УДК [004.056.5:342.828.4](043.2)

М. Л. Сірацький
О. О. Войцеховська

ДЕЦЕНТРАЛІЗОВАНА ІНФОРМАЦІЙНА СИСТЕМА АНОНІМНОГО ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА БАЗІ ТЕХНОЛОГІЇ ZERO-KNOWLEDGE PROOFS

Вінницький національний технічний університет

Анотація

Дослідження присвячене розробці децентралізованої інформаційної системи для анонімного електронного голосування з використанням криптографії з нульовим розголошенням (Zero-Knowledge Proofs). Проаналізовано вразливості традиційних централізованих баз даних та обґрунтовано переваги парадигми Self-Sovereign Identity для забезпечення 100% приватності користувачів. Практична реалізація системи включає смарт-контракти мовою Solidity у тестовій мережі Ethereum (Sepolia), клієнтський веб-додаток на базі React та інтеграцію сервера-ретранслятора (Relayer) для забезпечення безкоштовних транзакцій). Запропоноване рішення забезпечує математичний захист від фальсифікації результатів та унеможливлює деанонімізацію виборців.

Ключові слова: інформаційна система, електронне голосування, децентралізований додаток, блокчейн, смарт-контракт, Zero-Knowledge Proof, Semaphore, Web3.

Abstract

The study is devoted to the development of a decentralized information system for anonymous electronic voting using Zero-Knowledge Proofs (ZKP) cryptography. The vulnerabilities of traditional centralized databases were analyzed, and the advantages of the Self-Sovereign Identity (SSI) paradigm for ensuring 100% user privacy were substantiated. The practical implementation of the system includes Solidity smart contracts on the Ethereum test network (Sepolia), a React-based client web application, and the integration of a backend server (Relayer) to enable gasless transactions (Gasless Voting). The proposed solution provides mathematical protection against the falsification of results and makes the deanonymization of voters impossible.

Keywords: information system, electronic voting, decentralized application, blockchain, smart contract, Zero-Knowledge Proof, Semaphore, Web3.

Вступ

У сучасному цифровому суспільстві електронні системи голосування стають ключовим інструментом корпоративного та громадського управління. Проте традиційні інформаційні системи, побудовані на базі централізованих архітектур, мають фундаментальну архітектурну вразливість – проблему єдиної точки відмови. Зберігання персональних даних користувачів на єдиному сервері не лише створює високі ризики масштабних витоків інформації внаслідок кібератак, але й вимагає абсолютної довіри до адміністратора бази даних. У таких умовах адміністратор зберігає технічну можливість маніпулювати результатами волевиявлення або деанонімізувати виборців, зіставивши таблиці ідентифікаторів із таблицями голосів.

Перехід до децентралізованих систем на базі технології блокчейн ефективно вирішує проблему прозорості підрахунку та незмінності даних. Однак публічний характер блокчейну за замовчуванням порушує таємницю голосування, оскільки всі транзакції є відкритими. Вирішенням цієї проблеми є концепція суверенної ідентифікації та інтеграція криптографічних протоколів доведення з нульовим розголошенням. Завдяки цій технології виборець може математично довести смарт-контракту своє право на участь у голосуванні, не розкриваючи при цьому своєї особистості [1-3].

Отже, метою даної роботи є проєктування архітектури та програмна реалізація децентралізованої інформаційної системи для проведення анонімних електронних голосувань. Застосування ZKP дозволить гарантувати криптографічний захист від підробки голосів, а використання механізму делегованих мета-транзакцій забезпечить зручність користувацької взаємодії без необхідності оплати мережевих комісій (Gas fees) кінцевими виборцями.

Результати дослідження

Для вирішення проблеми безпечного та анонімного електронного голосування було спроєктовано та реалізовано децентралізовану мікросервісну архітектуру, що складається з трьох ключових компонентів: смарт-контракту в блокчейні Ethereum-Sepolia (тестова мережа), сервера-ретранслятора (Relayer) на базі Node.js та клієнтського веб-додатка, розробленого з використанням бібліотеки React [4].

