Public Ledger for Auctions - Group 26

Diogo Gomes - 201805367
MIERSI
DCC - FCUP

Gabriel Alves - 201709532
MIERSI
DCC - FCUP

Guilherme Bica - 201705374
MIERSI
DCC - FCUP

***Abstract*—This report presents the implementation of a decentralized public blockchain specifically designed for auction transactions. The blockchain system is built using Java and consists of three key components: a secure ledger module supporting Proof-of-Work (PoW) and Delegated Proof-of-Stake (DPoS) consensus algorithms, a secure peer-to-peer (P2P) layer employing Kademlia for data gossiping, and an auction system based on a single attribute English auction. The report provides an overview of the project, describes the implemented components, and discusses the work completed thus far, including the implementation of PoW and Kademlia.**

***Index Terms*—blockchain, PoW, DPoS, P2P, Kademlia**

I. Introduction

The development of a decentralized public blockchain that is especially suited for auction transactions is essential for the following reasons: auctions demand a high degree of transparency and confidence among participants. All auction transactions and activity can be tracked and confirmed among different network users by using a decentralized public blockchain. By generating confidence between buyers and sellers and assuring fairness, this transparency lowers the possibility of fraud or manipulation. Due to their typical centralization, traditional auction platforms are susceptible to single points of failure. By spreading out the auction network among several nodes, a decentralized public blockchain makes sure that no single entity has influence over the system. Decentralization increases the system's resilience by strengthening its defenses against intrusions and guaranteeing constant accessibility of the auction services. To fulfill certain auction prerequisites, a modular architecture enables flexible customization and integration of various components. The blockchain system can be more easily scaled and modified as needed by being designed with modularity in mind. Due to its adaptability, the system can support different auction types, auction rules, and other features without sacrificing its general functionality. Since auction transactions frequently include priceless objects and substantial financial transactions, security is of the utmost importance. The integrity and immutability of auction records are protected by built-in security measures provided by blockchain technology, such as cryptographic algorithms and consensus procedures. Due to the decentralized structure of the blockchain, it is impossible to change the transaction history, creating a reliable and auditable record of auction operations. Specialized features and procedures created specifically for the auction environment can be included in a blockchain created specifically for auction transactions. Smart contracts, for instance, can automate and enforce auction rules to guarantee fair bidding procedures. Between buyers, sellers, and the auction platform, secure communication and verification are made possible through the integration of public key cryptography. Real-time updates and notifications to participants during the auction process can also be made possible by adding a publisher/subscriber system on top of the blockchain [1].

II. System Architecture Overview

The secure ledger module, secure P2P layer, and auction system are interconnected components that work together to facilitate auction transactions within the blockchain. The blockchain system makes it easier to execute auction transactions in a secure and transparent manner by coordinating the actions between the secure ledger, the secure P2P layer, and the auction system. The peer to peer layer enables secure communication and data propagation to nodes in the network, the ledger module ensures the reliability and validity of the auction transaction history, and the auction system offers the required functionality to handle and run auctions inside the blockchain environment [2].

A. Secure Ledger Module

The secure ledger module, which is in responsibility for keeping track of and preserving the auction's transaction history, functions as the foundation of the blockchain system. It guarantees the ledger's security, reliability, and consistency. The module implements the selected consensus algorithm, which may be either Delegated Proof-of-Stake (DPoS) or Proof-of-Work (PoW), enabling the agreement and validation of transactions [3].

B. Secure P2P Layer

The secure P2P layer facilitates the communication and interaction among network nodes in a secure and decentralized manner. It employs the Kademlia protocol, which enables efficient data gossiping and ensures resistance against Sybil and Eclipse attacks.

III. Secure Ledger Module

Proof-of-Work (PoW) and Delegated Proof-of-Stake (DPoS) are two majority decision-making algorithms commonly used in blockchain networks.

A. Proof-of-Work (PoW)

Proof-of-Work is an agreement process in which miners compete to find the solution to a challenging mathematical dilemma in order to add new blocks to the blockchain (mining). Miners must allocate resources to take part in block validation because the challenge demands a lot of processing and energy to complete. Based on the level of difficulty established by the network, miners compete to find a hash value that satisfies specific requirements. The first miner to finish the puzzle announces the answer to the network, where other users are able to verify it. The miner adds a new block to the blockchain when the solution has been verified, which contains a list of verified transactions. For their efforts in resolving the puzzle and validating transactions, miners are paid with cryptocurrency tokens, which are often native to the blockchain network.

