SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 2, 8-15

https://doi.org/10.51301/ce.2024.i2.02

Blockchain-Enabled Zero-Knowledge Proof for Confidential Electronic Auction Systems

A. Akhmedov, T. Khafiz, A. Razaque, Zh. Kalpeyeva*

Satbayev University, Almaty, Kazakhstan

**Corresponding author: zh.kalpeyeva@satbayev.university*

Abstract. Blockchain technology, although relatively recent, has already been successfully integrated into our society. Decentralized systems (DS), and blockchain networks in particular, raise important questions about the security and privacy of data storage and transmission, attracting an increasing number of users. One promising application of blockchain is the organization of auctions, where participants can sell goods or services while maintaining complete privacy and integrity of the conduct. This paper proposes an auction model in DC using Zero- Knowledge Proofs (ZKP), including techniques such as zk-SNARK, zk-STARK and Bulletproofs. These approaches allow participants to confirm the validity of their bets without revealing their content. State-of-the-art cryptography techniques including hashing (SHA-256, SHA-3), elliptic curves (ECC), asymmetric encryption (RSA) and digital signatures are used to ensure data security. The experimental part of the work emphasizes on performance analysis of the proposed system using queueing theory to simulate network load and computational cost. The results show that the developed model provides a high level of privacy and scalability, which makes it promising for use in real applications.

Keywords: *decentralized systems, ZKP, hashing, blockchain, auction*.

1. Introduction

The quick growth of blockchain technology has probably caused changes in many industries, like auction systems. Traditional centralized auctions often struggle with trust, transparency and privacy issues, usually depending on intermediaries that are not very efficient and might be manipulated. Blockchain, known for being decentralized and unchangeable, offers a strong alternative by giving transparent and tamper-proof systems. Yet, the very transparency of blockchain brings new issues, especially in keeping the privacy of participants and their bids during auctions [1]. Zero-Knowledge Proofs (ZKPs) now help with privacy concerns in a very interesting way. These proofs let people check bids without showing private details, keeping everything secret and fair. New ideas like zk-SNARKs, zk-STARKs and Bulletproofs have really increased how useful and efficient ZKPs are in real decentralized systems. Bullet- proofs stand out because they create short and non-interactive range proofs, probably important for checking bid amounts while keeping participants unknown [2]. Besides privacy, the growth and efficiency of auction systems are very important. Modern cryptographic tools like elliptic curve cryptography (ECC) and homomorphic encryption increase security and improve function. Homomorphic encryption allows bid checking without showing bid amounts, while ECC offers strong security with less computing power [3]. Furthermore, queueing theory provides a robust framework for modeling network loads and computational costs, ensuring that the system can scale effectively under varying configurations [4].

This paper introduces a new decentralized auction system that uses blockchain, zero-knowledge proofs (ZKPs) and cutting-edge cryptographic techniques to solve issues related to privacy, size and fairness. Researchers tested this system with detailed theoretical analysis and experimental simulations, checking its performance under a variety of cryptographic and network situations. By mixing cryptographic advances with performance studies, this study helps create secure and scalable auction systems for both public and private use [5]. Figure 1 shows auction system in decentralized networks.

The remainder of this paper is organized as follows: Section II reviews related works on blockchain-based auctions and the application of ZKP. Section III describes the proposed auction model, including its theoretical framework and algorithms. Section IV presents the experimental setup and performance evaluation. Section V discusses the results and their implications, and Section VI concludes the paper with insights and future directions.

1.1. Research Motivation and Contribution

Auctions are a cornerstone of economic activity, utilized across diverse sectors to allocate resources efficiently. Governments leverage auctions for critical tasks such as distributing radio frequencies, granting subsidies, and allocating land. In the corporate world, auctions determine strategic contracts, such as selecting partners for refining resources or providing services. Despite their broad applicability, traditional auction systems often lack transparency, fairness, and participant confidentiality. Addressing these challenges is essential to ensure trust and optimal outcomes.

The main contributions of this study are summarized as follows:

• This study implements Zero-Knowledge Proofs (ZKPs), such as Bulletproofs, to ensure bid confidentiality while maintaining fairness, enhancing trust in auction processes.

• By integrating blockchain technology, the proposed model ensures immutable records and reduces reliance on intermediaries, fostering transparency and integrity.

• This study rigorously analyzes the network load and computational efficiency under varying cryptographic configurations, providing actionable insights for deployment.

• The proposed model addresses auction needs across governmental, corporate, and individual domains, making it versatile and practical for real-world scenarios.

1.2. Problem Identification

Traditional auction systems face significant challenges in terms of privacy, transparency, and scalability. Participants often hesitate to disclose sensitive bid information due to the risk of manipulation or leakage, which undermines trust in the auction process. Additionally, centralized auction platforms rely heavily on intermediaries, making them prone to inefficiencies, tampering, and single points of failure. Blockchain technology offers a decentralized alternative with transparency and tamper-proof records.

