КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.867
УДК 004.056.5

Овсянко Дмитро Олексійович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0003-7758-0613
dmytro.o.ovsianko@lpnu.ua

Нємкова Олена Анатоліївна
д.т.н., професор, професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

СМАРТ-КОНТРАКТИ ЯК МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ В РОЗПОДІЛЕНИХ СИСТЕМАХ ЦИФРОВИХ ДВІЙНИКІВ

Анотація. Розгортання розподілених цифрових систем-двійників у таких сферах, як охорона здоров'я, виробництво та критична інфраструктура, загострило питання захисту приватності даних. У цих системах цифрові двійники взаємодіють з великою кількістю пристроїв та користувачів, що підвищує ризики витоку або несанкціонованого доступу до чутливої інформації. Традиційні централізовані механізми управління ідентифікацією та контролем доступу не відповідають вимогам сучасних розподілених систем, оскільки обмежені в масштабованості, автономності та рівні приватності. У статті досліджено можливості використання смарт-контрактів, що функціонують у блокчейн-середовищі, для забезпечення децентралізованого управління доступом до даних цифрових двійників. Смарт-контракти здатні забезпечити прозоре і надійне виконання політик доступу без участі централізованих посередників. В роботі розглянуто інтеграцію сучасних криптографічних технологій у процеси роботи смарт-контрактів, зокрема використання доказів з нульовим розголошенням, децентралізованих ідентифікаторів (DID) та конфіденційних обчислень. Застосування таких рішень дозволяє підтверджувати права доступу, забезпечувати приватність і безпеку операцій без розкриття конфіденційної інформації. Також проаналізовано обмеження існуючих підходів, серед яких висока вартість транзакцій у публічних блокчейнах, низька продуктивність традиційних смарт-контрактів та складності з інтеграцією конфіденційних обчислень у пристрої з обмеженими ресурсами. Запропоновано напрями подальших досліджень, зокрема оптимізацію архітектур другого рівня (Layer 2) для підвищення продуктивності, розробку безпечних механізмів аудиту та забезпечення сумісності з суверенними системами ідентифікації. У висновках наголошується, що приватність повинна стати базовою властивістю цифрових двійників. Смарт-контракти у таких системах повинні виконувати не лише логіку управління, але й функцію довірених агентів, які гарантують дотримання політик доступу та нормативних вимог у децентралізованих екосистемах.

Ключові слова: цифрові двійники; приватність даних; смарт-контракти; блокчейн і децентралізоване управління доступом; докази з нульовим розголошенням (ZKP); децентралізовані ідентифікатори (DID); конфіденційні обчислення.

ВСТУП

Цифрові двійники — це віртуальні моделі фізичних систем, які у реальному часі відображають їхню поведінку та стан. Вони все частіше застосовуються у таких важливих сферах, як охорона здоров'я, промислове виробництво та управління критичною інфраструктурою. У міру того як ці системи стають дедалі більш розподіленими та взаємопов'язаними, зростають виклики щодо забезпечення безпеки даних, контролю доступу та захисту приватності користувачів. Традиційні централізовані механізми

виявляються недостатніми для забезпечення конфіденційності, довіри та аудиту в таких динамічних і децентралізованих середовищах.

Смарт-контракти на блокчейн-платформах становлять перспективне рішення, оскільки забезпечують автоматизовану, верифіковану та захищену від стороннього втручання реалізацію політик приватності. Однак притаманна їм прозорість і обчислювальні обмеження створюють значні ризики при роботі з конфіденційними даними. У статті досліджується, як смарт-контракти, у поєднанні з передовими криптографічними методами та децентралізованими системами ідентифікації, можуть забезпечити високий рівень приватності в розподілених архітектурах цифрових двійників.

Постановка проблеми. Основна проблема полягає в тому, що традиційні централізовані механізми управління ідентифікацією та контролем доступу, які застосовувалися в інформаційних системах попередніх поколінь, виявилися неспроможними ефективно захищати дані в умовах сучасних розподілених архітектур. Вони не відповідають критичним вимогам масштабованості, автономності, гнучкості та забезпечення приватності в динамічних і міжорганізаційних середовищах, де довіра до централізованих посередників часто є обмеженою або взагалі відсутня.

Таким чином, існує нагальна потреба у пошуку нових підходів до управління доступом і захисту даних, які б враховували специфіку розподілених цифрових систем-двійників. Впровадження децентралізованих рішень на основі блокчейн-технологій та смарт-контрактів розглядається як перспективний напрямок подолання зазначених обмежень. Смарт-контракти, здатні автоматично виконувати заздалегідь визначені правила, створюють потенційно надійну основу для реалізації прозорих, контрольованих і незалежних політик доступу у складних розподілених екосистемах. Однак ефективність та безпечність такого підходу потребує подальшого дослідження та вдосконалення, особливо у контексті забезпечення приватності в цифрових двійниках нового покоління.

Метою статті є систематизація сучасних підходів до забезпечення приватності в розподілених системах цифрових двійників із фокусом на використання смарт-контрактів і децентралізованих технологій, а також окреслення перспектив подальших досліджень у цій галузі.

У статті вирішені наступні **завдання**:

- проведено аналіз сучасного стану досліджень і практик впровадження цифрових двійників у критичних галузях (охорона здоров’я, виробництво, критична інфраструктура) з погляду ризиків для приватності,
- надана оцінка ефективності традиційних централізованих рішень для управління доступом і ідентифікацією у децентралізованих середовищах,
- розглянуто потенціал смарт-контрактів у підвищенні приватності через автоматизоване, прозоре та незмінне застосування політик доступу,
- проаналізовано сучасні криптографічні методи (докази з нульовим розголошенням, DID, конфіденційні обчислення), придатні для інтеграції у розподілені цифрові двійники,
- визначено обмеження наявних рішень і окреслено напрями майбутніх досліджень, включаючи масштабування, аудит та взаємодію з системами цифрової ідентичності.

Враховуючи зростаючу роль цифрових двійників у критичних сферах, дослідження таких підходів є надзвичайно актуальним. Це дозволяє формувати надійні основи для створення децентралізованих безпечних систем, що відповідатимуть сучасним вимогам до приватності та довіри.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні підходи до забезпечення приватності в розподілених системах

Історично розподілені системи покладаються на відомі механізми контролю доступу: контроль доступу на основі ролей (Role-Based Access Control, RBAC) та контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC). RBAC визначає права доступу на основі попередньо визначених ролей в організації, тоді як ABAC надає доступ відповідно до атрибутів користувача, типів ресурсів та умов середовища [1]. Обидві моделі широко використовуються в корпоративних системах і хмарних платформах, але не підходять для динамічних, децентралізованих чи розподілених середовищ, таких як IoT і екосистеми цифрових двійників. У розподілених системах автентифікація зазвичай здійснюється через централізовані сервери, які видають і перевіряють облікові дані з використанням схем OAuth 2.0 або JSON Web Token (JWT) [2]. Незважаючи на свою ефективність, ці моделі створюють єдину точку відмови (рис. 1) і збільшують поверхню атаки, особливо в сценаріях, що включають кілька незалежних джерел даних і учасників.

