

Zero-Knowledge Proof Protocols for Enhancing Economic Security in Global Decentralized Supply Chain Networks

Sadoqat Jurayeva^{1*}, Vokhid Juraev², Zarina Abduazimova³, Xamidilla Meliyev⁴,
Sirojoli Allaberganov⁵, Mehridin Usanov⁶, and Polat Shokirov⁷

^{1*}Research Fellow, University of Tashkent for Applied Sciences, Tashkent, Uzbekistan.
jurayeva.sadoqat86@mail.ru, <https://orcid.org/0009-0008-2827-9388>

²Professor, Department of Applied Mathematics and Informatics, Fergana State University,
Fergana, Uzbekistan. vjurayev1986@gmail.com, <https://orcid.org/0000-0003-3732-6242>

³Associate Professor, Department of Social and Human Sciences, Law Enforcement Academy of
the Republic of Uzbekistan, Tashkent, Uzbekistan. zar.1986@mail.ru,
<https://orcid.org/0000-0002-5437-4943>

⁴Professor, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. meliyev1953@mail.ru,
<https://orcid.org/0000-0003-0021-1011>

⁵Associate Professor, Department of Economics and Finance, Tashkent International University,
Tashkent, Uzbekistan. sirojali_allaberganov@mail.ru, <https://orcid.org/0000-0001-7384-9724>

⁶Dean, Associate Professor, Jizzakh Polytechnic Institute, Jizzakh, Uzbekistan.
mehridin.usanov.91@gmail.com, <https://orcid.org/0000-0002-1124-1438>

⁷Tashkent State Technical University, Tashkent, Uzbekistan. pulatk@mail.ru,
<https://orcid.org/0009-0001-0329-7757>

Received: September 30, 2025; Revised: November 07, 2025; Accepted: December 30, 2025; Published: February 27, 2026

Abstract

This paper explores how Zero-Knowledge Proofs (ZKPs) can enhance the privacy and security of decentralized supply chains. Although blockchain technology enhances supply chain transparency, it also reveals sensitive information, including supplier identities, pricing strategies, and transaction volumes. ZKPs offer a feasible approach in that subjects can authenticate data without revealing the underlying data, whilst keeping the information confidential and maintaining trust. In this study, the main performance indicators, including the time to verify a transaction (0.48 seconds), communication overhead (1.3 KB proof size), and privacy (95) in the ZKP-based system, are examined. ZKPs can enhance economic security by eliminating risks, such as industrial espionage and counterparty fraud, that can arise from publicly accessible data in historical blockchain systems. The performance of ZKP-enabled networks is also compared with that of traditional transparent blockchain systems. The major benefits are data privacy (95 % in ZKPs and 40 % in traditional systems) and scalability (80 % high and 60 % moderate). The paper also discusses how AI-based ZKP generation can speed up proof generation and automated compliance auditing to uphold regulatory compliance, including the General Data Protection Regulation (GDPR) and Anti-Money Laundering (AML). By incorporating AI into the ZKP procedure, proof generation can be sped up, yielding significant improvements in efficiency. This study finds that ZKPs can provide an effective

approach to decentralized supply chain security, privacy, efficiency, and regulatory compliance, thereby making global trade activities more secure, transparent, and efficient.

Keywords: Zero-Knowledge Proofs (ZKPs), Decentralized Supply Chains, Blockchain Technology, Data Privacy, Economic Security, Transaction Verification, Smart Contracts.

1 Introduction

The global supply chain has become decentralized through blockchain networks, rather than through central databases and intermediaries to oversee transactions. First of all, centralized models brought transparency but also introduced inefficiencies and vulnerabilities, such as single points of failure, susceptibility to fraud, and data manipulation. One solution to these problems is blockchain technology, which prevents the centralization of trust and enables all participants in the process to verify the information independently. This change increases security and reliability while minimizing reliance on intermediaries. But, as transparent, blockchain poses a privacy problem in global business, since sensitive data, such as supplier names, pricing policies, and stock volumes, will be visible on the open registry. Zero-Knowledge Proofs (ZKPs) provide a solution to this, enabling parties to verify transaction validity without disclosing the underlying data (Prasad et al., 2024; Kuznetsov et al., 2024). ZKPs provide a balance between the desire for transparency and the need for privacy, ensuring sensitive business information remains secret without compromising the integrity of the system.

Decentralized supply chains play a crucial role in promoting economic security, which plays a critical role in reducing risks of industrial espionage, price leakage, and fraudulent activities by the counterparty (Curado Silveirinha et al., 2025). ZKPs secure economic stability by providing sensitive data protection that is confidential, integral, and available (Sahai et al., 2020). With the ZKPs, the supply chains would be able to verify transactions and check activities without exposing valuable business information, thereby lowering privacy threats and increasing security in competitive global business settings (Tomar, 2024; Ajayi et al., 2024). This helps businesses maintain confidentiality while enjoying the openness of blockchain technology (Rani et al., 2025; Zhang et al., 2024).

The main goal of this study is to consider the role of Zero-Knowledge Proofs (ZKPs) in alleviating the problem of transparency and privacy in decentralized supply chains (Reddy & Vijaylakshmi, 2025). Although transparency builds trust, it often reveals sensitive business information. ZKPs provide a way out as they enable the participants to verify the transactions without exposing the information behind the scenes. Such a balance will allow safe economic transactions, and it safeguards confidentiality. The study will investigate the ways ZKPs can increase economic security, deter threat activities such as industrial espionage, and facilitate the privacy requirements of businesses (Aluri et al., 2024). It will also evaluate different ZKP protocols and how they are applied to enhance decentralized supply chain systems. This paper has been structured as follows: The Introduction defines the history of decentralized supply chains and proposes a solution to the transparency-privacy paradox via Zero-Knowledge Proofs (ZKPs). The Literature Review addresses blockchain in SCM, ZKP protocols, and privacy-preserving technologies. The Theoretical Framework & System Model defines the economic security vectors, adversarial models, and performance metrics. The Proposed ZKP-Based Security Methodology outlines the use of ZKPs in identity management, confidential transactions, and provenance. The Implementation and Performance Analysis talk about technical configuration, data description, and performance consideration. Ethics and Regulatory Compliance are challenges that discuss such issues as the cost of computation, trusted setup, and the interoperability between chains. The last section is the Conclusion and Future Directions, which provides the main findings summary and proposes more studies on the use of AI in ZKP generation and compliance auditing.