В основу забезпечення анонімності покладено криптографічний протокол Semaphore, який реалізує доведення з нульовим розголошенням (zk-SNARKs) [5]. Процес ідентифікації виборця базується на генерації локальних секретних ключів (Trapdoor та Nullifier) безпосередньо у браузері користувача за допомогою технології WebAssembly. З цих секретів обчислюється публічний відбиток (Identity Commitment), який адміністратор системи додає до смарт-контракту. Смарт-контракт не зберігає лінійний масив виборців, а використовує структуру даних «Дерево Меркла» (рис. 1). Це дозволяє оптимізувати витрати газу у мережі Ethereum- Sepolia: смарт-контракт зберігає лише один 32-байтний кореневий хеш (Merkle Root), а перевірка належності виборця до списку виконується за логарифмічний час O(log N).

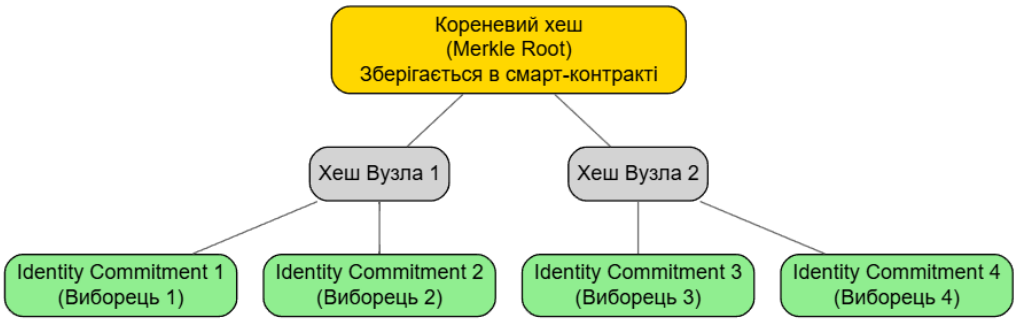


Рис. 1 Структура Дерева Меркла для збереження Identity Commitments

Під час голосування клієнтський додаток генерує криптографічний доказ (ZK-Proof), який математично підтверджує наявність виборця в Дереві Меркла, не розкриваючи його особистості [6]. Для захисту від подвійного голосування система генерує унікальний Nullifier Hash, прив'язаний до ідентифікатора конкретного опитування. Якщо смарт-контракт фіксує спробу повторного використання того самого хешу, транзакція автоматично відхиляється.

Важливим практичним результатом дослідження є вирішення проблеми масштабованості та покращення користувацького досвіду (UX) шляхом впровадження механізму делегованих мета-транзакцій (Gasless Voting). На рисунку 2 представлено архітектуру делегованого виконання транзакцій за допомогою сервера-ретранслятора.

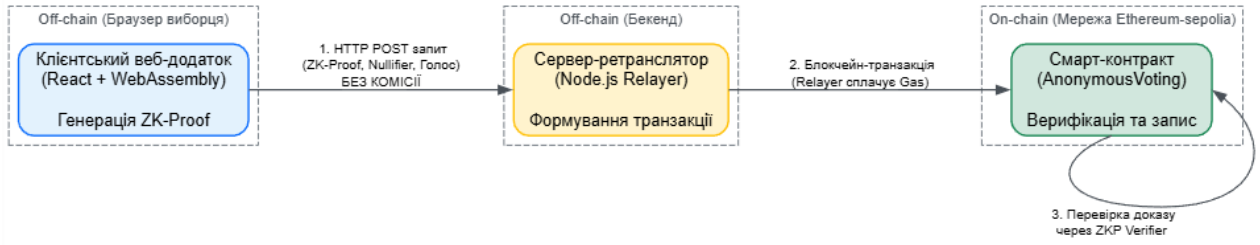


Рис. 2 Архітектура делегованого виконання транзакцій за допомогою сервера-ретранслятора

Як показано на рис. 2, виборець не взаємодіє зі смарт-контрактом напряму і не сплачує комісію мережі у криптовалюті. Замість цього згенерований ZK-доказ передається через стандартний HTTP-запит на сервер-ретранслятор. Сервер верифікує структуру доказу, формує блокчейн-транзакцію, підписує її власним приватним ключем і сплачує комісію за свій рахунок [7]. Оскільки сервер не має доступу до секретних ключів користувача, він технічно не здатний підробити або змінити голос. Така архітектурна модель забезпечує високий рівень стійкості: ретранслятор виконує виключно транспортну

функцію, тоді як криптографічна перевірка валідності доказу здійснюється ізольовано на рівні смарт-контракту. Навіть у випадку компрометації сервера зловмисник не зможе сфальсифікувати волевиявлення або деанонімізувати виборця.

