ISSN (Print) 2307-6968, ISSN (Online) 2663-2209
Вчені записки Університету «КРОК» №3 (75), 2024

УДК 005.4: 336.7
DOI: 10.31732/2663-2209-2024-75-108-119

УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ КРИПТОВАЛЮТНИХ ТЕХНОЛОГІЙ НА ОСНОВІ ІНТЕГРАЦІЇ СМАРТ-КОНТРАКТІВ І РОЛАПІВ

***Юрій Ковальчук*[1]**

[1]*Аспірант, ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна, e-mail: kovalchukyr@krok.edu.ua, ORCID: https://orcid.org/0000-0001-6093-142X*

MANAGEMENT OF CRYPTOCURRENCY TECHNOLOGY BUSINESS PROCESSES BASED ON THE INTEGRATION OF SMART CONTRACTS AND ROLLUPS

***Yurii Kovalchuk*[1]**

[1]*Graduate student, KROK University, Kyiv, Ukraine, e-mail: kovalchukyr@krok.edu.ua, ORCID: https://orcid.org/0000-0001-6093-142X*

***Анотація**. В статті досліджуються актуальні технології ролапів, які дозволяють масштабувати використання смарт-контрактів в управлінні бізнес-процесами технологій на основі блокчейну. Особлива увага приділяється важливості децентралізації в сучасному цифровому світі. З огляду на збільшення потреби в автоматизації та ефективності в бізнес-процесах, визначено, що дана тематика є надзвичайно важливою для подальшого розвитку управлінських, фінансових і адміністративних систем по всьому світу. Встановлено, що поглиблений аналіз і порівняння можливостей різних технологій ролапів забезпечує ефективніший, безпечніший і економічний підхід до використання блокчейн-технологій в управлінні бізнесом. Використано метод порівняльного аналізу, що дозволив оцінити вплив різних рівнів масштабування блокчейну – від рівня 0 до рівня 3 – на загальну продуктивність та вартість транзакцій. Наукові результати дослідження визначили значні перспективи застосування ролапів для мінімізації витрат і часу на обробку транзакцій, а також для зниження залежності від централізованих посередницьких служб. Встановлено, що особливо важливим є виявлення та аналіз компромісів між децентралізацією, безпекою та масштабованістю, відомих як «трилема блокчейну», що впливає на можливості та обмеження в розгортанні цих технологій. Запропоновано подальші дослідження базувати на розробці нових методів і технічних рішень, спрямованих на вирішення проблем, виявлених у трилемі блокчейна. Наголошується на тому, що особливу увагу варто приділяти впровадженню інноваційних підходів, які могли б допомогти досягти оптимального балансу між ключовими характеристиками блокчейну. Крім того, встановлено, що актуальним залишається аналіз правових та економічних аспектів інтеграції ролапів у існуючі системи управління, що може сприяти їх ширшому впровадженню та визнанню на міжнародному рівні. Результати проведеного дослідження доводять необхідність аналізу розвитку системи знань про масштабування блокчейн-технологій. Це створює основу для подальшої роботи у цьому напрямку, маючи на меті більшу децентралізацію, безпеку та ефективність управлінських процесів.*

***Ключові слова**: менеджмент, управління, блокчейн, смарт-контракти, ролапи, інтеграція, технології.*
Формули: 0; рис.: 2; табл.: 1, бібл.: 16

***Abstract**. The article explores current rollup technologies that enable the scaling of smart contract usage in managing business processes based on blockchain technology. Special attention is given to the importance of decentralization in the modern digital world. Given the increasing need for automation and efficiency in business processes, it is determined that this topic is extremely important for the further development of management, financial, and administrative systems worldwide. It has been established that an in-depth analysis and comparison of the capabilities of various rollup technologies provides a more efficient, secure, and economical approach to using blockchain technologies in business management. A comparative analysis method was used to assess the impact of different levels of blockchain scaling - from level 0 to level 3 - on overall performance and transaction costs. The scientific results of the study identified significant prospects for the use of rollups to minimize costs and transaction processing time, as well as to reduce reliance on centralized intermediary services. It is established that it is particularly important to identify and analyze the trade-offs between decentralization, security, and scalability, known as the "blockchain trilemma", which affects the possibilities and limitations in deploying these technologies. It is proposed that further research be based on the development of new methods and technical solutions aimed at addressing the problems identified in the blockchain trilemma. Emphasis is placed on the importance of implementing innovative approaches that could help achieve an optimal balance between the key characteristics of blockchain. Additionally, it is noted that the analysis of legal and economic aspects of integrating rollups into existing management systems remains relevant, which could contribute to their broader adoption and recognition at the international level. The results of the study demonstrate the necessity of analyzing the development of knowledge systems about blockchain scaling technologies. This lays the foundation for further work in this direction, aiming for greater decentralization, security, and efficiency in management processes.*

***Keywords**: management, administration, blockchain, smart contracts, rollups, integration, technologies.*
Formulas:0; fig.: 2; tabl.: 1; bibl.:16

Постановка проблеми. У сучасному динамічному бізнес-середовищі криптовалютного ринку, ефективність управління бізнес-процесами стає ключовим фактором успіху. Смарт-контракти, які автоматично виконують, контролюють або документують юридично значимі події та дії згідно з умовами контракту, стають невід'ємним інструментом у цьому процесі. Вони забезпечують прозорість, знижують ризики і підвищують довіру між сторонами, зменшуючи при цьому необхідність у посередниках.

Проте, незважаючи на значні переваги, смарт-контракти стикаються з декількома викликами. Однією з основних проблем є масштабованість: з ростом кількості контрактів та їх складності, вартість і час обробки транзакцій на блокчейні, як Ethereum, можуть суттєво зрости. Це обмежує їхню практичність у великомасштабних або складних корпоративних бізнес-процесах.

Одним із способів вирішення проблеми масштабованості є застосування технології ролапів, які дозволяють виконувати транзакції поза основним блокчейном, значно знижуючи вартість та час обробки. Ролапи забезпечують збільшену пропускну спроможність і швидкість, що є критично важливим для бізнесу, який прагне використовувати смарт-контракти для управління складними процесами та великою кількістю транзакцій.