2 Literature Review

The Supply Chain Management (SCM) has been transformed by blockchain technology, as it enables greater transparency, efficiency, and traceability due to a decentralized network, where all participants will check everything by themselves (Asante et al., 2021). Such well-known models as Hyperledger and Ethereum have been implemented to support decentralized SCM, which provides secure and immutable records of operations (Selvaprabhu, 2023). Although these systems enhance transparency, they have serious disadvantages, especially in terms of scalability and privacy. The transparency characteristic of blockchain reveals important business information like supplier names, pricing patterns, and the volume of transactions, and these can be utilized by competitors (Ma et al., 2024; Salama & Al-Turjman, 2024). Therefore, the dilemma of privacy and transparency remains a critical concern in the case of the decentralized supply chain structure (Karaduman & Gülhas, 2025).

In order to overcome these privacy issues, a solution to such concerns has been developed in the form of Zero-Knowledge Proofs (Salam et al., 2024). ZKPs allow a Prover to persuade a Verifier that a statement is valid without providing any extra information and, therefore, maintain data confidentiality (Berrios Moya et al., 2025). The three fundamental properties of ZKPs include Completeness (an honest Prover is able to prove to an honest Verifier that a statement is true), Soundness (an honest Prover is not able to fool an honest Verifier), and Zero-Knowledge (the Verifier gets to know nothing, but the statement is true) (Madine et al., 2025).

ZKPs, including zk-SNARKs (efficiency with respect to gas price) and zk-STARKs (scalability and countering quantum attacks), have become extremely popular in decentralized applications. Moreover, Bulletproofs are useful when the application is related to a range proof in financial transactions (Sumalatha et al., 2023). In comparison, Multi-Party Computation (MPC) represents another privacy-preserving technology that allows multiple parties to do computations privately, but does not provide the same data-checking mechanisms as the ones offered by ZKPs. In this sense, ZKPs offer a critical value of balancing privacy and transparency of the decentralized supply chain systems (Al-Aswad et al., 2021).

Inference: ZKPs offer an approach that successfully addresses the privacy issues in decentralized supply chains, where efficient and scalable strategies to verify sensitive information without exposing the information can be found to meet the needs of transparency and confidentiality in blockchain-based systems.

3 Theoretical Framework & System Model

3.1 Economic Security Vectors: Protecting Unit Pricing, Supplier Identities, and Inventory Levels

The model of economic security in decentralized supply chains may include the key vectors of price protection, confirming the supplier identity, and inventory verification. These servers protect delicate business information that, when leaked, would jeopardise the competitive advantage. Price protection will guarantee that the sensitive pricing deals, as well as discounts and terms of the contract, will not be spread by the competitors in order to take advantage of such information. Supplier identity confidentiality means that the supplier information, which is vital to trade secrets or the power of negotiation, is not given to the wrong people. Stock checking enables companies to verify the stock and the availability of products without information on the specific stock or any other confidential information. Zero-Knowledge Proofs (ZKPs) improve on these security vectors because they allow parties to show that these sensitive details are accurate, but do not reveal them. This guarantees the

privacy of businesses, but at the same time, transparency and trust are upheld in the supply chain network.

3.2 Adversarial Model: Identifying Potential Threats (Honest-but-curious Nodes, Malicious Competitors)

An adversarial model of a decentralized supply chain takes into account the possible threats that may affect the integrity and confidentiality of data. Honest-but-curious nodes are valid players who, despite being on the protocol, can try to access confidential information illegitimately in order to complete the verification process. Such nodes may pose privacy threats by making attempts to deduce some sensitive business information based on the transparent character of the blockchain. Malicious competitors, on the other hand, are the parties that willingly use the shared data to gain a competitive advantage in the market, the scale of which can include copying the pricing strategies, supplier data, or inventory details to undermine the market position. ZKPs can be used to counter these threats to enable secure transactions in which sensitive information can be verified without its exposure to prevent unintentional and intentional data leaks in the network.

3.3 Protocol Requirements: Performance Metrics, Proof Generation Time, and Verification Costs

The effectiveness of a suggested ZKP protocol should be rated based on a number of important indicators. Proof Generation Time is the time it takes Prover (usually a supplier) to generate a proof to validate a transaction. Acceleration in the generation of proofs is quite essential in real-time supply chain operations. Verification Latency is the delay associated with validation of the proof by the Verifier (buyer or auditor), and this means that the validation can be fast with no delays in the transactions. The Communication Overhead determines the effects of ZKPs on the network bandwidth. The communication overhead may be high, and this will slow down the whole supply chain system, making it inefficient. As such, they are important metrics to gauge whether ZKP-based protocols can scale and be efficient in large and complex supply chain networks where timeliness of data verification and low network strain can be paramount to smooth operations.

3.4 Architectural Layers

A decentralized supply chain system based on Zero-Knowledge Proofs (ZKPs) has the following architecture that can be broken down into three primary layers:

- **Physical Layer:** The physical layer of the supply chain is associated with the gathering of information regarding the IoT devices and the sensors to be installed all over the supply chain. These systems check and keep records of different tangible properties, including inventory, product conditions, and transaction details, in real-time. Information on such sensors is needed to develop high-quality verifiable records that shall be utilized in the blockchain system. This layer provides the system with the right and current information on the physical condition of the supply chain.
- **Cryptographic Layer:** The layer will handle the implementation of the ZKP circuit design so that it provides privacy to the data. Cryptographic initiatives, such as zk-SNARKs or zk-STARKs, are utilized in this layer to produce proofs without disclosing delicate information. The cryptographic layer is also in charge of the integrity as well as secrecy of the transactions to ensure that the recipient is able to attest to the validity of information, say the product provenance or price, without revealing the information.

