DOI: https://doi.org/10.32782/2524-0072/2025-71-167

УДК 005.7:658.7

СТВОРЕННЯ РОЗПОДІЛЕНОЇ МОДЕЛІ УПРАВЛІННЯ ЛАНЦЮГАМИ ПОСТАЧАННЯ ІЗ ЗАСТОСУВАННЯМ ZK-ROLLUPS ДЛЯ ПІДВИЩЕННЯ МАСШТАБОВАНОСТІ ТА ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ

DEVELOPMENT OF A DISTRIBUTED SUPPLY CHAIN MANAGEMENT MODEL USING ZK-ROLLUPS TO ENHANCE SCALABILITY AND DATA PRIVACY

Кузяк Вікторія Вікторівна
кандидат економічних наук, доцент кафедри маркетингу і логістики,
Інститут економіки і менеджменту
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0000-0003-4183-117X

Заторський Данило Богданович
аспірант,
Інститут економіки і менеджменту
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0009-0000-7716-5522

Kuziak Viktoria, Zatorskyi Danylo
Institute of Economics and Management of Lviv Polytechnic National University

Стаття присвячується розробці розподіленої моделі управління ланцюгами поставок із використанням ZK-Rollups для підвищення масштабованості та захисту конфіденційних даних. Дослідження зосереджене на оптимізації логістичних процесів, де ключовими є прозорість, ефективність і безпека. Аналіз блокчейн-рішень у логістиці демонструє потенціал ZK-Rollups у створенні масштабованих мереж, що обробляють великі обсяги транзакцій без розкриття конфіденційної інформації. Особливу увагу приділено механізму «згортання» транзакцій, що знижує витрати й підвищує пропускну здатність, а також ролі приватних смарт-контрактів у збереженні комерційної таємниці. Практичний внесок полягає в рекомендаціях щодо впровадження цього підходу для підвищення прозорості та безпеки ланцюгів постачання. Висновки вказують на перспективність комбінування публічних і приватних реєстрів та важливість стандартів для глобального масштабування.

Ключові слова: децентралізовані системи, ZK-Rollups, масштабованість, захист даних, логістика, блокчейн, смарт-контракти.

The article is dedicated to the development and justification of a distributed supply chain management model using ZK-Rollups technology, aimed at enhancing system scalability and ensuring the protection of confidential data. The relevance of the topic is driven by the need to optimize logistics processes in multi-level supply networks, where transparency, efficiency, and security of interactions between participants are of critical importance. The research methodology includes a comprehensive analysis of blockchain solutions in the logistics sector, as well as an in-depth study of decentralized mechanisms for ensuring data privacy. The findings highlight the potential of ZK-Rollups in creating highly scalable decentralized networks capable of processing large transaction volumes without revealing confidential information. Special attention is given to the transaction "roll-up" mechanism, which reduces computational costs and fees while maintaining high throughput. The practical contribution of the study lies in recommendations for implementing this approach in enterprises seeking to enhance supply chain transparency and minimize fraud risks and behaviour. The practical value of the results is significant for logistics managers and IT specialists searching for new ways to ensure seamless and secure interactions in supply chains. The developed model provides a strategic vision for the application of decentralized solutions, particularly blockchain technology and ZK-Rollups, to optimize costs, accelerate processes, and mitigate operational and other risks. The research findings indicate the prospects of combining public and private ledgers to maintain an innovative balance between transparency and confidentiality while emphasizing the importance of standards and regulatory frameworks for

global scalability. The generalized recommendations for integrating ZK-Rollups and decentralized management principles may serve as a foundation for building sustainable logistics ecosystems and enhancing competitiveness in rapidly changing market conditions.

Keywords: decentralized systems, ZK-Rollups, scalability, data protection, logistics, blockchain, smart contracts.

Постановка проблеми. Стрімке зростання глобальної торгівлі та конкуренції вимагає нових підходів до управління ланцюгами постачання. Традиційні централізовані логістичні системи часто не здатні оперативно реагувати на ринкові зміни, стикаючись із проблемами прозорості, захисту даних та ефективності. Однією з ключових проблем є недостатній рівень довіри між учасниками ринку та відсутність єдиного джерела правдивих даних, що призводить до бюрократії, дублювання інформації та ризику маніпуляцій. Це ускладнює оформлення угод, підвищує витрати та створює загрози шахрайства.