У проєкті MyDigiTwin питання приватності цифрових двійників вирішується за рахунок використання федеративного навчання, яке дозволяє тренувати прогностичні моделі на розподілених даних без передачі самих даних за межі установ. Замість централізованого збору медичної інформації, алгоритми «подорожують» до місць зберігання даних (концепція Personal Health Train), де виконують локальні обчислення, після чого повертаються лише агреговані результати. Це забезпечує відповідність вимогам загального регламенту захисту даних (GDPR) та дозволяє безпечно співпрацювати між різними організаціями. Окрім цього, MyDigiTwin інтегрується з особистими медичними середовищами, що дає пацієнтам змогу самостійно ініціювати симуляції сценаріїв (наприклад, зміну способу життя) та отримувати прогнози ризику без передачі своїх даних назовні. Для забезпечення сумісності даних у системі реалізовано механізм гармонізації відповідно до стандарту FHIR, що дозволяє уніфікувати різнорідні медичні записи без розкриття змісту. Таким чином, MyDigiTwin поєднує персоналізацію, інтероперабельність і дотримання приватності, що є критично важливим для безпечного застосування цифрових двійників у медицині [3].

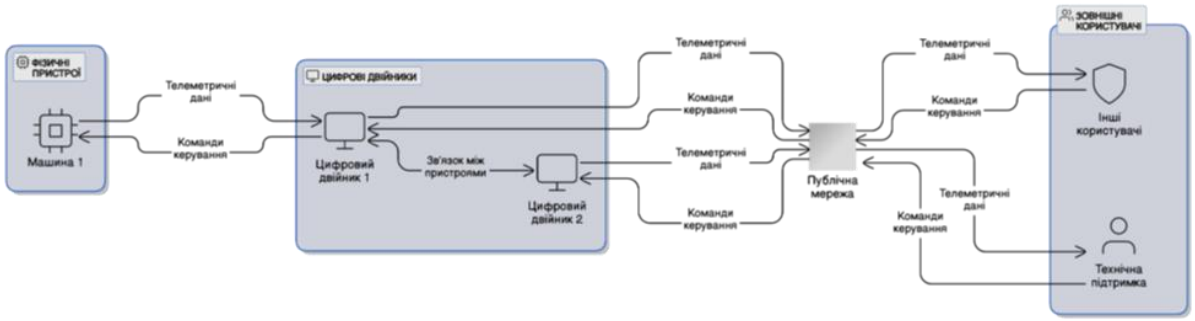

Рис. 1. Архітектура взаємодії фізичного пристрою з цифровими двійниками та зовнішніми користувачами через централізований шлюз

У статті «*Analysis of Personal Privacy Leakage under the Background of Digital Twin*» автори досліджують ризики витоку персональних даних, спричинені впровадженням цифрових двійників, зокрема через зловживання великими даними, непрозорість алгоритмів (ефект «чорної скриньки») та низьку обізнаність громадськості щодо захисту конфіденційності. Аналізуються приклади судових справ, де компанії незаконно використовували або продавали особисту інформацію користувачів. У відповідь на ці

виклики пропонується модель правового співуправління, що включає координацію зусиль держави, суспільства та окремих громадян. Автори наголошують на необхідності комплексного підходу — через вдосконалення законодавства, етичних норм, технічного регулювання та підвищення правової грамотності населення — для побудови безпечного середовища застосування цифрових двійників [4].

Технології блокчейн пропонують децентралізовані альтернативи традиційним моделям безпеки. Забезпечуючи незмінність реєстрів і децентралізований консенсус, блокчейн усуває потребу в центральних системах керування і підтримує захист від несанкціонованого доступу до журналів подій [5]. Смарт-контракти, розгорнуті на таких платформах, як Ethereum, Hyperledger Fabric та Polkadot, діють як автономні агенти, що виконують код при виконанні заздалегідь визначених умов. Вони все частіше використовуються для впровадження децентралізованого контролю доступу, забезпечення дотримання політик щодо даних та управління цифровими активами.

Однак, блокчейн-системи стикаються з невід'ємними проблемами конфіденційності, в тому числі:

- Відкритість даних: публічні блокчейни зберігають дані про транзакції прозоро, що може суперечити вимогам конфіденційності.
- Витрати на газ — блокчейн платформи використовують цей термін для позначення вартості однієї транзакції. Виконання складних операцій в ланцюжку може бути дорогим.
- Негнучкість: Смарт-контракти як правило є незмінними, що обмежує їхню адаптивність після розгортання.

Щоб пом'якшити ці проблеми, часто використовують гібридні моделі, що поєднують мережеві смарт-контракти з позамережевим сховищем (наприклад, IPFS, Filecoin), хоча це призводить до додаткової архітектурної складності.

Приклад інтеграції блокчейн з цифровими двійниками було описано у статті «*Blockchain-enabled digital twin system for brain stroke prediction*». Де запропоновано модель цифрового двійника для медицини, яка поєднує алгоритми машинного навчання з консорціумною блокчейн-технологією для точного передбачення ризику інсульту. Основною інновацією є інтеграція блокчейн-системи, що забезпечує незмінність даних, виявлення спроб їх підробки та автоматичне відновлення оригінальних значень. Система має масштабовану архітектуру, що дозволяє легко адаптувати її до інших патологій (інфаркт, рак, епілепсія) без зміни коду, а також підтримує підключення медичних носимих пристроїв. Автори наголошують, що така система не лише підвищує точність медичних прогнозів, а й забезпечує високий рівень захисту приватності та цілісності даних, що критично важливо для широкого впровадження цифрових двійників у сфері охорони здоров'я [6].

Огляд існуючих рішень для цифрових двійників

Цифрові двійники (DT) зазвичай моделюються за допомогою централізованих платформ, таких як Azure Digital Twins, GE Predix або Siemens MindSphere, які пропонують хмарні інструменти для синхронізації, моделювання та управління життєвим циклом. Хоча ці платформи надійні та масштабовані, вони часто залежать від пропрієтарних архітектур з обмеженою прозорістю щодо практик обробки даних.

Розподілені моделі DT — особливо ті, що інтегровані з периферійними обчисленнями або блокчейном — набувають все більшої популярності завдяки своїй здатності покращувати латентність, відмовостійкість та безпеку [7]. Ці моделі децентралізують контроль над даними, але вони також вимагають нових механізмів

застосування політики приватності, управління ідентифікацією та управління даними. Існує кілька підходів до вирішення проблеми приватності в системах цифрових двійників.

Децентралізовані ідентифікатори (DID) та системи самоідентифікації (SSI) дозволяють користувачам або пристроям підтверджувати свою ідентичність, не покладаючись на централізовані органи влади [8]. DID можна використовувати для контролю доступу до даних і послуг, пов'язаних з двійниками.

Політики обробки даних, що враховують приватність, включаючи управління згодою користувачів і мінімізацію даних, включаються в платформи DT, хоча вони, як правило, забезпечуються центральними контролерами.

Походження та автентичність даних забезпечуються за допомогою таких механізмів, як криптографічні підписи, захищене позначення часу та протоколи атестації. Вони мають вирішальне значення в системах, де DT використовуються в регульованих сферах, таких як охорона здоров'я та фінанси. Незважаючи на активні дослідження в галузі розподілених систем і конфіденційності на основі блокчейну, залишається кілька прогалин щодо приватності цифрових двійників:

1. Відсутність загальних стандартів: Не існує єдиної системи управління приватністю в системах DT. Підходи суттєво відрізняються в різних галузях, а інтероперабельність залишається головною перешкодою.
2. Неефективність традиційних моделей: Централізовані моделі контролю доступу та управління даними погано масштабуються в децентралізованих або периферійних розгортаннях DT. Вони також погано підходять для середовищ, де автономія в реальному часі та міжорганізаційна взаємодія є важливими.
3. Недостатнє використання смарт-контрактів: Хоча смарт-контракти продемонстрували свою корисність у системах DeFi та ланцюгах поставок, їхнє застосування в управлінні приватністю DT лише зароджується. Більшість реалізацій зосереджені на відстеженні активів або реєстрації даних, а не на обчисленнях і контролі доступу, що зберігають приватність.
4. Ризики витоку даних: Інтеграція публічного блокчейну без належних рівнів приватності може призвести до ненавмисного розкриття конфіденційних цифрових телеметричних даних двійників або ідентифікаційних даних.

