DOI: 10.25140/2411-5363-2024-2(36)-137-150
УДК 004.623

Антон Миколайович Іскрижицький[1], Артем Олександрович Задорожній[2]

[1]аспірант, здобувач наукового ступеня доктор філософії за спеціальністю 122
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: a.iskryzhytskyi@gmail.com **ORCID:** https://orcid.org/0009-0005-4153-2075

[2] кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та програмної інженерії,
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: zaotroy@gmail.com **ORCID:** https://orcid.org/0000-0002-3424-7293

ДОСЛІДЖЕННЯ НАЯВНИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ ДЛЯ ДЕЦЕНТРАЛІЗОВАНОГО ЗБЕРІГАННЯ ТА АДМІНІСТРУВАННЯ ПУБЛІЧНИХ ДАНИХ

Стаття надає всебічний огляд існуючих технологій, включаючи блокчейн та IPFS, детально аналізуючи їхні переваги, недоліки та потенційні сценарії використання для зберігання та обробки публічних даних у децентралізований спосіб. Розглянуто наявні дослідження в цій сфері, які демонструють ефективність децентралізованих рішень у порівнянні з традиційними централізованими системами зберігання даних. У статті детально обговорюються потенційні виклики та обмеження, пов'язані з децентралізованими системами зберігання даних. Зокрема, розглянуто питання сумісності з існуючими інформаційними системами, проблеми виконання операцій у розподіленому середовищі, а також аспекти прийняття цих технологій на ринку. Окремо виділено питання безпеки та конфіденційності, критично важливі при роботі з публічними даними. Стаття містить аналіз перспектив розвитку та можливих напрямків подальших досліджень у цій галузі, що можуть сприяти вдосконаленню та впровадженню децентралізованих технологій для зберігання даних.

Ключові слова: *публічні дані; IPFS; блокчейн; аутентифікація; децентралізовані системи.*
Рис.: 4. Бібл.: 38.

Актуальність теми дослідження. Стаття є оглядово-інформаційною. На сьогодні для України постають питання надійного зберігання даних, забезпечення безперервного доступу та безпеки даних, зокрема, публічних даних та відкритих державних реєстрів відповідно до закону про доступ до публічної інформації [1]. Створюються різні типи державних відкритих і закритих реєстрів, які дозволяють інтеграцію зовнішнім споживачам та стороннім організаціям [2]. Це дозволяє отримувати статистичні та інші дані, які необхідні для побудови державної стратегії розвитку та стратегій приватних та державних організацій. Для забезпечення стабільної роботи таких реєстрів та захисту і підтвердження автентичності публічних даних доцільно застосовувати розподілені системи зберігання та адміністрування, такі як IPFS, блокчейн та різні їх імплементації.

Постановка проблеми. На сьогодні для зберігання та обробки публічної інформації здебільшого використовуються централізовані рішення, які мають недоліки, такі як вразливість до атак, централізовані точки відмови, обмежена масштабованість та потенційні проблеми з приватністю даних. Водночас децентралізовані рішення набирають популярності, і доцільно вивчити їх з точки зору науки та наукового підходу. Важливо визначити, які децентралізовані рішення є корисними та здатні підвищити характеристики надійності, безпеки, доступності та ефективності для зберігання даних, а які – ні.

Мета дослідження. Метою цієї оглядової статті є всебічний аналіз існуючих методів та технологій для децентралізованого зберігання та адміністрування публічних даних, зокрема, визначення їх основних характеристик, переваг та обмежень. Також передбачається оцінка потенційного впливу цих технологій на безпеку, приватність та доступність публічних даних, а також обговорення можливостей для подальшого розвитку та вдосконалення в цій галузі.

Виклад основного матеріалу.

Опис ключових понять і термінології. Глибоке розуміння принципів та основ децентралізованих технологій є необхідним для адекватного аналізу та оцінки їх застосування в контексті зберігання та адміністрування публічних даних. У цьому розділі будуть викладені та розглянуті ключові концепції, які становлять фундамент децентралізованих систем, включаючи їхні характеристики, принципи роботи та потенційні сфери застосування.

У цій сфері ключове місце посідають розподілені файлові системи та блокчейн-технології, що лягають в основу розвитку суміжних технологій. Зокрема, розподілені хеш-таблиці (DHT) використовуються для підвищення ефективності зберігання та доступу до даних, тоді як розумні контракти та консенсусні алгоритми є невід'ємними складовими блокчейн-систем, забезпечуючи надійність, безпеку та прозорість у процесах обробки та зберігання даних.

Розподілені системи. Одноранговi мережі. Розподілена система – це система, у якій апаратні або програмні компоненти розташовані на мережевих комп’ютерах, спілкуються та координують свої дії лише за допомогою передача повідомлень [3, с. 1]. Розподілені системи та одноранговi мережі створювалися як відповідь на постійно зростаючу кількість навантаження - як для зберігання великих об'ємів даних, так і для обчислення задач. Так, одноранговi мережі дозволяють залучати ресурси всіх користувачів мережі, що призводить до збільшення ресурсомісткості мережі в міру зростання кількості користувачів [3, с. 47]. Загальна схема будови одноранговової мережі зображена на рис. 1.

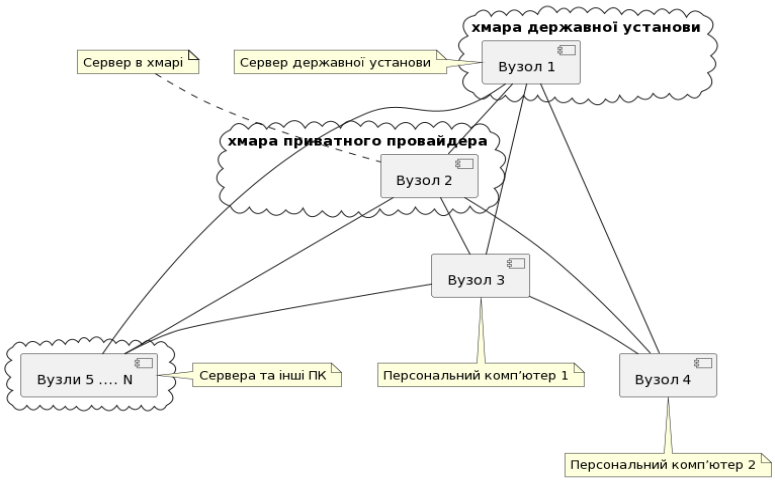

Рис. 1. Приклад одноранговової мережі

Розподілені файлові системи. **IPFS.** Розподілені файлові системи – це системи, що використовуються для дозволу багатьом користувачам мати доступ та зберігати файли в спільній файловій системі через мережі [4]. Або більш розгорнуто-розподілена файлова система є додатком на базі архітектури клієнт/сервер, що забезпечує доступ та обробку даних, збережених на кількох серверах, і реагує на клієнта, як і у випадку даних, збережених у локальній системі. Процес полягає в тому, що клієнт отримує копію файлу, яка кешується в локальній системі. Цей тип файлової системи організує файли з індивідуальних серверів у глобальну директорію, тому здається, що доступ до файлу віддалено не залежить від його місцезнаходження, але все ж залишається ідентичним з погляду клієнта. Розподілені файлові системи мають механізми для уникнення конфліктів та намагаються поділитися найсвіжішою версією даних, коли цього вимагає клієнт [5].