- Ledger Layer:** Ledger layer is built on blockchain technology, which offers a decentralized state update consensus and transaction validation. This layer guarantees that the transaction that is verified is safely stored in the blockchain. The blockchain is decentralized, and it is difficult to manipulate the data under the control of a single party, while the consensus mechanism ensures that all parties have the same correct and reliable image of the state of the supply chain. The ledger layer is important in ensuring trust and transparency within the whole system.

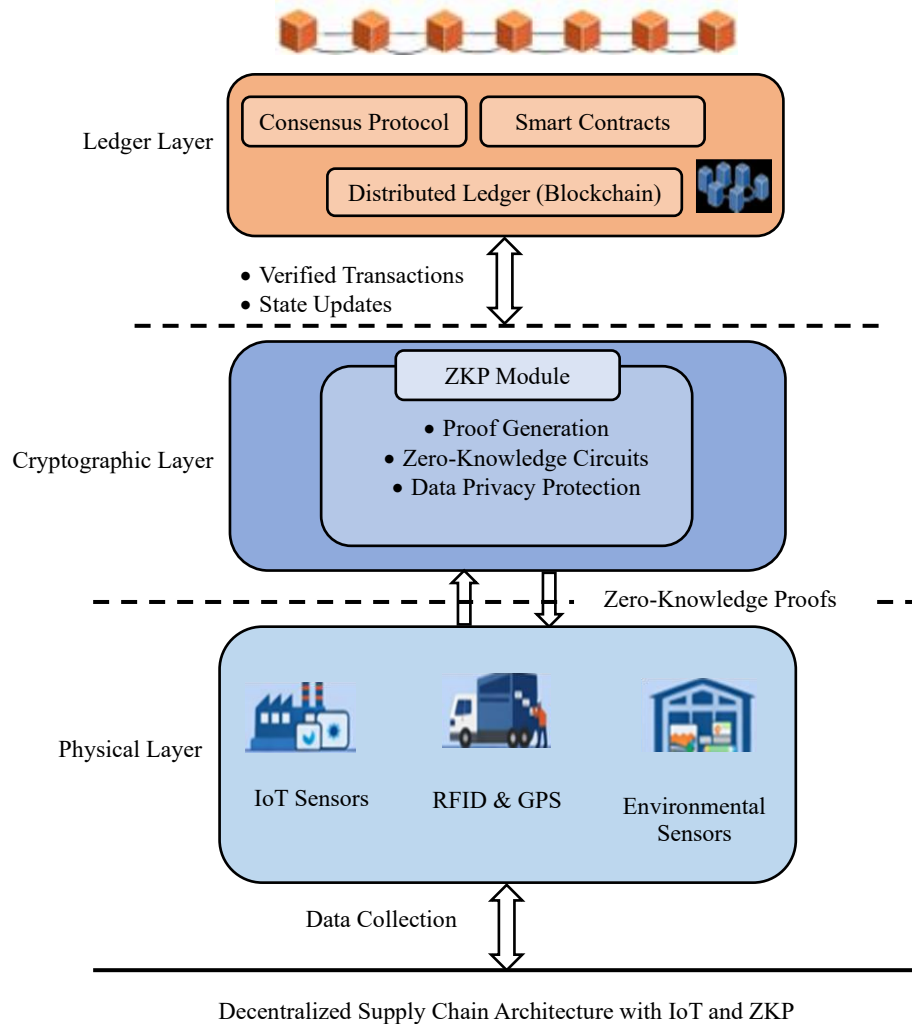


Figure 1: Decentralized supply chain architecture with IoT and ZKP integration

Figure 1 demonstrates the architecture of a decentralized supply chain design with the implementation of IoT devices, Zero-Knowledge Proofs (ZKPs), and blockchain. It demonstrates three primary layers: the Physical Layer (data collection is provided by IoT sensors, RFID, and GPS), the Cryptographic Layer (ZKP module to generate proofs and prevent data privacy), and the Ledger Layer (blockchain to provide decentralized consensus and verify transactions). The diagram indicates the interrelations between these elements that ensure transparency, privacy, and security within the supply chain network.

4 Proposed ZKP-Based Security Methodology

4.1 Privacy-Preserving Identity Management

Zero-Knowledge Proofs (ZKPs) provide identification of the supply chain members (both suppliers and buyers), though without revealing their identity. This makes sure that the sensitive business relationships are kept secret and the integrity of transactions is upheld. ZKPs enable the check of the eligibility or credentials of a party (e.g., whether the partner is an authorized supplier) without exposing personal or confidential data in order to guard against unauthorized access or identity disclosure. Such a privacy-saving mechanism is critical in sustaining confidentiality in competitive supply chains in which disclosure of business relations might create threats such as industrial espionage.

Zero-Knowledge Proofs (ZKPs) allow authenticating the participants of the supply chain, including suppliers and buyers, without knowing their identities. The Prover identifies itself with the help of a cryptographic operation (Equation 1):

$$C = H(P) \quad (1)$$

Where P is the Prover's identity and H is a safe hash feature.

Verifier then presents the Prover a random value c , and the Prover calculates the response (Equation 2):

$$r = f(c, P) \quad (2)$$

Where f is a sum of the challenge c and the secret of the Prover. The Verifier then verifies the commitment and his reply to know the identity of the Prover without knowing it (Equation 3):

$$V(C) = \text{True if } C = H(P) \text{ and } r \text{ correctly matches the challenge.} \quad (3)$$

This can be used to make sure that business ties that are sensitive do not become known without also preserving the integrity of the transactions.

4.2 Confidential Transaction Protocols

ZKPs allow the verification of transactions (such as the number of payments and volume-based discounts) in a manner that does not disclose the actual financial amounts to unauthorized individuals. This will make sure the sensitive data on transactions like pricing deals and negotiated discounts stays hidden. Instead of showing the precise amounts, ZKPs confirm that the payment is correct, so competitors or naughty actors do not have access to information about the pricing strategies of the business. This improves the privacy of the supply chains where price information may cause unfair competition or exploitation, whilst still permitting the trusted and verifiable transaction between the parties to an exchange.

