РОЗДІЛ VI. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 681.3.06:005.336.4:37.02 DOI https://doi.org/10.26661/2786-5622-2024-3-22

РОЗВИТОК КІБЕРБЕЗПЕКОВОЇ КОМПЕТЕНТНОСТІ ЗДОБУВАЧІВ ОСВІТИ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ НУЛЬОВОГО РОЗГОЛОШЕННЯ

Колесніченко Ю. В.
студент другого (магістерського) рівня вищої освіти
спеціальності Професійна освіта (Цифрові технології)
Центральноукраїнський державний університет
імені Володимира Винниченка
вул. Шевченка, 1, Кропивницький, Україна
orcid.org/0009-0002-4632-4900
kolesnichenkoyuriu@gmail.com

Трифонова О. М.
доктор педагогічних наук, професор,
завідувач кафедри математики та цифрових технологій
Центральноукраїнський державний університет
імені Володимира Винниченка
вул. Шевченка, 1, Кропивницький, Україна
orcid.org/0000-0002-6146-9844
olenatrifonova82@gmail.com

Соменко Д. В.
кандидат педагогічних наук,
старший викладач кафедри математики та цифрових технологій
Центральноукраїнський державний університет
імені Володимира Винниченка
вул. Шевченка, 1, Кропивницький, Україна
orcid.org/0000-0001-6426-1507
somenkod@gmail.com

Садовий М. І.
доктор педагогічних наук, професор,
професор кафедри математики та цифрових технологій
Центральноукраїнський державний університет
імені Володимира Винниченка
вул. Шевченка, 1, Кропивницький, Україна
orcid.org/0000-0001-6582-6506
smikdpu@i.ua

Ключові слова: *кібербезпекова компетентність, освітній процес, технології*

У статті детально розглянуто переваги та виклики застосування технологій нульового розголошення (Zero-Knowledge, ZK) у криптографічному шифруванні фінансових даних, особливо у сфері професійної та

нульового розголошення, криптографічне шифрування, фінансові дані, кібербезпека, професійна освіта, практичні заняття, проектна діяльність.

професійно-технічної освіти. Ці технології стають все більш актуальними в сучасному цифровому світі, де безпека й конфіденційність даних є пріоритетом.

Розкрито основні принципи роботи ZK-технологій, зокрема, як вони дають можливість довести істинність певного твердження без розголошення додаткової інформації. Описано різні види ZK-протоколів, такі як інтерактивні й неінтерактивні докази, а також zk-SNARKs та zk-STARKs, їх особливості та сфери застосування.

Особливу увагу приділено практичній інтеграції ZK-технологій в освітній процес і розвитку кібербезпекової компетентності здобувачів освіти. Описано кроки створення вузла для підключення до блокчейну як навчального інструменту, включно з налаштуванням програмного забезпечення та виконанням смарт-контрактів із використанням ZK.

Розглянуто можливості застосування ZK у фінансовій сфері: забезпечення анонімності транзакцій, захист конфіденційної інформації та підвищення безпеки операцій. Визначено переваги цих технологій, зокрема високий рівень конфіденційності та масштабованість.

Також проаналізовано виклики впровадження ZK, такі як складність реалізації, високі обчислювальні витрати й потреба в спеціалізованих знаннях. Обговорено питання стандартизації та сумісності з наявними системами.

Запропоновано методики впровадження ZK-технологій в освітній процес закладу професійної освіти, включно з практичними заняттями та проєктною діяльністю. Це сприяє розвитку навичок роботи із сучасними блокчейн-технологіями, підготовці здобувачів освіти до викликів цифрової епохи та розвитку в студентів кібербезпекової компетентності.

DEVELOPMENT OF CYBERSECURITY COMPETENCE OF EDUCATION SEEKERS THROUGH THE APPLICATION OF ZERO-KNOWLEDGE TECHNOLOGIES

Kolesnichenko Y. V.
Student of the Second (Master's) Level of Higher Education
Specialty: Vocational Education (Digital Technologies)
Volodymyr Vynnychenko Central Ukrainian State University
Shevchenko str., 1, Kropyvnytskyi, Ukraine
orcid.org/0009-0002-4632-4900
kolesnichenkoyuriu@gmail.com