Прикладом таких системи є IPFS (англ. *InterPlanetary File System*, міжпланетна файлова система) – глобальна одноранговa файлова система з версіями, яка пропонує новаторську парадигму у сфері розподіленого зберігання даних, базуючись на принципах децентралізації та peer-to-peer мережевих архітектур [6; 7]. Ця технологія вирізняється з-поміж інших своєю поширеністю, наявністю численних клієнтських застосунків, активним розвитком та відкритим доступом до коду, що публікується на GitHub. Ці характеристики сприяють її популярності та забезпечують широкі можливості для модифікації та адаптації в різних контекстах використання. Останні дослідження в галузі продуктивності, безпеки та надійності імплементації розподіленої файлової системи виявили певні ключові характеристики, які відіграють вирішальну роль в інтеграції системи IPFS у те-

хнічні рішення, пов’язані з децентралізованим зберіганням та адмініструванням публічних даних. Так, наприклад, у досліджені «Transparency Analysis of Distributed File Systems» [4] було виявлено такі особливості IPFS як:

1. Відсутність механізму базового контролю доступу в системі IPFS веде до того, що будь-які дані, які розповсюджуються через мережу, стають загальнодоступними й підлягають поширенню серед учасників мережі. Це створює обмеження у можливостях видалення або обмеження доступу до даних, оскільки, попри те, що видалення даних можливе з вузлів, які перебувають під контролем користувача, інші учасники мережі, володіючи непідконтрольними вузлами, можуть зберігати копії даних на своїх пристроях. Таким чином, одноразово розповсюджені через IPFS дані можуть залишатися в мережі навіть після спроб їх видалення з певних вузлів [4, с. 40].

2. Низька продуктивність IPFS, спостережена при високому рівні реплікації даних у мережі під час операцій запису. Цей феномен свідчить про те, що збільшення кількості реплік вузлів, задіяних у процесі зберігання, може значно уповільнити загальну продуктивність системи, особливо під час проведення операцій запису даних [4, с. 40].

3. Однією з особливостей IPFS є потенційна вразливість до атак типу DDOS, схожих на атаку slowloris. Зловмисники можуть створити власні вузли в мережі та навмисно сповільнювати доступ до популярних файлів, значно знижуючи загальну швидкість завантаження для користувачів. Це створює важливий аспект безпеки та надійності для IPFS, оскільки така поведінка може підривати довіру до системи та її ефективність [4, с. 44].

У контексті зберігання публічних даних, ключовими з виокремлених характеристик є здатність до реплікації даних та їх розміщення на зовнішніх вузлах, які не контролюються первинним джерелом. Це має значний вплив на відмовостійкість та надійність системи децентралізованого зберігання та адміністрування публічних даних, забезпечуючи стабільність роботи у випадку проблем з серверним обладнанням первинного джерела, таких як хакерські атаки або блекаути (рис. 2). Надійність та стабільність системи вважається більш важливим параметром, ніж продуктивність запису. Натомість відсутність механізму базового контролю доступу та вразливість до атак, описаних у пункті 3, вимагає додаткового дослідження та можливої компенсації за допомогою інших шарів системи, у які може бути інтегрований IPFS як технологія для дистрибутивного зберігання файлів.

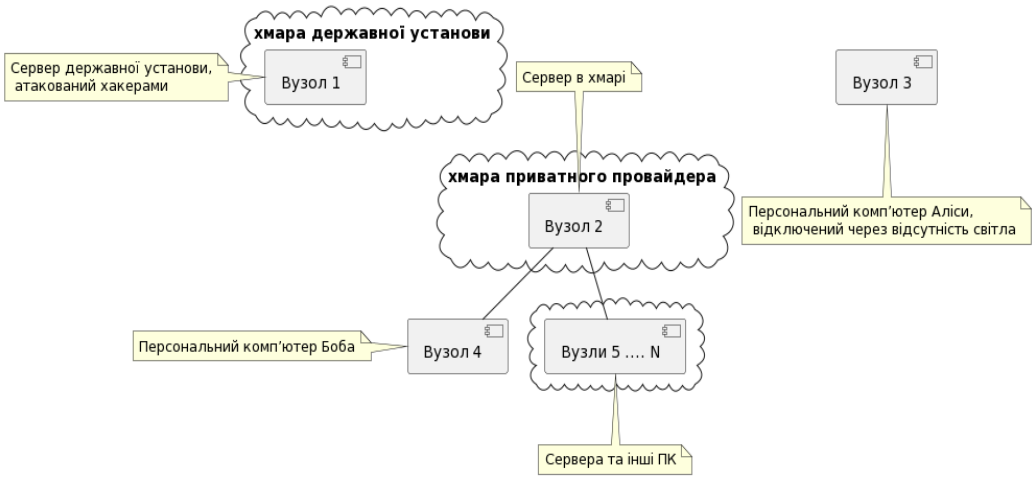

Рис. 2. IPFS під час хакерської атаки та відключень світла

Блокчейн системи. Механізми консенсусу. Блокчейн можна визначити як незмінну розподілену цифрову книгу послідовних записів, яка захищена за допомогою вдосконаленої криптографії, тиражується серед однорангових вузлів у одноранговій мережі та використовує механізм консенсусу для узгодження журналу транзакцій [8, с. 3]. Залежно від механізму консенсусу розрізняють публічні блокчейни та блокчейни з контрольованим доступом. Останні своєю чергою поділяють на консорціумні та повністю приватні (рис. 3) [9].