Окрім того, централізовані логістичні системи вразливі до кібератак. У 2021 році кількість атак на ланцюги постачання зросла у 4 рази [1]. Прикладом є атака вірусу NotPetya у 2017 році, яка вивела з ладу IT-системи Maersk, спричинивши значні збитки [2]. Середні фінансові втрати від витоку даних оцінюються у $4,35 млн, а усунення наслідків триває до 277 днів [3].

Ще однією проблемою є обмежений доступ малого бізнесу до сучасних логістичних і фінансових послуг, що ускладнює їхню інтеграцію в глобальну економіку [4].

Блокчейн-технології можуть вирішити ці проблеми завдяки децентралізації, прозорому механізму перевірки транзакцій та криптографічному захисту даних. Відсутність єдиного контролюючого центру знижує ризик маніпуляцій, а незмінність записів у розподіленому реєстрі сприяє довірі між учасниками.

Таким чином, впровадження блокчейну в логістику може зробити управління ланцюгами постачання більш прозорим, безпечним та ефективним. Подальші дослідження масштабування блокчейну та забезпечення конфіденційності є критично важливими для розвитку інноваційних бізнес-моделей та глобальної конкурентоспроможності.

Аналіз останніх досліджень і публікацій. У сфері блокчейну дедалі більше уваги приділяється питанням масштабованості, безпеки та збереження конфіденційності даних, особливо в галузі управління ланцюгами поставок. При цьому дослідники зосереджуються на різних аспектах упровадження, залежно від специфіки використання технології та пріоритетів конкретних секторів економіки.

У низці робіт, зокрема в дослідженні Deloitte (2020), підкреслюється вплив блокчейн-технологій на прозорість логістичних процесів та покращення співпраці між партнерами. Автори зазначають, що блокчейн дозволяє уникати дублювання даних у централізованих базах і знижує ризики шахрайства, забезпечуючи більшу довіру між сторонами. Водночас у звіті наголошується на технічних викликах, таких як швидкість обробки транзакцій та їх масштабованість. Хоча ZK-Rollups згадуються як потенційний інструмент вирішення цих проблем, дослідження не пропонує детального аналізу їхньої реалізації в логістичних системах [5].

У своїй статті "An Incomplete Guide to Rollups" Віталік Бутерін описує ролапи як перспективний підхід до масштабування блокчейн-систем, який може стати ключовим для Ethereum у найближчому майбутньому. Ролапи дозволяють виконувати транзакції поза основним ланцюгом (Layer 1), зберігаючи при цьому дані транзакцій на ньому, що забезпечує безпеку та зменшує навантаження на мережу. Це досягається шляхом компресії даних та використання доказів з нульовим розголошенням (Zero-Knowledge Proofs), що дозволяє значно підвищити пропускну здатність без компромісів у безпеці [6].

Chang у своїй статті про гібридні блокчейн-рішення наголошує на поєднанні публічних і приватних реєстрів, що дозволяє застосовувати децентралізовані технології в тих ланцюгах, де чутливі дані вимагають додаткового захисту [7]. Автор робить висновок про ефективність такого підходу на локальних прикладах, але питання інтеграції Rollups як конкретного механізму масштабованості й конфіденційності лишається поза увагою, що відкриває простір для поглибленого аналізу.

Загалом результати наведених публікацій свідчать, що сфера блокчейну в логістиці і, зокрема, застосування ZK-Rollups для підвищення продуктивності та безпеки мережі, має значний потенціал. Проте жодне з досліджень не пропонує комплексного розгляду проблеми створення розподіленої моделі управління ланцюгами поставок з урахуван-

ням економічних, технічних і регуляторних чинників, а також особливостей масштабного впровадження. Цим і зумовлена необхідність глибшого аналізу та розробки власної моделі, яка б враховувала різноманітність учасників логістичного процесу, специфіку захисту даних і можливості масштабування на базі технології ZK-Rollups.