Аналіз останніх досліджень і публікацій. Останні дослідження щодо масштабування смарт-контрактів із використанням технології ролапів зосереджені на таких аспектах, як використання технологій рівня 2 для зниження вартості операцій. Як свідчать дані, перехід на системи, де агрегація даних відбувається поза ланцюгом блокчейну, може знизити оперативні витрати до 76%, при цьому збільшуючи децентралізацію та знижуючи концентрацію ринку (The FinReg Blog, 2023).

Наступний напрям досліджень – це оптимістичні та ролапи з нульовим розкриттям, кожна з яких має свої переваги та недоліки з точки зору безпеки та швидкості обробки (Gemini, n.d.) (FHE-Rollups, n.d.).

Далі слід зазначити застосування інновацій у передачі активів між ролапами, дослідження яких виявило, що новітні системи передачі між ролапами можуть значно підвищити ефективність, використовуючи методи пакетного розрахунку завдяки існуючим міжбанківським технологіям розрахунків (Jeong & Lee, 2023).

Важливим є також вивчення системи Арбітрум та її вплив на масштабування, адже система Арбітрум використовує стек-архітектуру для організації держави віртуальної машини, що дозволяє ефективно масштабувати смарт-контракти з високим рівнем приватності і мінімальними транзакційними витратами (Smart Contract Research Forum, n.d.).

Для прогнозування ринків криптовалют важливим є дослідження особливостей та характеристик методів технічного аналізу, на що вказують Пилипченко, Кузьмінський & Чумаченко (2021).

Інноваційні технологічні рішення можна застосовувати для дослідження й інших фінансових ринків та інструментів, зокрема дорогоцінних металів (Rumyk, I., Kuzminsky, V., Pylypenko O., & Yaroshenko, O., 2024).

Наукові пошуки вказують на потенційну роль технологій ролапів у реалізації ефективніших і безпечніших методів масштабування смарт-контрактів, що може мати значний вплив на управління бізнес-процесами в контексті використання блокчейн технологій. Але оскільки технології розвиваються дуже швидко і кожного дня створюються нові рішення, а тема досить нова, тому є потреба виконання поглибленого дослідження даного питання.

Формулювання цілей статті. Мета статті полягає у аналізі та порівнянні технологій ролапів, що дозволяють масштабувати можливості використання смарт-контрактів в управлінні бізнес-процесами технологій на базі криптовалют.

Для виконання досліджень було застосовано метод аналізу відкритих джерел. Основною стратегією збору даних стало вивчення наявних публікацій, онлайн-ресурсів і технічних звітів з метою збору актуальної інформації про застосування смарт-контрактів та технологій ролапів в управлінні бізнес-процесами. Системний аналіз дозволив об'єктивно оцінити поточні тренди та ідентифікувати передові практики у використанні цих технологій. За допомогою порівняльного аналізу оцінено різні технічні рішення, що виявило їхні ключові переваги та можливі обмеження в контексті бізнес-управління.

Виклад основного матеріалу дослідження. З давніх часів люди здійснювали транзакції один з одним у прямий спосіб. Однак, як цивілізація розвивалася, і транзакції ставали більш масштабними та складними, з'явилася потреба у довіреній третій стороні або посереднику. Ці посередники, такі як банки, уряди та адвокати, займалися управлінням та посередництвом у транзакціях, діючи в інтересах учасників. На жаль, залежність від таких посередників мала недоліки. Люди втрачали контроль над своїми транзакціями, а витрати, пов'язані з посередниками, ставали дедалі обтяжливими. Вони диктували процес і не завжди враховували інтереси окремих осіб. Але, оскільки суспільство розвивалося, люди ставали все більше залежними від цих посередників (Polishchuk, et al., 2019).

Відповідь прийшла у вигляді технології блокчейн. Блокчейн – це децентралізована система від одного користувача до іншого, яка усуває потребу у посередниках. Замість того, щоб покладатися на банк, люди можуть мати власні гаманці та здійснювати транзакції між собою. Замість того, щоб потребувати адвоката, вони можуть використовувати смарт-контракти, вбудовані в блокчейн, які автоматично виконують попередньо визначені дії, коли зустрічаються конкретні умови. І замість того, щоб покладатися тільки на уряд, децентралізовані автономні організації дозволяють будь-кому брати участь в управлінні та процесах прийняття рішень (Чіков, та ін., 2023).

Фінансові інновації в економічній діяльності країни питання не нове та вивчалося протягом тривалого часу (Румик, 2007). Однак, первинним застосуванням блокчейн-технології було у сфері грошей, як це видно на прикладі Bitcoin, першої децентралізованої криптовалюти, створеної у 2008 році під псевдонімом Сатоші Накамото. Ще одним відомим фінансовим інструментом є Ethereum, який служить децентралізованою обчислювальною платформою, що дозволяє створювати смарт-контракти.

Завдяки децентралізації, відсутності єдиного регулювального органу та можливості здійснення швидких транскордонних платежів, криптовалюти забезпечують інноваційні можливості для бізнесу, відкриваючи шляхи для ефективного капіталовкладення та розширення ринків (Румик, & Ковальчук, 2024).

Однак, існує серйозна проблема з цією технологією – вона має труднощі з ефективним масштабуванням (Yatsenko, et al., 2022). Наприклад, PayPal та Visa можуть обробляти відповідно 195 та 1700 транзакцій за секунду, тоді як Bitcoin обмежений лише сімома транзакціями за секунду (Ledger Academy, 2023). З огляду на таку значну різницю, виникають сумніви щодо можливості широкого прийняття блокчейн технології. Виникає питання – чи не можна просто швидше налаштувати технологію? Хоча це може здатися простим рішенням, насправді все набагато складніше, адже існують певні компроміси. Це приводить нас до концепції «Трилеми блокчейну», термін який запровадив співзасновник Ethereum Віталій Бутерін (Buterin, 2021).

