Course Project Report on

BLOCKCHAIN BASED AUCTION PLATFORM

Submitted in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
INFORMATION TECHNOLOGY
by

ADITYA HEGDE (201IT105)
RAKSHITH JAIN (201IT147)
SATYAM VATS (201IT156)

under the guidance of

Dr. BHAWANA RUDRA

DEPARTMENT OF INFORMATION TECHNOLOGY
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575025

NOVEMBER, 2023

ACKNOWLEDGEMENT

We would like to express our gratitude and appreciation to our course instructor **Dr. Bhawana Rudra**, for her invaluable guidance and expertise throughout this project. She consistently made herself available to discuss about our project. Her insights and feedback were instrumental in shaping the direction of this work.

ABSTRACT

Blockchain technology's impact transcends industries, and our "Blockchain-Based Auction Platform" embodies innovation with the introduction of Blind Auctions. In this report, we delve into the platform's development, where blockchain's security and transparency meet the novel concept of concealed bids, enhancing privacy and fairness.

Traditional auctions often lack privacy, opening doors to insincere bidding practices that erode trust and distort fair market values. To address this, we introduce Blind Auctions, where participants submit sealed bids without knowledge of competitors' offers, fostering genuine price discovery.

This report comprehensively explores our platform's development process, covering system architecture, smart contract design, user interface, security measures, and cryptocurrency wallet integration. Blind Auctions are a central focus, offering enhanced privacy and fairness.

We discuss the implications and advantages of Blind Auctions, setting our platform apart by providing a secure, transparent, and genuine bidding environment. As blockchain and auction industries evolve, Blind Auctions represent a leap forward in ensuring trust, privacy, and fairness in online auctions. This report showcases our platform's development and underscores blockchain's transformative potential in traditional systems, facilitating a more equitable and secure marketplace.

Keywords— Blockchain, User Registration, Immutable, Smart Contracts, Blind Auctions

CONTENTS

LIST OF FIGURES **iii**

1 INTRODUCTION **1**

1.1 Overview 1

1.2 Motivation 2

2 LITERATURE REVIEW **3**

2.1 Background and Related Works 3

2.2 Outcome of Literature Review 5

2.3 Problem Statement 5

2.4 Objectives of the Project 5

3 PROPOSED METHODOLOGY **7**

3.1 System Architecture 7

3.2 Implementation 7

4 RESULTS AND ANALYSIS **11**

4.1 Key Findings 11

5 CONCLUSIONS AND FUTURE WORK **15**

REFERENCES **16**

LIST OF FIGURES

3.2.1 Blockchain Architecture 10

4.1.1 Auction Deploy 12
4.1.2 User Bidding 13
4.1.3 Final Balances after auction 14

CHAPTER 1

INTRODUCTION

1.1 Overview

In the modern era of digital transformation, blockchain technology has emerged as a disruptive force that transcends traditional boundaries, reshaping how industries operate and innovate. Among the many sectors undergoing revolutionary change, the auction industry stands as a notable candidate for transformation. Our project, the "Blockchain-Based Auction Platform," represents a pioneering effort to harness the potential of blockchain in redefining auctions.

The core premise of this report is to explore and detail the development and deployment of our blockchain-based auction platform, featuring a novel feature known as Blind Auctions. Blockchain's core attributes, including transparency, immutability, and enhanced security, form the foundation upon which this platform has been built. By introducing blockchain into the auction arena, we aspire to address some of the persistent challenges that have plagued conventional auction systems.

Our innovation centers around the concept of Blind Auctions, a groundbreaking approach that enables participants to submit concealed bids. This innovation profoundly enhances the privacy and fairness of the auction process, addressing issues such as strategic bidding and lack of transparency that have often hindered the authenticity of traditional auctions.

This report will provide an extensive account of the platform's development journey, covering essential aspects like system architecture, smart contract design, user interface considerations, and integration with cryptocurrency wallets. Moreover, it will delve into the implications of introducing blockchain to the auction industry, underscoring how the core principles of trust, privacy, and fairness can be instilled in the digital auction landscape. In summary, our "Blockchain-Based Auction Platform" offers not only a technological innovation but a reimagining of the auction experience, promising a future where users can trust, transact, and bid with confidence.

1.2 Motivation

The motivation behind embarking on the development of our ”Blockchain-Based Auction Platform” is deeply rooted in the recognition of the fundamental issues that have long plagued traditional auction systems. These issues, including a lack of transparency, security concerns, and the prevalence of strategic bidding practices, have not only undermined the integrity of auction processes but have also eroded the trust of participants. It is this backdrop that has fueled our drive to innovate and create a solution that is more equitable, transparent, and trustworthy.