Можливе використання смарт-контрактів для підвищення приватності

Смарт-контракти все активніше розглядаються як інструмент для автономного виконання цифрових політик у розподілених системах. Проте їх використання у контекстах, де обробляються конфіденційні дані — зокрема в системах цифрових двійників — створює серйозні виклики. Прозорість більшості блокчейн-платформ суперечить потребі в приватності, адже всі транзакції та логіка виконання смарт-контрактів зазвичай є відкритими. Це обмежує можливість їх використання в системах, які працюють з медичними записами, критичною інфраструктурою чи персональними сенсорними даними. Зростання складності цифрових двійників, особливо в контексті децентралізованих або розподілених середовищ, вимагає переосмислення підходів до забезпечення приватності. Традиційні централізовані моделі автентифікації та контролю доступу (наприклад, OAuth або RBAC) демонструють слабку масштабованість і підвищену вразливість у системах, що передбачають міжорганізаційну взаємодію та автономність пристроїв.

Одним із перспективних напрямів є впровадження смарт-контрактів на блокчейн-платформах, які дозволяють програмно реалізовувати політики доступу, аудит і обробку подій. Як зазначають Amofa et al. (2024), «смарт-контракти керують відповідями цифрового двійника при запитах, базуючись на політиках, визначених для кожного

пацієнта», що дозволяє зменшити ризики витоку даних і зловживання доступом [9]. Крім того, інтеграція цифрових двійників із блокчейном відкриває можливості для розподіленого управління потоками даних у IoT. У роботі Samaniego & Deters (2023) описується модель, де «довірчі структури, реалізовані у вигляді смарт-контрактів, керують доступом до цифрових двійників, а не до IoT-ресурсів безпосередньо», тим самим захищаючи ресурси від стороннього доступу [10]. Іншим важливим аспектом є забезпечення гнучкості смарт-контрактів. Corradini et al. (2024) запропонували підхід, у якому цифровий двійник виступає як агент зворотного зв'язку, що дозволяє виявляти відхилення у логіці контракту та пропонувати оновлення — ключовий компонент для «динамічного вдосконалення смарт-контрактів» [11]. У роботі «Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency» автори розглядають інтеграцію блокчейн-технологій з цифровими двійниками як засіб покращення їхньої безпеки, прозорості та цілісності даних. Запропоновано інноваційну архітектуру, в якій приватна блокчейн-мережа забезпечує автентифікацію суб'єктів, контроль доступу, а також перевірку достовірності даних через смарт-контракти. Для забезпечення відстежуваності та незмінності інформації використовуються хеш-функції, а також ролева модель доступу, що мінімізує ризики витоку або фальсифікації даних у цифрових двійниках. Дослідження включає приклад практичного впровадження у системі відеоспостереження AiWatch, де цифрові двійники представляють фізичні простори, а дані з камер проходять верифікацію через блокчейн перед оновленням моделей. Завдяки використанню протоколу QBFT система досягає високої пропускної здатності при збереженні надійності, що робить її придатною для масштабованих промислових рішень, орієнтованих на захист цифрових репрезентацій у середовищах IoT [12].

Отже, майбутні дослідження мають виходити за межі традиційних реалізацій смарт-контрактів і зосереджуватись на їх розширенні шляхом інтеграції криптографічних механізмів захисту приватності, обчислень поза блокчейном (off-chain) та децентралізованих ідентифікаторів. Метою є не просто використання смарт-контрактів як допоміжних інструментів, а побудова архітектур із вбудованою приватністю (privacy-by-design architectures), де контракти відіграють центральну роль у регулюванні доступу, контролі відповідності та безпечній співпраці — без шкоди для конфіденційності чи автономії учасників системи.

Zero-Knowledge Proofs: приватна взаємодія без розголошення даних

Одним із можливих напрямів є застосування доказів із нульовим розголошенням (Zero-Knowledge Proofs, ZKP). Ці криптографічні протоколи дозволяють довести істинність певного твердження без розкриття додаткової інформації. У контексті розумних міст, Ahmadi-Assalemi et al. (2022) підкреслюють необхідність впровадження захисту даних «як невід'ємної частини архітектури цифрового двійника в рамках стратегії defense-in-depth» [13]. У контексті цифрових двійників ZKP можуть забезпечити підтвердження прав доступу або відповідність політикам без розкриття особистих даних, внутрішніх параметрів чи конфігурацій пристроїв [14]. Це відкриває нові підходи до автентифікації та аудиту. Наприклад, технік може довести, що має сертифікацію на зміну налаштувань певного компонента цифрового двійника, не розкриваючи свої персональні дані чи роботодавця. Аналогічно, смарт-контракт може підтвердити, що значення датчика залишалося в допустимих межах, не публікуючи фактичні цифри (рис. 2).

Забезпечення безпеки й приватності при обміні даними є ключовим викликом для сучасних розподілених обчислювальних систем. Для його подолання автори статті «A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing» пропонують модель, що поєднує блокчейн, смарт-контракти та неінтерактивні

докази з нульовим розголошенням (zk-SNARKs). Такий підхід дозволяє здійснювати верифікацію атрибутів даних без розкриття їх змісту, зберігаючи конфіденційність учасників обміну. Архітектура передбачає поетапний обмін із реєстрацією, підбором сторін та транзакцією, яка супроводжується подвійним шифруванням і перевіркою доказів. Для зменшення навантаження на блокчейн використовується позаланцюгове зберігання (IPFS), що підвищує масштабованість. Модель протестована у середовищі промислового IoT і демонструє високу ефективність, а також потенціал для застосування в медичних, фінансових та виробничих сценаріях із високими вимогами до безпеки [15].

Одним з методів вдосконалення захисту приватності для блокчейн-систем, є поєднання інтерактивних доказів з нульовим розголошенням (ZKP) з гомоморфним шифруванням та оптимізаційними математичними методами (наприклад алгоритми Монтгомері й Карацуби). Такий підхід дозволяє перевіряти коректність транзакцій без розкриття їх змісту, зберігаючи конфіденційність учасників і підвищуючи обчислювальну ефективність. В роботі [16] була запропонована система реалізована на Hyperledger Fabric що довела свою здатність забезпечувати безпечні, приватні й масштабовані транзакції в розподілених обчисленнях. Це відкриває перспективи для ширшого застосування в сферах з високими вимогами до безпеки даних.