Трилема блокчейну полягає у складності одночасного досягнення трьох ключових характеристик у мережі блокчейн: децентралізації, безпеки та масштабованості. Згідно з цією концепцією, мережа може ефективно реалізувати лише дві з цих характеристик одночасно. Це означає, що для підвищення

масштабованості доведеться пожертвувати деяким рівнем децентралізації, або навпаки – збільшення децентралізації може послабити масштабованість.

Розглянемо детальніше ці характеристики блокчейну.

Децентралізація: Відсутність централізованого контролю, що сприяє демократичному та незалежному функціонуванню мережі.

Безпека: Захист даних та транзакцій від атак, гарантування незмінності та цілісності інформації.

Масштабованість: Здатність мережі обробляти велику кількість транзакцій ефективно, забезпечуючи швидке підтвердження транзакцій при збільшенні числа користувачів і транзакцій (рис. 1).

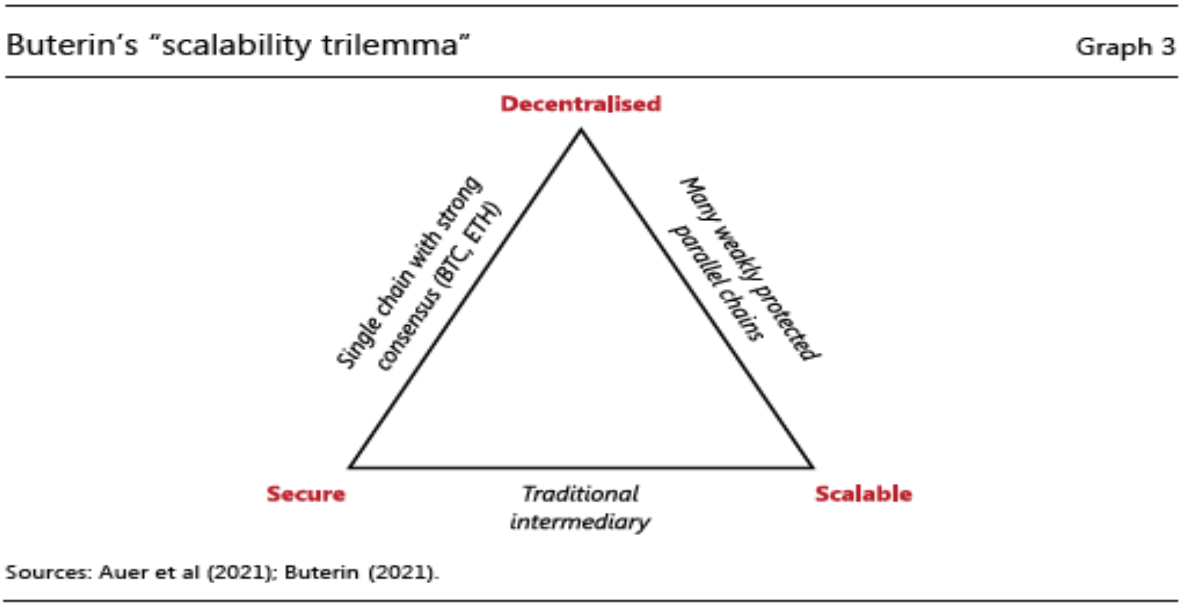

Рис. 1. Схема трилеми масштабування блокчейну

Джерело: побудовано на основі Auer at al (2021); Buterin (2021)

Якщо безпека є пріоритетом, то потрібно балансувати між децентралізацією та масштабованістю, де збільшення одного може відбуватися за рахунок іншого. Хоча Трилема блокчейну ще не має остаточного доказу чи спростування, вона висвітлює властиві труднощі у досягненні досконалого балансу між цими характеристиками.

Тим часом, важливо зауважити, що існують різні техніки та ідеї, які впроваджуються для вирішення проблеми масштабування. Це приводить нас до необхідності поглибленого розгляду цього питання.

Інфраструктура блокчейну складається з п'яти рівнів: апаратне забезпечення, дані, мережа, консенсус та додатки. Рішення для масштабування блокчейну полягають у оптимізації цих шарів для прискорення роботи мережі та зниження витрат. Ці рішення поділяють на рівні 0, 1, 2 і 3, кожен з яких відіграє роль у покращенні функціональності та масштабованості технології блокчейн. Розглянемо ці рівні, приклади їхнього застосування та конкретні проблеми, які вони вирішують.

Рівень 0 є основною мережевою архітектурою екосистеми блокчейну, яка включає апаратні засоби, протоколи, з'єднання та інші компоненти. Цей шар можна вважати мережею взаємопов'язаних блокчейнів. Однією з ключових функцій Рівня 0 є забезпечення міжланцюгової взаємодії, що дозволяє різним блокчейнам комунікувати та взаємодіяти. Таке спілкування є критично важливим для вирішення викликів масштабування у майбутніх шарах блокчейну.

Рівень 0 часто включає власний токен, який сприяє участі та розвитку в мережі. Прикладами мереж Рівня 0 є Aptos, Sui, Avalanche, та Cosmos, що демонструють реалізацію архітектури рівня 0 і забезпечують інфраструктуру для міжопераційності та масштабування в екосистемі блокчейну.

Рішення для масштабування блокчейну рівня 0 забезпечують ефективну обробку великих обсягів транзакцій при забезпеченні високого рівня безпеки та приватності. Ці блокчейни використовують такі технології, як шардінг і паралельну обробку, що дозволяє оптимізувати процеси досягнення консенсусу та зберігання даних. Це значно підвищує пропускну здатність мережі, забезпечуючи швидку та ефективну обробку транзакцій. Завдяки покращенню продуктивності та масштабованості, рівень 0 також зменшує вартість транзакцій, що робить блокчейн-рішення доступнішими для бізнесу та приватних осіб та сприяє їх ширшому впровадженню.