Клієнтський інтерфейс розроблено з акцентом на інтуїтивну зрозумілість та забезпечення безшовного користувацького досвіду, наближеного до традиційних Web2-додатків. Взаємодія з блокчейном відбувається через провайдер Ethers.js та EVM-гаманець (наприклад, MetaMask), який на етапі голосування використовується лише як міст для зчитування даних, а не для підпису платних транзакцій [8-10]. Це кардинально знижує поріг входження для нових користувачів, звільняючи їх від необхідності купувати криптовалюту для участі в опитуванні.

Детальний алгоритм цієї клієнт-серверної взаємодії та етапів перевірки доказу наведено на UML-діаграмі послідовності (рис. 3).

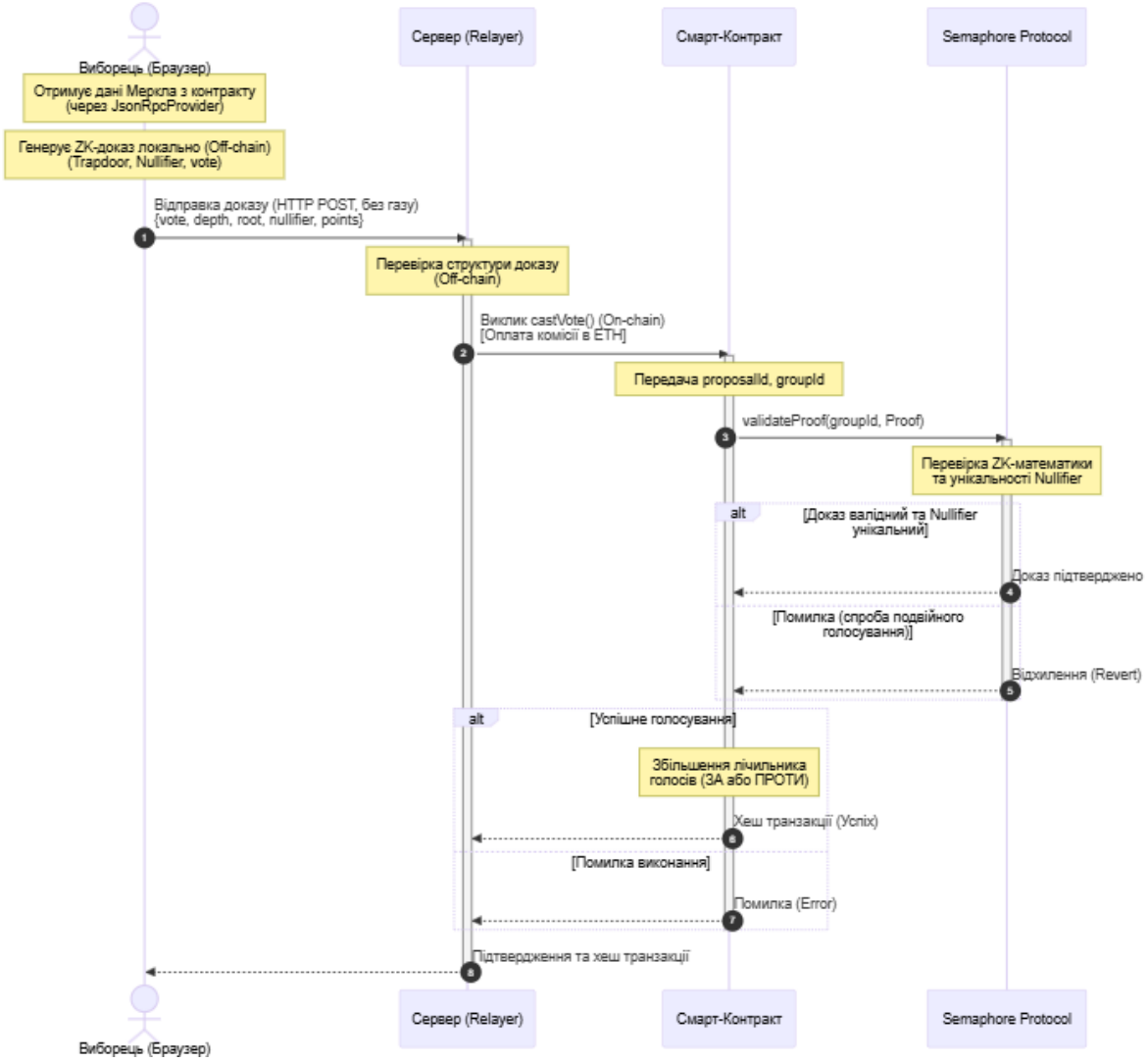


Рис. 3 Архітектура делегованого виконання транзакцій за допомогою сервера-ретранслятора