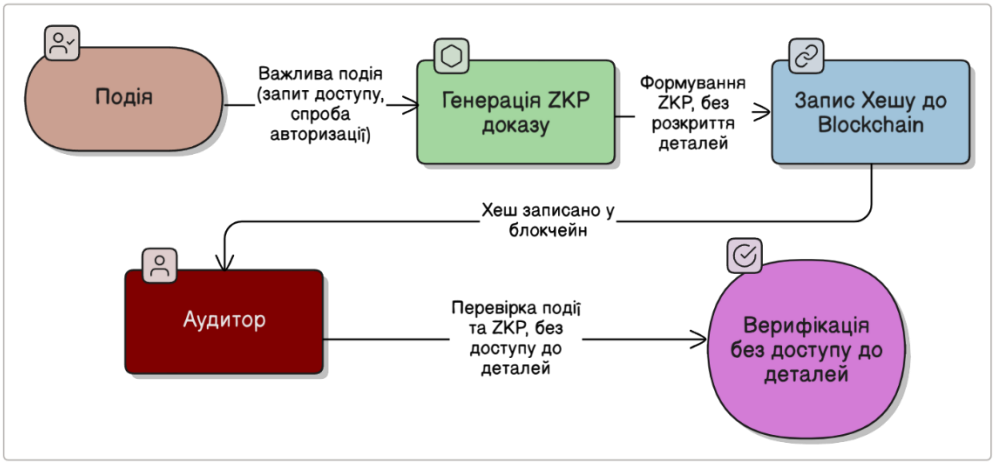

Рис. 2. Процес фіксації події з використанням ZKP та блокчейн

Втім, реалізація ZKP у реальних блокчейн-системах залишається складною. zk-SNARKs вимагають попереднього налаштування довіри (trusted setup) і складних обчислень. zk-STARKs позбавлені цієї проблеми, але є ще більш ресурсомісткими. Більшість блокчейн-платформ мають обмежену підтримку вбудованої верифікації ZKP, що робить її дорогою та технічно складною. Майбутні дослідження мають бути спрямовані на розробку доменно-специфічних доказів, оптимізованих схем перевірки та сумісних бібліотек для інтеграції в системи цифрових двійників [17].

Архітектури другого рівня (Layer 2): продуктивність і приватність через off-chain обчислення

Оскільки виконання контрактів на блокчейні часто повільне та затратне, з'являються рішення другого рівня (Layer 2), які дозволяють перенести більшість операцій за межі основного ланцюга (рис. 3). Rollups, Plasma та state channels — це приклади таких рішень, що забезпечують масштабованість і конфіденційність [18].

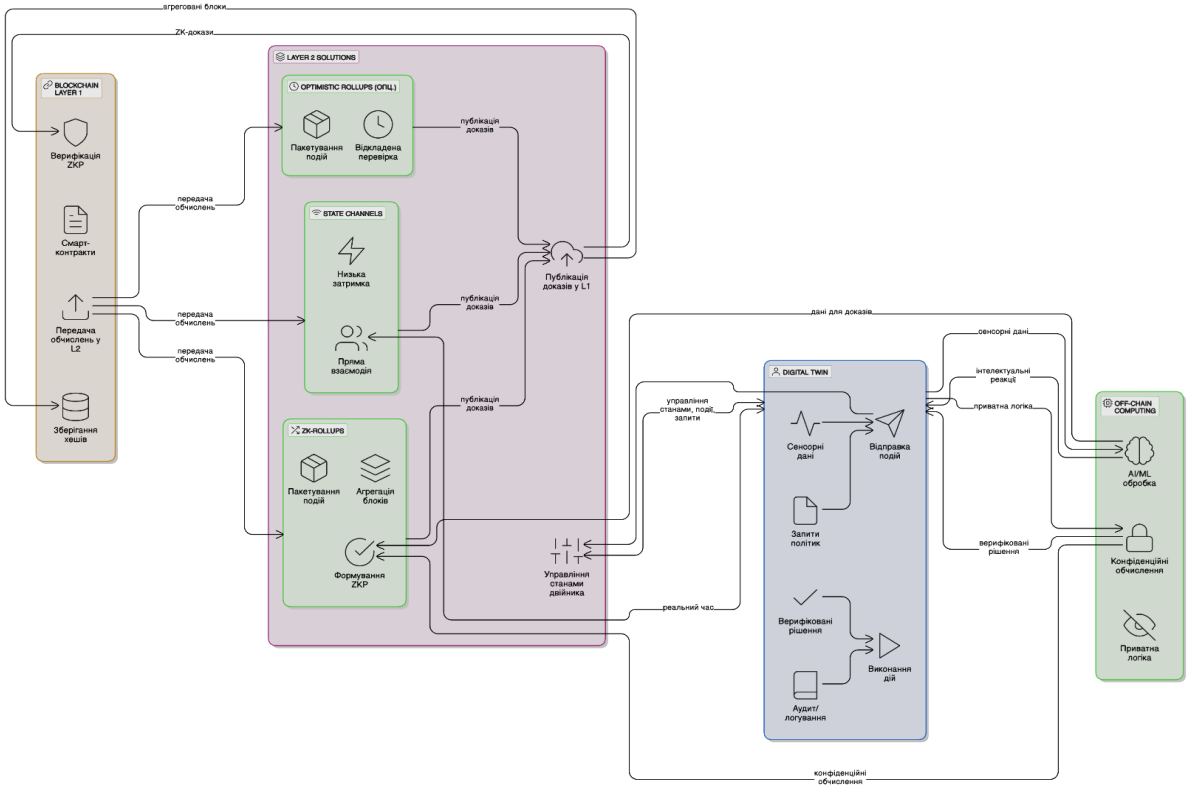

Рис. 3. Архітектура з використанням Layer 2

У сфері цифрових двійників такі рішення дозволяють здійснювати часті або чутливі взаємодії (наприклад, сенсорні оновлення чи команди управління) поза блокчейном. Наприклад, zk-Rollups можуть агрегувати тисячі транзакцій і формувати один доказ коректності для запису в ланцюг. Приклад такої системи описано в роботі «Integrating zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management» представлено архітектуру для безпечного та масштабованого управління медичними даними, яка об'єднує технології блокчейн, zk-Rollup (zero-knowledge rollups) та IPFS. Основна мета дослідження — покращити конфіденційність, цілісність і продуктивність у зберіганні та обміні електронними медичними записами (EMR) шляхом використання децентралізованого підходу. Запропонована система забезпечує автентифікацію доступу до даних за допомогою доказів з нульовим розголошенням, дозволяючи верифікувати права користувачів без розкриття змісту запитів. Результати експериментів показують, що рішення на базі zk-Rollup має кращу масштабованість, точність та меншу затримку у порівнянні з традиційними та базовими блокчейн-системами, що робить його перспективним для застосування у цифровій охороні здоров'я та підтримки Цілей сталого розвитку ООН [19].

Одним із перспективних рішень для масштабування блокчейн-систем є використання state channels — технології, що дозволяє сторонам здійснювати серію транзакцій поза основним блокчейном (off-chain) і записувати лише фінальний підсумок на ланцюг. Такий підхід значно зменшує затримки та розвантажує основну мережу, що критично важливо для високочастотних або мікроплатежів. У статті «Advances in Blockchain Solutions for Secure and Efficient Cross-Border Payment Systems» state channels згадуються як частина ширшого класу layer-two рішень (разом з Lightning Network, zk-Rollups та Optimistic Rollups), які розкривають потенціал блокчейну для створення швидких, дешевих і надійних у глобальному масштабі [20].

Попри переваги, такі архітектури складно інтегрувати у традиційні системи цифрових двійників. Вони потребують нових протоколів синхронізації, надійних операторів і додаткового контролю за відповідністю фізичних і цифрових станів. Потрібні дослідження щодо стандартизації інтерфейсів між L2-рішеннями та платформами DT, розробки middleware-рішень для гібридних сценаріїв, а також оцінки ризиків і вразливостей таких моделей.