Блокчейни рівня 0 також використовують передові криптографічні техніки, такі як докази з нульовим розголошенням і багатосторонні обчислення, що підвищує безпеку та приватність транзакцій. Ці заходи захищають від шахрайства, зломів та інших видів порушень безпеки, що робить їх особливо привабливими для корпоративних застосувань, де критично важливі конфіденційність і безпека даних.

Однією з ключових особливостей блокчейнів рівня 0 є їх здатність до легкої інтеграції з іншими блокчейнами та технологіями. Це сприяє інтеграції децентралізованих додатків (dApps) та сервісів у існуючі системи, що сприяє співпраці та інноваціям у рамках екосистеми блокчейну.

Мережі рівня 1 у технології блокчейну служать основою для побудови інших додатків та мереж, наприклад, мереж рівня 2. Операційні характеристики такої мережі, включаючи швидкість, безпеку та місткість, визначаються її механізмом консенсусу. Мережі рівня 1 обробляють розрахунки транзакцій і управління користувацькими гаманцями за допомогою унікальних пар ключів та відстежують баланси криптовалют або токенів. Вони зазвичай асоційовані з рідним токеном, який використовується для доступу до ресурсів мережі та для таких послуг, як передача криптовалюти, створення токенів або виконання смарт-контрактів.

Рішення масштабування блокчейну рівня 1 спрямовані на підвищення потенціалу основного блокчейну для обробки транзакцій. Основні методи включають:

- збільшення швидкості створення блоків: прискорення процесу додавання нових блоків дозволяє збільшити кількість оброблених транзакцій у певний часовий проміжок;
- збільшення розміру блоків: розширення блоків для зберігання більшої кількості даних та транзакцій збільшує загальну пропускну здатність мережі, дозволяючи обробляти більше транзакцій одночасно;
- зміна протоколу консенсусу: важливі зміни у способі досягнення консенсусу в мережі, як зміна з Proof of Work на Proof of Stake у Ethereum 2.0, можуть значно підвищити швидкість транзакцій, знизити витрати та додати нові функціональні можливості, наприклад стейкінг криптовалют;
- шардінг: розділення даних блокчейну на менші фрагменти або «шарди», кожен з яких може обробляти транзакції незалежно та паралельно, значно збільшує загальну пропускну здатність мережі.

Ці методи мають потенційні переваги, але також стикаються з викликами, такими як зростання вимог до обчислювальних ресурсів, що може призвести до збільшення централізації, або необхідність зміни інфраструктури, яка може зустріти опір від майнерів, не бажаючих інвестувати в додаткову потужність або компрометувати свої поточні доходи. Такі міркування підкреслюють складнощі та компроміси, пов’язані з впровадженням рішень масштабування блокчейну рівня 1 (рис. 2).

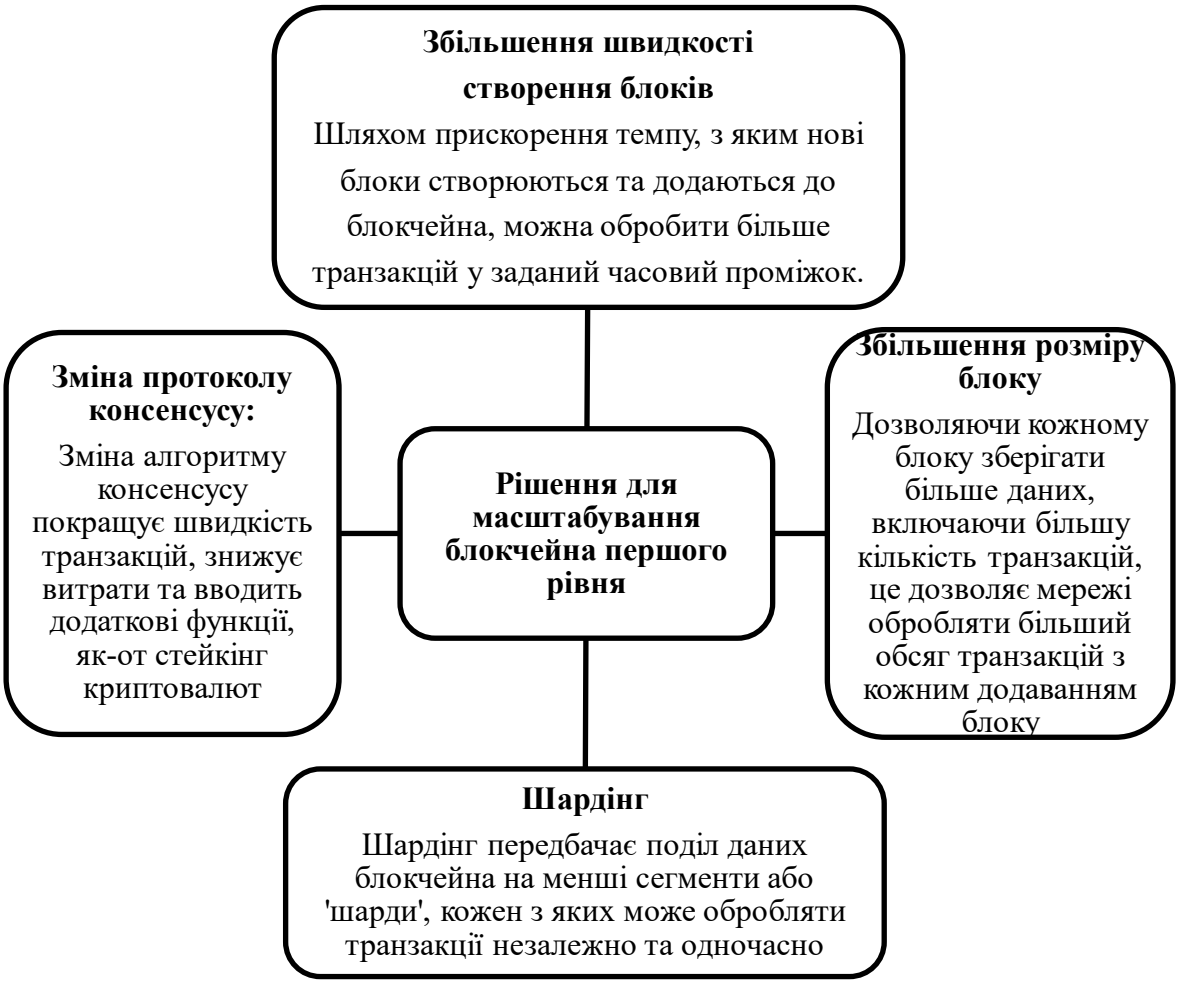

Рис. 2. Основні методи для вирішення масштабування блокчейну
Джерело: власні дослідження автора