Як видно з діаграми, життєвий цикл голосування чітко розділено на локальні (Off-chain) та мережеві (On-chain) процеси. Спочатку браузер виборця завантажує актуальні дані Дерева Меркла та локально генерує криптографічний ZK-доказ, використовуючи секретні ключі (Trapdoor, Nullifier). Після передачі доказу на сервер, Relayer ініціює блокчейн-транзакцію castVote(). Далі смарт-контракт делегує перевірку вищої математики протоколу Semaphore. У блоці альтернативних сценаріїв (alt) відображено базовий механізм захисту системи: якщо Nullifier є унікальним – голос зараховується і лічильник збільшується, а у випадку спроби подвійного голосування транзакція миттєво відхиляється (Revert) на рівні смарт-контракту.

Для практичної реалізації цього алгоритму було розроблено зручний графічний інтерфейс. Процес участі в системі розпочинається для користувача з генерації локальної ZK-ідентичності (рис. 4).

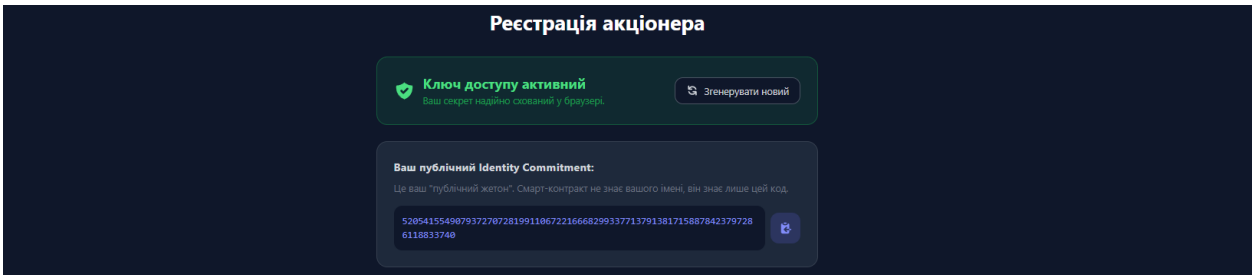


Рис. 4 Інтерфейс генерації криптографічної ідентичності виборця

На цьому етапі система створює публічний відбиток (Identity Commitment), який користувач передає адміністратору для реєстрації, тоді як критичні секретні ключі назавжди залишаються у локальному сховищі браузера. Після підтвердження статусу виборця, користувач отримує доступ до панелі активних опитувань (рис. 5).

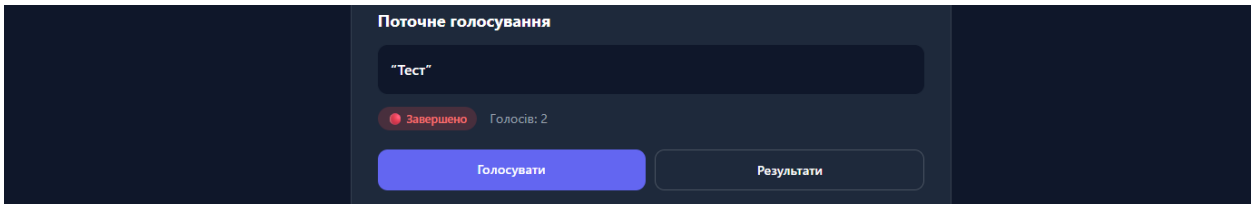


Рис. 5 Інтерфейс процесу анонімного голосування

Після здійснення вибору ініціюється найважливіший криптографічний етап – локальна генерація доказу з нульовим розголошенням.