Конфіденційні смарт-контракти: обчислення над зашифрованими даними

Ще одним напрямом є розвиток конфіденційних смарт-контрактів, які дозволяють обробляти зашифровані дані без їх розкриття. Такі можливості реалізовані в платформах, як-от Secret Network, Oasis Network та у FHE-мережах (Fully Homomorphic Encryption). Вони дозволяють зберігати конфіденційність даних навіть під час обчислень. Це особливо важливо в медичних, енергетичних та інших критичних сферах, де розголошення навіть метаданих може створити серйозні ризики. Наприклад, цифровий двійник медичного пристрою може провести обробку діагностичних даних і згенерувати рекомендації, не розкриваючи ані вхідних даних, ані логіки прийняття рішень [21].

Водночас ці підходи мають обмеження. TEE-рішення потребують довіри до апаратного середовища, а FHE залишається надзвичайно обчислювально важким. Крім того, екосистема таких контрактів лише розвивається, з обмеженою підтримкою у стандартних середовищах. Дослідження мають бути спрямовані на створення портативних конфіденційних середовищ, підвищення ефективності, а також на розробку моделей вибіркового розкриття.

Децентралізовані ідентифікатори: контрольований доступ без посередників

У багатьох системах цифрових двійників потрібно керувати доступом до ресурсів між численними учасниками — користувачами, сервісами, постачальниками. Традиційні механізми автентифікації з паролями чи централізованими серверами не відповідають вимогам масштабованих та автономних систем. Децентралізовані ідентифікатори (DID) та Verifiable Credentials (VC) дають змогу суттєво змінити підхід до керування ідентичністю [22].

Смарт-контракти можуть перевіряти дійсність наданих атрибутів, не знаючи реальної особи, що їх надала. Це дає змогу реалізувати динамічні, контекстно залежні права доступу, що можна обмежувати в часі, просторі чи умовами. Крім того, DID забезпечують псевдонімність із верифікацією, що дозволяє проводити аудит дій без розкриття особистості користувача (Рис. 4). Це має вирішальне значення у сценаріях із високими вимогами до якості доказів, але водночас — до приватності. А роботі «Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology» запропоновано децентралізовану модель управління ідентичностями для пристроїв Інтернету речей (IoT) на основі технології IOTA Tangle — безблокової розподіленої книги, яка забезпечує безкомісійні, паралельні транзакції. Автори впроваджують систему, що інтегрує Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), IOTA Streams для безпечної передачі даних та IOTA Stronghold для захисту криптографічних ключів. У дослідженні реалізовано proof-of-concept на Raspberry Pi, що демонструє реальну придатність цього підходу для пристроїв з обмеженими ресурсами. Результати підтверджують можливість створення масштабованої, безпечної та приватної інфраструктури для управління ідентичностями в IoT без потреби у централізованих посередниках. Дослідження узгоджується з принципами Web 3.0, роблячи акцент на автономії користувачів, децентралізації та цифровому суверенітеті [23].

Інший підхід використання децентралізованих ідентифікаторів розглядається в роботі «DidTrust: Privacy-preserving Trust Management for Decentralized Identity» автори пропонують новий підхід до управління довірою. Основна ідея полягає у збереженні приватності користувацьких відгуків і одночасному збереженні здатності системи виявляти недобросовісні дії (наприклад, маніпуляції з довірою або змови між

учасниками). Запропонований протокол DidTrust дозволяє проводити оцінку довіри без розкриття самих відгуків, використовуючи криптографічні механізми, а також містить модуль стиснення даних для ефективної роботи з великими наборами зворотного зв'язку. Результати дослідження показали, що система досягає високої точності у виявленні аномалій і забезпечує надійний баланс між безпекою та продуктивністю [24].

При цьому DID не обов'язково має бути цифро-чисельним ідентифікатором, а мати довільну форму. Автори роботи «Blockchain-Powered Integrated Health Profile and Record Management System for Seamless Consultation» розробили платформу для зберігання медичних записів на базі блокчейну, де кожен пацієнт має унікальний ідентифікатор у вигляді фізичної картки з QR-кодом. Ідея полягає в тому, що пацієнт сам вирішує, яку саме інформацію відкривати лікарю, з використанням двофакторної автентифікації. Такий підхід дає змогу зберегти конфіденційність даних, уникнути зайвого адміністрування та прискорити процес медичного обслуговування. Платформа також інтегрує API-зв'язки між користувацькими та медичними сервісами, що робить її зручною для масштабування та використання в різних сферах охорони здоров'я [25].

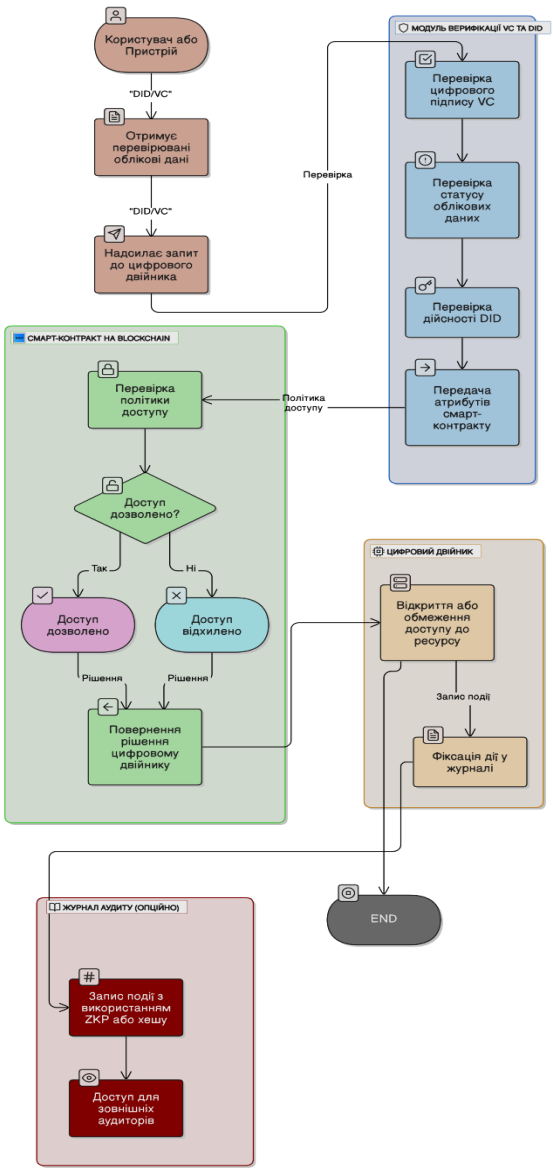

Рис. 4. Взаємодія DID, VC та смарт-контрактів у цифрових двійниках

Незважаючи на переваги, проблема впровадження DID залишається актуальною. Потрібні крос-платформенні стандарти, підтримка DID у основних блокчейн-мережах, та адаптація до вимог нормативних актів, таких як GDPR або HIPAA. Важливим напрямом дослідження є інтеграція DID з уже наявними платформами цифрових двійників, а також розробка моделей делегування та відкликання прав доступу.

