УДК 004.056.5

А. В. Грицак
Т. М. Скидан

ПОБУДОВА ДОВІРЧИХ ВІДНОСИН У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ ЗА ДОПОМОГОЮ ZKP ТА MFA

Вінницький національний технічний університет

Анотація:
В умовах сучасного інформаційного суспільства, де особливо важливими є конфіденційність, доступність і контрольованість взаємодії, постає потреба у побудові надійних довірчих відносин у децентралізованих системах, що може бути досягнуто шляхом впровадження протоколу Zero-Knowledge Proof та мультифакторної автентифікації. Запропоноване рішення дозволяє забезпечити перевірку автентичності користувачів і цілісність взаємодії без розкриття критичних даних, що особливо актуально в умовах відсутності централізованого контролю. Запропонована модель орієнтована на підвищення рівня безпеки та довіри між учасниками системи, а також може бути адаптована для використання у розподілених середовищах, таких як блокчейн або IPFS.
Ключові слова: децентралізовані системи, Zero-Knowledge Proof, мультифакторна автентифікація, довіра, безпека даних, конфіденційність.

Abstract:
In today's information society, where confidentiality, accessibility, and controllability of interaction are especially important, there is a need to build reliable trust relationships in decentralized systems, which can be achieved by implementing the Zero-Knowledge Proof protocol and multi-factor authentication. The proposed solution allows to ensure user authentication and interaction integrity without disclosing critical data, which is especially important in the absence of centralized control. The proposed model is focused on increasing the level of security and trust between system participants, and can be adapted for use in distributed environments such as blockchain or IPFS.
Keywords: decentralized systems, Zero-Knowledge Proof, multi-factor authentication, trust, data security, privacy.

Вступ

У сучасних умовах цифрової трансформації особливої актуальності набуває проблема формування довірчих відносин у децентралізованих системах. Відсутність централізованого контролю вимагає використання ефективних механізмів автентифікації та захисту даних. Використання Zero-Knowledge Proof у поєднанні з мультифакторною аутентифікацією забезпечує високий рівень довіри між сторонами взаємодії, дозволяючи підтверджувати особу або право доступу без розголошення самої конфіденційної інформації, що істотно підвищує безпеку взаємодії.

Результати дослідження

Zero-Knowledge Proof (ZKP) – це криптографічний протокол, який дозволяє одній стороні (доказувачу) переконати іншу сторону (верифікатора) у тому, що певне твердження є істинним, не розкриваючи при цьому жодної додаткової інформації про саме твердження або його секретні дані. Для досягнення цієї властивості ZKP використовує низку криптографічних примітивів, серед яких важливе місце займають схеми зобов’язань (commitment schemes) [1].

Схема зобов’язань дозволяє доказувачу «закріпити» певне значення або повідомлення у вигляді спеціального криптографічного зобов’язання, яке публікується, не розкриваючи самих даних. Пізніше доказувач може розкрити це зобов’язання, надавши часткову або повну інформацію, яку верифікатор може перевірити на відповідність початковому зобов’язанню. Такий механізм гарантує цілісність і незмінність прихованої інформації, що є фундаментальним для реалізації ZKP. Загальна архітектура ZKP-протоколу наведена на рисунку 1.

До основних етапів протоколу ZKP відносять [2]:

Крок 1. Створення двох ключів: ключ оцінки (передається Доказувачу) та ключ перевірки (передається Верифікатору).

Крок 2. Користувач надсилає до Точки обчислення відкриті (вхідні) дані, необхідні для виконання обчислень.

Крок 3. Користувач надсилає Доказувачу приватні дані разом із копією вхідних даних. Ці дані необхідні для створення доказу правильності обчислень.

Крок 4. На основі отриманих даних та ключа оцінки Доказувач формує доказ правильності обчислень і передає його до Точки обчислення.

Крок 5. Точка обчислення виконує необхідні обчислення та формує результат разом із згенерованим доказом, який потім надсилається Користувачу.

Крок 6. Користувач надсилає Верифікатору запит на підтвердження отриманого доказу. Разом із запитом передаються вхідні дані та сам доказ.

Крок 7. Верифікатор використовує ключ перевірки для перевірки достовірності отриманого доказу. У разі успішної перевірки він надсилає Користувачу підтвердження правильності обчислень.

Рисунок 1 – Архітектура протоколу Zero-Knowledge Proof

Таким чином, використання протоколів з нульовим розголошенням (ZKP) дозволяє гарантувати достовірність обчислень і передачі даних без необхідності розкривати їх зміст.

Однак ефективний захист інформації вимагає також надійного контролю доступу до самих систем. Одним із найважливіших аспектів такого контролю є автентифікація користувача [3]. Порівняння найпоширеніших методів автентифікації наведено у таблиці 1.