However, its inherent openness poses a critical challenge: maintaining confidentiality while ensuring the validity of bids. Without proper privacy measures, the public visibility of blockchain transac- tions compromises participant anonymity. Furthermore, cryptographic methods, including Zero-Knowledge Proofs (ZKPs), require sub- stantial computational resources, raising concerns about scalability in real-world applications. Ensuring the system performs efficiently under varying loads while safeguarding privacy and fairness remains a pressing challenge. This study addresses these problems by proposing a scalable, privacy-preserving decentralized auction model leveraging blockchain and ZKP technologies.

Figure 1. Auction system in decentralized networks

2. Materials and methods

Numerous studies have been conducted to explore the application of cryptographic mechanisms, including Zero-Knowledge Proofs (ZKP), in online auctions to enhance security, privacy, and transparency. This section reviews relevant literature on the implementation of cryptographic schemes, blockchain integration, and their impact on online auction systems. Research on cryptographic approaches for electronic auctions highlights the importance of preserving confidentiality and fairness in competitive bidding environments. Early works focused on traditional cryptographic techniques, such as RSA and ElGamal encryption, to ensure secure communication channels and data integrity in online auctions. These methods laid the foundation for more advanced schemes, including homomorphic encryption and secure multi-party computation, which provide stronger guarantees of privacy during bid submission and evaluation.

The adoption of blockchain technology has introduced new paradigms for improving transparency and accountability in online auctions. Platforms like Ethereum and Hyperledger Fabric have been utilized to build decentralized auction systems, enabling immutable recording of transactions and eliminating the need for a trusted central authority. For example, Nguyen et al. (2018) proposed a blockchain-based auction framework where smart contracts automate bid evaluation and winner determination, ensuring fairness and reducing human intervention. However, these systems often face challenges in maintaining the confidentiality of bids, as blockchain's transparency can inadvertently expose sensitive information. To address this limitation, researchers have incorporated ZKP protocols into blockchain-based auction systems. Zero-Knowledge Succinct Non- Interactive Arguments of Knowledge (zkSNARKs) and Bulletproofs have emerged as popular choices for implementing privacy-preserving mechanisms. For instance, Zhang et al. (2020) demonstrated the use of zkSNARKs to verify bid correctness without revealing the bid amounts, achieving both privacy and verifiability in sealed-bid auctions. Similarly, the application of Bulletproofs offers compact and efficient proofs, reducing computational overhead while maintaining strong privacy guarantees.

Several studies have also explored hybrid approaches combining ZKP with other cryptographic techniques. For example, methods integrating homomorphic encryption with ZKP have been proposed to enable secure computation of winning bids without revealing individual bid values. Additionally, recursive zkSNARKs have been employed to optimize proof generation and verification processes, significantly enhancing the scalability of auction systems with large numbers of participants. Despite these advancements, challenges remain in achieving optimal trade-offs between efficiency, scalability, and security in ZKP-based auction systems. Recent works continue to focus on improving the usability and computational efficiency of these protocols, making them more practical for real-world applications. Table 1 illustrates the comparison between different proposed solutions.

2.1 Proposed Solution

The decentralized auction model proposed in this study aims to address critical challenges such as privacy, scalability, and fair- ness. The system leverages blockchain technology as its backbone for transparency and immutability, while advanced cryptographic techniques, including Zero-Knowledge Proofs (ZKPs), digital signatures, and hashing, ensure bid confidentiality and integrity [10]. The integration of cryptographic components addresses the dual need for secure bid processing and participant anonymity. By combining these technologies, the model facilitates a trustless environment where neither participants nor organizers can ma-

nipulate the process. This model is particularly relevant for use cases in government allocations, corporate procurement, and individual transactions, offering a flexible framework adaptable to varying needs.

The blockchain serves as a decentralized and immutable ledger, recording all interactions and commitments during the auction process. While blockchain provides transparency, its inherent openness introduces challenges in maintaining the confidentiality of bid values. To resolve this, ZKPs are employed to validate bids without revealing sensitive details, ensuring fairness while maintaining privacy [11]. Additionally, standard cryptographic methods, including elliptic curve cryptography (ECC) for encryption and SHA-256 for hashing, are integrated to further enhance system security. The auction process is divided into several phases: announcement, participant registration, bid submission with cryptographic commitments, verification, winner determination, and finalization. Each phase incorporates cryptographic methods and blockchain features to ensure security and efficiency.

2.2 Proposed Decentralized Auction System

The proposed decentralized auction system leverages blockchain technology and cryptographic primitives, including encryption, hashing, digital signatures, and Zero-Knowledge Proofs (ZKP), to address the core challenges of privacy, fairness, and transparency. The algorithm is designed to ensure bid confidentiality while maintaining the integrity and efficiency of the auction process. The auction workflow consists of distinct phases that ensure secure communication and verifiable outcomes, as outlined below.

The auction begins with the Auction Announcement Phase, where the organizer broadcasts the auction details, such as the item description, minimum acceptable bid, and bidding rules, to potential participants. The announcement is sent as an encrypted message to ensure authenticity and prevent tampering. In the Participation Phase, participants decide whether to join the auction. Those who agree to participate submit a request to the organizer containing their unique identifiers and encrypted credentials. These requests are authenticated using digital signatures to ensure the integrity of the participants' identities. If a participant opts not to join, they exit the process without further interaction.