Блокчейни рівня 2 розроблені як розширення блокчейнів рівня 1 для вирішення проблем масштабування. Їхньою основною метою є підвищення масштабованості рівня 1, зберігаючи при цьому його безпеку. Розміщуючись поверх мереж рівня 1, блокчейни рівня 2 оптимізують функціональність, знімаючи частину обробки транзакцій з основного ланцюга. Це знижує вартість транзакцій і підвищує пропускну спроможність, сприяючи швидшим та економічно ефективнішим транзакціям. Серед рішень рівня 2 відомі Lightning Network, Omni Layer, та Polygon, які забезпечують безпеку рівня 1 та високу ефективність обробки транзакцій.

Рішення масштабування блокчейну рівня 2 використовують різноманітні підходи для подолання викликів, пов'язаних з масштабуванням, працюючи поряд або незалежно від блокчейну рівня 1. Нижче представлено кілька прикладів таких рішень.

1. Державні канали (State Channels): Вони дозволяють здійснювати транзакції поза основним блокчейном, при цьому фінальне врегулювання відбувається в блокчейні. Наприклад, Bitcoin Lightning Network дозволяє учасникам проводити транзакції в межах каналу поза ланцюгом, що збільшує ємність транзакцій і прискорює процес.

2. Бічні ланцюги (Sidechains): Це незалежні блокчейни, які працюють

паралельно до основного блокчейну, дозволяючи безперешкодний переказ криптоактивів між двома ланцюгами, що знижує час обробки та вартість транзакцій.

3. Ролапи (Rollups): Ці системи групують багато транзакцій, виконаних поза ланцюгом, в одну транзакцію, яка реєструється на основному блокчейні. Оптимістичні ролапи і ZK-ролапи обробляють транзакції поза ланцюгом, перш ніж вони будуть подані на головний блокчейн.

4. Вкладені мережі (Nested Networks): Такі системи, як Polygon, діють в рамках ієрархічної структури блокчейнів, де Ethereum виступає як основний ланцюг рівня 1, а Polygon – як дочірній ланцюг рівня 2. Це забезпечує масштабованість та взаємодію, розширюючи можливості блокчейн-екосистеми.

Ці рішення мають істотні переваги, але також стикаються з викликами, такими як безпека через взаємодію мереж рівня 1 та 2, складність технічної реалізації, яка може бути складною для новачків і досвідчених користувачів, а також ризик централізації, якщо рішення рівня 2 не має достатньої децентралізації або контролюється обмеженою кількістю вузлів.

Рівень 3 у блокчейн-екосистемі визначається як шар застосунків. Це платформа, де розробляються та реалізуються децентралізовані застосунки (dApps), що використовують базову інфраструктуру, створену на мережах Рівнів 1 та 2. Цей шар відіграє важливу роль у втіленні технологій блокчейну в практичне використання через різноманітні додатки, які адресують специфічні потреби різних індустрій.

На Рівні 3 розроблені такі dApps, як децентралізовані біржі типу Uniswap і PancakeSwap, які дозволяють користувачам торгувати криптовалютами без залучення централізованих посередників. Також тут існують платформи для позик і кредитування, як Compound, що дозволяють користувачам безпосередньо позичати або кредитувати цифрові активи один одному.

Інші знакові випадки використання включають блокчейн-ETF (фонди, які торгуються на біржі), що забезпечують інвесторам доступ до диверсифікованих портфелів цифрових активів. Крім того, численні проєкти DeFi пропонують рішення для децентралізованих фінансів, такі як фармінг доходів, протоколи децентралізованого кредитування, і автоматизовані маркет-мейкери, які забезпечують динамічне ціноутворення в ринкових операціях.

Слід зазначити, що хоча розмежування шарів блокчейну допомагає зрозуміти різні компоненти та рішення, які використовуються для створення масштабованих та безпечних екосистем, категоризація шарів не є абсолютною і може варіюватися залежно від контексту.

Трилема блокчейну створює виклики у одночасному досягненні децентралізації, безпеки та масштабованості у мережах блокчейну. Зазвичай, необхідно пріоритизувати дві з цих функціональностей. Для оптимізації продуктивності та ємності застосовуються рішення рівня 0 та рівня 1, зберігаючи при цьому децентралізацію та безпеку. Рішення рівня 2, які базуються на рівні 1, покращують масштабованість.

Ролапи (Rollups) – це спосіб масштабування Ethereum, який передбачає виконання транзакцій поза основним блокчейном (рівень 1), але збереження даних транзакцій на ньому. Це дозволяє масштабувати мережу, зберігаючи при цьому безпеку, яка базується на консенсусі. Завдяки переносу обчислень та зберігання стану за межі основного ланцюга, ролапи зменшують обсяг даних, які потрібно обробляти та зберігати. Існує два основних типи ролапів: zero-knowledge rollups (ZK-Rollups) і optimistic rollups (ORs), що відрізняються способом верифікації транзакцій і розглядом спорів.

Zero-knowledge Rollups (ZK-rollups) використовують докази з нульовим розголошенням для верифікації транзакцій, що відбуваються поза основним блокчейном, гарантуючи їх відповідність стану в основному ланцюзі, не

розкриваючи при цьому жодної конфіденційної інформації. Наприклад, особа А може довести особі Б, що вона знає пароль до сайту, не повідомляючи про це. Виконання здійснюється за допомогою математичних операцій. Такі докази генеруються спеціалізованими вузлами, які називаються провайдерами, та перевіряються за допомогою смарт-контрактів на першому рівні блокчейну.

