель.

Результати дослідження показують, що збалансованого використання передових криптографічних методів і підходів може ефективно забезпечити необхідний рівень приватності, не жертвуючи при цьому перевагами децентралізації.

Список літератури:

1. Корнійчук О. В., Граф М. С. Аналіз існуючих механізмів прийняття рішень в децентралізованих системах для застосування в державних закупівлях. *Технічні науки та технології*. 2023. № 1(91). С. 156-160. URL:https://doi.org/10.26642/ten-2023-1(91)-156-160.
2. Nakamoto S. Bitcoin: A peer-to-peer electronic cash. 2009. URL: https://bitcoin.org/bitcoin.pdf.
3. Bernabe J. B., Canovas J. L., Hernandez-Ramos J. L., Moreno R. T., Skarmeta A. Privacy-preserving solutions for Blockchain: review and challenges. *IEEE Access*. 2019. DOI: 10.1109/ACCESS.2019.2950872. URL: https://www.researchgate.net/publication/336937331.
4. Junejo A. Z., Hashmani M. A., Alabdulatif A. A. A Survey on Privacy Vulnerabilities in Permissionless Blockchains. *International Journal of Advanced Computer Science and Applications*. 2020. Vol. 11, № 9. P. 130. URL: www.ijacsa.thesai.org.
5. Корнійчук О.В., Граф М.С. Дослідження переваг використання децентралізованих систем. Тези доповідей V Всеукраїнської науково-технічної конференції "Комп'ютерні технології: інновації, проблеми, рішення". Житомир: Житомирська політехніка, 2022. С. 142-143. ISBN 978-966-683-593-5.
6. Kappos G., Yousaf H., Maller M., MeikleJohn S. An Empirical Analysis of Anonymity in Zcash. *27th USENIX Security Symposium*. USA. 2018.
7. Pieprzyk, J., Hardjono, T., and Seberry, J. Fundamentals of Computer Security. 2nd ed. [Berlin, Germany]: Springer Science & Business Media, 2013. 697 p. ISBN 978-3-540-43101-5.

Korniichuk O.V., Hraf M.S. METHODS AND ALGORITHMS OF PRESERVING CONFIDENTIALITY IN DECENTRALIZED SYSTEMS ON THE EXAMPLE OF BUILDING PUBLIC PROCUREMENTS SYSTEM

This article is dedicated to the exploration of methods and algorithms for ensuring data privacy in decentralized systems, focusing specifically on the development of a platform for public procurement using blockchain technology. In light of the growing significance of data privacy in decentralized networks, especially in the field of public procurement, the authors have conducted a comprehensive analysis of existing cryptographic methods such as mixing, ring signatures, commitment schemes, homomorphic hiding, and zero-knowledge proofs, aiming to determine their effectiveness in ensuring user privacy and data protection.

Particular emphasis was placed on non-interactive zero-knowledge proofs and homomorphic encryption, which emerged as key in the context of implementing privacy and confidentiality on blockchain platforms for public procurement. The authors highlight the importance of balancing transaction transparency, processing efficiency, and ensuring an adequate level of data confidentiality, considering requirements such as the GDPR. It is emphasized that the use of advanced cryptographic methods can provide the necessary level of privacy without losing the benefits of decentralization, which is crucial for the successful integration of blockchain technologies in public procurement.

The study emphasizes the significant role of various cryptographic methods in addressing challenges associated with ensuring confidentiality in blockchain systems, especially in the context of public procurement, where the demands for transparency and confidentiality are simultaneously high. The possibilities and limitations of each analyzed method are illuminated, providing a clear understanding of how each can be utilized to achieve an optimal balance between security and efficiency in public procurement. This approach allows for a comprehensive solution to the issue of confidentiality in decentralized systems, opening new perspectives for the development of blockchain technologies in the public sector.

Key words: *blockchain, government procurement, electronic platforms, methods of preserving confidentiality, Zero-Knowledge Proof, encryption.*