Table 1. Comparison of studies on blockchain-based auction systems

Study	Methods/Approaches	Solutions/Advantages	Limitations
Hao et al. [6]	Blockchain-based auction with ZKP to maintain bid confidentiality.	Ensures privacy by keeping nonwinning bids confidential. Utilizes blockchain for transparency and immutability, enhancing trust in the auction process.	High computational costs associated with ZKP, especially for large- scale auctions with multiple participants.
Lee and Kim [7]	Sealed-bid auction protocol using zkSNARKs.	Provides strong privacy guarantees by ensuring that the winning bid is verifiable without revealing other bids. Reduces computational complexity compared to traditional ZKP implementations.	Implementation requires advanced cryptographic infrastructure, and zkSNARKs may introduce initial setup costs that limit accessibility for smaller auctions.
Chen et al. [8]	Hybrid approach combining ElGamal encryption and blockchain for auction result verification.	Enables end-to-end security with encryption to safeguard bids and blockchain to ensure tamper-proof results. Supports public verifiability and prevents replay attacks.	The reliance on ElGamal encryption can increase the complexity of the decryption process, and the model might not scale efficiently with a high number of participants.
Zhao et al. [9]	Privacy-preserving auction system using Bulletproofs for bid verification.	Efficient use of Bulletproofs minimizes proof size and verification time, enhancing scalability. Offers robust privacy while enabling transparent verification of auction results.	Requires significant expertise to implement, and Bulletproofs can be computationally intensive when generating proofs for a large dataset.
Our solution	Integration of ZKP, blockchain, and recursive zkSNARKs to build a secure, privacy-preserving auction system.	Combines the scalability of recursive zkSNARKs with the transparency of blockchain and the privacy guarantees of ZKP. Reduces the number of proofs in large auctions, making the system efficient and scalable.	Initial implementation costs and computational requirements might make it inaccessible for smaller organizations. Compatibility with existing auction platforms might require customization.

During the Bid Submission Phase, participants send their bids as cryptographic commitments using a secure hash function:

$$C = H(\text{bid} \parallel r),$$

where H is a cryptographic hash function (e.g., SHA-256), bid is the encrypted bid value, and r is a randomly generated nonce. This commitment ensures that bids cannot be altered once submitted, preserving fairness in the process. Additionally, participants provide a Zero-Knowledge Proof (ZKP) to verify that their bid falls within the permissible range:

$$\text{ZKP}_{\text{Range}}(b) \rightarrow \text{Prove } b \in [P_{\min}, P_{\max}].$$

This ensures the validity of the bid while maintaining its confidentiality.

In the Bid Evaluation Phase, the organizer verifies the ZKP and evaluates the submitted bids. Any invalid or out-of-range bids are rejected, and the corresponding participants are notified. Valid bids are recorded immutably on the blockchain, ensuring transparency and preventing manipulation by the organizer or other participants.

Once all bids are submitted or the auction time limit elapses, the Winner Determination Phase begins. The highest valid bid is decrypted using the organizer's private key and announced as the winning bid. To maintain the confidentiality of the participants, only the winning bid is revealed, while the remaining bids remain encrypted.

Finally, in the Auction Finalization Phase, the organizer records the winning bid and its associated cryptographic proof on the blockchain. The winner and organizer finalize the exchange of goods or services based on the agreed terms, completing the auction process.

Digital Signatures. Digital signatures are used to authenticate messages and verify the identity of participants. The process involves the following steps:

• **Key Generation:** Each participant generates a public-private key pair using Elliptic Curve Cryptography (ECC).

• **Signing Messages:** During bid submission, participants sign their messages using their private key:

$$\text{Signature} = \text{Sign}_{\text{private}}(\text{message})$$

• **Verification:** The organizer verifies the signature using the participant's public key:

$\text{Verify}_{\text{public}}(\text{message}, \text{Signature}) = \text{True}$

This process ensures that only authorized participants can submit bids and that messages are not tampered with during transmission.