ZK-rollups мають кілька переваг:

1. Забезпечують миттєву фіналізацію транзакцій, оскільки вони підтверджуються відразу після перевірки доказу на Рівні 1.

2. Висока пропускна здатність, оскільки вони можуть обробляти тисячі транзакцій за секунду з мінімальними даними на блокчейні.

3. Низькі витрати, оскільки користувачі платять тільки за генерацію та перевірку доказів, що дешевше, ніж виконання транзакцій на Рівні 1.

4. Висока безпека, оскільки вони залежать від криптографії, а не від економічних стимулів чи припущень.

До прикладів проектів ZK-rollup відносяться:

- Loopring: децентралізований протокол обміну, який підтримує торгівлю, узгодження замовлень і платежі.

- zkSync: протокол платежів, що забезпечує швидкі та дешеві перекази.

- StarkWare: платформа, що надає рішення для масштабування та приватності, базуючись на ZK-rollups та інших техніках з нульовим розкриттям інформації.

Доказ з нульовим розкриттям – це спосіб доведення істинності твердження без розкриття будь-якої інформації про нього. Твердження може бути будь-яким, що піддається перевірці за допомогою обчислень, наприклад, «Я знаю рішення цієї головоломки» або «На моєму рахунку достатньо коштів».

Суть таких доказів полягає у можливості довести наявність інформації, не розкриваючи саму інформацію або будь-які додаткові дані. Доказ з нульовим розкриттям містить три компоненти: сторона, що доводить/наводить інформацію/дані; сторона, що перевіряє, та протокол, за яким вони діють.

Цей протокол повинен задовольняти трьом властивостям: повноті, надійності та нульовому розкриттю. Повнота гарантує, що якщо твердження істинне та обидві сторони дотримуються протоколу, перевіряюча сторона з високою ймовірністю приймає доказ. Надійність означає, що якщо твердження хибне, жоден нечесний, який доводить інформацію, не може переконати перевіряючого прийняти доказ. Нульове знання означає, що якщо твердження істинне, нечесний перевіряючий не дізнається нічого з доказу, крім того, що твердження правдиве.

Існують різні типи доказів з нульовим розкриттям, такі як інтерактивні та неінтерактивні, статистичні та обчислювальні, короткі та не дуже. Вони відрізняються тим, як вони досягають цих властивостей та які компроміси вони включають.

Один з найпоширеніших та інтуїтивно зрозумілих типів доказів з нульовим розкриттям – це інтерактивні докази з нульовим розкриттям. Вони вимагають взаємодії між обидвома сторонами, зазвичай у вигляді кількох раундів спілкування. У кожному раунді той, хто доводить, відправляє деяку інформацію тому, хто перевіряє, а перевіряючий відправляє назад у запит. Після цього той, хто доводить, відповідає на виклик, а перевіряючий вирішує, чи приймати або відхиляти доказ.

Для ілюстрації базової ідеї інтерактивних доказів з нульовим розкриттям візьмемо приклад, наведений Цемом Дільмегані: одна сторона – той, хто доводить, друга сторона – той, хто перевіряє, який страждає на кольорову сліпоту і не може відрізнити зелений м’яч від червоного (не має знань про те, чи відрізняються кольори м’ячів). Потрібно довести, що кольори м’ячів різні, але другій стороні потрібно більше, ніж просто слова, щоб переконатися в цьому (Dilmegani, 2023).

Метод доказу з нульовим розкриттям для цієї проблеми виглядав би так:

1. Перевіряючий бере два м’ячі та показує тому, хто доводить, який м’яч знаходиться в якій руці.

2. Далі ховаються м’ячі за спиною, де можна їх поміняти місцями або залишити на місці.

3. Далі демонструються м’ячі і дається запит, чи змінились вони місцями.

4. Оскільки той, хто доводить, може відрізнити зелений м’яч від червоного, він легко дає правильну відповідь.

5. Перевіряючий не переконаний, оскільки у того, хто доводить, було 50% шансів вгадати, чи змінилися місцями м’ячі, і м’ячі можуть бути одного кольору.

6. Однак, якщо цей процес повторити кілька разів, імовірність того, що той, хто доводить, постійно вгадує, чи змінювались м’ячі, буде дуже низькою. Це дозволяє перевіряючому перевірити, що м’ячі різних кольорів, не знаючи їхніх реальних кольорів.

Цей приклад задовольняє три властивості доказів з нульовим розкриттям:

- повнота: якщо той, хто доводить, дійсно знає кольори м’ячів, він завжди дає правильні відповіді та переконує перевіряючого з високою ймовірністю;

- надійність: якщо той, хто доводить, не знає кольори м’ячів, він можете лише здогадуватися, і перевіряючий з високою ймовірністю відхилить доказ;

- нульове знання: перевіряючий не дізнається нічого про кольори м’ячів з наданих відповідей.

У реальних застосуваннях докази з нульовим розкриттям використовують складні математичні техніки та алгоритми для генерації та верифікації доказів. Наприклад, докази, що використовують евристику Фіата-Шаміра для перетворення інтерактивних доказів з нульовим розкриттям у неінтерактивні за допомогою хеш-функцій як джерела випадковості, а також zk-SNARKs та zk-STARKs.

Optimistic Rollups (ORs) використовують альтернативний метод для верифікації транзакцій, які відбуваються поза основним ланцюгом. На відміну від криптографічних доказів, вони застосовують систему стимулів та штрафів для забезпечення чесності та безпеки.

У оптимістичних ролапах транзакції виконуються спеціальними вузлами, званими секвенсерами, які згруповують їх у пакети і відправляють до рівня 1. Ці пакети приймаються за дійсні за замовчуванням, доки їх не оскаржать протягом певного часу.