Постановка завдання. Метою даної статті є розробка розподіленої моделі управління ланцюгами поставок на основі технології ZK-Rollups, яка покликана підвищити масштабованість та захист конфіденційних даних у логістичних процесах. Зокрема, у межах дослідження передбачено порівняти децентралізовані блокчейн-рішення із традиційними централізованими логістичними системами, визначити переваги й обмеження кожного підходу, а також проаналізувати ключові виклики, пов'язані з інтеграцією ZK-Rollups у сфері ланцюгів постачання, включно з технологічними й регуляторними аспектами.

Виклад основного матеріалу дослідження. Управління ланцюгами постачання стає дедалі складнішим через зростаючу глобалізацію, вимоги до прозорості й швидкості взаємодії між учасниками. Традиційні централізовані системи управління часто стикаються з обмеженнями, такими як відсутність довіри між сторонами, затримки у виконанні транзакцій та ризики шахрайства. У відповідь на ці виклики блокчейн-технології пропонують революційний підхід, базуючись на розподіленій природі даних і смарт-контрактах, які автоматизують бізнес-процеси.

Блокчейн технологія забезпечує цілісність даних за допомогою криптографічних хеш-функцій. Кожен блок у ланцюгу містить хеш попереднього блоку, що створює взаємозв'язок між усіма блоками в ланцюгу. Таким чином, функція, що забезпечує цілісність усього ланцюга може бути описана як:

$$B_i = \{H(B_{i-1}), T_i, H(T_i)\}$$

де: B_i — поточний блок у ланцюгу (з індексом і).

$H(B_{i-1})$ — хеш попереднього блоку B_{i-1}. Цей елемент зв'язує поточний блок із попереднім, формуючи ланцюг.

T_i — набір транзакцій, що містяться в блоці.

$H(T_i)$ — хеш усіх транзакцій у блоці, який гарантує, що дані всередині блоку неможливо змінити.

Смарт-контракти є невід'ємною складовою сучасних блокчейн систем і являють собою програмний код, який автоматично виконує умови договору, закладені в ньому. Він зберігається та виконується на блокчейні, забезпечуючи прозорість, незмінність та безпеку транзакцій оскільки в його основі лежать принципи забезпечення цілісності даних описана вище.

Використання смарт-контрактів у ланцюгах постачання забезпечує:

– Прозорість даних. Смарт-контракти забезпечують доступність даних для всіх учасників ланцюга постачання, що підвищує довіру між сторонами та мінімізує ризик шахрайства.

– Автоматизація процесів. Виконання умов контракту відбувається автоматично при виконанні заздалегідь визначених умов, що знижує потребу у ручній роботі та людському втручанні.

– Зменшення витрат. Автоматизація процесів скорочує витрати на посередників і адміністративні процедури.

– Покращення безпеки. Дані, що зберігаються на блокчейні, захищені від змін, забезпечуючи високий рівень безпеки та недоторканності інформації.

– Підвищення точності даних. Відсутність посередників та автоматизація зменшують ризик помилок при обробці даних.

– Гнучкість управління контрактами. Смарт-контракти дозволяють створювати складні умови, адаптовані до специфіки лан-

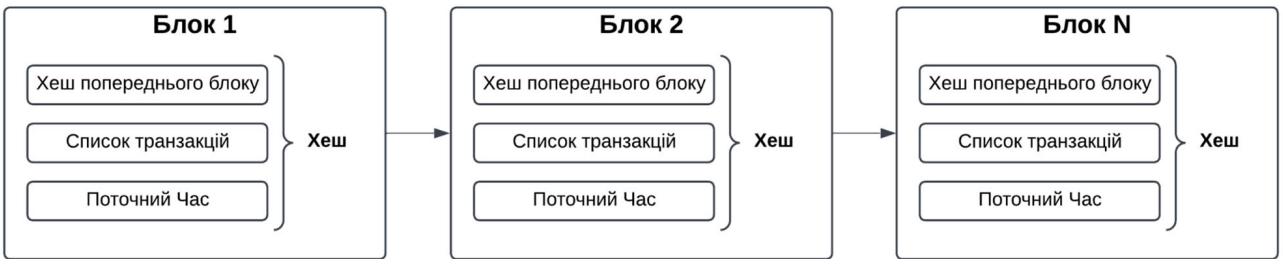

Рис. 1. Принцип забезпечення цілісності блокчейну

Джерело: сформовано авторами

цюга постачання, включаючи багатосторонні угоди.