1) Advantages of PoW: Security: Due to the computational work needed to solve the problem, PoW offers a high level of security, making it difficult for attackers to alter the blockchain. Decentralization: PoW promotes a decentralized network because anyone with enough processing power can become a miner.

2) Disadvantages of PoW: High Energy Consumption: Mining requires a lot of computational power, which uses a lot of energy and raises environmental issues. PoW may experience scalability problems as the quantity and number of transactions rise, which will result in a delay in the processing time for transactions.

B. Delegated Proof-of-Stake (DPoS)

Delegated Proof-of-Stake incorporates aspects of both a voting-based and a PoW architecture. DPoS tries to establish agreement through a smaller number of trusted block validators, known as ”delegates” or ”witnesses,” as opposed to including all network users in the validation process. In DPoS, the blockchain network's token holders place votes to choose a predetermined number of delegates who would be in charge of validating transactions and creating blocks. Each chosen delegate gets allocated a certain time slot to produce a block, and the delegates create blocks in a round-robin way. As they risk being removed by token holders if they behave fraudulently or fail to perform their duties, validators have an incentive to operate honestly. Reputation mechanisms are frequently used in DPoS networks to evaluate the effectiveness and reliability of delegates, which might affect their chances of getting elected.

1) Advantages of DPoS: Scalability: DPoS can process more transactions per second than PoW because there are fewer validators, which results in quicker confirmation times for transactions. Energy Efficient: Since DPoS does not rely on complex computing calculations, it uses a lot less energy than PoW.

2) Disadvantages of DPoS: Centralization Issues: Because DPoS relies on fewer elected delegates, there is a chance of centralization if a small number of strong entities hold a sizable majority of the voting power. Potential dangers to security: The security of the network may be jeopardized if a delegate's reputation mechanism is compromised or if a majority of delegates conspire [4].

IV. Secure Peer-to-Peer Layer

A. Overview of the Kademlia Protocol

Kademlia is a peer-to-peer (P2P) distributed hash table (DHT) that offers a framework for creating highly distributed applications. Nodes can enter and exit the systems without endangering or interrupting the systems. Without relying on a centralized server, it offers effective lookup and storing of key-value pairs throughout a network of collaborating with nodes. Due to its scalability, fault-tolerance, and resistance to different assaults, Kademlia is frequently utilized in blockchain systems and other decentralized applications [5].

B. Implementation of Kademlia and Key Features

1) Distributed Key-Value Storage: Kademlia organizes participating nodes into a binary tree-like structure called a k-bucket. Each node maintains a set of k-buckets, and each k-bucket represents a range of nodes in the network. Key-value pairs are stored and distributed across the network based on the XOR distance metric, ensuring efficient storage and retrieval operations.

2) Efficient Node Lookup: Kademlia uses iterative node lookup to efficiently locate nodes in the network. It employs a recursive algorithm where each node contacts other nodes that are closer to the target node based on their XOR distance. This iterative process helps rapidly locate the desired node with a minimal number of network interactions.

3) XOR Metric and Routing Table: Kademlia employs an XOR metric to measure the distance between nodes. The metric ensures that nodes close in value are likely to be near each other in the network's overlay topology. Each node maintains a routing table that stores information about other nodes in different k-buckets, enabling efficient routing and lookup operations.

C. Resistance to Sybil and Eclipse Attacks

1) Sybil Attack Resistance: Kademlia is inherently resistant to Sybil attacks, where an attacker creates multiple malicious nodes to gain control or influence over the network. In Kademlia, nodes are identified by their unique cryptographic node IDs. By using cryptographic IDs, an attacker is prevented from producing numerous unique IDs that may be used to impersonate various nodes because doing so would be computationally impossible. Moreover, Kademlia employs the XOR distance metric to determine the proximity between nodes in the network. The XOR distance metric ensures that the attacker would need an impractical number of nodes to have a significant impact on the network's behavior. As a result, in order to substantially change the behavior of the network, an attacker would need to have access to an excessively high number of nodes with IDs that are closer to the target nodes. Attacks via Sybil are problematic and resource-intensive to carry through successfully in Kademlia because of this requirement.