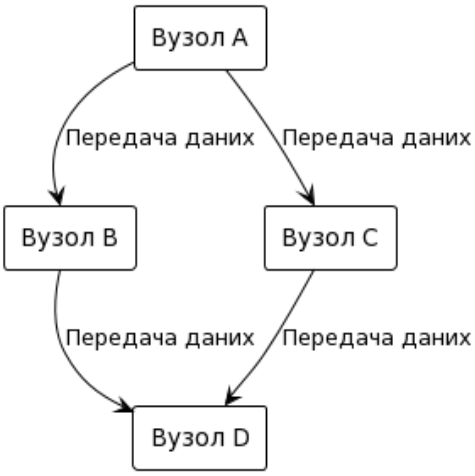

Рис. 3. Публічна однорангова блокчейн мережа

Виділяють чотири основні ознаки, за якими консорціумні блокчейни відрізняються від публічних [10]:

Ідентифікація. У публічних блокчейнах приєднання до мережі анонімні, особи учасників транзакції не можна перевірити. У консорціумному блокчейні для проведення транзакцій учасники спочатку повинні авторизуватися, тому їх особу можна встановити.

Вибір вузлів. У публічному блокчейні вузлом мережі може стати будь-який комп'ютер. Внаслідок цього надійність системи зростає зі збільшенням кількості вузлів, але одночасно зростає і складність досягнення консенсусу, оскільки потрібна згода від більшості обслуговуючих вузлів. У консорціумному блокчейні вузлами можуть стати лише авторизовані машини. Оскільки валідатори відомі, а їх кількість буде порівняно невеликою, досягти консенсусу легше. Це полегшує зміну правил, скасування транзакцій або інші зміни в блокчейні. Однак така підвищена гнучкість може бути недоліком, якщо метою блокчейну є абсолютна незмінність, щоб уникнути будь-яких форм маніпулювання даними.

Консенсус. У випадку публічних блокчейнів, участь у механізмі консенсусу можуть брати всі вузли. У випадку консорціумних блокчейнів лише вибрані вузли можуть виступати валідаторами в механізмі консенсусу, а їх кількість можна контролювати, тож механізм консенсусу виявляється дешевшим та простішим, порівняно з публічним блокчейном. За рахунок меншої кількості вузлів, блоки додаватимуться з більшою швидкістю.

Прозорість транзакцій. Публічні блокчейни є повністю прозорими, оскільки будь-хто може ознайомитися з вмістом блоків. Водночас це може створювати проблеми, якщо вміст блоків пов'язаний з конфіденційною або чутливою інформацією. У консорціумних блокчейнах розробники можуть приховати вміст блоків та зробити його доступним лише для певних користувачів, яких стосується певна транзакція, таким чином вирішуючи проблему конфіденційності.

Приватні блокчейни, по суті, є централізованими системами, оскільки вони використовують модель єдиної сутності з високим рівнем довіри, доповнюючи її певним ступенем криптографічної перевірки [10].

Незважаючи на те, що найбільш популярним та відомими нині є публічні блокчейни, які забезпечують функціонування різних криптовалют, у контексті систем зберігання та адміністрування публічних даних цікавішими є блокчейни з контрольованим доступом [8, с. 3] (рис. 4) або гібридні варіанти [11].

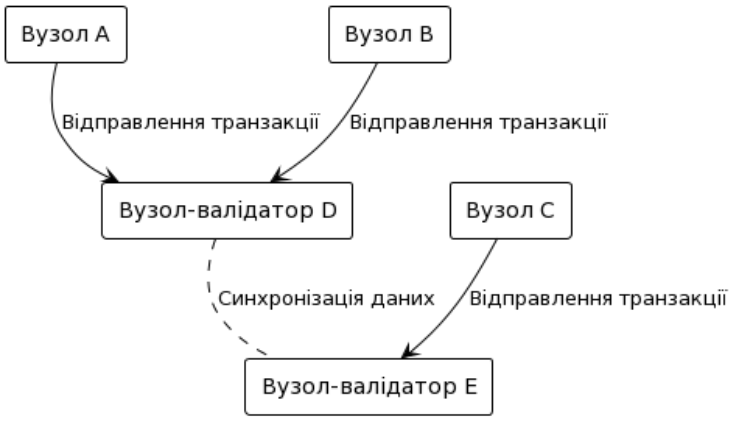

Рис. 4. Блокчейн мережа з контрольованим доступом

Для досягнення згоди між вузлами блокчейн мережі щодо валідності транзакцій та порядку їх додавання до блокчейну використовуються спеціальні протоколи, які називаються механізмами консенсусу. До найбільш типових механізмів консенсусу належать Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). Розглянемо їх детальніше.

Proof of Work (PoW, доказ роботи). Висловлюючись коротко, PoW — це криптографічне підтвердження нульового знання, у якому одна сторона доводить іншим, що певна кількість зусиль (енергії) була витрачена на певне надскладне обчислювальне завдання. Ключовою особливістю концепції PoW є те, що незалежні сторони можуть перевірити ці витрати з мінімальними зусиллями. PoW є найбільш поширеним механізмом криптовалютного ринку [12]. Важливою перевагою системи є її безпечність: для втручання в систему порушнику необхідно витратити надзвичайно велику кількість енергії. Деякі автори стверджують, що цей механізм потенційно вразливий до атаки 51 %, однак, за деякими розрахунками, ресурсні витрати такої атаки для зловмисників будуть більші ніж завдана шкода та отримані прибутки [13]. Найбільш важливим недоліком механізму Proof of Work є надзвичайно високе споживання електроенергії: усі вузли блокчейну витрачають енергію для розв’язання складних математичних задач, однак, лише вузол, який розв’язує задачу першим, може додати новий блок до системи й отримати винагороду. Також гостро постає проблема масштабування, оскільки зі зростанням мережі зростає і кількість ресурсів для додавання нових блоків [14].

Більш ефективним механізмом є Proof of Stake (PoS, Доказ частки) [15]. Суть механізму полягає в тому, що для створення блоків алгоритм на основі певних критеріїв вибирає осіб, яких називають валідаторами. Вони обираються рандомно, імовірність обрання вузла валідатором зростає пропорційно до частки токенів та віку суб’єкта в системі. Захист системи ґрунтується на тому припущенні, що суб’єкти, які мають частку в системі, зацікавлені у її захисті, оскільки із послабленням безпеки системи їхня частка втрачає вартість [16]. Проте цей механізм є вразливим до Nothing-at-Stake проблеми.

Proof of Stake та Proof of Work є найбільш ефективними механізмами для блокчейнів з нульовою довірою учасників і дозволяють проводити повністю анонімні транзакції [14].