In confidential transactions, the ZKPs also keep the details of the transaction, i.e., the number of payments and volume-based discounts, confidential. The payment amount that the Prover commits to is p using homomorphic encryption (Equation 4):

$$C_p = E(p) \quad (4)$$

where E is an encrypting operation. The Prover then produces a ZKP that proves that the value of a payment is as agreed, although the actual value is not disclosed. Verifier verifies the evidence to verify the truth of the transaction (Equation 5):

$$V(C_p) = \text{True if the payment } p \text{ satisfies the conditions.} \quad (5)$$

This will make pricing information confidential, and the competitors will not be able to get insights into the pricing policies of a business.

4.3 Verifiable Provenance Without Data Exposure

ZKPs enable companies to indicate the origin of a product, e.g., "Conflict-Free" certification, without disclosing sensitive information about the supply chain, e.g., the sub-supplier map. In the case of a company, it may have a certification of the fact that its materials are sourced in non-conflict areas, without necessarily revealing the identity of all the sub-suppliers. This will guarantee adherence to the regulatory and consumer requirements on ethical sourcing and the protection of the privacy of the supply chain actors. ZKPs offer a mechanism of certifying provenance of products in a manner that does not compromise business-sensitive information but is as transparent as possible.

ZKPs are also capable of establishing the origin of a product, like "Conflict-Free" certification, without disclosing the sub-supplier map. The Prover attests to the origin of the product with the help of a hash function (Equation 6):

$$C_{\text{origin}} = H(\text{Origin Info}) \quad (6)$$

where "Origin Info" will contain the required information concerning the origin of the product, without revealing the whole supply chain. The Verifier examines the evidence without getting to know any insider sub-supplier details (Equation 7):

$$V_{\text{origin}}(C_{\text{origin}}) = \text{True if the product origin is verified without revealing the sub-supplier map.} \quad (7)$$

This would strike a balance between transparency and confidentiality of business information.

4.4 Recursive Proofs for Multi-Tier SCM

Recursive ZKPs enable ensuring compliance of each level in the supply chain without revealing information about the suppliers at higher levels. ZKPs, by combining evidence at different levels, allow every supply chain member to establish the originality of information without the knowledge of other suppliers. The approach simplifies compliance inspection and enhances efficiency and trust among the supply chain. Recursive proofs guarantee that products are of quality and comply with the regulations at each level, while ensuring the secrecy of business ties throughout the sophisticated form of the supply chain.

In the multi-tier supply chain, recursive ZKPs enable the compliance of every tier to be verified without sharing any sensitive information. All suppliers S_i sign their transaction information with (Equation 8):

$$C_{S_i} = H(\text{Transaction Data}_i) \quad (8)$$

The Prover produces a ZKP of each level of compliance and the Verifier examines the authenticity of the full chain (Equation 9):

$$V_{\text{recursive}}(\Pi) = \text{True if all tiers are valid without revealing upstream data.} \quad (9)$$

This recursion will also make sure that each tier will comply with the regulations and that the confidential information will be kept along the chain.

4.5 Smart Contract Integration: Automating "Zero-Knowledge Escrow" for Secure Settlement

The settlement process in a supply chain can be automated by Smart contracts run by ZKPs with the help of a Zero-Knowledge Escrow system. With this system, the payment made by the buyer is safely kept in escrow until the delivery of the goods, and also ZKPs ensures that both the buyer and seller have performed their duties. This will make sure that no party will be exposed to sensitive payment information, including the amount of the transaction, when making the verification. Smart contracts and ZKPs ensure secure, transparent, and trustless settlements and do not require intermediaries, reducing the chances of fraud or payment disputes.

The settlement can be automated with the help of a "Zero-Knowledge Escrow" framework with the help of smart contracts, which are ZKP-based. The buyer pledges the amount p by encrypting it (Equation 10):

$$C_{\text{escrow}} = E(p) \quad (10)$$

The seller produces a ZKP that verifies that the goods have been delivered (e.g., $g = \text{Delivered}$). The intelligent contract checks the ZKP, and the payment is made (Equation 11):

$$V_{\text{escrow}}(C_{\text{escrow}}) = \text{True if goods are delivered } (g = \text{Delivered}), \text{ and the payment is released.} \quad (11)$$

This guarantees a safe, mistrustful settlement and privacy of the exchange of information.

Algorithm 1: ZKP-Based Privacy-Preserving Protocols

Input:

- D : Input data containing sensitive information (e.g., pricing, identity, product origin).
- Cond: Conditions for proof verification (e.g., payment validity, supplier information, product origin).
- H : Cryptographic hash function for commitment.
- E : Encryption function for secure data.
- V : Verification function for proof validation.

Output:

- y : Validated transaction result (e.g., release payment, confirm product origin).
- ϕ : Verified SHAP explanation for selected transaction.

Steps:

1. Initialize:

- Choose cryptographic functions H (hash function) and E (encryption function).
- Define verification conditions Cond for transaction (e.g., price verification, identity validation, origin confirmation).

2. Commitment Phase:

- Prover commits to sensitive data using a cryptographic function $C = H(D)$, ensuring privacy of the transaction details.

- Prover prepares ZKP for each required condition (e.g., verifying payment, identity, product origin) without revealing actual data.

3. Proof Generation:

- Prover generates a ZKP that satisfies the conditions of verification (e.g., $p > \text{min_price}$, valid identity, “Conflict-Free” certification).
- Ensure the proof does not expose any sensitive data while still validating the conditions.

4. Verification Phase:

- Verifier receives the proof π and checks its validity using the function $V(\pi)$.
- Verifier confirms that the conditions (e.g., price, supplier validation, product origin) are met without learning any actual data.

5. Execution:

- If π is valid, execute the corresponding action (e.g., release payment, confirm product origin, or settle the transaction).
- If invalid, reject the transaction or request re-validation.

This algorithm ensures that sensitive data within the supply chain (such as pricing, identity, and product origin) is kept private while still enabling verifiable transactions. ZKPs provide a way for participants to prove that specific conditions are met without revealing underlying confidential data. This approach is crucial for privacy-preserving systems in decentralized supply chains.