Таблиця 1 – Порівняння методів автентифікації

Метод автентифікації	Опис	Переваги	Недоліки	Рівень безпеки	Зручність
Пароль / PIN-код	Використання секретного слова або числової комбінації.	Простота реалізації, не потребує додаткових пристроїв.	Вразливість до атак перебору, фішингу, соціальної інженерії; слабкі паролі.	Низький	Висока
Біометрія	Розпізнавання обличчя, відбитків пальців, райдужки ока.	Унікальність, зручність використання, не потребує запам’ятовування.	Може бути підроблена, складно змінити при компрометації.	Середній/Високий	Висока
Одноразовий пароль (OTP)	Тимчасовий код, який надсилається або генерується для кожної сесії.	Високий рівень захисту, особливо в поєднанні з іншими методами.	Може бути перехоплений, залежність від пристрою, можливість атак типу «людина в браузері».	Високий	Середня

Продовження таблиці 1.

Смарт-картка / Токен	Апаратний носій, що містить сертифікати або ключі користувача.	Висока безпека, складність підробки, підходить для корпоративного використання.	Можлива втрата або крадіжка, потреба у спеціальному обладнанні, ризик ретрансляційних атак.	Високий	Низька/ Середня
Профілювання (поведінкова модель)	Аналіз звичної поведінки: місце, час, пристрій, стиль набору тощо.	Адаптивність, зручність, можливість безперервної автентифікації.	Низька надійність при нетиповій поведінці, складність реалізації, помилкові блокування.	Середній	Висока

З огляду на переваги та недоліки кожного з методів автентифікації, найбільш ефективним підходом до забезпечення високого рівня безпеки є використання мультифакторної автентифікації (MFA). Мультифакторна автентифікація – механізм, що поєднує декілька факторів перевірки особи з метою посилення безпеки доступу до системи. У контексті IT-безпеки це називається багаторівневою безпекою, яка зменшує ймовірність того, що зловмисник зможе подолати всі етапи. За допомогою мультифакторної автентифікації вразливості в системі безпеки можна обійти або принаймні зменшити їхню кількість, але слід пам’ятати про зручність, масштабованість і простоту використання [4].

Поєднання Zero-Knowledge Proof та мультифакторної автентифікації дозволяє учасникам децентралізованої системи підтверджувати свою ідентичність без розкриття чутливої інформації. Це створює основу для довіри навіть між незнайомими сторонами, адже автентифікація відбувається з високим ступенем достовірності, але без передачі паролів або ключів. Таким чином, система стає не лише безпечною, а й більш надійною в умовах відсутності єдиного центру контролю.

Крім того, застосування ZKP знижує ризик компрометації даних навіть у разі перехоплення трафіку, а MFA гарантує, що доступ до системи можливий лише за наявності кількох незалежних факторів підтвердження. Така комбінація не лише підвищує загальний рівень безпеки, але й формує середовище, де цифрова довіра ґрунтується не на централізованих сертифікатах чи реєстрах, а на математично обґрунтованій приватності та підтвердженні дійсності. Це відкриває нові можливості для створення масштабованих, прозорих і водночас захищених децентралізованих екосистем.

Висновки

Отже, у роботі проаналізовано ключові механізми забезпечення довіри в децентралізованих системах – Zero-Knowledge Proof та мультифакторну автентифікацію. Встановлено, що поєднання цих технологій дозволяє досягти високого рівня безпеки автентифікації без розкриття конфіденційних даних. ZKP забезпечує перевірку достовірності без доступу до змісту, а MFA знижує ризики несанкціонованого доступу. Такий підхід сприяє побудові ефективних довірчих відносин у системах без централізованого контролю, забезпечуючи прозорість, стійкість до атак і відповідність сучасним вимогам кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Circularise. Zero-knowledge proofs explained in 3 examples. URL: https://www.circularise.com/blogs/zero-knowledge-proofs-explained-in-3-examples
2. Thomas Chen, Hui Lu, Teeramet Kunpittaya, Alan Luo. A Review of zk-SNARKs: scientific work. arXiv:2202.06877, 2022, 34 p.
3. Rashad Mahmood Saqib, Adnan Shahid Khan1, Yasir Javed, Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security. City of the Samaritans, Malaysia, 2021, P. 1633-1647.
4. Monther Aldwairi, Saoud Aldhanhani. Multi-Factor Authentication System. Conference: International Conference on Research and Innovation in Computer Engineering and Computer Sciences (RICCES). At: Langkawi, Malaysia, 2017, 8 p.

Грицак Анатолій Васильович **–** кандидат технічних наук за спеціальністю 125«Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: grytsak.a.v@gmail.com

Скидан Тетяна Миколаївна **–** студентка групи 2КІТС-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: tanaskidan1@gmail.com

Hrytsak Anatoliy V. – Candidate of Technical Sciences in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail

Skydan Tetyana Mykolaivna – student group 2CITS-21b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: tanaskidan1@gmail.com