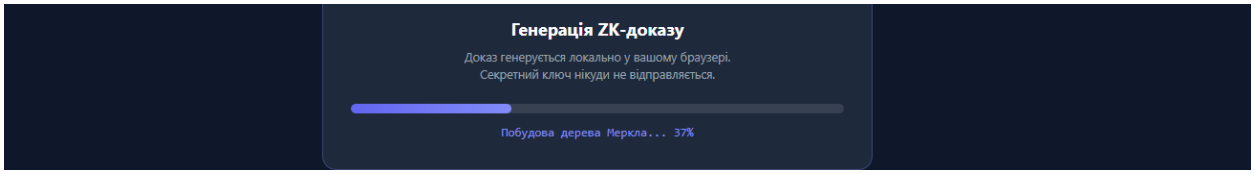


Рис. 6 Візуалізація процесу локальної генерації ZK-доказу у браузері

Після завершення обчислень та делегованої відправки доказу через сервер-ретранслятор, система надає виборцю кінцеве підтвердження успішності операції (рис. 7). Інтерфейс виводить криптографічний хеш транзакції, за допомогою якого можна верифікувати факт запису голосу в блокчейні (через сканер Etherscan), зберігаючи при цьому повну анонімність відправника.

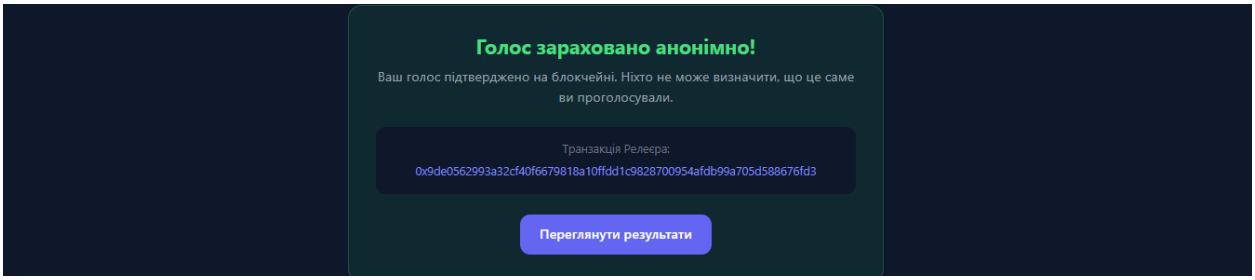
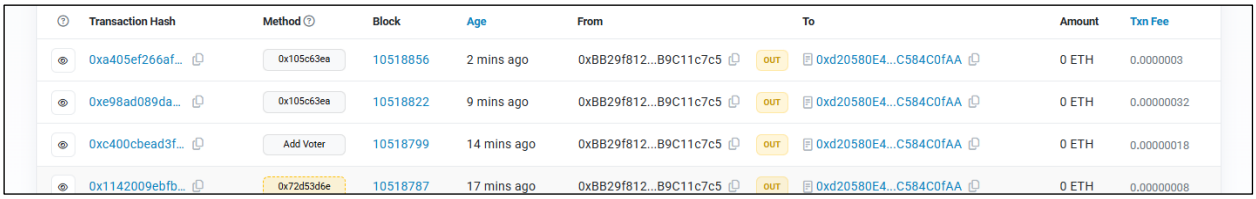


Рис. 7 Екран підтвердження успішного голосування з відображенням хешу транзакції

Інтерфейс дозволяє зробити вибір одним кліком, після чого під капотом ініціюється вищеописаний процес генерації доказу та його ретрансляції. Успішне зарахування голосу підтверджується відповідним сповіщенням, а загальна статистика автоматично оновлюється на блокчейні, що гарантує 100% прозорість підрахунку (рис. 8).

Рис. 8 Відображення результатів голосування в реальному часі

Смарт-контракт успішно верифікує ZK-доказ та безповоротно фіксує голос у мережі. Деталі транзакції підтверджують, що мережеву комісію було сплачено адресою сервера-ретранслятора, тоді як особа виборця залишається криптографічно прихованою (рис. 9).



Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
0xa405ef266af...	0x105c63ea	10518856	2 mins ago	0xBB29f812...B9C11c7c5	OUT	0xd20580E4...C584C0fAA	0 ETH	0.0000003
0xe98ad089da...	0x105c63ea	10518822	9 mins ago	0xBB29f812...B9C11c7c5	OUT	0xd20580E4...C584C0fAA	0 ETH	0.00000032
0xc400cbead3f...	Add Voter	10518799	14 mins ago	0xBB29f812...B9C11c7c5	OUT	0xd20580E4...C584C0fAA	0 ETH	0.00000018
0x1142009ebfb...	0x72d53d6e	10518787	17 mins ago	0xBB29f812...B9C11c7c5	OUT	0xd20580E4...C584C0fAA	0 ETH	0.00000008

Рис. 9 Дані з блокчейн-оглядача sepolia-Etherscan

Висновки

У результаті проведеного дослідження було спроєктовано, розроблено та успішно протестовано прототип децентралізованої інформаційної системи для електронного голосування, в основу якої покладено концепцію Web3 та криптографічні протоколи з нульовим розголошенням (Zero-Knowledge Proofs). Практична реалізація логіки у вигляді смарт-контрактів у блокчейні дозволила фундаментально вирішити проблему єдиної точки відмови (SPOF), притаманну класичним базам даних, та забезпечити математично підтверджену незмінність результатів.

Інтеграція протоколу Semaphore стала ключовим фактором забезпечення абсолютної анонімності виборців. Завдяки виконанню ресурсоємних обчислень виключно у локальному середовищі браузера користувача (за допомогою технології WebAssembly), система гарантує, що секретні ключі ніколи не перетинають межі клієнтського пристрою. Це створює надійне "trustless" середовище, де навіть розробник або адміністратор бази даних математично позбавлений можливості деанонімізувати користувачів, зберігши при цьому 100% захист від подвійного голосування.

Вагомим науково-практичним здобутком роботи є вирішення проблеми складного користувацького досвіду (UX), що є типовим бар'єром для децентралізованих додатків. Впровадження архітектури з використанням автономного сервера-ретранслятора (Relayer) дозволило реалізувати механізм делегованих мета-транзакцій. Це зробило процес голосування повністю безкоштовним (Gasless) та інтуїтивно зрозумілим для кінцевого користувача, абстрагуючи його від складностей взаємодії з EVM-мережами.

Розроблений програмний комплекс є повністю працездатним і розгорнутий у тестовій мережі Ethereum Sepolia. Запропоноване архітектурне рішення володіє високим рівнем масштабованості і може слугувати надійною інноваційною базою для організації безпечних виборчих процесів у корпоративному секторі, децентралізованих автономних організаціях (DAO), а також в органах студентського та громадського самоврядування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Jafar U., Aziz M. A., Shukur Z. Blockchain for Electronic Voting System Review and Open Research Challenges. *Sensors*, 2021. Vol. 21(17). P. 5874. doi: 10.3390/s21175874
2. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014. Vol.151. P.1-32. URL:https://ethereum.github.io/yellowpaper/paper.pdf
3. Ammous S. The Bitcoin Standard: The Decentralized Alternative to Central Banking. Wiley; 1st edition, 2018. 304 p.
4. React: The library for web and native user interfaces [Електронний ресурс]. – Режим доступу: https://react.dev/
5. Semaphore Protocol Documentation [Електронний ресурс]. – Режим доступу: https://docs.semaphore.pse.dev/
6. Jing S., Zheng X., Chen Z. Review and Investigation of Merkle Tree's Technical Principles and Related Application Fields. *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE),* 2021. P. 249-253. doi: 10.1109/CAIBDA53561.2021.00026

7. Antonopoulos A. M., Wood G. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol: O'Reilly Media, 2018. 424 p.
8. Ethers.js: A complete and compact library for interacting with the Ethereum Blockchain [Електронний ресурс]. – Режим доступу: https://docs.ethers.org/v6/
9. EIP-2771: Secure Protocol for Native Meta Transactions [Електронний ресурс]. – Режим доступу: https://eips.ethereum.org/EIPS/eip-2771
10. Solidity Programming Language [Електронний ресурс]. – Режим доступу: https://docs.soliditylang.org

Сірацький Максим Леонідович – студент групи 2ICT-236, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, e-mail: maxsiratskiy123@gmail.com

Войцеховська Ольга Олександрівна – PhD, доцент кафедри системного аналізу та інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: olgav1085@gmail.com.

Siratskyi Maksym L. – student of group 2IST-23b, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: maxsiratskiy123@gmail.com

Voitsekhovska Olha O. – PhD, Associate Professor of the Department of System Analysis and Information Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: olgav1085@gmail.com.