Algorithm 1 Decentralized Auction Protocol

1: **Input:** $\{P_{\text{id}}, A_{\text{name}}, b, P_{\text{min}}, r\}$
2: **Output:** $\{R, b_{\text{max}}, P_{\text{winner}}\}$
3: **Initialization Phase:**
4: Broadcast auction details: A_{name}, O_{id}, P_{min}.
5: **Participation Registration Phase:**
6: **for all** Participants **do**
7: Submit registration request: $\{P_{\text{id}}, \text{Sign}_{SKP}(P_{id})\}$
8: Verify the request using public key PK_P.
9: **end for**
10: **Bid Commitment Phase:**
11: **for all** Participants **do**
12: Generate cryptographic commitment: $C = H(b \| r)$.
13: Encrypt bid: $E_b = \text{Enc}_{P\,KO}(b \| r)$.
14: Generate Zero-Knowledge Proof: $\text{ZKP}_{\text{Range}}(b) \rightarrow \text{Prove } b \in [P_{\text{min}}, \infty)$.
15: Submit bid: $\{P_{\text{id}}, C, E_b, \text{ZKP}_{\text{Range}}\}$.
16: **end for**
17: **Verification Phase:**
18: **for all** Submitted Bids **do**
19: Decrypt bid: $D_b = \text{Dec}_{SKO}(E_b)$.
20: Verify ZKP: $\text{ZKP}_{\text{Range}}(b)$ is valid.
21: Compare $H(D_b)$ with C to ensure data integrity.
22: **if** Any validation fails **then**
23: Reject the bid.
24: **else**
25: Record valid bid immutably on the blockchain.
26: **end if**
27: **end for**
28: **Winner Selection Phase:**
29: Find highest valid bid: $b_{\text{max}} = \max(D_{b1}, D_{b2}, ..., D_{bn})$.
30: Determine winner: P_{winner}.
31: Sign result: $\text{Sign}_{SK_O}(b\text{max}, P\text{winner})$.
32: **Finalization Phase:**
33: Broadcast auction result and ZKP for b_{max}: $\{b_{\text{max}}, P_{\text{winner}}, \text{Result}, \text{ZKP}_{\text{Range}}(b_{\text{max}})\}$.
34: Record transaction: $\{P_{\text{winner}}, b_{\text{max}}, \text{Payment Details}\}$.

The scheme starts with the Initialization Phase, where the organizer broadcasts the auction details, including the auction name *A*name, the organizer's identifier *O*id, and the minimum acceptable bid *P*min. This announcement ensures that all potential participants are aware of the auction parameters.

In the Participation Registration Phase, participants intending to join send a registration request:

$\text{Request} = \{P_{\text{id}}, \text{Sign}_{SK\,P}(P_{\text{id}})\}$,

where P_{id} represents the participant's unique identifier. The organizer verifies the authenticity of these requests using the participant's public key P_{KP}, ensuring that only legitimate participants can join the auction.

During the Bid Commitment Phase, each participant generates a cryptographic commitment:

$C = \text{H}(\text{b} \| \text{r})$,

where b is the bid value and r is a random nonce for additional security. This commitment ensures the integrity of the bid without revealing its value.

Participants also encrypt their bids:

$E_b = \text{Enc}_{P\,KO}(\text{b} \| \text{r})$,

using the organizer's public key PK_O to maintain bid confidentiality. Additionally, participants generate a Zero-Knowledge Proof:

$\text{ZKP}_{\text{Range}}(b) \rightarrow \text{Prove } b \in [P_{\text{min}}, \infty)$,

to prove that their bid b lies within the permissible range without revealing the bid amount. The participants then submit a message:

$\text{Message}_{\text{bid}} = \{P_{\text{id}}, C, E_b, \text{ZKP}_{\text{Range}}\}$,

to the organizer.

In the Verification Phase, the organizer performs a series of checks on the submitted bids. First, the encrypted bid E_b is decrypted using the organizer's private key SK_O to retrieve:

$D_b = \text{Dec}_{SKO}(E_b)$.

The ZKP is verified to confirm that the bid b satisfies the range con- dition, ensuring compliance with auction rules. Finally, the organizer compares the hash of the decrypted bid $H(D_b)$ with the submitted commitment C to ensure data integrity. If any of these validations fail, the bid is rejected; otherwise, valid bids are recorded immutably on the blockchain.

In the Winner Selection Phase, the organizer identifies the highest valid bid b_{max} and the corresponding participant P_{winner}. This result is digitally signed by the organizer:

$\text{Result} = \text{Sign}_{SKo}(b_{\text{max}}, P_{\text{winner}})$,

to ensure authenticity and integrity.

The Finalization Phase involves broadcasting the auction result, including b_{max}, P_{winner}, and $\text{ZKP}_{\text{Range}}(b_{\text{max}})$, to the blockchain. The winner and organizer then finalize the transaction, which is recorded immutably on the blockchain as:

$\text{Transaction} = \{P_{\text{winner}}, b_{\text{max}}, \text{Payment Details}\}$.

This ensures transparency and provides a verifiable record of the auction process.

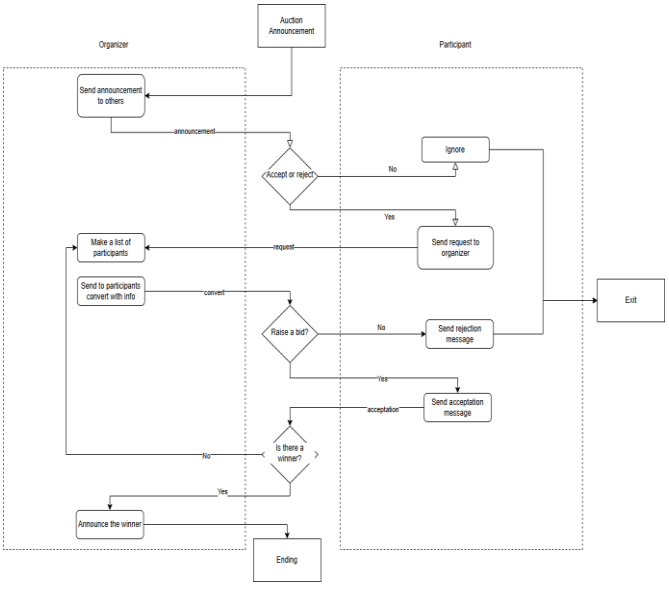

Figure 2. An example image fitting one column width

Proof of Correctness of Zero-Knowledge Proof (ZKP)