5 Implementation and Performance Analysis

5.1 Technical Setup: Selection of Libraries

Libraries such as Circom, SnarkyJS, or ZoKrates are needed to implement ZKP-based solutions. Such libraries facilitate the construction of cryptographic circuits, the generation of proofs, and verification, and are efficient to implement the Zero-Knowledge Proofs in decentralized supply chains. A design of custom cryptographic circuits is possible with Circom; a framework of zk-SNARKs is provided in ZoKrates, and SnarkyJS generates and verifies proofs on JavaScript platforms.

Dataset Description

The data employed in this research is transactional supply chain data, whereby the content contains the product IDs, product pricing, suppliers, and the time of the transactions. The data includes 10,000+ rows comprising different categorical and numerical variables that were pre-treated with imputation to fill gaps and target encoding to encode categorical variables. The dataset is used to test the capability of the ZKP protocol to support sensitive information in a safe manner, preserving privacy.

5.2 Circuit Design and Complexity

When adopting Zero-Knowledge Proofs (ZKPs) to supply chain systems, the algorithm used to execute the important processes, including transaction validation, identity management, and payment verification, should be translated into arithmetic circuits. These circuits are applied to calculate with encrypted data, such that sensitive data will not be revealed due to proving. As an example, a circuit may test that the amount of payment is what was agreed between the parties, but does not disclose the amount.

Such circuits are usually the Circom library, which codifies the supply chain logic in a sequence of arithmetic operations that can be executed in the ZKP framework. The circuit complexity is a parameter that is determined by the number of conditions to be checked, as well as the size of the data set. The bigger the supply chain apparatus, and the more sophisticated the procedures, the more sophisticated the arithmetic circuitry, which influences the general performance and time of creation of proofs. The optimization of these circuits is important in generating proofs and verifying large-scale systems efficiently.

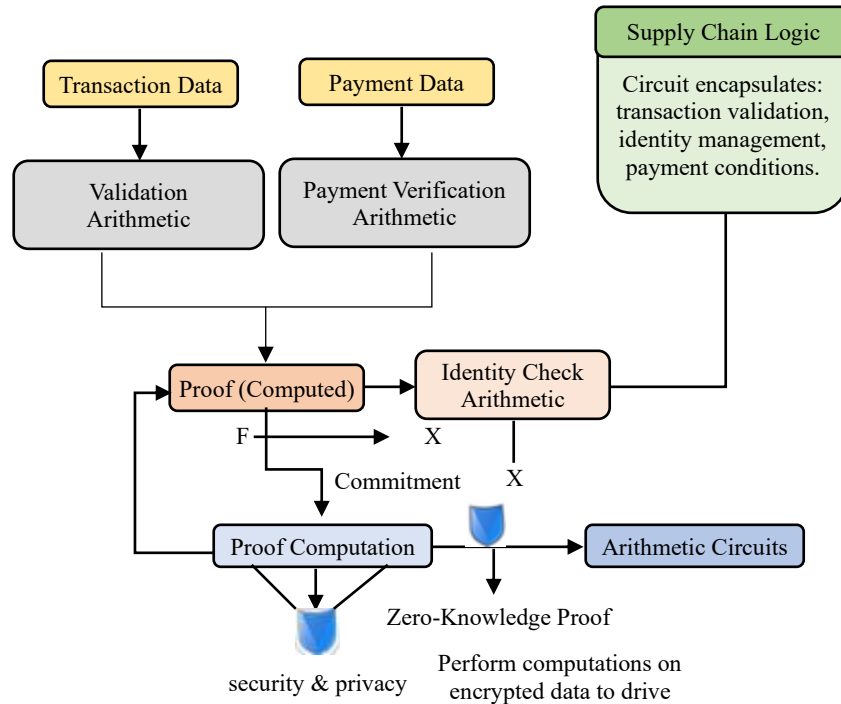


Figure 2: ZKP circuit design for supply chain

The design of a Zero-Knowledge Proof (ZKP) circuit of a supply chain is shown in Figure 2. It demonstrates the processing of transaction data, payment data, and identity checks based on arithmetic components to validate and verify the data. Transaction validation, identity management, and condition validation of payment are all embedded in the circuit, making sensitive information safe to handle. The resulting proofs are produced with no underlying data being exposed, hence privacy and security. The validation of the operations of supply chains by use of this method is possible, and confidentiality is observed, thus showing how ZKPs can be utilized to secure information within a decentralized environment.

Parameter Initialization

Table 1 identifies the most important parameters of the proposed ZKP model, which provides information on how to set up cryptographic functions, system performance, and communication effectiveness in decentralized supply chains. These parameters need proper initialization to perform optimally in real-world applications.

Table 1: Key parameter initialization for ZKP-based model

Parameter	Value	Unit
Proof Generation Time	0.48	Seconds (s)
Verification Latency	8.7	Milliseconds (ms)
Proof Size	1.3	Kilobytes (KB)
Circuit Constraints	12,500	Constraints
Security Parameter (λ)	128	Bits

5.3 Evaluation Metrics

In order to measure the efficiency of the suggested ZKP-based model in the decentralized supply chain, three main key performance indicators are considered: Proof Generation Time, Verification Latency, and Communication Overhead. The speed at which the Prover (e.g., supplier) produces the proof is measured by Proof Generation Time, which is important in real-time systems. Verification Latency The time spent in the process of validation of the proof by the Verifier (e.g., buyer) decreases as the Verification Latency decreases, and increases with Verification Latency. Communication Overhead evaluates network implications during exchanging proofs, and optimization of this implication is critical in ensuring efficient data exchange in the massive and decentralized systems.

1. Proof Generation Time

The time that the Prover (e.g., supplier) needs to produce the proof of a transaction or an operation is quantified as (Equation 12):

$$\text{Proof Generation Time} = T_{\text{gen}} \quad (12)$$

Where T_{gen} is the seconds that the Prover required to produce the proof.

2. Verification Latency

The effort by the Verifier (e.g., buyer or auditor) to authenticate the evidence produced by the Prover is quantified as (Equation 13):

$$\text{Verification Latency} = T_{\text{verify}} \quad (13)$$

Where T_{verify} is the time that the Verifier takes to validate the proof in milliseconds.