2) Eclipse Attack Resistance: Kademlia also provides inherent resistance to Eclipse attacks, which aim to isolate a target node by surrounding it with malicious nodes controlled by the attacker. In Kademlia, the XOR metric and the iterative node lookup process contribute to the mitigation of Eclipse attacks. During the node lookup process, legitimate nodes iteratively query other nodes in the network to locate the target node. The iterative lookup ensures that even if some malicious nodes are present and attempt to misdirect or prevent the discovery of the target node, legitimate nodes can still find alternative routes to reach the target node. By traversing the network in an iterative manner and maintaining a record of the nodes encountered, Kademlia allows legitimate nodes to circumvent regions of the network dominated by malicious nodes, thereby mitigating the impact of Eclipse attacks. By leveraging the XOR distance metric and the iterative lookup process, Kademlia provides robust resistance against both Sybil and Eclipse attacks, enhancing the security and reliability of the decentralized P2P network. These inherent properties make Kademlia a suitable choice for building a secure and resilient peer-to-peer layer in the decentralized public blockchain architecture for auction transactions.

D. Integration of Trust Mechanisms

Additional trust methods can be incorporated in the Kademlia-based P2P network to increase confidence:

1) Reputation Score: Nodes can be assigned reputation scores based on their behavior and performance. Nodes with higher scores may be considered more trustworthy, and their messages and data may be given higher priority.

2) Web of Trust: Nodes can establish a web of trust by exchanging and validating digital certificates or endorsements. This helps verify the authenticity and integrity of participating nodes and their communications. Consensus-Based Trust: Consensus mechanisms can be used to establish trust among nodes. By requiring multiple nodes to agree on a certain event or transaction, consensus helps mitigate the influence of malicious or untrustworthy nodes [6].

E. Importance of Trust Mechanisms

In a P2P network built on Kademlia, trust measures are essential for creating reliable communication and reducing malicious activity. They aid in ensuring that participating nodes follow the network's policies, uphold a positive reputation, and behave in the network's and its users' best interests. The decentralized network's overall security and trustworthiness are improved through trust mechanisms, which encourage cooperation, deter malicious activity, and encourage good behavior [7].

V. Auction System

A. Auction System Design

The auction system is designed to support sellers and buyers using a single attribute English auction [8].

Auction Creation: Sellers initiate auctions by specifying the item for sale, starting price, bidding increment, and auction duration. The auction is assigned a unique identifier.

Bidding Process: Buyers participate in the auction by placing bids on the item. Each bid includes the bidder's identification and the bid amount. Bids must exceed the current highest bid, and the auction duration may be extended if new bids are received near the end.

Auction Completion: Once the auction duration expires, the highest bidder is declared the winner, and the item is transferred to them. The winning bid amount is also recorded.

B. Transaction Security and Integrity using Public Key Cryptography

To ensure the security and integrity of auction transactions, public key cryptography is used within the blockchain.

Key Pair Generation: Each participant (seller and buyer) generates a public-private key pair. The public key is shared with others, while the private key remains confidential.

Transaction Creation: When a buyer places a bid or a seller initiates an auction, a transaction is created. The transaction includes details such as the auction ID, bid amount, buyer's identification, and a digital signature.

Digital Signatures: The buyer signs the transaction using their private key. The signature verifies the authenticity and integrity of the transaction. The signature can be verified by anyone using the buyer's public key.

Transaction Verification: Other participants and nodes in the network can verify the transaction's integrity by verifying the digital signature using the buyer's public key. The transaction can be added to the blockchain and recognized as genuine if the verification is successful [9].

C. Implementation of Publisher/Subscriber Model on Top of Kademlia

The publisher/subscriber model is implemented on top of the Kademlia protocol to support auctions and facilitate efficient communication between participants.

Auction Publication: Sellers publish auction details (e.g., auction ID, item description, starting price) as messages to the Kademlia network. These messages are propagated to interested subscribers (buyers) within the network.

Subscription and Notification: Buyers interested in specific auctions subscribe to relevant auction topics or specific auction IDs. When a new auction message is published, subscribers receive notifications about the newly created auction.

Bid Placement and Updates: Buyers can place bids on auctions by sending bid messages to the respective auction's participants. These bid messages are propagated through the Kademlia network, ensuring that relevant participants receive the bid updates.

Auction Result Notification: Once an auction is completed, the winner and the auction outcome (winning bid, item transfer) are broadcasted to all interested subscribers. This ensures that participants are informed about the auction results [10].

VI. Assumptions and Limitations

During the architecture design process, several assumptions are made to define the system's behavior and capabilities. These assumptions and limitations can impact the overall functionality and performance of the blockchain-based auction system [11].

A. Network Connectivity

Assumption: Participants have stable network connectivity and can communicate with each other without significant network delays or failures.

Limitation: In reality, network connectivity can be unreliable, and participants may experience intermittent disconnections or high latency. These limitations can affect the real-time nature of auction interactions and introduce delays in message propagation and consensus.