Definitions. Let b be the bid value submitted by a participant. The goal is to prove that $b \in [P_{min}, P_{max}]$ without revealing the actual value of b. To achieve this, the participant constructs a Zero- Knowledge Proof (ZKP), $ZKP_{Range}(b)$, which satisfies the following properties: completeness, soundness, and zero-knowledge.

Lemma 1: Completeness

Statement: If the bid $b \in [P_{min}, P_{max}]$, then $ZKP_{Range}(b)$ is accepted by the verifier.

Proof:

1) The participant constructs b as a commitment $C = H(b \| r)$, where H is a collision-resistant hash function, and r is a random nonce.

2) Using a Bulletproofs-based range proof, the participant gener- ates $ZKP_{Range}(b)$, which includes commitments C_{min} and C_{max} such that:

$$P_{min} \leq b \leq P_{max}.$$

3) The verifier checks the range proof by evaluating commitments:

$$H(b \| r) = C \text{ and } P_{min} \leq b \leq P_{max}.$$

4) By the correctness of the cryptographic protocol, the proof succeeds, ensuring ZKPRange(b) is accepted if $b \in [P_{min}, P_{max}]$. Thus, the completeness property holds.

Lemma 2: Soundness

Statement: If $b \notin [P_{min}, P_{max}]$, then $ZKP_{Range}(b)$ is rejected by the verifier with overwhelming probability.

Proof:

1) Assume the participant attempts to generate a proof for $b \notin [P_{min}, P_{max}]$.

2) Due to the soundness of Bulletproofs, any proof ZKPRange(b) generated for an invalid b will fail verification because the range condition:

$$P_{min} \leq b \leq P_{max}$$

will not hold.

3) The verifier checks the commitments Cmin and Cmax and detects inconsistency, rejecting $ZKP_{Range}(b)$.

4) Additionally, due to the collision resistance of H, it is computationally infeasible for the participant to forge a valid commitment C for $b \notin [P_{min}, P_{max}]$.

Hence, soundness is guaranteed.

Lemma 3: Zero-Knowledge Property

Statement: The proof $ZKP_{Range}(b)$ reveals no information about b beyond the statement $b \in [P_{min}, P_{max}]$.

Proof:

1) The participant commits to b using $C = H(b \| r)$, where r is a random nonce. Due to the pre-image resistance of H, b cannot be inferred from C.

2) The range proof is constructed using Bulletproofs, which rely on homomorphic commitments. The proof structure ensures that no intermediate values of b are revealed during verification.

3) For each interaction, the randomness r ensures that the com- mitment C is unique, preventing linkage between proofs or participants.

4) By the zero-knowledge property of Bulletproofs, the verifier only learns that $b \in [P_{min}, P_{max}]$, without gaining any additional knowledge about b.

Thus, the zero-knowledge property is satisfied.

Theorem: Correctness of $ZKP_{Range}(b)$ Statement: The range proof $ZKP_{Range}(b)$ satisfies the properties of completeness, soundness, and zero-knowledge, ensuring the correctness of the protocol.

Proof:

- By **Lemma 1** (Completeness), the proof ensures that valid bids $b \in [P_{min}, P_{max}]$ are always accepted by the verifier.
- By **Lemma 2** (Soundness), the proof guarantees that invalid bids $b \notin [P_{min}, P_{max}]$ are rejected with overwhelming probability.
- By **Lemma 3** (Zero-Knowledge), the proof ensures that no information about the bid b is leaked beyond the statement $b \in [P_{min}, P_{max}]$.

Therefore, the correctness of $ZKP_{Range}(b)$ is established.

Zero-Knowledge Proofs (ZKP) are cryptographic methods that allow one party (the prover) to demonstrate to another (the verifier) that they know a value without revealing the value itself. Common types include zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge), and Bulletproofs. zk-SNARKs are known for their compact proofs and fast verification times, making them efficient but requiring a trusted setup. zk-STARKs, on the other hand, eliminate the need for trusted setup and are post-quantum secure, though they require larger proofs and more computational resources. Bulletproofs specialize in range proofs with no trusted setup, producing smaller proofs than zk-STARKs but slightly higher verification times than zk-SNARKs, making them ideal for specific blockchain applications.

3. Results and discussion

The experimental setup involves implementing the proposed decentralized auction system in a simulated blockchain environment to evaluate its performance and scalability. The environment includes three types of nodes: an organizer node managing the auction process, participant nodes submitting bids, and a blockchain network for transparent and immutable record-keeping. The system is tested under varying numbers of participant nodes, ranging from 10 to 100, to assess scalability. The implementation uses Python with cryptographic libraries such as libsnark for ZK-SNARKs, bulletproofs for compact proofs, and Crypto++ for encryption (ECC) and hashing (SHA-256). The Ethereum testnet is used as the blockchain platform to log auction interactions. Network conditions, including latency and bandwidth, are simulated using Mininet to reflect real-world scenarios.