Tryfonova O. M.
Doctor of Pedagogical Sciences, Professor,
Head of the Department of Mathematics and Digital Technologies
Volodymyr Vynnychenko Central Ukrainian State University
Shevchenko str., 1, Kropyvnytskyi, Ukraine
orcid.org/0000-0002-6146-9844
olenatrifonova82@gmail.com

Somenko D. V.
Candidate of Pedagogical Sciences,
Senior Lecturer at the Department of Mathematics and Digital Technologies
Volodymyr Vynnychenko Central Ukrainian State University
Shevchenko str., 1, Kropyvnytskyi, Ukraine
orcid.org/0000-0001-6426-1507
somenkod@gmail.com

Sadovyi M. I.
Doctor of Pedagogical Sciences, Professor,
Professor at the Department of Mathematics and Digital Technologies
Volodymyr Vynnychenko Central Ukrainian State University
Shevchenko str., 1, Kropyvnytskyi, Ukraine
orcid.org/0000-0001-6582-6506
smikdpu@i.ua

Key words: *cybersecurity competence, educational process, zero-knowledge technologies, cryptographic encryption, financial data, cybersecurity, vocational education, practical classes, project activities.*

The article examines in detail the advantages and challenges of applying zero-knowledge (ZK) technologies in cryptographic encryption of financial data, especially in the field of professional and vocational education. These technologies are becoming increasingly relevant in today's digital world, where data security and confidentiality are a priority.

The main principles of ZK technologies are revealed, particularly how they allow proving the truth of a certain statement without disclosing additional information. Various types of ZK protocols are described, such as interactive and non-interactive proofs, as well as zk-SNARKs and zk-STARKs, along with their features and application areas.

Special attention is paid to the practical integration of ZK technologies into the educational process and the development of cybersecurity competence among education seekers. The steps for creating a node to connect to the blockchain as an educational tool are outlined, including software configuration and the execution of smart contracts using ZK.

The possibilities of applying ZK in the financial sector are considered: ensuring transaction anonymity, protecting confidential information, and enhancing the security of operations. The advantages of these technologies are identified, including a high level of confidentiality and scalability.

The challenges of implementing ZK are also analyzed, such as the complexity of realization, high computational costs, and the need for specialized knowledge. Issues of standardization and compatibility with existing systems are discussed.

Methodologies for implementing ZK technologies into the educational process of vocational education institutions are proposed, including practical classes and project activities. This approach fosters the development of skills in working with modern blockchain technologies, prepares education seekers for the challenges of the digital era, and enhances their cybersecurity competence.

Постановка проблеми. У сучасному світі інформаційні технології відіграють ключову роль у розвитку фінансового сектору, забезпечуючи швидкий та надійний обмін інформацією [1]. Проте зростання обсягів даних і кількості транзакцій супроводжується зростанням кіберзагроз і ризиків, пов'язаних із витоком конфіденційної інформації [2]. Використання передових криптографічних методів, зокрема технологій нульового розголошення (Zero-Knowledge, ZK), стає необхідністю для забезпечення безпеки та конфіденційності фінансових даних. У сучасних умовах фахівці повинні бути готові до впровадження новітніх технологій.

Педагогічні дослідження [10] свідчать, що метод проєктів є найефективнішим під час інтеграції інновацій в освітній процес. Тому ми вважаємо, що найкращий спосіб ознайомити здобувачів освіти з використанням технологій нульового розголошення (ZK) у криптографічному шифруванні фінансових даних – це залучення їх до практичних проєктів зі створення блокчейн-вузлів. Це дає змогу підготувати фахівців, здатних працювати з передовими технологіями захисту даних, сприятиме розвитку в студентів кібербезпекової компетентності.

Технологія нульового розголошення є методом криптографічного захисту, який дає змогу одній стороні (доказувачу) довести іншій стороні (верифікатору) правильність певного твердження без розкриття самої інформації, на основі якої це твердження робиться [1]. Це означає, що верифікатор може переконатися в правильності заяви, не отримуючи при цьому жодної додаткової інформації про самі дані. Такий підхід забезпечує високий рівень конфіденційності й безпеки, що є надзвичайно важливим для фінансових транзакцій та обробки персональних даних.

Розвиток технологій нульового розголошення став можливим завдяки розвитку складних математичних методів і алгоритмів, таких як ZK-SNARKs (Succinct Non-Interactive Arguments of Knowledge) та ZK-STARKs (Scalable Transparent Arguments of Knowledge) [7]. Ці методи дають змогу створювати компактні й ефективні криптографічні докази, які можуть бути легко перевірені без необхідності розкривати самі дані. Вони вже успішно застосовуються в різних криптовалютах, таких як Zcash, для забезпечення анонімності та конфіденційності транзакцій.