B. Participant Behavior

Assumption: Participants follow the protocol rules, engage in fair bidding, and act in the best interest of the auction system.

Limitation: In practice, participants may deviate from expected behavior and engage in malicious activities, such as collusion, bid manipulation, or attempting to disrupt the system. These malicious behaviors can undermine the fairness and integrity of the auction process, requiring additional measures to detect and mitigate such activities.

C. Computational Resources

Assumption: Participants have sufficient computational resources to perform cryptographic operations, execute consensus algorithms, and process auction-related transactions.

Limitation: Real-world hardware and systems could only be able to perform a certain amount of computing, particularly in circumstances with little resources or when using low-powered hardware. This may have an effect on the blockchain network's efficiency and scalability and put real-world restrictions on the volume and complexity of auction transactions.

D. Scalability and Performance Trade-offs

Assumption: The system can scale to accommodate a large number of participants and handle increasing transaction volumes without significant degradation in performance.

Limitation: Blockchain systems face inherent scalability challenges. As the number of participants and transactions grows, the network's throughput, consensus latency, and storage requirements can become bottlenecks. Balancing scalability with security and maintaining acceptable performance levels is a critical challenge that may require trade-offs and optimizations.

E. Resource Requirements

Assumption: Participants have sufficient storage capacity to store the blockchain's growing transaction history.

Limitation: Blockchain systems, particularly those with non-permissioned public ledgers, accumulate a significant amount of data over time. Storing the entire blockchain history may become resource-intensive for individual participants. The limitations of storage capacity can impact the ability of participants to fully validate and synchronize with the blockchain [12], [13].

VII. Conclusion

In conclusion, the implementation of a decentralized public blockchain specifically tailored for auction transactions has made significant progress, although not all aspects have been fully implemented due to constraints such as limited knowledge and time. Nonetheless, the achieved milestones and the design choices made provide valuable insights into the architecture's potential and highlight areas for further improvement.

The Proof-of-Work (PoW) consensus mechanism, keeps the security of the blockchain by demanding computational work from members to validate transactions and avoid double-spending attacks, was effectively implemented by the secure ledger module. The integration of PoW provides a robust foundation for securing auction transactions and maintaining the integrity of the blockchain.

Furthermore, the implementation of the Kademlia protocol in the secure P2P layer enables efficient communication and data propagation across the decentralized network. Kademlia's key features, including distributed key-value storage and efficient node lookup, contribute to the scalability and fault-tolerance of the system. The resistance to Sybil and Eclipse attacks inherent in Kademlia enhances the security of the P2P network.

Regarding the auction system, the design supports sellers and buyers using a single attribute English auction. Participants can create auctions, place bids, and complete transactions within the blockchain. The utilization of public key cryptography ensures the security and integrity of auction transactions, as each transaction is signed using the bidder's private key and verified using their public key.

While the implementation of a decentralized public blockchain for auction transactions poses challenges, the achieved milestones and the outlined future steps demonstrate the potential for creating a secure, transparent, and efficient platform for conducting auctions. By addressing the identified limitations and continuously improving the system, it has the potential to revolutionize the auction industry and provide a decentralized and trustworthy platform for participants.

References

[1] NIST, *Blockchain Technology Overview*, 2018.

[2] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, 2017.

[3] I. Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*, 2018.

[4] M. Swan, *Blockchain: Blueprint for a New Economy*, 2015.

[5] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in *International Workshop on Peer-to-Peer Systems*, 2002.

[6] A. S. Tanenbaum and M. Van Steen, *Distributed Systems: Principles and Paradigms*, 2016.
[7] A. Oram and D. Stutz, *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, 2001.
[8] J. Leshno, S. Oren, and W. R. Zame, "ebay auctions: Auction mechanisms and the properties of the vickrey auction," *The American Economic Review*, vol. 105, no. 1, pp. 298–335, 2015.
[9] D. Levin, A. Skrzypacz, and T. Rabin, *Online Auctions: Theory and Practice*, 2019.
[10] P. R. Milgrom and R. J. Weber, *Designing Auction Mechanisms: Principles and Practice*, 2020.
[11] S. U. Khan, J. Ahmed, and S. U. Khan, "Blockchain technology: Opportunities and challenges," *Journal of Innovation Knowledge*, vol. 3, no. 3, pp. 112–120, 2018.
[12] P. McCorry, "Blockchain scalability: A guide to blockchain scalability issues and solutions," *IEEE Access*, vol. 7, pp. 46 195–46 209, 2019.
[13] P. De Filippi and A. Wright, *Blockchain and the Law: The Rule of Code*, 2018.