Варіацією цього ж механізму є Delegated Proof-of-Stake (DPoS, делегований доказ частки), у якому вибрані вузли, яких називають виробниками блоків або свідками, по черзі генерують блоки мережі та отримують певну винагороду. Власники часток пропорційно до своїх часток голосують за вузли, які будуть виробниками. Вони також можуть звільнити виробників, які погано виконують свою роботу, та призначити нових, що стимулює виробників стежити за своєю репутацією [17]. Оскільки кількість виробників блоків обмежена (зазвичай від 20 до 100), цей механізм краще масштабується, ніж Proof of

Stake та Proof of Work, має вищу пропускну здатність за кількістю транзакцій за одиницю часу та потребує суттєво менших затрат для додавання нових блоків, однак, обмежена кількість делегатів відкриває вразливість до атаки 51 % [8]. Також серед недоліків зазначають його нижчу децентралізацію, порівняно з механізмами Proof of Stake та Proof of Work, втім для консорціумних або приватних блокчейнів цей недолік є несуттєвим [18].

Ще одним подібним по суті, але менш децентралізованими по факту механізмом є Proof-of-Importance (PoI, доказ значущості), у якому кожному вузлу присвоюється певна оцінка важливості, яка демонструє його значення для сукупної цінності системи. Вузли, що мають вищі оцінки важливості, з більшою імовірністю отримують право генерувати або збирати блоки. Оскільки вхідними даними для визначення важливості вузла є кількість транзакцій за останні 30 днів, накопичена цінність та взаємозв'язки з іншими вузлами блокчейну, більш активні вузли отримують винагороду за рахунок менш активних, таким чином концентруючи вплив на собі та знижуючи децентралізацію [8].

Також механізми консенсусу можуть використовувати як доказ фізичні носії. Proof-of-Space (PoSpace, доказ простору) – алгоритм, заснований на дисковому просторі: основним ресурсом для доказу є простір жорстких дисків учасників блокчейну, яке резервується під спеціальні функції блокчейну, наприклад, заповнення хеш-кодами для подальшої валідації блоків.

Багато механізмів у чистому вигляді є малопридатними для використання у публічних блокчейнах, однак можуть бути корисними у приватних.

Proof-of-Authority (PoA, доказ авторитету) – алгоритм консенсусу, заснований на авторитеті валідаторів. У ньому валідатори як доказ використовують власну репутацію. Валідаторів обирають учасники мережі шляхом голосування, і зазвичай кількість валідаторів обмежена. Відсутність винагородження валідаторів та ризик централізації робить цей механізм більш ефективним для використання у приватних блокчейнах, в яких проблема децентралізації не актуальною.

Practical Byzantine Fault Tolerance (Практична візантійська відмовостійкість) – був розроблений для вирішення проблем, пов'язаних із механізмом Byzantine fault tolerance. На відміну від останнього, цей механізм не вимагає синхронної взаємодії учасників, тому є більш практичним. Консенсус досягається у випадку, коли більшість вузлів голосують за приєднання блоку. Вузли в системі розподілені послідовно, один вузол є провідним, інші – вторинними. Провідний вузол відповідає за сортування запитів та їх послідовну відправку вторинним вузлам. У випадку відмови первинного вузла, його місце посідає вторинний [19]. Зазвичай, системи з використанням Practical Byzantine Fault Tolerance використовують менш як 20 попередньо вибраних вузлів перевірки, оскільки кількість повідомлень за експонентою зростає зі збільшенням кількості вузлів. Алгоритм є досить ефективним, але в основному використовується в приватних блокчейнах. Оскільки для ефективної роботи системи необхідно, щоб кількість небезпечних вузлів не перевищила або не дорівнювала 1/3 від всіх вузлів системи, цей алгоритм може використовуватися лише в умовах присутності часткової довіри.

В цілому, проблеми масштабування, децентралізації та безпеки присутні у всіх механізмах консенсусу, формуючи «трилему» блокчейну, оскільки неможливо одночасно забезпечити максимальну ефективність за трьома показниками: безпека, децентралізація та швидкість (придатність до масштабування). У випадку, якщо підтвердження транзакції вимагається від всіх вузлів, страждає швидкість; в умовах призначення валідаторів страждає децентралізація; використання мультичейнів вирішує проблеми масштабування та забезпечує децентралізацію, однак, знижує безпечність системи [20]. Таким чином, вибір алгоритмів консенсусу повинен здійснюватися з урахуванням потреб та пріоритетів організації.

Смартконтракти в блокчейн системах. Смартконтракт – це програма, яка може використовуватися в екосистемі блокчейну для механічного узгодження, виконання та забезпечення виконання умов юридичної угоди [21]. Концепцію смартконтракту вперше запропонував Нік Сабо, який визначив її як комп'ютеризований протокол транзакцій контракту [22, с. 15-18]. По суті, смартконтракти – це контейнери коду, які інкапсулюють і відтворюють умови реальних контрактів у цифровій сфері. Тобто вони є юридичною угодою між двома чи більше сторонами, кожна з яких зобов'язується виконувати свої зобов'язання. Хоча така угода має бути забезпечена законом, смартконтракти замінюють надійних третіх сторін або посередників між договірними сторонами завдяки автоматичному поширенню коду та його перевірки вузлами мережі в децентралізованому блокчейні [23]. Крім того, вони дозволяють здійснювати транзакції між ненадійними сторонами без необхідності прямого контакту між сторонами, довіри до третіх сторін і комісійних витрат на посередників [24], таким чином дозволяючи укладання ділових угод в середовищі нульової довіри [10]. Потрапивши в блокчейн, смартконтракти знаходяться за певною адресою, не контролюються жодним власником і не можуть бути видалені.

Смартконтракт виконується в такій послідовності:

1. Смартконтракт програмується та компілюється в байт-код компілятором.
2. Договір розгортається як правочин.
3. Майнер перевіряє видобуту транзакцію.
4. Транзакція прийнята в блокчейн, і контракту присвоєно адресу.
5. Щоб скористатися контрактом, користувачі надсилають транзакції на адресу контракту, вказуючи, яку функцію вони хочуть викликати.
6. Після перевірки транзакцій і майнінгу кожен вузол у мережі виконує функцію смартконтракту.

Смартконтракти написані в стилі, подібному до написання класу в об'єктноорієнтованому програмуванні.

Слід, втім, зазначити, що деякі дослідники права вважають незмінність та однозначність смартконтрактів потенційно проблематичними, оскільки полісемія трактування традиційних контрактів може служити не технічним недоліком, але цілеспрямованою особливістю, що підтримує їхню соціальну функцію та забезпечує гнучкість у вирішенні правових питань [10].

SSI, DID, Аутентифікація та підтвердження автентичності даних. Концепція SSI (самосуверенної ідентичності) була розроблена Крістофером Алленом (2016) як вираження особистого цифрового суверенітету. Він використовував його для опису заснованої на принципах структури, яка створить децентралізовану систему орієнтованих на користувача, самокерованих, сумісних цифрових ідентифікаторів [25]. Головна ідея SSI полягає у переданні сутностям контролю над своїми особистими даними з можливістю вибірково розкривати атрибути ідентифікації та зберігати конфіденційність, цілісність і достовірність даних, не покладаючи цю відповідальність на традиційні органи влади [26; 27].