Упровадження технологій нульового розголошення в професійній (професійно-технічній) освіті є важливим кроком для підготовки фахівців, здатних працювати із сучасними криптографічними методами захисту даних, і розвитку в студентів кібербезпекової компетентності. Це не лише підвищує рівень знань і навичок здобувачів освіти, але й сприяє розвитку інноваційних підходів до захисту інформації у фінансовій сфері. Здобувачі освіти, які володіють знаннями та навичками роботи з технологіями нульового розголошення, будуть здатні ефективно вирішувати завдання із забезпечення конфіденційності та безпеки даних, що є надзвичайно важливим у сучасному світі, де інформаційна безпека є ключовим фактором успішної роботи будь-якої організації.

У цій статті детально розглянуто основні принципи технологій нульового розголошення, їх види та можливості використання у фінансовій сфері. Особливу увагу приділено захисту конфіденційності транзакцій, верифікації фінансових даних без розкриття їх змісту та захисту персональних даних. Наведені переваги та виклики, пов'язані з реалізацією технологій нульового розголошення, а також методи їх впровадження в освітній процес закладів професійної освіти.

Аналіз останніх досліджень і публікацій. Одними з перших дослідників, які заклали теоретичні основи технологій нульового розголошення, були Шафі Ґольдвассер, Сільвіо Мікалі та Чарльз Раков, які в 1985 році представили концепцію нульових доказів знання [3]. Їхні роботи стали фундаментом для подальшого розвитку ZK-технологій та їх застосування в різних галузях, включно з освітою.

У контексті впровадження технологій нульового розголошення в освітній процес дослідження зосереджені на розробці методики навчання криптографічних методів із метою підготовки фахівців, здатних працювати з передовими технологіями захисту даних, і розвитку в здобувачів освіти кібербезпекової компетентності.

Дослідники з провідних університетів, таких як Массачусетський технологічний інститут (MIT) і Стенфордський університет, активно працюють над впровадженням курсів, присвячених технологіям нульового розголошення та їх застосуванню в різних сферах [5]. Вони розробляють навчальні матеріали та програми, які допомагають здобувачам освіти зрозуміти складні математичні концепції та застосувати їх на практиці. Наприклад, курс Applied Cryptography в MIT містить модулі, присвячені Zero-Knowledge доказам та їх використанню в сучасних криптосистемах.

Аналіз досвіду ряду університетів і дослідницьких інститутів по всьому світу свідчить, що вони активно працюють над розробкою методики навчання технологій нульового розголошення та розвитку на її основі кібербезпекової компетентності здобувачів освіти:

Професор Домінік Унру (Dominique Unruh) з Університету Тарту (https://ut.ee/en/) спеціалізується на дослідженнях у галузі нульових доказів та їх застосуванні в блокчейні та криптовалютах [9]. Він розробляє курси й навчальні матеріали, що дають змогу здобувачам освіти глибоко зрозуміти математичні основи ZKP та їх практичне застосування.

Під керівництвом професора Уелі Маурера (Ueli Maurer), Інститут інформаційної безпеки ETH Zurich (https://infsec.ethz.ch/) активно досліджує криптографічні протоколи, включаючи ZKP [8]. Вони пропонують курси для магістрів та аспірантів, що передбачають сучасні криптографічні методи та їх застосування.

Дослідники Університету Джорджа Вашингтона (https://cs.engineering.gwu.edu/) займаються проєктами, спрямованими на інтеграцію ZKP

у навчальні програми з комп'ютерних наук та інформаційної безпеки. Вони розробляють лабораторні роботи та практичні завдання, що допомагають здобувачам освіти застосовувати теорію на практиці.

Відповідні дослідження щодо впровадження ZKP проводяться і в Україні:

Кафедра математичних методів захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (https://kpi.ua/mmzi/) активно досліджує криптографічні протоколи, включно з нульовими доказами знання (ZKP). Вони проводять наукові семінари й публікують роботи, присвячені сучасним методам криптографії та їх застосуванню в інформаційній безпеці.