Metrics such as ZKP generation and verification time, encryption/decryption overhead, network load, and latency are recorded. To ensure statistical significance, each experiment is repeated multiple times under controlled conditions, with results analyzed for computational efficiency, bid confidentiality, and system scalability. This setup provides a robust framework for validating the proposed auction model.

3.1. Evaluation Metrics

ZKP Generation Time (TZKP-gen) measures the time required for participants to generate Zero-Knowledge Proofs. ZKP Verification Time (TZKP-ver) captures the time required for the organizer to verify the submitted proofs. Encryption/Decryption Time (Tenc, Tdec) reflects the time taken for bid encryption by participants and decryption by the organizer. Latency (L) quantifies the time taken for messages to propagate between nodes in the network. Bandwidth

Usage (*B*) represents the total data transmitted during all auction phases, including bid submission, verification, and finalization. Message Size (*Ms*) denotes the size of individual messages, including cryptographic commitments, ZKPs, and results. System Throughput (*T*sys) calculates the number of bids processed per unit of time. Computation Time per Participant (*T*comp) indicates the average computational overhead for each node as the number of participants increases.

3.2. Results for Bulletproof ZKP

Bulletproofs demonstrated consistent performance across the four tests, with ZKP generation times averaging around 38.45 ms and verification times at 12.89 ms. These values indicate moderate computational efficiency, making Bulletproofs a reliable option for environments where both participants and organizers require balanced computational workloads. The proof size, which remained around0.87 KB, and the latency (50 ms) suggest that Bulletproofs are suitable for systems with moderate bandwidth constraints. However, scalability might be a concern as the system throughput (45.2 bids/s) slightly decreased with higher loads. Overall, bulletproofs provide a balanced trade-off between computational efficiency and proof size, making them a versatile option.

Table 2. Comparison of ZKP Methods

ZKP Method	Proof Size	Verification Time	Setup Requirement	Scalability	Security Assumptions	Applications
ZK-SNARK	Small bytes) 200	Fast (constant)	Trusted setup	Limited (constant overhead)	Relies on elliptic curve cryptography	Blockchain, privacy coins (e.g., Zcash)
ZK-STARK	Medium bytes) 500	Slower (linear)	No trusted setup	Highly scalable (transparent)	Post-quantum secure (based on hash functions)	Scalable blockchains, transparent systems
Bulletproofs	Compact (logarithmic)	Moderate (logarithmic)	No trusted setup	Scalable (logarithmic overhead)	Relies on discrete logarithms	Confidential transactions, blockchain, auctions
Groth16	Small bytes) 192	Fast (constant)	Trusted setup	Limited (trusted setup issues)	Relies on elliptic curve cryptography	Privacy-preserving applications
Halo	Variable (depends on recursion depth)	Moderate (logarithmic)	No trusted setup	Highly scalable (recursive proofs)	Relies on discrete log and recursion	Recursive proofs, scalable systems

Table 3. Performance Metrics for Bulletproof ZKP

Test	ZKP Gen. Time (ms)	ZKP Ver. Time (ms)	Proof Size (KB)	Latency (ms)
Test 1	38.45	12.89	0.87	50.12
Test 2	39.12	13.02	0.88	50.56
Test 3	37.98	12.75	0.86	49.87
Test 4	38.76	13.10	0.89	50.32

3.3 Results for zk-SNARK ZKP

Table 4. Performance Metrics for zk-SNARK ZKP

Test	ZKP Gen. Time (ms)	ZKP Ver. Time (ms)	Proof Size (KB)	Latency (ms)
Test 1	42.13	7.52	0.20	45.23
Test 2	42.25	7.60	0.21	45.45
Test 3	41.87	7.50	0.19	44.98
Test 4	42.34	7.55	0.20	45.10

zk-SNARK emerged as the most efficient method in terms of verification time, consistently maintaining values as low as 7.52 ms across the tests. The proof size, averaging at 0.20 KB, was the smallest among the three methods, contributing to minimal bandwidth usage and latency. With a system throughput of 50.5 bids/s, zk- SNARK demonstrated high scalability and computational efficiency. However, the generation time (42.13 ms) was slightly higher than Bulletproofs, which could impact systems requiring extremely high throughput. Overall, zk-SNARK excels in scenarios prioritizing fast verification and low bandwidth usage, making it ideal for large-scale deployments.