Смарт-контракти для приватного автоматизованого аудиту

Цифрові двійники в багатьох випадках використовуються у галузях, де аудит та регуляторна відповідність є критичними вимогами. Смарт-контракти можуть автоматизувати збір і зберігання журналів подій — таких як запити доступу, зміни стану чи порушення політик — забезпечуючи при цьому незмінність даних і перевірюваність (рис. 5). Особливої цінності набуває поєднання смарт-контрактів із ZKP, що дозволяє створювати аудиторські докази без розкриття змісту журналів [26]. Наприклад, медичний заклад зможе підтвердити, що до певного цифрового двійника зверталися лише авторизовані особи, не розкриваючи, коли, хто і з якою метою.

Однак реалізація таких систем має низку викликів. Повний запис подій у блокчейн є дорогим з точки зору вартості транзакцій і обсягу зберігання. Часткове рішення — використання off-chain журналів із хешами в блокчейні — потребує ефективних механізмів перевірки та вирішення спорів. Також виникає потреба у відповідності існуючим стандартам аудиту, включно з політиками зберігання, доступу та видалення.

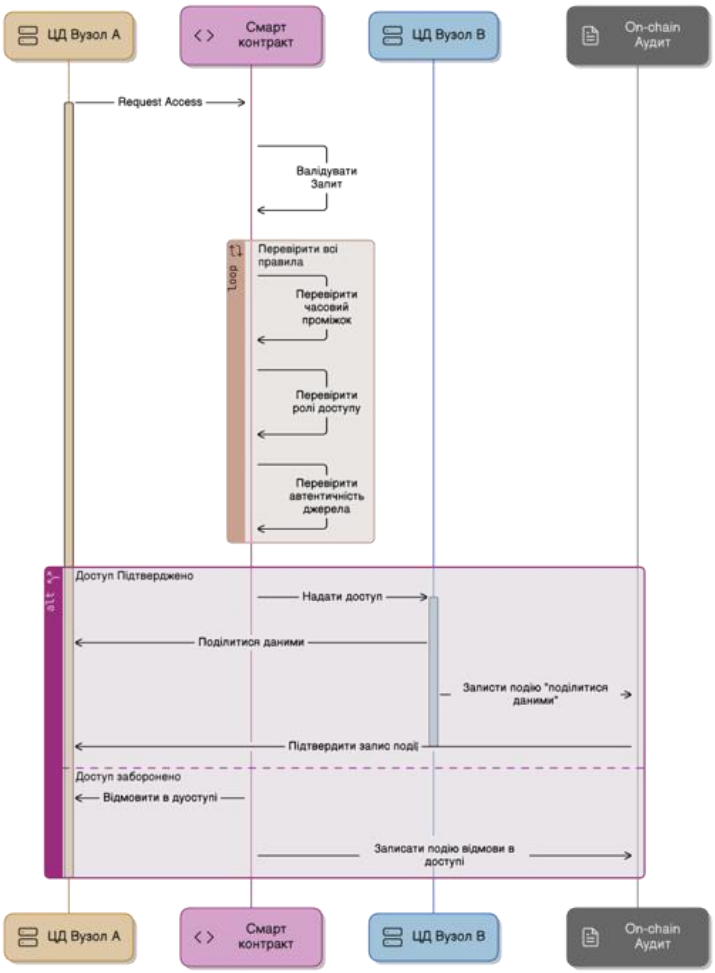

Рис. 5. Приклад автоматичного аудиту з використання смарт-контрактів

Дослідження останніх років демонструють перспективність інтеграції смарт-контрактів у сферу аудиту та дотримання стандартів безпеки. У роботі *Guo et al.* представлено прототип системи, де аудиторські правила кодуються мовою Solidity, що дозволяє автоматично виявляти аномальні транзакції згідно із заздалегідь визначеними критеріями — фактично створюючи самоперевіряючі моделі відповідності. Такий підхід дозволяє суттєво підвищити ефективність розподілу аудиторських ресурсів та оперативність реагування на ризики [27]. Водночас стаття *Modak et al.* зосереджується на проблемі балансу між прозорістю та приватністю у сертифікаційних системах. Автори пропонують механізм вибіркового розкриття на основі Zero-Knowledge Proofs та атрибутного шифрування, який дає змогу доводити відповідність вимогам без необхідності повного розкриття інформації. Обидві роботи формують підґрунтя для розробки децентралізованих, масштабованих і конфіденційних систем аудиту, здатних автоматично забезпечувати відповідність таким стандартам, як ISO/IEC 27001 чи NIST CSF [28].

Важливими напрямами дослідження є поєднання таких рішень із існуючими стандартами аудиту (ISO/IEC 27001, NIST), розробка протоколів вибіркового розкриття, а також створення самоперевіряючих моделей відповідності, де сам смарт-контракт виступає гарантом дотримання політик.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Оскільки системи цифрових двійників продовжують перетворюватися на складні, розподілені інфраструктури, важливість надійних, масштабованих механізмів, що зберігають конфіденційність, стає все більш нагальною. Традиційні централізовані моделі контролю доступу та управління ідентифікацією практично не пристосовані до вимог автономних, інтероперабельних цифрових двійників, що працюють у різних сферах і з різними зацікавленими сторонами. У цьому контексті смарт-контракти пропонують трансформаційну можливість забезпечити дотримання політики приватності у децентралізований, прозорий і перевірений спосіб. У цій статті досліджено перетин смарт-контрактів і цифрових двійників через призму захисту приватності. У ній визначено основні проблеми, такі як відкритість середовища блокчейну, обмежена масштабованість криптографічних методів і відсутність стандартизації в системах ідентифікації особи. Для вирішення цих проблем було розглянуто низку технологій — докази з нульовим рівнем знання, архітектури другого рівня, конфіденційні смарт-контракти, децентралізовані ідентифікатори та аудит, що зберігає конфіденційність — як потенційні шляхи для підвищення рівня приватності в екосистемах цифрових двійників.