Будь-хто може оскаржити пакет, надавши докази того, що він містить недійсні або шахрайські транзакції. Ці докази називаються доказами шахрайства. Якщо оскарження вдається, пакет відхиляється, а секвенсер отримує штраф. Якщо оскарження не надходить протягом встановленого терміну, пакет приймається та фіксується.

Оптимістичні ролапи мають декілька переваг:

1. Вони сумісні з існуючими смарт-контрактами Ethereum, оскільки використовують ту ж віртуальну машину та мови програмування, що і рівень 1.

2. Вони мають високу пропускну здатність, оскільки можуть обробляти тисячі транзакцій на секунду з мінімальними даними на блокчейні.

3. Вони мають низькі витрати, оскільки користувачі платять тільки за виконання та відправлення транзакцій, що дешевше, ніж виконання транзакцій на рівні 1.

Деякі приклади проектів оптимістичних ролапів:

- Optimism: платформа, яка дозволяє масштабувати та забезпечувати взаємодію смарт-контрактів на ORs.

- Arbitrum: платформа, яка забезпечує рішення для масштабування, конфіденційності та взаємодії на базі ORs.

- Fuel: протокол оплати, який дозволяє здійснювати швидкі та дешеві перекази на ORs.

Секвенсер – це вузол, що збирає, упорядковує та виконує транзакції поза основним ланцюгом, а потім подає пакети транзакцій до першого рівня як вхідні дані (calldata).

Верифікатор – це вузол, який слідкує за роботою ролапа і перевіряє правильність

транзакцій. Верифікатор має можливість оскаржувати будь-який пакет, що містить недійсні або шахрайські транзакції, надаючи докази шахрайства на першому рівні.

Доказ шахрайства – це доказ, який показує, як транзакція була виконана неправильно або нечесно секвенсером. Такий доказ може створити будь-хто, хто може запустити віртуальну машину ролапа і порівняти результати з виводом секвенсера. Велика кількість компаній використовує проактивний моніторинг/аналіз даних, невід'ємною частиною якого є технологія блокчейн (Мігус, 2022).

Період виклику – це часове вікно після подання пакета на перший рівень, протягом якого будь-хто може подати доказ шахрайства для оскарження пакету. Тривалість періоду виклику може варіюватися в залежності від конструкції і припущень безпеки ролапа.

Контракт ролапа – це смарт-контракт, розгорнутий на першому рівні, який керує депозитами, виведеннями коштів, викликами і нагородами ролапа. Контракт також зберігає кореневий стан ролапа.

Основний робочий процес оптимістик ролапа виглядає так:

1. Користувач вносить кошти в контракт ролапа на першому рівні, щоб отримати еквівалентну суму на ролапі.

2. Користувач підписує транзакцію і відправляє її секвенсеру. Секвенсер перевіряє транзакцію і додає її до черги.

3. Секвенсер періодично збирає транзакції з черги та виконує їх поза ланцюгом. Він також генерує кореневий стан, який представляє оновлений стан ролапа після виконання транзакцій.

4. Секвенсер подає пакет транзакцій і кореневий стан на перший рівень як вхідні дані. Пакет вважається дійсним, якщо протягом періоду виклику його не оскаржено.

5. Верифікатор моніторить ролап і перевіряє кожен пакет на валідність. Якщо верифікатор виявляє недійсну або шахрайську транзакцію, він створює доказ шахрайства і подає його на перший рівень протягом періоду виклику. Контракт ролапа перевіряє доказ шахрайства і визначає, чи приймати або відхилити пакет. Якщо доказ визнаний дійсним, пакет відхиляється і секвенсер штрафується. Якщо доказ шахрайства недійсний або не подано вчасно, пакет приймається і фіналізується. Користувачі можуть знімати кошти, відправляючи транзакції на виведення секвенсеру, який включає їх у пакет і подає на перший рівень.

Оптимістичні ролапи мають ряд компромісів і ризиків, про які користувачам варто знати перед використанням. Зокрема, вони вводять затримки у фіналізації і виведенні коштів, оскільки користувачам доводиться чекати закінчення періоду виклику. Вони залежать від економічних стимулів і припущень, вимагаючи від користувачів довіряти чесності секвенсера і достатності верифікаторів. Також потрібна додаткова інфраструктура і координація, оскільки користувачам потрібно взаємодіяти з секвенсером та контрактом ролапа, а іноді й використовувати власних верифікаторів або послуги третіх сторін.

ZK-ролапи та оптимістичні ролапи (ORs) обидва є видами ролапів, які мають на меті масштабування Ethereum шляхом виконання транзакцій поза ланцюгом, але з розміщенням даних транзакцій у ланцюгу. Однак, вони пропонують різні переваги та недоліки, що робить їх більш або менш підходящими для різних варіантів використання та уподобань.

У таблиці 1 зроблено узагальнення деяких з основних відмінностей між ZK-ролапами та оптимістичними ролапами.

Таблиця 1. Порівняння основних відмінностей між оптимістичними ролапами та ролапами з нульовим розкриттям

Особливість	Ролапи	
	Оптимістичні	З нульовим розкриттям
Верифікація	Економічні стимули	Криптографічні докази
Завершеність	Відкладена	Миттєва
Пропускна здатність	Висока	Висока
Комісії	Низькі	Низькі
Безпека	Середня	Висока
Компактність	Висока	Низька

Джерело: власні дослідження автора

ZK-ролапи забезпечують миттєву фінальність, високу безпеку та низькі витрати, але вони потребують складнішої та спеціалізованої криптографії і є менш сумісними з існуючими смарт-контрактами Ethereum.

Оптимістичні ролапи пропонують високу сумісність, високу пропускну здатність і низькі витрати, але вони вводять затримки у фінальності та виведенні коштів, залежать від економічних стимулів та припущень і потребують додаткової інфраструктури та координації.

Залежно від конкретних потреб та уподобань користувачів і розробників, вони можуть вибирати тип ролапу, який найкраще підходить для їх випадку використання. Наприклад, ZK-ролапи можуть бути більш підходящими для застосувань, що вимагають швидких і безпечних транзакцій, таких як платежі або обміни. Оптимістичні ролапи можуть бути більш підходящими для застосувань, які потребують високої сумісності та гнучкості, наприклад, для ігор або соціальних мереж.