Факультет комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка (https://csc.knu.ua/uk/) пропонує курси з криптографії та інформаційної безпеки, де розглядаються нульові докази знання. Викладачі й дослідники публікують наукові статті [3; 4; 6] та беруть участь у міжнародних конференціях [11] з криптографії.

Кафедра безпеки інформаційних технологій Харківського національного університету радіоелектроніки (https://its.nure.ua/) займається дослідженнями в галузі криптографії, зокрема ZKP. Вони реалізують проєкти, спрямовані на вдосконалення методів захисту інформації та інтеграцію сучасних криптографічних протоколів у навчальні програми.

Метою статті є дослідження переваг і викликів застосування технологій нульового розголошення в криптографічному шифруванні фінансових даних у контексті розвитку кібербезпекової компетентності здобувачів освіти.

Завданнями є аналіз основних принципів ZK-технологій, їх видів, можливостей використання у фінансовій сфері, розробка методик розвитку кібербезпекової компетентності здобувачів освіти та впровадження цих технологій в освітній процес на прикладі створення вузла системи для підключення до блокчейну.

Виклад основного матеріалу. Технології нульового розголошення (Zero-Knowledge, ZK) – це інноваційний напрям у криптографії, який дає змогу забезпечити безпрецедентний рівень конфіденційності та безпеки фінансових даних. В основі цих технологій лежать складні математичні концепції, які дають можливість одній стороні (доказувачу) переконати іншу сторону (верифікатора) у правдивості певного твердження, не розкриваючи при цьому жодної додаткової інформації.

Під час розвитку кібербезпекової компетентності здобувачів освіти варто звернути увагу на ключові принципи ZK-технологій:

Збереження конфіденційності (доведення правильності тверджень без розкриття зайвих даних).

Компактність доказів (створення стислих криптографічних доказів, які легко перевірити).

Стійкість до маніпуляцій (неможливість створення фальшивих доказів, які могли б пройти перевірку).

У сучасній криптографії [1] найбільш відомими видами ZK-технологій є ZK-SNARKs та ZK-STARKs. ZK-SNARKs (Succinct Non-Interactive Arguments of Knowledge), які відрізняються компактністю та швидкою верифікацією, що робить їх особливо привабливими для використання у криптовалютах. ZK-STARKs пропонують підвищену прозорість та масштабованість, що робить їх ідеальними для децентралізованих систем.

Застосування ZK-технологій у фінансовій сфері надає широкі можливості для:

захисту конфіденційності транзакцій (забезпечення анонімних платежів та приватності в децентралізованих фінансах (DeFi);

верифікації фінансових даних без розкриття їх змісту (можливість підтвердження платоспроможності або здійснення платежів без розкриття конкретних сум);

захисту персональних даних (забезпечення відповідності регуляторним вимогам щодо захисту особистої інформації).

У межах освітнього процесу увагу здобувачів освіти варто звернути на те, що ці технології мають переваги в прозорості, оскільки не потребують довіреного початкового встановлення і є стійкими до квантових атак, що робить їх перспективними для майбутніх застосувань. Вони також відрізняються високою масштабованістю, що дає змогу обробляти великі обсяги даних. Однак ZK-STARKs мають більший розмір доказів порівняно із ZK-SNARKs, що може впливати на швидкість передачі.

Як приклад, пропонуємо розглянути фрагмент заняття, яке відображає принцип роботи протоколів нульового розголошення, використовуючи просту аналогію.

Задача з кольоровими кульками

Сценарій

Уявіть, що у вас є дві кульки однакового розміру та форми, але різних кольорів – червона та зелена. Ваш друг, який не розрізняє кольорів (або перебуває в кімнаті з приглушеним світлом), не вірить, що кульки дійсно різного кольору. Він хоче, щоб ви довели йому, що кульки відрізняються за кольором, але ви не бажаєте розкривати, яка кулька якого кольору.

Протокол доведення

Підготовка: ви і ваш друг перебуваєте в одній кімнаті. Він може бачити, що у вас є дві кульки, але не може відрізнити їх за кольором.

Процес доведення: ваш друг бере обидві кульки і ховає їх за спиною. Він випадково вибирає одну кульку і показує її вам. Потім він ховає кульку знову за спину. Після цього він може або залишити ту саму кульку в руці або поміняти її на іншу (знову випадково). Він знову показує вам кульку і запитує: «Чи поміняв я кульку?»