– Можливість аудиту. Усі транзакції фіксуються на блокчейні, їх неможливо змінити і вони являються публічними, а отже кожен може проаналізувати дані про ланцюг постачання без сторонньої допомоги.

– Стійкість до збоїв. Децентралізована природа блокчейна забезпечує стабільність системи навіть у разі виходу з ладу окремих елементів мережі.

Попри велику кількість переваг виконання програмного коду у мережі блокчейн через смарт-контракти несе за собою чимало викликів, серед яких можна виділити наступні:

– Обмежена масштабованість. Блокчейни, що використовуються для смарт-контрактів, часто мають низьку пропускну здатність, що призводить до затримок у виконанні транзакцій, особливо при високому навантаженні.

– Високі комісії за транзакції. Збільшення попиту на транзакції в блокчейні, особливо на публічних мережах, таких як Ethereum, призводить до значного зростання вартості комісій (gas fees), що ускладнює економічну доцільність використання смарт-контрактів у масштабних логістичних системах.

– Обмеження конфіденційності даних. Дані про транзакції та учасників, записані в блокчейні, доступні для перегляду усіма учасниками мережі, що може створювати ризики для конфіденційної комерційної інформації.

– Відсутність гнучкого підходу до обробки великої кількості транзакцій. У поточних системах важко одночасно обробляти велику кількість взаємодій між учасниками ланцюга постачання, що обмежує їх ефективність у складних логістичних мережах.

Нижче подано орієнтовну модель розподіленої системи управління ланцюгами постачання (ЛП) із застосуванням ZK-Rollups, яка спрямована на підвищення масштабованості та захисту конфіденційних даних. Модель поєднує публічний (або приватний) блокчейн, off-chain інфраструктуру ZK-Rollups та спеціальні криптографічні механізми задля безпечної і ефективної обробки великого обсягу транзакцій.

Модель виокремлює наступних учасників системи:

– Постачальники (Suppliers) – забезпечують вхідні ресурси та оприлюднюють дані про обсяги поставок.

– Виробники (Manufacturers) – перетворюють сировину та комплектуючі в готові товари.

– Дистриб'ютори (Distributors) – займаються транспортуванням та зберіганням продукції.

– Роздрібні мережі (Retailers) – реалізують товари кінцевим споживачам.

– ZK-агрегатор (Rollup Operator) – офчейн-компонента, що обробляє транзакції, формує ZK-докази та передає їх на блокчейн.

– Блокчейн-мережа (On-chain layer) – основний ланцюг для верифікації доказів та фінальної фіксації транзакцій.

Учасники ланцюга постачання формують транзакції (наприклад, надсилають дані про відвантаження чи оплату) та надсилають їх до ZK-агрегатора.

ZK-агрегатор приймає транзакції, обробляє їх у пакет (batch), генерує криптографічний доказ (ZK-proof), що підтверджує коректність здійснених змін стану, і відправляє цей доказ разом з оновленим коренем стану (state root) до блокчейна.

Блокчейн зберігає мінімальну необхідну інформацію (корінь нового стану, сам доказ і, за потреби, підтвердження валідності від смарт-контракту). Учасники можуть перевіряти актуальний стан системи або вимагати деталі транзакцій, але при цьому конфіденційні дані лишаються захищеними за рахунок Zero-Knowledge механізмів.

Таким чином можна виділити наступні етапи обробки транзакцій з використанням ZK-Rollups:

– Створення транзакцій: Кожен учасник формує транзакцію (наприклад, запис про зміну кількості товару на складі, оплату, відправлення вантажу тощо) та надсилає її до ZK-агрегатора.

– Пакетування та формування доказу: ZK-агрегатор об'єднує транзакції в один блок (batch), оновлює локальний стан системи (наприклад, структуру на основі дерев Меркла) і генерує криптографічний доказ нульового розголошення (Zero-Knowledge Proof), який підтверджує коректність усіх транзакцій без розкриття конфіденційних деталей.

– Верифікація та фіксація: Смарт-контракт у блокчейні отримує від агрегатора пакет із доказом. Якщо доказ валідний, новий корінь стану (state root) та відповідна мінімальна інформація про зміни фіксуються у блокчейні.