Оцінка перспектив подальших досліджень в управлінському контексті виявляє ключові напрямки для розвитку цієї тематики. Одним із пріоритетних напрямів є вивчення можливостей смарт-контрактів та ролапів для оптимізації внутрішніх бізнес-процесів і покращення прийняття стратегічних рішень як компаній, так і держав у цілому. Це може включати розробку методики для аналізу впливу цих технологій на продуктивність, гнучкість та інноваційність компаній. Крім того, існує потреба у дослідженнях впливу впровадження цих технологій на корпоративну культуру і лідерство. Також важливою є розробка рамок для оцінювання ризиків і безпеки при використанні смарт-контрактів і ролапів у бізнес-управлінні. Окрім того, зростає потреба в ідентифікації і мінімізації етичних дилем, що можуть виникнути при широкомасштабному впровадженні таких інновацій.

Висновки. Ролапи в управлінській діяльності є потужним і перспективним рішенням для масштабування використання смарт-контрактів у процесах управління бізнесом, яке може значно покращити продуктивність і зручність використання. Виконуючи транзакції поза ланцюгом, але публікуючи дані транзакцій у ланцюгу, ролапи можуть збільшити швидкість транзакцій, пропускну здатність і безпеку, одночасно знижуючи витрати на транзакції та перевантаження.

Залежно від їхнього дизайну та реалізації, ролапи також можуть пропонувати різні компроміси та особливості, такі як миттєва завершеність, сумісність зі смарт-контрактами або конфіденційність. Ролапи вже використовуються різними проєктами та застосунками на Ethereum і, як очікується, відіграватимуть ключову роль у майбутньому оптимізації бізнес-процесів у блокчейн мережах.

Література:

1. Auer, R., Monnet, C., & Shin, H. S. (2021, October). Distributed ledgers and the governance of money. *BIS Working Papers, 924.* Bank for International Settlements. Retrieved from: https://www.bis.org/publ/work924.htm

2. Buterin, V. (2021, April 7). Why sharding is great: Demystifying the technical properties. Retrieved from: https://vitalik.ca/general/2021/04/07/sharding.html

3. Dilmegani, C. (2023, December 21). Zero-Knowledge proofs: How it works & use cases in 2024. *AIMultiple*. Retrieved from: https://research.aimultiple.com/zero-knowledge-proofs

4. FHE-Rollups: Scaling confidential smart contracts on Ethereum and beyond. (n.d.). Retrieved from: https://www.fhenix.io/fhe-rollups-scaling-confidential-smart-contracts-on-ethereum-and-beyond-whitepaper

5. Gemini. (n.d.). Blockchain scalability and privacy: The rollup ecosystem. Retrieved from: https://www.gemini.com/cryptopedia/layer-2-scaling-zk-rollup-optimistic-rollup-ethereum

6. Jeong, H., & Lee, H. (2023). Efficiency-improved inter-rollup transfer system leveraging batch settlement methods. *Radius Lab and Seoul National University*. Retrieved from: https://ar5iv.labs.arxiv.org/html/2305.19514

7. Ledger Academy. (2023, July 18). Transactions per second (TPS) meaning. Retrieved from: https://www.ledger.com/academy/glossary/transactions-per-second-tps

8. Мігус, І. (2022). Можливості використання технологій блокчейну для захисту від шахрайства. *Вчені записки Університету «КРОК», 1*(65), 84-94. DOI: https://doi.org/10.31732/2663-2209-2022-65-84-94

9. Пилипченко, О.І, Кузьмінський, В.З. & Чумаченко, О.О. (2021). Використання методів технічного аналізу для прогнозування ринку криптовалют. *Вчені записки Університету «КРОК»*, *4*(64), 28-35. DOI: https://doi.org/10.31732/2663-2209-2021-64-28-35

10. Polishchuk, Y., Ivashchenko, A., & Dyba, O. (2019). SMART-Contracts via Blockchain as the Innovation Tool for SMEs Development. *Economic Studies journal, 6,* 39-53. Retrieved from: https://www.ceeol.com/search/article-detail?id=831391

11. Rumyk, I., Kuzminsky, V., Pylypenko, O., & Yaroshenko, O. (2024). Precious metals market forecasting in the current environment. *Economics, Finance and Management Review, 1*(17), 45-56. DOI: https://doi.org/10.36690/2674-5208-2024-1-45

12. Румик, І., & Ковальчук, Ю. (2024). Управління фінансами та процесами з використанням криптовалютних технологій. *Вчені записки Університету «КРОК»*, *2*(74), 11-21. DOI: https://doi.org/10.31732/2663-2209-2024-74-11-21

13. Smart Contract Research Forum. (n.d.). Research summary: Arbitrum: Fast, scalable, private smart contracts. Retrieved from https://www.smartcontractresearch.org/t/research-summary-arbitrum-fast-scalable-private-smart-contracts/885

14. The FinReg Blog. (2023, February 3). Using layer-2 technologies to improve smart contract scalability. Duke University. Retrieved from: https://sites.duke.edu/thefinregblog/2023/02/03/using-layer-2-technologies-to-improve-smart-contract-scalability

15. Чіков І.А., Коляденко С.В., Суприган В.А., Табенська О.І., Ніценко В.С., Голінько О.В. (2023). Смарт-контракти та автоматизація бізнес-процесів: технічний аспект. *Науковий вісник Вінницького національного аграрного університету, 5*(197), 186-197. DOI: https://doi.org/10.33271/nvngu/2023-5/186

16. Yatsenko, V. V., Kovalov, B. L., Kubatko, O. V., Kharchenko, M. O., Mazin, Yu. O., & Piven, V. S. (2022). Smart contract in banking for Ukraine's economy digitalization. *Вісник СумДУ. Серія «Економіка», 2,* 92-97. DOI: https://doi.org/10.21272/1817-9215.2022.2-10