У цій моделі присутні три діючих сутності: власник ідентифікаційної інформації – той, кому належать облікові дані, емітент – сутність, відповідальна за видачу власникам документів, які підтверджують облікові дані (verifable credentials) та верифікатор – сутність, що використовують надані облікові документи для автентифікації та перевірки представленої особи. Власники конфіденційної інформації зберігають документи, що підтверджують дані у цифрових гаманцях. Така модель дозволяє сутностям безпечно обмінюватися обліковими даними з верифікаторами, встановлюючи довіру та полегшуючи широкий спектр цифрових взаємодій без необхідності централізованих посередників. Система SSI мінімізує довіру до третіх сторін і використовує криптографічні технології, розподілені книги та стандартизовані протоколи для забезпечення безпеки, конфіденційності та сумісності ідентифікаційних даних [29].

Для забезпечення унікальності посилання на учасників SSI використовуються стандартизовані Консорціумом Всесвітньої мережі (W3C) децентралізовані ідентифікатори (DID). DID здатні розв'язуватися у відповідні документи, які містять інформацію, асоційовану з конкретним ідентифікатором, такі як криптографічні ключі та пакети автентифікації. Крім того, документ може містити службові кінцеві точки, які описують, як досягти суб'єкта DID та встановити зв'язок. Створення документів забезпечують системні компоненти, які називаються DID резолверами.

Для зберігання DID та надання необхідних даних для генерації DID документів, використовуються реєстри даних, що підлягають верифікації (Verifiable data registry, VDR). Ці реєстри можуть бути реалізовані в різних формах: розподілені книги, децентралізовані файлові системи, бази даних, однорангові мережі тощо. Довіра до системи може ґрунтуватися або на надійності технології, або на довірі до власника системи.

Взаємодія осіб один з одним та з обліковою книгою відбувається через програмні об'єкти, які називаються агентами. Зазвичай агент отримує доступ до цифрового гаманця для зберігання, отримання та виконання криптографічних операцій з ідентифікаційними даними. Агент SSI здатний підписувати, шифрувати та пересилати повідомлення, пов'язані з обліковими даними та встановленням з'єднань між агентами. Ці дії можуть виконуватися або агентом, автоматично, або користувачем, вручну. Роль агента полягає в тому, щоб захищати цифровий гаманець з даними так, щоб тільки власник гаманця мав до нього доступ.

У SSI облікові дані розглядаються як набір заяв із цифровим підписом емітента, де кожна претензія (claim) є твердженням стосовно суб'єкта (користувача). Верифіковані облікові дані (VC, verifiable claims) – це захищені від підробки облікові дані, які можна перевірити криптографічно. З метою забезпечення можливості перенесення даних та постійності ідентифікації суб'єктів були створені різні стандарти облікових даних, такі як W3C VC, AnonCreds і стандарти ISO mDL, кожен з яких підтримує різні криптографічні докази. Ці формати мають спільну мету: дозволити емітентам пакетувати заяви щодо організацій та запечатувати облікові дані за допомогою криптографії. Заяви можуть включати або облікові дані, які надають суб'єкту ідентифікації права доступу чи привілеї, або перевірку інформації, такої як посилання на документи, що посвідчують особу, професійні сертифікати, кредитну історію або будь-які інші дані чи інформацію. За допомогою криптографічних підписів верифікатори можуть оцінити цілісність облікових даних на основі відкритих ключів емітента [29].

Щоб перевірити будь-які облікові дані, верифікатор робить запит на підтвердження власнику (пруверу), запитуючи певні атрибути та предикати. Деякі з них обов'язково підлягають перевірці (наприклад, номер соціального страхування, вік тощо), а деякі можуть бути підтверджені самим власником особи (наприклад, ім'я, псевдонім або номер телефону). Під час перевірки встановлюється, чи збігаються ключі підписів з ключами особи, яка їх підписує [30].

SSI технологія може бути надзвичайно корисною у сфері аутентифікації/авторизації в різних системах. Наприклад, було запропоновано схему використання, у якій постачальник послуг (Service Provider) виступає одночасно емітентом та верифікатором. Постачальник послуг видає користувачеві сертифікат, що може бути верифікованим, який потім зберігається в його гаманці. Під час доступу до послуги користувач пред'являє сертифікат постачальнику послуги. Якщо сертифікат перевіряється успішно - користувач проходить аутентифікацію [31].

Хоча технологія SSI знаходиться в процесі розвитку, серед потенційних сфер її використання називають систему охорони здоров'я, фінансові установи [31], торгівлю [32], інтернет речей, урядові системи, зокрема, виборчі системи голосування [33].

Серед потенційних небезпек використання SSI зазначають необхідність високої грамотності користувачів стосовно питань безпеки, оскільки їх концепція передбачає те, що користувачі несуть повну відповідальність за розкриття власної конфіденційної інформації. Також поки що не з'ясованим лишається питання сумісності децентралізації контролю над особистими даними з геополітичними реаліями та юридичними вимогами [34]. Ще одним важливим проблемним аспектом цієї технології є неможливість відновлення втрачених ключів до цифрових гаманців, що призводить до незворотної втрати власником доступу до даних та можливостей управління ними.

Розгляд недосліджених частин загальної проблеми та подальший розвиток. Децентралізовані мережі мають значний потенціал у сфері державного управління та адміністрування завдяки їх постійності, стійкості та прозорості. Зокрема, у випадку блокчейну науковці [35] звертають увагу на такі його потенційно корисні особливості/можливості:

1. Токенізація: права на виконання дій з активом можуть бути перетворені в елементи даних, які можна передавати, або токени в блокчейнах.

2. Самозабезпечення та формалізація правил: смартконтракти дозволяють спільнотам користувачів кодувати правила таким чином, що вони однозначно розуміються машинами та виконуються самостійно.

3. Автономна автоматизація: після введення інформації децентралізовані автономні організації (DAO) можуть взаємодіяти між собою.

4. Підвищення прозорості: операційні процеси та пов'язані дані стають відкритими й не можуть бути змінені постфактум.

5. Децентралізація управління інфраструктурою: блокчейни дозволяють децентралізовану розробку правил для управління мережею.

6. Кодифікація довіри: блокчейн дозволяє не залучати треті сторони для перевірки угод.