Рис. 2. Візуалізація етапів обробки транзакцій з використанням ZK-Rollups

Джерело: сформовано авторами

Для опису переходу системи зі стану S_i у стан S_{i+1} під дією набору транзакцій $\{Tx_j\}$ запишемо:

$$S_{i+1} = f(S_i, \{Tx_j\})$$

де

$f(\cdot)$ – функція переходу стану (наприклад, оновлення записів про залишки товарів, відомостей про відвантаження та ін.).

ZK-агрегатор формує доказ π, який містить інформацію про правильність застосування кожної транзакції до поточного стану:

$$\pi = \text{GenProof}(S_i, S_{i+1}, \{Tx_j\})$$

Смарт-контракт на блокчейні виконує перевірку за допомогою функції верифікації:

$$\text{Verify}(\pi, S_i, S_{i+1}) \rightarrow \{\text{True, False}\}$$

Якшо Verify(π) = True, тоді новий стан S_{i+1} вважається дійсним і фіксується в блокчейні.

У даному підході захист конфіденційних даних забезпечується за допомогою наступних механізмів:

– Zero-Knowledge Proofs [8]. Дозволяють перевірити валідність транзакцій без розкриття повних даних. Учасники ланцюга постачання бачать лише «доказ коректності», тоді як деталі (кількість товару, ціни, умови контрактів) лишаються прихованими.

– Шифрування off-chain даних: Учасники зберігають деталі угод в зашифрованому вигляді; доступ до розшифровки мають лише ті сторони, які безпосередньо залучені в операцію.

Маскування ідентифікаторів: У транзакціях можуть використовуватись псевдоніми чи хеші, щоб унеможливити просту ідентифікацію сторін третіми особами.

Для оцінки ефективності масштабованості системи можемо використати наступну формулу:

$$TPS_{zk} = \frac{N}{t}$$

де:

TPS_{zk} – кількість транзакцій за секунду у системі ZK-Rollups;

N – кількість транзакцій, об'єднаних в один пакет (batch);

t – час (у секундах), необхідний для формування пакету і генерування відповідного ZK-доказу.

У традиційній ончейн-системі (без ZK-Rollups) $TPS_{onchain}$ зазвичай значно нижча, оскільки кожна транзакція пишеться до блоку окремо, відповідно N завжди рівне 1. Як результат, ефективність традиційних блок-

чейн систем на менше ніж систем які використовують ZK-Rollups. Єдине виключення із правил, коли в ZK-Rollup батч записується лише одна транзація що на практиці зустрічається вкрай рідко, а отже, справедливим буде формула:

$$TPS_{onchain} \ll TPS_{zk}$$

Підхід із застосуванням ZK-Proofs для управління ланцюгами постачання на основі технології блокчейн допомагає вирішити наступні проблеми традиційних децентралізованих підходів з використанням блокчейн технологій:

– Завдяки ZK-Rollups велика кількість транзакцій обробляється off-chain, а в блокчейн надсилається лише зведена інформація та доказ. Це суттєво збільшує пропускну здатність системи.

– Об'єднання багатьох транзакцій у один блок суттєво скорочує загальні витрати на блокчейн-комісії, адже плата сплачується переважно за зберігання (і верифікацію) одного ZK-доказу.

– Завдяки Zero-Knowledge Proofs комерційно чутливі дані (обсяги, ціни тощо) не розголошуються іншим учасникам або стороннім спостерігачам, залишаючись доступними лише для вузького кола уповноважених.

– Обробка транзакцій поза основним ланцюгом підвищує загальну пропускну здатність, скорочує затримку підтвердження та прискорює ланцюгові операції.

– Незважаючи на прихованість деталей, кожен транзакційний пакет має криптографічний доказ коректності. Це дає можливість проводити аудит операцій без розкриття повних даних про них.

Висновки. Запропонована модель управління ланцюгами постачання із використанням ZK-Rollups поєднує сильні сторони децентралізованого зберігання даних з можливістю масштабування та захисту конфіденційної інформації. Завдяки механізмам нульового розголошення, система дозволяє автоматизувати контроль за виконанням смарт-контрактів без необхідності публікувати всю комерційно чутливу інформацію, що робить її привабливою для компаній, яким важлива як прозорість, так і комерційна таємниця. При цьому транзакційні витрати суттєво знижуються, оскільки одночасно обробляється великий обсяг операцій, а до основного блокчейну передається лише підтвердження їхньої коректності у вигляді ZK-доказу.