Ваша відповідь: оскільки ви бачите кольори, ви можете точно сказати, чи поміняв він кульку, чи ні. Якщо кольори збігаються, ви відповідаєте: «Ні, не поміняв». Якщо кольори різні, ви відповідаєте: «Так, поміняв».

Повторення: цей процес повторюється кілька разів (наприклад, 10 разів), щоб виключити можливість випадкового вгадування.

Аналіз протоколу

Нульове розголошення: ви доводите, що можете відрізнити кульки, не розкриваючи їхні кольори.

Переконання: після багаторазового повторення ваш друг переконується, що ймовірність випадкового вгадування надзвичайно мала.

Безпека: ви не розкриваєте жодної додаткової інформації про самі кульки.

Використання на занятті

Демонстрація викладача: викладач проводить цю демонстрацію перед групою здобувачів освіти, пояснюючи кожен крок.

Групова робота: здобувачі освіти діляться на пари й відтворюють протокол між собою.

Обговорення

На завершення заняття бажано поставити перед здобувачами освіти питання, які б розкрили глибину розуміння ними обговорюваної проблеми:

Як цей протокол забезпечує нульове розголошення?

Чому багаторазове повторення підвищує довіру до доведення?

Можливі вдосконалення або варіації.

Використання протоколу Fiat-Shamir

Ініціалізація:

Користувач і сервер домовляються про публічне модульне число n, яке є добутком двох великих простих чисел p і q:

$$n = p \times q.$$

Наприклад, візьмемо:

$$p = 11,\ q = 13,\ n = 11 \times 13 = 143.$$

Користувач вибирає секретне число s, взаємно просте з n: $s = 7$.

Обчислення публічного ключа (v):

$$v = s^2 \ mod\ n,$$

$$\mathrm{v} = 7^2 \ mod\ 143 = 49.$$

Користувач повідомляє серверу v, але тримає s в секреті.

Аутентифікація:

Користувач генерує випадкове число r, взаємно просте з n: $r = 10$.

Обчислює x:

$$x = r^2 \ mod\ n = 10^2 \ mod\ 143 = 100.$$

Відправляє x серверу.

Сервер генерує випадковий біт запиту $e \in \{0, 1\}$: $e = 1$.

Користувач обчислює відповідь y:

$$y = r * s^e \ mod\ n.$$

Оскільки $e = 1$:

$$y = 10 * 7 \ mod\ 143 = 70.$$

Відправляє y серверу.

Перевірка на сервері:

Сервер перевіряє таку рівність:

$$y^2 \ mod\ n = x * v^e \ mod\ n.$$

Підставляємо значення:

$$y^2 \ mod\ n\ 70^2 \ mod\ 143 = 4900 \bmod 143 = 38,$$

$$x * v^e \ mod\ n = x * v \ mod\ n = 100 * 49 \ mod\ 143 = 4900 \ mod\ 143 = 38.$$

Оскільки ліва і права частини рівні, перевірка успішна. Користувач довів серверу, що знає секретне число s, оскільки рівність виконується, але сервер не може обчислити s зі знання y, x, v, n.

Висновки. Упровадження технологій нульового розголошення в професійну освіту є стратегічно важливим кроком для підготовки фахівців, здатних забезпечити високий рівень захисту даних у фінансовій сфері. Це сприяє розвитку інновацій у галузі кібербезпеки й підвищує конкурентоспроможність випускників на ринку праці. Застосування ZK-технологій в освіті забезпечує здобувачам освіти необхідні знання та навички для успішної кар'єри в сучасному цифровому світі.

Використання практичних прикладів, таких як задача з кольоровими кульками, дає змогу здобувачам освіти глибше зрозуміти складні теоретичні концепції нульових доказів. Цей підхід сприяє активному залученню здобувачів освіти в освітній процес, розвиває критичне мислення та вміння застосовувати знання на практиці. Така методика не лише полегшує розуміння матеріалу, але й робить навчання цікавим та інтерактивним. Здобувачі освіти мають можливість брати участь у рольових іграх, обговорювати різні сценарії та аналізувати безпекові аспекти протоколів.

З огляду на досвід провідних університетів і дослідницьких інститутів акцент на педагогічних аспектах є ключовим для успішного впровадження технологій нульового розголошення в освітній процес. Розробка навчальних програм, що поєднують теоретичні знання з практичними завданнями, сприяє формуванню кібербезпекової компетентності здобувачів освіти та забезпечує стійкий розвиток інформаційного суспільства.