Blockchain technology, with its inherent characteristics of immutability, transparency, and security, serves as the catalyst for our motivation. We firmly believe that blockchain has the potential to offer a transformative solution to the challenges faced by the auction industry. Moreover, our motivation is further ignited by the introduction of Blind Auctions, an innovative concept that allows participants to submit concealed bids, promoting fairness and authenticity in the auction process.

Our project's motivation rests on the conviction that by integrating blockchain technology and Blind Auctions, we can redefine the auction landscape. We seek to provide a secure and transparent platform where users can participate with confidence, knowing that their bids are private and that the entire process is conducted with the highest level of fairness and trustworthiness.

In conclusion, our motivation is to leverage technology to bring about a substantial positive change in the auction industry, creating an environment where trust, privacy, and fairness are paramount. This project represents our commitment to ensuring that the auction experience of the future is both innovative and deeply rooted in user-centric principles.

CHAPTER 2

LITERATURE REVIEW

2.1 Background and Related Works

[1] This paper introduces a decentralized electronic-based bidding system based on blockchain and smart contracts. The system uses blockchain to replace the traditional database and uses chain code to process business logic. In data interaction, encryption techniques such as zero-knowledge proof based on graph isomorphism are used to improve privacy protection, which improves the anonymity of participants, the privacy of data transmission, and the traceability and verifiable of data.

[2] In this paper, the aim is to provide a prototype of a secure blockchain e-auction system that lowers the uncertainties about identities of long-distance complex trade in an e-auction system that can be implemented in UAE services, especially, UAE Auction. In this implementation, they use smart contracts in order to guarantee the necessary security requirements. The smart contract contains important information about the transaction details such as auctioneer data, the start time and the deadline of the auction, the current winner data, and the current highest price.

[3] In this study, the first decentralized electronic voting and bidding systems based on a blockchain and smart contract are introduced. It also uses cryptographic techniques such as oblivious transfer and homomorphic encryptions to improve privacy protection. The proposed systems allow voters and bidders to participate in the opening phase and improve participant anonymity, the privacy of data transmission, and data reliability and verifiability. Moreover, compared with other electronic voting and bidding systems, the systems are safer and more efficient.

[4] In this paper, the smart contract, proposed in 1990 and implemented via the Ethereum platform, can ensure the bill is secure, private, non-reputability and inalterability owing to all the transactions being recorded in the same but decentralized ledgers. The smart contract is composed of the address of the Auctioneer, the start auction time, the deadline, the address of the current winner, and the current highest price. In the experiments, the accounts are created through the Ethereum wallet. In the miner stage, the MinerGate is used in miner stage for obtaining money to pay the

transaction fee. At the recorder stage, the nodes of the blockchain are synchronized to generate smart contracts

[5] In paper "Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges“,This paper discussed about various representative auction model types which are very important for the blockchain integration to auctions.We got different auction mechanisms ,scenarios and solutions through which we can handle the auction.Limitations found in this paper are :- auction privacy protection, transaction ordering fairness, decentralization of auction front-end.

[6] In paper "An anonymous and fair auction system based on blockchain“, September , 2022:This paper used IPFS(interplanetary file system) a distributed file system in order to address the issue of excessive file redundancy. It showcases the signature scheme to generate and verify the key for the auction messages in order to maintain the privacy effectively. Some Limitations of this paper are:- This process is a lot more complex than the existing as using IPFS for storing auction details and implementing the generation of keys.

[7] The paper "Secure Online E-Auction System using Blockchain Technology" designs an online system using blockchain technology and smart contracts. They developed a user-friendly, reliable, trustworthy, and secure web application for the auction of electronic goods and items. They have used css, html, react js, AI, machine learning, chatbots, Ui path for automation on the frontend, and MySQL, MongoDB on the backend to fetch data from the database.There are different modules for seller, bidder and admin with the provision of report generation as well.

[8] This paper "Blockchain Based M+1st-Price Auction With Exponential Bid Upper Bound" describes the famous m+1st auction that sell identical goods to b bidders. The top m winners can buy the goods at m+1st price. The bidders send their bids secretly to manager as a bidding vector. In their proposal, the role of manager was done by a smart contract. By utilizing Smart Contracts, binary format bidding vector and the ZkAnd zero-knowledge proof, they built the first secure M+1 st-price auction protocol that can reach an exponential bid upper bound without a manager and SHE or FHE. The invention can not only be used in sealed-bid auction protocols but can also be used in cryptographic protocols that need to compare secret values such as the Millionaire's Problem and Multi-Party Computation.