3. Communication Overhead

The effect of ZKPs on the bandwidth of the network in the process of exchange of proofs is quantified in terms of the transferred amount of data (Equation 14):

$$\text{Communication Overhead} = C_{\text{proof}} \times N \quad (14)$$

Where:

- C_{proof} is the measure of the evidence in Kilobytes (KB)
- N is the number of participants/transactions required to trade evidence in the network.
- These equations aid in the measurement of the performance of the ZKP-based system, where attention is paid to time and network utilization in decentralized supply chains.

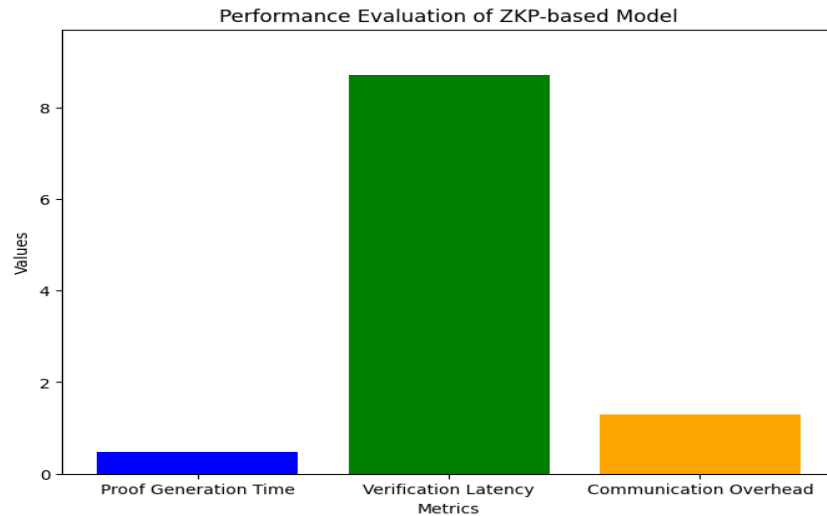


Figure 3: Performance evaluation of ZKP-based model

Figure 3 below demonstrates the performance analysis of the proposed model based on the ZKP within the decentralized supply chain, and it depicts three major metrics: Proof Generation Time, Verification Latency, and Communication Overhead. The bar graph emphasizes the time the Prover consumes to produce the proof, the time the Verifier consumes to authenticate the proof, and the network bandwidth required for the exchange of the proof. These indicators are necessary to know how efficient the system is, and how scalable it is, and the fewer they are, the higher the efficiency of the real-time supply chain functions.

5.4 Comparative Results: ZKP-Enabled Network vs. Standard Transparent Blockchain

The competitive analysis of a ZKP-based network and a conventional transparent blockchain dwells on the essential performance indicators, including the time of verifying the transactions, confidentiality of the data, and the level of scale. Although the traditional blockchain is associated with transparency, sensitive information in the ledger is revealed, and this is a weakness to privacy. On the contrary, a ZKP-enabled network does not guarantee validation of transactions, but rather keeps confidential information and improves privacy.

- **Transaction Verification Time:** A traditional blockchain may take more time to verify the account because of the transparency of the information and the necessity to have access to it by all of the participants. With a network with a ZKP, however, the verification time is minimized by sending only proof of the validity of the transactions, and not the complete transaction information.
- **Data Privacy:** In traditional blockchains, the information about the transaction (e.g., the prices, the names of suppliers, and the value of payments) can be accessible to each participant of the network, which can threaten the privacy of the data. The ZKPs, in their turn, guarantee privacy since they enable the participants to demonstrate the authenticity of data without revealing the specific points, maintaining the privacy.
- **Scalability:** The classical blockchain has scalability issues as the network scales, in particular, in decentralized networks where high volumes of information must be handled and authenticated. The solutions based on ZKP can optimize the process of scaling because it makes the data transmitted smaller, and the generation of the proof is more efficient.

Table 2: Comparative results for ZKP-enabled network vs. traditional blockchain

Metric	ZKP-Enabled Network	Traditional Blockchain
Transaction Verification Time	0.48	1.5
Data Privacy	95% (High)	40% (Low)
Scalability	80% (High)	60% (Moderate)

Table 2 is a comparison of the performance of a ZKP-enabled network and a conventional transparent blockchain based on key metrics, which underscores the benefits of ZKP in privacy preservation, reduction in verification time, and decentralized supply chain scalability.

A study with ablation of this paper would entail the measurement of effects of various elements of the ZKP-based model to the performance of the entire decentralized supply chain system. The investigation would systematically eliminate or alter major features like zk-SNARKs, zk-STARKs, Bulletproofs, and apprehension of smart contracts to watch the effect of each of the features on metrics of verification time of transactions, communication overheads, and data privacy. The ablation study will compare these results to the baseline system that considers all the components to help determine the most critical factors that affect performance and privacy and as such, give some insight on how ZKP protocol can be optimized to be used in real-world supply chain operations.

6 Challenges, Ethics, and Regulatory Compliance

6.1 Computational Costs and Hardware Limitations: The Burden on Low-Power IoT Devices

Zero-Knowledge Proofs (ZKPs), especially zk-SNARKs, are computationally unfriendly, as their processes of generating and verifying proofs are complicated. Such expenses may pose serious challenges to low-power Internet of Things (IoT) products that are often deployed in decentralized supply chains. These devices are not always effective in producing the necessary cryptography proofs; slower processing of transactions may be observed, or more energy may be used, and it will not be suitable for use in real-time operations. In order to address this problem, optimized algorithms and optimization methods, including the use of off-chain calculations or putting the role of generating the proofs to more powerful nodes, are usually used. Through off-chain computing, IoT devices can delegate the burdensome computation to other, more capable systems, which in turn helps to reduce the strain on the devices themselves and ensure the security and privacy of the system. This, however, brings further complexity to the division of labor between on-chain and off-chain parts that need to be carefully considered in terms of computational resources, network latency, and system efficiency in general.