Завдяки зазначеним можливостям впровадження систем на основі блокчейну та IPFS може бути корисним у як мінімум у таких сферах: ведення публічних записів і державної документації, завдяки збільшенню їх прозорості; операції з нерухомістю, завдяки зменшенню кількості посередників укладання угод; державні закупівлі – використання блокчейн систем потенційно обмежує можливості для корупції, лобіювання та махінації із залученням третіх сторін; видача документів про освіту, оскільки потенційно може вирішити питання зарахування верифікації цих документів між країнами. Слід зазначити, що на сьогодні вже здійснювалося впровадження пілотних блокчейн проєктів у зазначених сферах в Іспанії, Грузії, США, Південній Кореї, Гані, Україні (OpenMarket). Однак дані щодо їхньої ефективності виявилися суперечливими. Зокрема, постали проблеми недостатньої прозорості створених блокчейнів, надмірної децентралізації, неточності вхідних даних, неможливості вираження деяких величин дискретними значеннями (у сфері впорядкування земельних ділянок), гальмування процесів цифровізації даних [11; 36; 37]. Тому актуальним є пошук оптимальної організації систем з погляду централізації/децентралізації, а також визначення інших проблемних аспектів.

Для визначення найбільш продуктивних способів застосування децентралізованих систем для управління даними корисно також звертати увагу на їх застосування у неприбутковому секторі. Зокрема, набули популярності благодійні пожертви в криптовалюті. Особливо яскраво це спостерігали на початку російського вторгнення в Україну [38]. Використання блокчейн технологій благодійними організаціями може сприяти зростанню довіри, прозорості витрат та фандрейзингу, демонстрації ефективної витрати коштів (власне, також і оптимізації витрат) і, як наслідок, готовності донорів робити пожертви та зростанню ефективності роботи організацій. Дослідити ефективність блокчейн технологій для роботи громадських організацій можна через впровадження пілотних проєктів. Так, IBM з колегами після урагану «Харві» в Техасі запропонувала архітектуру на основі

proof of concept для створення інфраструктури надання допомоги при стихійних лихах. Ця інфраструктура забезпечує зменшення паперової роботи, підвищує довіру до уряду та допомоги [11]. Відповідно, необхідною та перспективною задачею є розробка, впровадження та оцінювання ефективності пілотних проєктів на основі блокчейну для децентралізованого зберігання та адміністрування публічних даних.

Висновки. Нині є очевидною необхідність розробки надійних і безпечних систем управління даними у сфері зберігання публічних даних. Оскільки в сучасну цифрову епоху обсяг і значення загальнодоступних даних продовжують зростати, потреба в ефективному управлінні та забезпеченні безпеки та прозорості стає дедалі гострішою. Децентралізовані системи, такі як блокчейн і IPFS є перспективними шляхами вирішення цих проблем, не лише забезпечуючи надійне зберігання даних, але і знижуючи ризики несанкціонованого доступу та підвищуючи стійкість системи до збоїв. Серед проблемних аспектів використання цих технологій слід зазначити питання сумісності, продуктивності, ефективності та аспект сприйняття їх ринком. Тим не менш, зазначені технології мають потенціал до революціонізування практики управління даними, сприяючи більшій прозорості, підзвітності та ефективності надання державних послуг, тож розробка децентралізованих систем управління даними є перспективним об’єктом інвестування для зацікавлених сторін в державному та приватному секторах.

Список використаних джерел

1. Про доступ до публічної інформації [Електронний ресурс]: Закон України від 13 січня 2011 р. № 2939-VI. – Режим доступу: https://minjust.gov.ua/m/str_35409.

2. Національні інформаційні системи[Електронний ресурс]. – Режим доступу: https://nais.gov.ua/registers.

3. Distributed Systems: Concepts and Design / G. Coulouris, J. Dollimore, T. Kindberg, G. Blair. – 5th Edition. – 2011. – 1067 p.

4. Wennergren, O. Transparency analysis of distributed file systems: With a focus on interplanetary file system: Bachelor Degree Project in Information Technology / O. Wennergren, M. Vidhall, J. Sörensen. – University of Scovde, 2021. – 83 p.

5. De, Suman. Comparative Study on Distributed File Systems / Suman De1, Megha Panjwan // Studies in Computational Intelligence. – 2021. – Vol. 956. – P. 41-51. DOI: 10.1007/978-3-030-68291-0_5

6. Welcome to the IPFS docs. IPFS docs: web-site. – Access mode: https://docs.ipfs.tech.

7. Kubo: IPFS Implementation in GO. GitHub: web-site. – Access mode: https://github.com/ipfs/kubo.

8. Gamage, H. T. M. A Survey on Blockchain Technology Concepts, Applications, and Issues / H. T. M. Gamage, H. D. Weerasinghe, N. G. J. Dias // SN Computer Science. – 2020. – № 1(2). DOI:10.1007/s42979-020-00123-0.

9. Buterin, V. On Public and Private Blockchains. 2015. Ethereum foundation Blog: web-site. – Access mode: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

10. Eenmaa-Dimitrieva, H. Creating markets in no-trust environments: The law and economics of smart contracts / H. Eenmaa-Dimitrieva, M. J. Schmidt-Kessen // Computer Law & Security Review. – 2018. – Vol. 35. – № 1. – P. 69-88. DOI: 10.1016/j.clsr.2018.09.003.

11. Alston, E. Introduction to the special issue: Blockchains and public administration / E. Alston, I. Murtazashvili, M. B. Weiss // Chinese Public Administration Review. – 2024. – Vol. 15(1). – Pp. 3-10. DOI: 10.1177/15396754241228530.

12. Milunovich, G. Assessing the Connectedness between Proof of Work and Proof of Stake/Other Digital Coins / G. Milunovich // Economics Letters. – 2022 – Vol. 211. DOI: 10.2139/ssrn.3970813.

13. Untangling blockchain: A data processing view of blockchain systems / T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang // IEEE transactions on knowledge and data engineering. – 2018. – Vol. 30(7). – P. 1366-1385.

14. Bergman, S. Permissioned blockchains and distributed databases: A performance study / S. Bergman, M. Asplund, S. Nadjm-Tehrani // Concurrency and Computation: Practice and Experience. – 2020. – Vol. 32(12). – Article. E 5227.

15. Saleh, F. Blockchain Without Waste: Proof-of-Stake / F. Saleh // Review of Financial Studies. 2021. – Vol. 34. – P. 1156-1190.

16. Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work / I. Bentov, A. Gabizon, A. Mizrahi // Lecture Notes in Computer Science. – 2016. – Article: 9604. – P. 142–57. DOI: 10.1007/978-3-662-53357-4_10.