Хоча інтеграція цих інструментів все ще перебуває на ранніх стадіях, спільне застосування криптографічних рішень і рішень на основі блокчейну вказує на багатообіцяюче майбутнє для безпечних цифрових середовищ-двійників. Тим не менш, попереду ще багато досліджень. Розробка масштабованих схем ZKP, стандартизованих протоколів DID і ефективних середовищ конфіденційного виконання буде мати важливе значення для перетворення цього бачення в операційну реальність. Зрештою, приватність в системах цифрових двійників повинна розглядатися не як додаткова функція, а як основоположний принцип проектування. Перспективні системи мають проєктуватися з урахуванням приватності як базової властивості, у межах якої смарт-контракти виконуватимуть функції не лише контролерів доступу, але й інтелектуальних, автономних агентів довіри, забезпечення нормативної відповідності та захисту даних в умовах дедалі більш децентралізованого цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Role-based access control models / R. S. Sandhu et al. *Computer*. 1996. Vol. 29, no. 2. P. 38–47. URL: https://doi.org/10.1109/2.485845 (date of access: 16.04.2025).
2. The OAuth 2.0 Authorization Framework / ed. by D. Hardt. RFC Editor, 2012. URL: https://doi.org/10.17487/rfc6749 (date of access: 16.04.2025).
3. Cadavid, H., Mo, H., Arends, B., Dziopa, K., Bron, E. E., Bos, D., Georgievska, S., & van der Harst, P. MyDigiTwin: A Privacy-Preserving Framework for Personalized Cardiovascular Risk Prediction and Scenario Exploration. *Elsevier*. 2025. URL: https://arxiv.org/abs/2501.12193 (date of access: 18.04.2025).
4. Zhang L., Xue J. Analysis of Personal Privacy Leakage under the Background of Digital Twin. *Scientific and Social Research*. 2024. Vol. 6, no. 10. P. 168–175. URL: https://doi.org/10.26689/ssr.v6i10.8437 (date of access: 14.05.2025).
5. Upadrista V., Nazir S., Tianfield H. Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*. 2025. Vol. 12, no. 1. URL: https://doi.org/10.1186/s40708-024-00247-6 (date of access: 14.04.2025).
6. Upadrista V., Nazir S., Tianfield H. Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*. 2025. Vol. 12, no. 1. URL: https://doi.org/10.1186/s40708-024-00247-6 (date of access: 16.04.2025).
7. A Digital Twin Approach for Blockchain Smart Contracts / F. Corradini et al. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland, 12 March 2024. 2024. P. 1–7. URL: https://doi.org/10.1109/saner-c62648.2024.00007 (date of access: 02.05.2025).
8. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge / E. Ben-Sasson et al. *Advances in Cryptology – CRYPTO 2013*. Berlin, Heidelberg, 2013. P. 90–108. URL: https://doi.org/10.1007/978-3-642-40084-1_6 (date of access: 16.04.2025).
9. Blockchain-secure patient Digital Twin in healthcare using smart contracts / S. Amofa et al. *PLOS ONE*. 2024. Vol. 19, no. 2. P. e0286120. URL: https://doi.org/10.1371/journal.pone.0286120 (date of access: 02.05.2025).
10. Samaniego M., Deters R. Digital Twins and Blockchain for IoT Management. *ASIA CCS '23: ACM Asia Conference on Computer and Communications Security*, Melbourne VIC Australia. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3594556.3594611 (date of access: 02.05.2025).
11. A Digital Twin Approach for Blockchain Smart Contracts / F. Corradini et al. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland, 12 March 2024. 2024. P. 7–11. URL: https://doi.org/10.1109/saner-c62648.2024.00007 (date of access: 02.05.2025).
12. Ferone A., Verrilli S. Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency. *Future Internet*. 2025. Vol. 17, no. 1. P. 31. URL: https://doi.org/10.3390/fi17010031 (date of access: 17.04.2025).
13. Ahmadi-Assalemi G., Al-Khateeb H., Aggoun A. Privacy-enhancing technologies in the design of digital twins for smart cities. *Network Security*. 2022. Vol. 2022, no. 7. URL: https://doi.org/10.12968/s1353-4858(22)70046-3 (date of access: 02.05.2025).
14. Zerocoin: Anonymous Distributed E-Cash from Bitcoin / I. Miers et al. *2013 IEEE Symposium on Security and Privacy (SP) Conference*, Berkeley, CA, 19–22 May 2013. 2013. URL: https://doi.org/10.1109/sp.2013.34 (date of access: 16.04.2025).
15. A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing / B. Zhang et al. *Electronics*. 2024. Vol. 13, no. 21. P. 4260. URL: https://doi.org/10.3390/electronics13214260 (date of access: 14.05.2025).
16. Zhuo Y. Research on Blockchain Interactive Zero Knowledge Proof Privacy Protection Scheme Based on Improved Paillier Homomorphic Encryption. *Frontiers in Science and Engineering*. 2024. Vol. 4, no. 10. P. 57–73. URL: https://doi.org/10.54691/9xb96p64 (date of access: 10.04.2025).
17. Dr. K. Baranidharan, Mahalakshmi.R, Anagha S. Blockchain Technology for Enhancing Supply Chain Transparency: Opportunities and Challenges. *International Journal of Advanced Research in Science, Communication and Technology*. 2025. P. 345–353. URL: https://doi.org/10.48175/ijarsct-23039 (date of access: 21.04.2025).
18. Gangwal A., Gangavalli H. R., Thirupathi A. A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications*. 2022. P. 103539. URL: https://doi.org/10.1016/j.jnca.2022.103539 (date of access: 16.04.2025).

19. Salunkhe, V., & Sujatha, R. *Integrating Zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management*. (2025). URL: https://doi.org/10.2139/ssrn.5070850 (date of access: 16.04.2025).
20. Advances in Blockchain Solutions for Secure and Efficient Cross-Border Payment Systems / N. L. Eyo-Udo et al. *International Journal of Research and Innovation in Applied Science*. 2025. Vol. IX, no. XII. P. 536–563. URL: https://doi.org/10.51584/ijrias.2024.912048 (date of access: 22.04.2025).
21. Kerl M., Bodin U., Schelén O. Privacy-preserving attribute-based access control using homomorphic encryption. *Cybersecurity*. 2025. Vol. 8, no. 1. URL: https://doi.org/10.1186/s42400-024-00323-8 (date of access: 21.04.2025).
22. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 49. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).
23. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 49. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).
24. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 62. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).
25. Blockchain-Powered Integrated Health Profile and Record Management System for Seamless Consultation Leveraging Unique Identifiers / Ganesh Khekare et al. *Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions*. 2025. P. 53–68. URL: https://doi.org/10.2174/9789815305210125010006 (date of access: 25.04.2025).
26. Péter B. Z., Kocsis I. Privacy-Preserving Noninteractive Compliance Audits of Blockchain Ledgers with Zero-Knowledge Proofs. *Acta Polytechnica Hungarica*. 2024. Vol. 21, no. 11. P. 7–27. URL: https://doi.org/10.12700/aph.21.11.2024.11.1 (date of access: 16.04.2025).
27. Guo X., Li D. A., Zuo Y. When Auditing Meets Blockchain: A Study on Applying Blockchain Smart Contracts in Auditing . *SSRN Electronic Journal*. 2025. URL: https://doi.org/10.2139/ssrn.5029553 (date of access: 15.05.2025).
28. SD-SmartCert: A Blockchain-Based Certification System with Selective Disclosure / A. Modak et al. *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, 17–19 October 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/icbds61829.2024.10837562 (date of access: 15.05.2025).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Dmytro Ovsianko
Postgraduate Student of Information Technology Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0003-7758-0613
dmytro.o.ovsianko@lpnu.ua

Elena Nyemkova
Doctor of Sciences, Professor
Professor of the Information Technology Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

SMART CONTRACTS AS PRIVACY-PRESERVING MECHANISMS IN DISTRIBUTED DIGITAL TWIN SYSTEMS

Abstract. The deployment of distributed digital twin systems in sectors such as healthcare, manufacturing, and critical infrastructure has significantly heightened the importance of data privacy. These systems interact with numerous devices and users, increasing the risk of data leakage or unauthorized access to sensitive information. Traditional centralized identity management and access control mechanisms no longer meet the scalability, autonomy, and privacy requirements of modern distributed architectures. This article explores how smart contracts operating in blockchain environments can provide decentralized access management for digital twin systems. Smart contracts enable transparent and reliable enforcement of access policies without relying on centralized authorities. The study examines the integration of modern cryptographic technologies into smart contract workflows, including zero-knowledge proofs, decentralized identifiers (DIDs), and confidential computing. These technologies make it possible to verify access rights and perform secure operations without revealing sensitive data. The article also analyzes the limitations of existing solutions, such as the high transaction costs of public blockchains, the limited performance of traditional smart contracts, and the challenges of integrating confidential computing into resource-constrained devices. The authors outline future research directions, including optimizing Layer 2 architectures to improve performance, developing secure auditing mechanisms, and ensuring compatibility with self-sovereign identity systems. The conclusions emphasize that privacy should be treated as a fundamental property of digital twin systems. In these environments, smart contracts must serve not only as governance logic but also as trusted agents that guarantee compliance with access policies and regulatory requirements in decentralized ecosystems.