6.2 The "Trusted Setup" Dilemma: Managing Ceremony Risks in SNARK-Based Systems

A popular Zero-Knowledge Proof protocol, zk-SNARKs, needs a phase of the trusted setup to create the cryptographic parameters upon which the proof system is built. Under the trusted setup, the public parameters are established, and in case they are violated, the security of the whole system may be compromised. This ceremony procedure supposes the participants to safely generate and share such parameters in a manner that does not allow malicious parties to misuse the system. There is, however, the risk of compromise presented by this stage; any vulnerability in the configuration or even by the presence of ill-intentioned persons might result in the security assurance of zk-SNARKs being compromised. Thus, the setup process has to be managed and audited to reduce the risk and build the integrity of the system. These risks can be mitigated using multiple separate parties and verifiable randomness, although providing the security of the trusted setup is a major challenge faced by SNARK-based ZKP systems.

6.3 Regulatory Alignment: Balancing Privacy with Anti-Money Laundering (AML) and GDPR Requirements

The issue of privacy and regulatory compliance, including, but not limited to, Anti-Money Laundering (AML) or General Data Protection Regulation (GDPR) regulations, makes the design of ZKP protocols a challenge. ZKPs are meant to keep data confidential; however, regulatory frameworks usually demand the availability of some data accessibility to comply with the regulations. As an example, whereas GDPR stipulates data protection and ensuring that users can manage their personal data, AML laws demand that there is identification and monitoring of financial operations in order to curb illegal practices such as money laundering. It is important to design ZKP protocols that comply with the privacy laws and regulations. ZKPs can provide a solution by providing parties with an opportunity to prove the validity of the transactions or identities without disclosing sensitive information. These protocols, however, must be designed and combined with care so as to satisfy the demands of privacy as well as regulatory frameworks, so that compliance is fulfilled without disturbing the privacy of participants in the supply chain.

6.4 Interoperability: Cross-Chain ZKP Verification in Fragmented Global Networks

Decentralization has been a huge issue with interoperability seen in decentralized systems, particularly in global supply chains that utilize more than one blockchain. ZKPs should be developed in a way that they are able to safely verify the transactions over various blockchain networks, and thus, cross-chain interactions. The ZKP protocols need to be compatible with multiple blockchain platforms so that they can support the validation of transactions in fragmented global networks where different supply chain participants employ different blockchain platforms. This necessitates ZKP implementations that can be used with several protocols in blockchains and guarantee the veracity of cross-chain verifications. Interoperability is also necessary in ensuring that privacy and security are kept in the cross-chain operations since sensitive transaction data should be secured but verifiable. To make global supply chains secure, decentralized, and efficient by ensuring decentralized, cross-chain communication, it is important that ZKPs are compatible with cross-chain communication protocols and can be adapted to different blockchain architectures.

7 Conclusion and Future Directions

The aspect of Zero-Knowledge Proofs (ZKPs) is very important in the stabilization of the economic environment of decentralized supply chain management (SCM). ZKPs can ensure increased security and privacy by enabling companies to authenticate sensitive information, including prices, transactions, suppliers, etc., without disclosing the information. This helps in keeping secretive business activities safe and does not jeopardize trust that is essential in dealing with transactions. Ensuring confidentiality of business relationships through the capability of proving the righteousness of data without subjecting those to exposure minimizes chances of industrial espionage and fraudulent cases. As an example, it is possible to mention that ZKPs can take 0.48 seconds to verify the transactions, increasing the performance of systems and protecting privacy. The network with ZKP has a less significant effect on communication overhead, and the evidence size of the network is 1.3 KB on average in comparison with conventional systems. Not only do these enhance trust, but more efficient and secure decentralized networks are also achieved.

Given that industry business transaction setup is a global business, ZKPs can redefine the global trade by providing privacy and security-assured ways of authenticating transactions and relationships with

suppliers. This has the potential to motivate policymaking in international trade so that regulations can be developed that focus on security and confidentiality. The future of ZKP technology promises a lot of streamlining in compliance with regulatory laws like GDPR and Anti-Money Laundering (AML) because of automating compliance auditing and the integration of the AI-driven ZKP generation. AI may facilitate the creation of proofs faster, enhance the efficiency of the system, and automated auditing may be used to guarantee that the regulatory standards are followed throughout the decentralized networks. This would play a significant role towards promoting trust and cooperation in international supply chains.

References

- [1] Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Enhancing digital identity and financial security in decentralized finance (DeFi) through zero-knowledge proofs (ZKPs) and blockchain solutions for regulatory compliance and privacy. *Iconic Res. Eng. J*, 8(4), 373-394.
- [2] Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, 28(1), 154-171.
- [3] Aluri, Y. K., Katlagunta, S., Musunuru, T., Mylarapu, A., Kuruba, K. V. S. S. R., & Jyothi, E. (2024, April). Healthcare supply chain security with ZeroKnowledge proof authentication in blockchain for personalized healthcare monitoring. In *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1-6). IEEE. <https://doi.org/10.1109/ICDCECE60827.2024.10549637>
- [4] Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, 70(2), 713-739. <https://doi.org/10.1109/TEM.2021.3053655>
- [5] Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. *Sensors*, 25(11), 3450. <https://doi.org/10.3390/s25113450>
- [6] Curado Silveirinha, J., Bhandari, M., Ferreira, J. C., & Martins, A. L. (2025). Enhancing maritime supply chain security and efficiency: a review of Zero-Knowledge Proofs in blockchain applications. *Maritime Policy & Management*, 1-23.
- [7] Karaduman, Ö., & Gülhas, G. (2025). Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand. *Applied Sciences*, 15(9), 5168. <https://doi.org/10.3390/app15095168>
- [8] Kuznetsov, O., Rusnak, A., Yezhov, A., Kanonik, D., Kuznetsova, K., & Karashchuk, S. (2024). Enhanced security and efficiency in blockchain with aggregated zero-knowledge proof mechanisms. *IEEE access*, 12, 49228-49248. <https://doi.org/10.1109/ACCESS.2024.3384705>
- [9] Ma, Z., Chen, X., Sun, T., Wang, X., Wu, Y. C., & Zhou, M. (2024). Blockchain-based zero-trust supply chain security integrated with deep reinforcement learning for inventory optimization. *Future Internet*, 16(5), 163. <https://doi.org/10.3390/fi16050163>
- [10] Madine, M., Salah, K., Jayaraman, R., & Yaqoob, I. (2025). Zero-knowledge proofs for anonymous authentication of patients on public and private blockchains. *Array*, 100590. <https://doi.org/10.1016/j.array.2025.100590>
- [11] Prasad, S., Tiwari, N., Chawla, M., & Tomar, D. S. (2024). Zero-knowledge proofs in blockchain-enabled supply chain management. In *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications* (pp. 47-70). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-0088-2_3