ЛІТЕРАТУРА

1. Ernstberger J., Chaliasos S., Zhou L., Jovanovic P., Gervais A. Do You Need a Zero Knowledge Proof? *Cryptology ePrint Archive*, Paper 2024/050, 2024. URL: https://eprint.iacr.org/2024/050.
2. Bowe S., Gabizon A., Green M. Zcash: Zerocash: Decentralized Anonymous Payments from Bitcoin. 2018. URL: https://ieeexplore.ieee.org/document/6956581[.
3. Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Cryptology ePrint Archive, Paper 2014/674, 2014. URL: https://eprint.iacr.org/2013/879.pdf.
4. Petkus M. Why and How zk-SNARK Works: Definitive Explanation. arXiv, 2019. URL: https://arxiv.org/abs/1906.07221.
5. Gogol K., Messias J., Silva M. I., Livshits B. The Writing is on the Wall: Analyzing the Boom of Inscriptions and Its Impact on Rollup Performance and Cost Efficiency. arXiv, 2024. URL: https://arxiv.org/abs/2404.11189.
6. Sober M., Scaffino G., Schulte S. Cross-Blockchain Communication Using Oracles With an Off-Chain Aggregation Mechanism Based on zk-SNARKs. arXiv, 2023. URL: https://arxiv.org/abs/2405.08395.
7. Chen T., Lu H., Kunpittaya T., Luo A. A Review of zk-SNARKs. arXiv, 2022. URL: https://arxiv.org/abs/2202.06877.
8. Профіль професора Уелі Маурера (Ueli Maurer). URL: https://people.inf.ethz.ch/maurer/.
9. Профіль професора Домініка Унру (Dominique Unruh). URL: https://scholar.google.com/citations?user=EROP4tsAAAAJ&hl=en/.
10. Тадеуш О. М. Метод проєктів як форма продуктивного навчання студентів. Електронний архів Національного педагогічного університету імені М. П. Драгоманова, 2017. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/19155/Tadeush.pdf?sequence=1.
11. ETH:Kyiv – конференція Premier Ethereum в Україні. URL: https://www.ethkyiv.org/.

REFERENCES

1. Ernstberger, J., Chaliasos, S., Zhou, L., Jovanovic, P., & Gervais, A. (2024). Do you need a zero knowledge proof? [Preprint]. Cryptology ePrint Archive. https://eprint.iacr.org/2024/050.
2. Bowe, S., Gabizon, A., & Green, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In 2014 IEEE Symposium on Security and Privacy (pp. 459–474). IEEE. https://doi.org/10.1109/SP.2014.36.
3. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2013). Succinct non-interactive zero knowledge for a von Neumann architecture [Preprint]. Cryptology ePrint Archive. https://eprint.iacr.org/2013/879.
4. Petkus, M. (2019). Why and how zk-SNARK works: Definitive explanation [Preprint]. arXiv. https://arxiv.org/abs/1906.07221.
5. Gogol, K., Messias, J., Silva, M. I., & Livshits, B. (2024). The writing is on the wall: Analyzing the boom of inscriptions and its impact on rollup performance and cost efficiency [Preprint]. arXiv. https://arxiv.org/abs/2404.11189.
6. Sober, M., Scaffino, G., & Schulte, S. (2023). Cross-blockchain communication using oracles with an off-chain aggregation mechanism based on zk-SNARKs [Preprint]. arXiv. https://arxiv.org/abs/2405.08395.
7. Chen, T., Lu, H., Kunpittaya, T., & Luo, A. (2022). A review of zk-SNARKs [Preprint]. arXiv. https://arxiv.org/abs/2202.06877.
8. Profile of Professor Ueli Maurer. Retrieved from https://people.inf.ethz.ch/maurer/.
9. Profile of Professor Dominique Unruh. Retrieved from https://scholar.google.com/citations?user=EROP4tsAAAAJ&hl=en/.
10. Tadeush, O.M. (2017). Metod proiektiv yak forma produktyvnoho navchannia studentiv [The project method as a form of productive learning for students]. Elektronnyi arkhiv Natsionalnoho Pedahohichnoho Universytetu imeni M.P. Drahomanova. https://enpuir.npu.edu.ua/handle/123456789/19155/.
11. ETH:Kyiv – Ukraine's Premier Ethereum Conference. Retrieved from https://www.ethkyiv.org/.