Компанії, що інтегрують таку модель, отримують можливість не лише прискорення логістичних процесів та зменшення операційних ризиків, а й нові інструменти для гнучкого управління взаємодією між усіма учасниками ланцюга постачання. Завдяки масштабуванню та децентралізації підвищується стійкість системи до збоїв, а прозорість механізмів обліку й аудиту дозволяє налаштовувати процеси чіткіше і швидше приймати рішення на основі актуальних даних. Усе це сприяє підвищенню рівня довіри всередині логістичної мережі та створює умови для появи додаткових сервісів на основі смарт-контрактів, наприклад, програм страхування вантажів чи платіжних послуг, здатних діяти в реальному часі без затримок з боку посередників.

Таким чином, запропонований підхід долає основні обмеження традиційних блокчейн-рішень, посилюючи їхню привабливість для корпоративного використання, де необхідні висока швидкість обробки, надійне зберігання даних та суворе дотримання конфіденційності. Використання ZK-Rollups у логістиці відкриває перспективи значної оптимізації ланцюгів постачання, зокрема прискорення товарообігу, зниження транзакційних витрат і підвищення рівня взаємної довіри між партнерами, що робить цей підхід конкурентною перевагою для сучасних інноваційних підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. ENISA. Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity, 2021, с. 22. URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (дата звернення: 28.01.2025).

2. Financial Times. How NotPetya Cyber Attack Devastated Maersk. URL: https://www.ft.com/content/c05c9b21-77bd-4ddf-82e1-02356acf0899 (дата звернення: 28.01.2025).

3. IBM. Cost of a Data Breach Report 2022. URL: https://www.ibm.com/security/data-breach (дата звернення: 28.01.2025).

4. World Bank. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution, 2018. URL: https://www.worldbank.org/en/publication/globalfindex (дата звернення: 28.01.2025).

5. Deloitte. Global Blockchain Survey, 2020. URL: https://www2.deloitte.com/content/dam/Deloitte/tw/Documents/financial-services/2020-global-blockchain-survey.pdf (дата звернення: 28.01.2025).

6. Buterin, V. (2021). An Incomplete Guide to Rollups. Retrieved from https://vitalik.eth.limo/general/2021/01/05/rollup.html (дата звернення: 28.01.2025)

7. Chang, C., Sun, J., & Sun, F. (2021). Hybrid Blockchain for IoT – Energy Analysis and Reward Plan. Sensors, 21(1), 305. URL: https://www.mdpi.com/1424-8220/21/1/305 (дата звернення: 28.01.2025).

8. Wikipedia. Zero-Knowledge Proof. URL: https://en.wikipedia.org/wiki/Zero-knowledge_proof (дата звернення: 28.01.2025).

REFERENCES:

1. ENISA. (2021). Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity, p. 22. Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (accessed January 28, 2025).

2. Financial Times. How NotPetya Cyber Attack Devastated Maersk. Available at: https://www.ft.com/content/c05c9b21-77bd-4ddf-82e1-02356acf0899 (accessed January 28, 2025).

3. IBM. (2022). Cost of a Data Breach Report. Available at: https://www.ibm.com/security/data-breach (accessed January 28, 2025).

4. World Bank. (2018). The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Available at: https://www.worldbank.org/en/publication/globalfindex (accessed January 28, 2025).

5. Deloitte. (2020). Global Blockchain Survey. Available at: https://www2.deloitte.com/content/dam/Deloitte/tw/Documents/financial-services/2020-global-blockchain-survey.pdf (accessed January 28, 2025).

6. Buterin, V. (2021). An Incomplete Guide to Rollups. Retrieved from https://vitalik.eth.limo/general/2021/01/05/rollup.html (accessed January 28, 2025)

7. Chang, C., Sun, J., & Sun, F. (2021). Hybrid Blockchain for IoT – Energy Analysis and Reward Plan. Sensors, 21(1), 305. Available at: https://www.mdpi.com/1424-8220/21/1/305 (accessed January 28, 2025).

8. Wikipedia. Zero-Knowledge Proof. Available at: https://en.wikipedia.org/wiki/Zero-knowledge_proof (accessed January 28, 2025).