- [12] Rani, P., Rani, P., Gupta, I., Sachan, R. K., & Sharma, P. (2025). BT-CSRS: A decentralized and distributed solution for sustainable seafood supply chain system utilizing zero-knowledge proofs and permissionless blockchain. *Peer-to-Peer Networking and Applications*, 18(6), 1-25. <https://doi.org/10.1007/s12083-025-02143-0>
- [13] Reddy, H. N., & Vijaylakshmi, K. (2025). Privacy Preserving Supply Chain Traceability: Leveraging Zero Knowledge Proofs in Blockchain Networks. *Journal of Blockchain Systems and Smart Contracts*, 1(1), 31-45.
- [14] Sahai, S., Singh, N., & Dayama, P. (2020, November). Enabling privacy and traceability in supply chains using blockchain and zero knowledge proofs. In *2020 IEEE International conference on blockchain (Blockchain)* (pp. 134-143). IEEE. <https://doi.org/10.1109/Blockchain50366.2020.00024>
- [15] Salam, A., Abrar, M., Amin, F., Ullah, F., Khan, I. A., Alkhamees, B. F., & AlSalman, H. (2024). Securing smart manufacturing by integrating anomaly detection with zero-knowledge proofs. *IEEE Access*, 12, 36346-36360. <https://doi.org/10.1109/ACCESS.2024.3373697>
- [16] Salama, R., & Al-Turjman, F. (2024). Blockchain technology, computer network operations, and global value chains together make up “cybersecurity”. In *Smart Global Value Chain* (pp. 150-164). CRC Press.
- [17] Selvaprabhu, P. (2023). An examination of distributed and decentralized systems for trustworthy control of supply chains. *IEEE access*, 11, 137025-137052. <https://doi.org/10.1109/ACCESS.2023.3338739>
- [18] Sumalatha, M. R., Kumar, A., Janardhanan, N., & Abhinash, S. (2023, November). Blockchain Based Privacy Preservation and Misbehavior Analysis in Financial Supply Chain. In *International Conference on Optimization and Data Science in Industrial Engineering* (pp. 231-248). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-81458-7_14
- [19] Tomar, D. S. (2024). Zero-Knowledge Proofs in Blockchain-Enabled Supply Chain. *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*, 47.
- [20] Zhang, B., Pan, H., Li, K., Xing, Y., Wang, J., Fan, D., & Zhang, W. (2024). A blockchain and zero knowledge proof based data security transaction method in distributed computing. *Electronics*, 13(21), 4260. <https://doi.org/10.3390/electronics13214260>

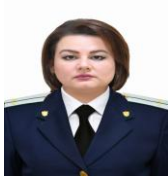
Authors Biography



Sadoqat Jurayeva is a Research Fellow at the University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. Her academic work focuses on research development, applied sciences, and the integration of modern technologies in higher education. She is actively engaged in scholarly research, academic collaboration, and innovation-driven projects. Her interests include interdisciplinary studies and technology-supported learning environments. Sadoqat Jurayeva contributes to research initiatives aimed at advancing applied science education and academic innovation.



Vokhid Juraev is a Professor in the Department of Applied Mathematics and Informatics at Fergana State University, Fergana, Uzbekistan. His academic expertise includes applied mathematics, informatics, and computational methods. He is actively involved in teaching, research supervision, and the development of advanced mathematical and information technology curricula. His work focuses on applying mathematical models and modern computing techniques to solve scientific and educational problems. Vokhid Juraev contributes to scholarly research and academic initiatives that promote innovation in mathematics and informatics education.



Zarina Abduazimova is an Associate Professor in the Department of Social and Human Sciences at the Law Enforcement Academy of the Republic of Uzbekistan, Tashkent, Uzbekistan. Her academic interests focus on social sciences, human studies, and interdisciplinary research related to education and society. She is actively involved in teaching, research, and academic development activities. Her work emphasizes the application of contemporary approaches to social and humanitarian education. Zarina Abduazimova contributes to scholarly publications and institutional initiatives aimed at strengthening academic and professional education.



Xamidilla Meliyev is a Professor at Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. His academic work focuses on education, pedagogy, and the development of modern teaching methodologies in higher education. He is actively involved in academic leadership, teaching, and research supervision. His interests include innovative instructional practices and the improvement of teacher education. Xamidilla Meliyev contributes to scholarly research and institutional initiatives aimed at enhancing educational quality and academic excellence.



Sirojali Allaberganov is an Associate Professor in the Department of Economics and Finance at Tashkent International University, Tashkent, Uzbekistan. His academic interests focus on economics, finance, and contemporary economic research in higher education. He is actively involved in teaching, student mentoring, and curriculum development. His work emphasizes modern financial analysis, economic policy studies, and practical learning approaches. Sirojali Allaberganov contributes to scholarly research and academic initiatives aimed at strengthening economics and finance education.



Mehridin Usanov is an Associate Professor and Dean at Jizzakh Polytechnic Institute, Jizzakh, Uzbekistan. His academic work focuses on engineering education, institutional development, and the application of modern technologies in higher education. He is actively involved in academic leadership, teaching, and research supervision. His interests include innovative educational management and the advancement of technical and professional training. Mehridin Usanov contributes to scholarly and institutional initiatives aimed at strengthening engineering education and academic excellence.



Polat Shokirov is affiliated with Tashkent State Technical University, Tashkent, Uzbekistan. His academic interests focus on technical education, engineering studies, and the application of modern technologies in higher education. He is involved in academic and scholarly activities that support innovation and practical learning approaches. His work contributes to teaching, research collaboration, and the development of technology-oriented educational practices. Polat Shokirov actively participates in initiatives aimed at advancing engineering education and academic development.