17. A new election algorithm for DPos consensus mechanism in blockchain / Luo Y. Chen Y. Chen Q. Liang Q. // 7th International Conference on Digital Home (ICDH), Piscataway. – 2018. – P. 116–120.

18. Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions / L. Hang, C. Chen, L. Zhang, J. Yang // IET Community. – 2022. – Vol. 16. – P. 2371-2393. DOI: 10.1049/cmu2.12488.

19. Castro, M. Practical byzantine fault tolerance / M. Castro, B. Liskov // Proceedings of the symposium on operating system design and implementation. – 1999. – Vol. 20. – Pp. 398–461.

20. Parashar, D., Sharma, M., Sharma, V., Nand, P. Approaching Solutions to Blockchain Security Trilemma and Consensus Mechanisms / D. Parashar, M. Sharma, V. Sharma, P. Nand // 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N): Greater Noida, India, 2022. – Pp. 2030-2036, DOI: 10.1109/ICAC3N56670.2022.100745224.

21. Rouhani, S. Security, performance, and applications of smart contracts: A systematic survey / S. Rouhani, R. Deters // IEEE Access. – 2019. – Vol. 7. – P. 50759-50779.

22. Mohanta, B. K. An Overview of Smart Contract and Use Cases in Blockchain Technology / B. K. Mohanta, S. S. Panda, D. Jena // 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT. 2018. – Pp. 15-18.

23. Taherdoost, H. Smart Contracts in Blockchain Technology: A Critical Review / H. Taherdoost // Information. – 2023. – Vol. 14. – № 2. – P. 117. DOI: 10.3390/info14020117.

24. Swan, M. Blockchain: Blueprint for a New Economy / Melanie Swan. – O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015. – 152c.

25. Allen, C. The path to self-sovereign identity [Blog post] / C. Allen // Life With Alacrity. – 2016. – April 25). URL: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212.

26. Renieris E. SSI? What we really need is full data portability [Blog post] / E. Renieris // Women in Identity. – 2020. URL: https://womeninidentity.org/2020/03/31/data-portability.

27. Herian, R. Blockchain, GDPR, and fantasies of data sovereignty / R. Herian // Law, Innovation and Technology. – 2020. – Vol. 12(1). – P. 156-174. DOI: 10.1080/17579961.2020.1727094.

28. Satybaldy, A. A Taxonomy of Challenges for Self-Sovereign Identity Systems / A. Satybaldy, M. S. Ferdous, M. A. Nowostawski // IEEE Access. – 2024. – Vol. 12. – Pp. 16151-16177. DOI: 10.1109/ACCESS.2024.3357940.

29. Bhattacharya, M. P. Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain / M. P. Bhattacharya, P. Zavarsky, S. Butakov // International Symposium on Networks, Computers and Communications (ISNCC). – 2020. DOI:10.1109/isncc49221.2020.9297357.

30. Ferdous, M. S. Ssi4web: A self-sovereign identity (ssi) framework for the web / M. S. Ferdous, A. Ionita, W. Prinz // Blockchain and Applications, 4th International Congress: Springer. 2023. – Pp. 366–379.

31. Kei,l J. Self-sovereign identity: Use cases, level of maturity, and adoption [Electronic resource] / J. Keil. –2022. Infopulse: web-site. – Access mode: https://www.infopulse.com/blog/self-sovereign-identityuse-cases-adoption.

32. Tobin A. The inevitable rise of self-sovereign identity. A white paper from the Sovrin Foundation [Electronic resource] / A. Tobin, D.Reed. – 2018. – Access mode: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

33. CBInsights. How blockchain could secure elections. 2018. – Access mode: https://www.cbinsights.com/research/report/blockchain-election-security.

34. Giannopoulou, A. Self-sovereign identity / A. Giannopoulou, F. Wang // Internet Policy Review. – 2021. – Vol. 10. – № 2. DOI: 10.14763/2021.2.155035.

35. Rozas, D. Analysis of the potentials of blockchain for the governance of global digital commons / D. Rozas, A. Tenorio-Fornés, S. Hassan // Frontiers in Blockchain. – 2021. – Vol. 4. – Pp. 577-680. DOI: 10.3389/fbloc.2021.577680.

36. Kenetey, G. Budgetary control and the adoption of consortium blockchain monitoring system in the Ghanaian local government / G. Kenetey, B. Popesko // International Journal of Public Sector Management. – 2024. – Vol. ahead-of-print No. ahead-of-print. DOI: 10.1108/IJPSM-07-2023-0212.

37. Proskurovska, Anetta.The blockchain challenge for Sweden's housing and mortgage markets / Anetta Proskurovska, Sabine Dörry // Environment and Planning A: Economy and Space. – 2022. – Vol. 54. – P. 1569-1585. DOI: 10.1177/0308518X221116896.

38. Chen, W. Is cryptoaltruism transforming the nonprofit sector? Lessons from the Ukrainian nonprofits during the Russia-Ukraine war / W. Chen, I. Murtazashvili // Chinese Public Administration Review. – 2024. – Vol. 15(1). DOI: 10.1177/15396754231222575.

References

1. Pro dostup do publichnoi informatsii [On access to public information], Law of Ukraine № 2939-VI (13, 2022). from https://minjust.gov.ua/m/str_35409.

2. Natsionalni informatsiiny systemy [National Informational Systems]. https://nais.gov.ua/registers.

3. Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (2011). *Distributed Systems: Concepts and Design* (5th ed.). Addison-Wesley.

4. Wennergren, O., Vidhall, M., & Sörensen, J. (2021). Transparency analysis of distributed file systems: With a focus on interplanetary file system. *Bachelor Degree Project in Information Technology*. University of Scovde.

5. De, S., & Panjwani, M. (2021). A Comparative Study on Distributed File Systems. *Studies in Computational Intelligence, 956*, 41-51. https://doi.org/10.1007/978-3-030-68291-0_5.

6. Protocol Labs. (n.d.). Welcome to the IPFS docs. https://docs.ipfs.tech.

7. IPFS. (n.d.). *Kubo: IPFS Implementation in GO*. https://github.com/ipfs/kubo.

8. Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A Survey on Blockchain Technology Concepts, Applications, and Issues. *SN Computer Science, 1*(2), 3. https://doi.org/10.1007/s42979-020-00123-0.

9. Buterin, V. (2015). On Public and Private Blockchains. Ethereum Foundation Blog. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

10. Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2018). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review, 35*(1), 69-88. https://doi.org/10.1016/j.clsr.2018.09.003.

11. Alston, E., Murtazashvili, I., & Weiss, M. B. (2024). Introduction to the special issue: Blockchains and public administration. *Chinese Public Administration Review, 15*(1), 3-10. https://doi.org/10.1177/15396754241228530.