Keywords: Digital Twins; Data Privacy; Smart Contracts; Blockchain and Decentralized Access Control; Zero-Knowledge Proofs (ZKP); Decentralized Identifiers (DID); Confidential Computing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Role-based access control models / R. S. Sandhu et al. *Computer*. 1996. Vol. 29, no. 2. P. 38–47. URL: https://doi.org/10.1109/2.485845 (date of access: 16.04.2025).
2. The OAuth 2.0 Authorization Framework / ed. by D. Hardt. RFC Editor, 2012. URL: https://doi.org/10.17487/rfc6749 (date of access: 16.04.2025).
3. Cadavid, H., Mo, H., Arends, B., Dziopa, K., Bron, E. E., Bos, D., Georgievska, S., & van der Harst, P. MyDigiTwin: A Privacy-Preserving Framework for Personalized Cardiovascular Risk Prediction and Scenario Exploration. *Elsevier*. 2025. URL: https://arxiv.org/abs/2501.12193 (date of access: 18.04.2025).
4. Zhang L., Xue J. Analysis of Personal Privacy Leakage under the Background of Digital Twin. *Scientific and Social Research*. 2024. Vol. 6, no. 10. P. 168–175. URL: https://doi.org/10.26689/ssr.v6i10.8437 (date of access: 14.05.2025).
5. Upadrista V., Nazir S., Tianfield H. Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*. 2025. Vol. 12, no. 1. URL: https://doi.org/10.1186/s40708-024-00247-6 (date of access: 14.04.2025).

6. Upadrista V., Nazir S., Tianfield H. Blockchain-enabled digital twin system for brain stroke prediction. *Brain Informatics*. 2025. Vol. 12, no. 1. URL: https://doi.org/10.1186/s40708-024-00247-6 (date of access: 16.04.2025).
7. A Digital Twin Approach for Blockchain Smart Contracts / F. Corradini et al. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland, 12 March 2024. 2024. P. 1–7. URL: https://doi.org/10.1109/saner-c62648.2024.00007 (date of access: 02.05.2025).
8. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge / E. Ben-Sasson et al. *Advances in Cryptology – CRYPTO 2013*. Berlin, Heidelberg, 2013. P. 90–108. URL: https://doi.org/10.1007/978-3-642-40084-1_6 (date of access: 16.04.2025).
9. Blockchain-secure patient Digital Twin in healthcare using smart contracts / S. Amofa et al. *PLOS ONE*. 2024. Vol. 19, no. 2. P. e0286120. URL: https://doi.org/10.1371/journal.pone.0286120 (date of access: 02.05.2025).
10. Samaniego M., Deters R. Digital Twins and Blockchain for IoT Management. *ASIA CCS '23: ACM Asia Conference on Computer and Communications Security*, Melbourne VIC Australia. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3594556.3594611 (date of access: 02.05.2025).
11. A Digital Twin Approach for Blockchain Smart Contracts / F. Corradini et al. *2024 IEEE International Conference on Software Analysis, Evolution and Reengineering - Companion (SANER-C)*, Rovaniemi, Finland, 12 March 2024. 2024. P. 7–11. URL: https://doi.org/10.1109/saner-c62648.2024.00007 (date of access: 02.05.2025).
12. Ferone A., Verrilli S. Exploiting Blockchain Technology for Enhancing Digital Twins' Security and Transparency. *Future Internet*. 2025. Vol. 17, no. 1. P. 31. URL: https://doi.org/10.3390/fi17010031 (date of access: 17.04.2025).
13. Ahmadi-Assalemi G., Al-Khateeb H., Aggoun A. Privacy-enhancing technologies in the design of digital twins for smart cities. *Network Security*. 2022. Vol. 2022, no. 7. URL: https://doi.org/10.12968/s1353-4858(22)70046-3 (date of access: 02.05.2025).
14. Zerocoin: Anonymous Distributed E-Cash from Bitcoin / I. Miers et al. *2013 IEEE Symposium on Security and Privacy (SP) Conference*, Berkeley, CA, 19–22 May 2013. 2013. URL: https://doi.org/10.1109/sp.2013.34 (date of access: 16.04.2025).
15. A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing / B. Zhang et al. *Electronics*. 2024. Vol. 13, no. 21. P. 4260. URL: https://doi.org/10.3390/electronics13214260 (date of access: 14.05.2025).
16. Zhuo Y. Research on Blockchain Interactive Zero Knowledge Proof Privacy Protection Scheme Based on Improved Paillier Homomorphic Encryption. *Frontiers in Science and Engineering*. 2024. Vol. 4, no. 10. P. 57–73. URL: https://doi.org/10.54691/9xb96p64 (date of access: 10.04.2025).
17. Dr. K. Baranidharan, Mahalakshmi.R, Anagha S. Blockchain Technology for Enhancing Supply Chain Transparency: Opportunities and Challenges. *International Journal of Advanced Research in Science, Communication and Technology*. 2025. P. 345–353. URL: https://doi.org/10.48175/ijarsct-23039 (date of access: 21.04.2025).
18. Gangwal A., Gangavalli H. R., Thirupathi A. A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications*. 2022. P. 103539. URL: https://doi.org/10.1016/j.jnca.2022.103539 (date of access: 16.04.2025).
19. Salunkhe, V., & Sujatha, R. *Integrating Zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management*. (2025). URL: https://doi.org/10.2139/ssrn.5070850 (date of access: 16.04.2025).
20. Advances in Blockchain Solutions for Secure and Efficient Cross-Border Payment Systems / N. L. Eyo-Udo et al. *International Journal of Research and Innovation in Applied Science*. 2025. Vol. IX, no. XII. P. 536–563. URL: https://doi.org/10.51584/ijrias.2024.912048 (date of access: 22.04.2025).
21. Kerl M., Bodin U., Schelén O. Privacy-preserving attribute-based access control using homomorphic encryption. *Cybersecurity*. 2025. Vol. 8, no. 1. URL: https://doi.org/10.1186/s42400-024-00323-8 (date of access: 21.04.2025).
22. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 49. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).
23. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 49. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).

24. Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology / T. Ramírez-Gordillo et al. *Future Internet*. 2025. Vol. 17, no. 1. P. 62. URL: https://doi.org/10.3390/fi17010049 (date of access: 21.04.2025).
25. Blockchain-Powered Integrated Health Profile and Record Management System for Seamless Consultation Leveraging Unique Identifiers / Ganesh Khekare et al. *Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions*. 2025. P. 53–68. URL: https://doi.org/10.2174/9789815305210125010006 (date of access: 25.04.2025).
26. Péter B. Z., Kocsis I. Privacy-Preserving Noninteractive Compliance Audits of Blockchain Ledgers with Zero-Knowledge Proofs. *Acta Polytechnica Hungarica*. 2024. Vol. 21, no. 11. P. 7–27. URL: https://doi.org/10.12700/aph.21.11.2024.11.1 (date of access: 16.04.2025).
27. Guo X., Li D. A., Zuo Y. When Auditing Meets Blockchain: A Study on Applying Blockchain Smart Contracts in Auditing . *SSRN Electronic Journal*. 2025. URL: https://doi.org/10.2139/ssrn.5029553 (date of access: 15.05.2025).
28. SD-SmartCert: A Blockchain-Based Certification System with Selective Disclosure / A. Modak et al. *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, 17–19 October 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/icbds61829.2024.10837562 (date of access: 15.05.2025).