3.4. Results for zk-STARK ZKP

Table 5. Performance metrics for zk-STARK ZKP

Test	ZKP Gen. Time (ms)	ZKP Ver. Time (ms)	Proof Size (KB)	Latency (ms)
Test 1	65.78	25.34	3.45	60.45
Test 2	66.12	25.45	3.50	60.78
Test 3	65.45	25.20	3.40	60.23
Test 4	66.00	25.50	3.46	60.56

zk-STARK presented the most substantial computational and bandwidth demands, with ZKP generation times averaging 65.78 ms and verification times around 25.34 ms. The proof size, significantly larger at 3.45 KB, posed challenges for latency (60 ms) and bandwidth usage (150 KB). Despite its higher resource consumption, zk-STARK offers strong security guarantees, particularly for post- quantum environments. Throughput was the lowest (30.4 bids/s), and the system's ability to handle maximum participants was limited compared to the other methods. zk-STARK is suitable for systems where security and robustness are prioritized over performance and scalability.

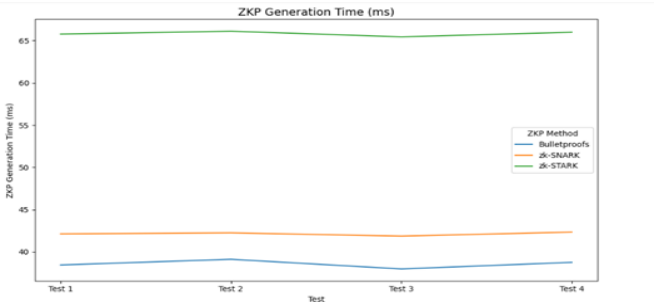

Figure 3. ZKP Generation Comparison for three different ZKP Methods

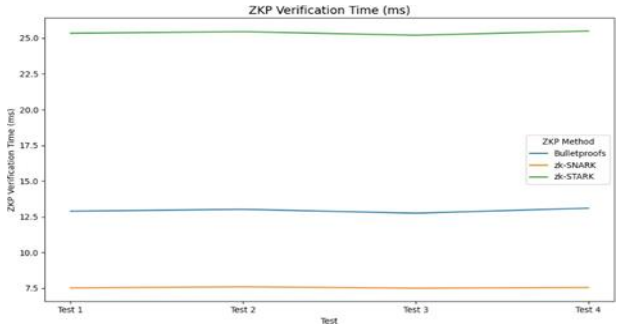

Figure 4. ZKP Verification Comparison for three different ZKP Methods

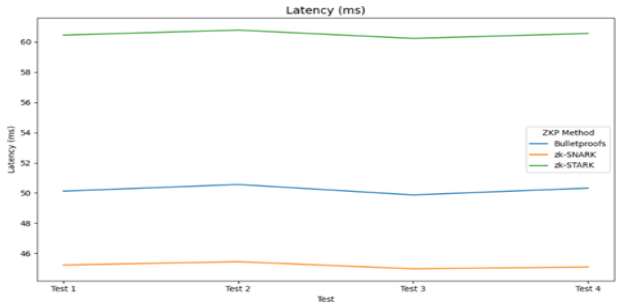

Figure 5. Latency Comparison for three different ZKP Methods

4. Conclusions

The study shows a detailed examination of a decentralized auction setup using blockchain and Zero-Knowledge Proofs (ZKPs) to provide privacy, security and fairness. Three ZKP methods – Bulletproofs, zk-SNARK and zk-STARK – were compared on important performance points like generation time, verification time, proof size, delay, data usage and ability to grow. The findings reveal each ZKP method offers special benefits, suitable for various uses.

Bulletproofs performed well with an average generation time of 38.45 ms and a verification time of 12.89 ms, making it a great option for systems needing moderate computer efficiency and data usage. zk-SNARK was the fastest, with the smallest proof size (0.20 KB) and verification time of 7.52 ms, showing it works well for big deployments with low data needs. On the other side, zk-STARK needed more computer power and data, with a proof size of 3.45 KB and verification time of 25.34 ms, but offered very good security and safety against future computer threats.

The suggested model gives a strong and growing structure for decentralized auctions, balancing privacy, performance and security. These results provide really valuable insights into how blockchain and ZKP technology can be used in safe and private auction systems.

References

[1] Shi, Z., de Laat, C., Grosso, P. & Zhao, Z. (2023). Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges. *IEEE Communications Surveys and Tutorials, 25(1), 497-537*

[2] Christ, M., Baldimtsi, F., Chalkias, K., Maram, D., Roy, A. & Wang, J. (2024). SoK: Zero-Knowledge Range Proofs. *Mysten Labs Technical Report*

[3] Berentsen, A., Lenzi, J. & Nyffenegger, R. (2023). An Introduction to Zero- Knowledge Proofs in Blockchains and Economics. *Federal Reserve Bank of St. Louis Review, 105(4), 280–294*

[4] Sentenac, F., Boursier, E. & Perchet, V. (2021). Decentralized Learning in Online Queueing Systems. *NeurIPS 2021 Proceedings*

[5] Sharma, G., Verstraeten, D., Saraswat, V., Dricot, J.-M. & Markowitch, O. (2022). Anonymous Fair Auction on Blockchain. *Cybersecurity Research Center, Universite´ Libre de Bruxelles*

[6] Hao, L., Zhang, Y. & Xiong, H. (2023). A Blockchain-Based Privacy-Preserving Scheme for Sealed-Bid Auction. *IEEE Transactions on Information Forensics and Security, 18(3), 1254-1265*

