Public Ledger for Auctions

Segurança de Sistemas e Dados

Carlos Santos - 201607406

Professores:
Rolando Martins
João Soares
Eduardo Correia

University of Porto
Faculty of Sciences
Computer Sciences Department
May 2025

1 Introduction

This project was developed as part of the course unit System and Data Security, having as its main goal the implementation of a secure , decentralized public blockchain for auction transactions to run on top of a Kademlia-based distributed hash table (DHT) for peer-to-peer communication and data dissemination, ensuring resilience and efficiency. Unlike Bitcoin and Ethereum, the purpose of this project is to design a decentralized system capable of storing transactions for an auction system.

2 System Architecture

The system was developed based on the following architecture, aiming to provide a clear organization in its implementation.

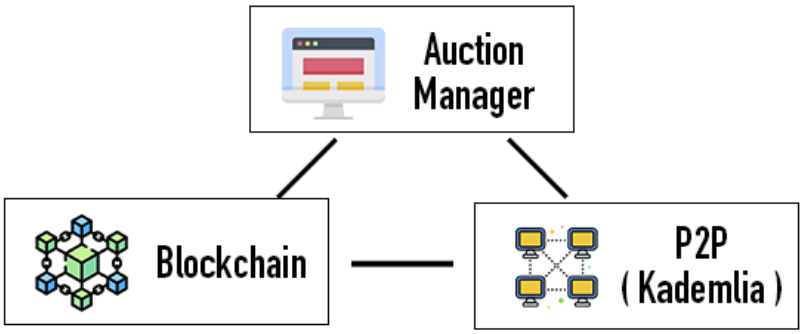

Figure 1: System Architecture

1. **Auction**: This component is responsible for managing auctions and their bids. It includes functionality to create auctions, list active ones, and close them automatically when their time expires. It also provides methods to display detailed information about each auction, including items, bids, and final results, ensuring transparency and efficient control throughout the process.

2. **P2P (Kademlia)**: This component implements a peer-to-peer (P2P) distributed hash table (DHT) network following the Kademlia protocol. It is responsible for managing the network connections between nodes, storing and retrieving data, and disseminating information across the decentralized system.

3. **Blockchain**: This component implements the core logic of a blockchain with a Proof of Work (PoW) mechanism and fork management using

a main chain and conflicting forks.

3 Design

The system uses Proof of Work (PoW) as the consensus mechanism, where all nodes have the capability to validate transactions and add new blocks to the blockchain. Both blocks and auction data are disseminated throughout the network to ensure consistency and transparency. In cases of blockchain divergence (forks), the network resolves conflicts by choosing the longest blockchain, or the one that grows fastest. Blocks from the resolved forks are revalidated, added to the main chain, and then propagated across the network to maintain synchronization among nodes. Auctions have a fixed and static duration defined by the nodes at the time of creation. When an auction concludes, a new block containing the final state of the auction is automatically generated and disseminated throughout the network. This behavior is consistent across all nodes, meaning every node that is aware of the auction follows the same protocol, ensuring uniform state updates across the distributed system.

3.1 Security

The system enforces several rules to ensure authenticity, integrity, and to limit access by malicious nodes. To join the network, a node must be validated by a Bootstrap node, which gives the node a unique identifier. All messages exchanged within the network carry a digital signature created by signing the with the sender's private key, and the sender's public key. This allows recipients to verify message integrity and sender identity. Additionally, all transactions, auctions, and bids are stored in the blockchain, and mined blocks are disseminated throughout the network. By applying these mechanisms, the system becomes more resilient against Eclipse and Sybil attacks, enhancing overall network security.

3.2 Auction Manager

The Auction Manager component is responsible for handling and managing auctions that are created or received from the network. It maintains a HashMap of initialized auctions and a HashMap of auctions received from other nodes. To enable automatic auction completion, a dedicated thread is launched whenever a new auction is created. This thread sleeps until the auction's end time and then triggers the corresponding logic to finalize the auction. The Auction Manager exposes key methods such as creating auctions, listing all auctions, placing bids, among others, to facilitate auction management within the system.

3.3 Blockchain

The Blockchain component has all the logic and management related to the blockchain. It consists of a list of lists of blocks, which allows storing one or more blockchains in the case of forks or divergences. Each block contains a nonce, a timestamp generated when the block is created, a hash, the hash of the previous block, and a transaction carrying all information related to an auction or bid. Importantly, the transaction structure includes a hash of its contents, a signature (which is the hash signed with the private key of the transaction initiator), and the corresponding public key to validate the signature, ensuring the authenticity and integrity of the data.

3.4 Kademlia

The Kademlia interface exposes the methods Ping, Store, Find Node, and Find Value, as well as a join method, which starts the joining procedure. To simplify networking, I used gRPC for the remote procedure calls as listed below:

```
rpc ping(NodeInfo) returns (NodeInfo);
rpc store (StoreRequest) returns (StoreResponse);
rpc findNode (FindNodeRequest)
    returns (stream FindNodeResponse);
rpc findValue (FindValueRequest)
    returns (stream FindValueResponse);
rpc join (JoinRequest) returns (JoinResponse);
```

4 Conclusion

This project successfully demonstrates the design and implementation of a decentralized auction system built on a Kademlia-based peer-to-peer network and secured by a Proof of Work blockchain. The system effectively ensures data authenticity and integrity through cryptographic mechanisms, such as digital signatures and transaction hashing. Architecture promotes decentralization and trust among nodes, with consistent dissemination of auction data and blockchain blocks across the network. However, the project faced significant challenges, particularly in network communication and block propagation using gRPC, which impacted system reliability and fault tolerance. Scalability and efficiency were considered but not attained due to these technical difficulties. Overall, this work lays a solid foundation for a secure and decentralized auction platform, highlighting key aspects of blockchain and distributed systems design while acknowledging areas for improvement in network robustness and scalability.