12. Milunovich, G. (2022). Assessing the Connectedness between Proof of Work and Proof of Stake/Other Digital Coins. https://doi.org/10.2139/ssrn.3970813.

13. Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30*(7), 1366–1385.

14. Bergman, S., Asplund, M., & Nadjm-Tehrani, S. (2020). Permissioned blockchains and distributed databases: A performance study. *Concurrency and Computation: Practice and Experience, 32*(12), Article e5227.

15. Saleh, F. (2021). Blockchain Without Waste: Proof-of-Stake. *Review of Financial Studies, 34,* 1156-1190.

16. Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. *Lecture Notes in Computer Science, 9604*, 142–157. https://doi.org/10.1007/978-3-662-53357-4_10.

17. Luo, Y., Chen, Y., Chen, Q., & Liang, Q. (2018). A new election algorithm for DPoS consensus mechanism in blockchain. In *2018 7th International Conference on Digital Home (ICDH)* (pp. 116–120). IEEE.

18. Hang, L., Chen, C., Zhang, L., & Yang, J. (2022). Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions. *IET Communications, 16*, 2371–2393. https://doi.org/10.1049/cmu2.12488.

19. Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. *Proceedings of the symposium on operating system design and implementation, 20*, 398–461.

20. Parashar, D., Sharma, M., Sharma, V., & Nand, P. (2022). Approaching Solutions to Blockchain Security Trilemma and Consensus Mechanisms. In *4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 2030-2036). https://doi.org/10.1109/ICAC3N56670.2022.100745224.

21. Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access, 7*, 50759–50779.

22. Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. In *9th International Conference on Computing, Communication and Networking Technologies* (ICCCNT 2018) (pp. 15–18).

23. Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information, 14*(2), 117. https://doi.org/10.3390/info14020117

24. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

25. Allen, C. (2016, April 25). The path to self-sovereign identity. Life With Alacrity. https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212.

26. Renieris, E. (2020). SSI? What we really need is full data portability [Blog post]. Women in Identity. https://womeninidentity.org/2020/03/31/data-portability.

27. Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology, 12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094.

28. Satybaldy, A., Ferdous, M. S., & Nowostawski, M. (2024). A Taxonomy of Challenges for Self-Sovereign Identity Systems. *IEEE Access, 12*, 16151-16177 https://doi.org/10.1109/ACCESS.2024.3357940.

29. Bhattacharya, M.P., Zavarsky, P., & Butakov, S. (2020). Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain. *International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/isncc49221.2020.9297357.

30. Ferdous, M. S., Ionita, A., & Prinz, W. (2023). Ssi4web: A self-sovereign identity (ssi) framework for the web. *Blockchain and Applications*, 4th International Congress. Springer (pp. 366–379).

31. Keil, J. (2022). Self-sovereign identity: Use cases, level of maturity, and adoption. *Infopulse*. https://www.infopulse.com/blog/self-sovereign-identityuse-cases-adoption.

32. Tobin, A., & Reed, D. (2018). The inevitable rise of self-sovereign identity. A white paper from the Sovrin Foundation. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

33. CBInsights. (2018). How blockchain could secure elections. https://www.cbinsights.com/research/report/blockchain-election-security.

34. Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review, 10*(2). https://doi.org/10.14763/2021.2.155035.

35. Rozas, D., Tenorio-Fornés, A., & Hassan, S. (2021). Analysis of the potentials of blockchain for the governance of global digital commons. *Frontiers in Blockchain, 4*, Article 577680. https://doi.org/10.3389/fbloc.2021.577680.

36. Kenetey, G., & Popesko, B. (2024). Budgetary control and the adoption of consortium blockchain monitoring system in the Ghanaian local government. *International Journal of Public Sector Management*. https://doi.org/10.1108/IJPSM-07-2023-0212.

37. Proskurovska, A., & Dörry, S. (2022). The blockchain challenge for Sweden's housing and mortgage markets. *Environment and Planning A: Economy and Space, 54.* https://doi.org/10.1177/0308518X221116896.

38. Chen, W., & Murtazashvili, I. (2024). *Is cryptoaltruism transforming the nonprofit sector? Lessons from the Ukrainian nonprofits during the Russia-Ukraine war*. Chinese Public Administration Review. https://doi.org/10.1177/15396754231222575.

Отримано 22.05.2024

UDC 004.623

Anton Iskryzhytskii[1], Artem Zadorozhnii[2]

[1]PhD student, recipient of the Doctor of Philosophy degree in specialty 122
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: a.iskryzhytskyi@gmail.com. **ORCID:** https://orcid.org/0009-0005-4153-2075

[2]PhD, Associate Professor, Associate Professor of the Department of Information Technology and Software Engineering.,
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: zaotroy@gmail.com. **ORCID:** https://orcid.org/0000-0002-3424-7293

STUDY OF AVAILABLE METHODS AND TECHNOLOGIES FOR DECENTRALIZED STORING AND ADMINISTRATION OF PUBLIC DATA

The article is an overview and information. In the modern digital world, where the storing and processing of large volumes of data are becoming increasingly relevant, reliable and secure data management is of great importance. The problem of effective management, security, and transparency of public data can be addressed through decentralized systems such as blockchain and IPFS (InterPlanetary File System), that are able to ensure reliable storing, reduce risks of unauthorized access, and increase system fault tolerance. In public registries, which store socially significant data, it is necessary to ensure continuous access and the integration with third-party services databases, increasing consumer trust in the authenticity of the data. This article provides a comprehensive review of various existing technologies, including blockchain and IPFS, their advantages, disadvantages, and potential application for decentralized storing and processing public data, based on existing research in this area. The article examines how blockchain contributes to the security, transparency, and immutability of data, and considers IPFS as an innovative method of data storage, differing from traditional centralized systems. Various aspects of decentralization are analyzed, including its impact on the efficiency and scalability of data storage systems. The article also covers the importance of authentication and authorization in decentralized systems, considering different approaches and protocols that can be used to ensure security and control access to data. Potential challenges and limitations based on previously published research related to decentralized data storage systems, including the problems of their compatibility, performance, and market acceptance, are discussed. Finally, the article discussing future development of these technologies and their potential impact on society and business.

Keywords: *Public Data; IPFS; Blockchain; Authentication; Decentralized Systems.*

Fig.: 4. References: 38.

Іскрижицький А. М., Задорожній А. О. Дослідження наявних методів та технологій для децентралізованого зберігання та адміністрування публічних даних. *Технічні науки та технології.* 2024. № 2(36). С. 137-150.