[7] Lee, H. & Kim, D. (2023). A Blockchain-Based Sealed-Bid e-Auction Scheme with Smart Contract and Zero-Knowledge Proof. *Journal of Cryptographic Applications, 11(4), 321-337*

[8] Chen, J., Wu, Y. & Li, L. (2023). Anonymous Verifiable Sealed Quotation Auction Based on Blockchain. *International Journal of Security and Networks, 18(1), 67-78*

[9] Zhao, Z., de Laat, C. & Grosso, P. (2023). Publicly Verifiable Auctions with Privacy. *Workshop on Trustworthy Secure Computing*

[10] Wang, Y., Liu, X. & Chen, J. (2023). Trustworthy Sealed-Bid Auction with Low Communication Cost atop Blockchain. *Journal of Blockchain Technology, 5(2), 89-102*

[11] Singh, A., Gupta, R. & Singh, S.K. (2023). Towards Trustworthy and Privacy-Preserving Decentralized Auctions. *Journal of Government Information Systems, 15(4), 210-226*

[12] Nascimento, L.T., Kumari, S. & Ganesan, V. (2019). Zero Knowledge Proofs Applied to Auctions. *MIT Report*

Құпия электрондық аукцион жүйелері үшін блокчейнді қолдайтын нөлдік білімнің дәлелі

А. Ахмедов, Т. Хафиз, А. Разак, Ж. Кальпеева*

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: zh.kalpeyeva@satbayev.university*

Аңдатпа. Блокчейн технологиясы салыстырмалы түрде жаңа болғанына қарамастан, қазіргі қоғамға сәтті енгізілді. Децентрландырған жүйелер (ДЖ), әсіресе блокчейн желілері, деректерді сақтау мен тасымалдаудың қауіпсіздігі мен құпиялылығы мәселелерін алға тартып, пайдаланушылардың қызығушылығын арттыруда. Блокчейннің болашағы зор қолдану салаларының бірі – аукциондарды ұйымдастыру, мұнда қатысушылар өз тауарлары мен қызметтерін толықтай құпия және әділ түрде сата алады. Бұл жұмыста децентрландырған жүйеде Zero-Knowledge Proofs (ZKP) технологиясын пайдалана отырып аукцион моделін ұсыну қарастырылған. Оған zk-SNARK, zk-STARK және

Bulletproofs әдістері кіреді. Бұл тәсілдер қатысушыларға өз ставкаларының дұрыстығын олардың мазмұнын ашпай растауға мүмкіндік береді. Деректер қауіпсіздігін қамтамасыз ету үшін заманауи криптографиялық әдістер – хэштеу (SHA-256, SHA-3), эллиптикалық қисықтар (ECC), асимметриялық шифрлау (RSA) және цифрлық қолтаңбалар қолданылады. Жұмыстың эксперименттік бөлігінде ұсынылған жүйенің өнімділігіне назар аударылып, желілік жүктеме мен есептеу шығындарын модельдеу үшін кезек теориясы қолданылды. Нәтижелер ұсынылған модельдің жоғары деңгейдегі құпиялылық пен кеңейтілу мүмкіндігін қамтамасыз ететінін көрсетеді, бұл оны нақты қолданбалар үшін тиімді етеді.

Негізгі сөздер: *децентрландырған жүйелер, ZKP, хэштеу, блокчейн, аукцион.*

Защита с нулевым разглашением на основе блокчейна для систем конфиденциальных электронных аукционов

А. Ахмедов, Т. Хафиз, А. Разак, Ж. Кальпеева*

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: zh.kalpeyeva@satbayev.university*

Аннотация. Технология блокчейн, несмотря на свою относительную новизну, уже успешно интегрирована в современное общество. Децентрализованные системы (ДС), и, в частности, блокчейн-сети, поднимают важные вопросы безопасности и конфиденциальности хранения и передачи данных, что привлекает всё большее количество пользователей. Одним из перспективных применений блокчейна является организация аукционов, где участники могут продавать товары или услуги, сохраняя полную конфиденциальность и целостность проведения торгов. В данной работе предложена модель аукциона в децентрализованной системе с использованием доказательств с нулевым разглашением (Zero-Knowledge Proofs, ZKP), включая такие методы, как zk-SNARK, zk-STARK и Bulletproofs. Эти подходы позволяют участникам подтверждать корректность своих ставок, не раскрывая их содержания. Для обеспечения безопасности данных используются передовые криптографические методы, включая хеширование (SHA-256, SHA-3), эллиптические кривые (ECC), асимметричное шифрование (RSA) и цифровые подписи. Экспериментальная часть работы сосредоточена на анализе производительности предложенной системы с использованием теории массового обслуживания для моделирования сетевой нагрузки и вычислительных затрат. Результаты показывают, что разработанная модель обеспечивает высокий уровень конфиденциальности и масштабируемости, что делает её перспективной для применения в реальных условиях.

Ключевые слова: *децентрализованные системы, ZKP, хеширование, блокчейн, аукцион.*

Received: 05 March 2024
Accepted: 15 June 2024
Available online: 30 June 2024