2.2 Outcome of Literature Review

Smart contracts are a fundamental aspect of blockchain technology. Literature survey discusses how smart contracts can automate and streamline various auction-related processes, such as bid validation, payment, and asset transfer. Ethereum, Known for its smart contract capabilities, Ethereum is often chosen for building decentralized applications, including auction platforms. Hyperledger Fabric, A permissioned blockchain platform that offers high customization and privacy features, making it suitable for enterprise-level auction applications. Cryptographic hash functions like SHA256 are used to create fixed-size, irreversible representations of data. These hashes are used in blockchain transactions and blocks to ensure data integrity. Since many blockchain-based auctions involve digital assets, integrating cryptocurrencies is common. Some papers incorporate wallets and payment gateways to facilitate transactions in cryptocurrencies like Ethereum (ETH) or other tokens.

2.3 Problem Statement

In traditional blockchain-based auction platforms, transparency and privacy concerns persist as participants can view each other's bids, leading to strategic and insincere bidding practices. This lack of privacy hampers genuine price discovery and fairness, undermining the auction process. The challenge is to enhance user privacy and promote honest bidding while maintaining the benefits of blockchain technology in our auction platform.

2.4 Objectives of the Project

(1) Implement blockchain technology to ensure transparency by recording all auction transactions and bid histories on an immutable ledger. This transparency will provide participants with equal access to information, fostering trust in the auction system.

(2) Enhance security by leveraging blockchain's robust cryptographic techniques to safeguard valuable assets and transactions, reducing the risk of fraud and

unauthorized access.

(3) Improve efficiency by automating various auction processes, such as bid verification and payment processing, thereby reducing the time and labor required and minimizing the need for intermediaries in the traditional auction model.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 System Architecture

A. Development Environment :-

The system uses ethereum server and solidity as the software for development, the system comprises interaction of blockchain technology, smart contracts and miners for transactions.

B. Auction Process :-

The proposed system takes details of the product from the seller and is been passed to the auctioneer , the auctioneer verifies and post it on the system with initial bid price , it allows the bidders (users) to bid on the product and if user 1 placed a bid which is lower than the user 2 then the user1 gets notified so that if he wants to bid more he can , in this the bidding continues to take place until the final day of placing the bids takes place. The auctioneer announces the highest bid in the system without mentioning the bidders details , so that the transparence should be maintained. The highest bidder gets notified and a smart contract is been made between the bidder and the auctioneer , and a time is given to the bidders to contact with the miners for transaction of the value , the system used for transaction is ethereum wallet when the auctioneer verifies that he has received the transaction the product transfer takes place . Then the funds are transferred to the seller .

3.2 Implementation

In the initialization data, we will announce the following information in advance. Auctioneer: The tenderer address used to record the originating contract. startblock: Used to denote the time of the contract. Endblock : Used to denote the ending time of the contract. highestBidder: The address of the bidder who currently bids the product with the highest price. highestBid: Used to record the current highest price.

- Functions :

  We define the following functions :-

  Auction(): The auctioneer announces the item or service to be auctioned and sets the rules, including the starting bid, minimum bid increment, and the deadline for submitting bids.

  Bid(): This function can be called by any person to perform the bidding action. Before the function is executed, AuctionStart and biddingTime are used to judge whether the contract is expired. The contract system will use highestBid and highestBidder to record the current highest price and the corresponding bidder's address.

  reveal(): Opens the bid by calling this function, and compares the prices of all the tickets to get the final winner.

  AuctionEnd(): In this function, AuctionStart and biddingTime are automatically used to determine the contract validity time. If the effective time ends, the successful bidder's Address and the current highest price will be automatically sent to the tenderer. This function will be disabled to avoid repeated execution.

  withdraw(): Returns the amount of bids tendered by bidders other than the successful bidder.

- Blind Auction :

  A blind auction is a type of auction in which bidders submit their bids without knowing the bids of other participants. The highest bidder wins the auction, and the amount they bid is the price they pay for the item or service being auctioned.

  1) Everything Implementations are same as the normal auction. But some rules and procedures are there in the blind auction.

  2) In order to make the bids sealed and confidential, the bid is represented by a hash produced by the keccak 256 hash function, an implementation of the SHA-3 hash algorithm. Bid hash hides the bid value. It is not possible to know the bid value until a later time when the bid is revealed. So far, only the deposit is known and required to make the bidder commit by depositing an amount with

the bid.
3) The bidder's deposit may differ from the enclosed bid value, which might confuse the competition by making them estimate the bid value based on the deposit. The bid value cannot exceed the deposit, but it can go as low as 0.

- Blind Auction Advantages:
  Reduced Strategic Bidding: In a traditional open auctions, bidders often engage in strategic bidding by trying to gauge the competition and bidding accordingly. This can result in inflated or inefficient prices. In a blind auction, bidders are not aware of the other participants' bids, reducing the incentive for strategic bidding. Bidders are more likely to bid their true valuation, leading to potentially fairer prices.
  Enhanced Privacy: Blind auctions provide more privacy for bidders. Participants do not need to reveal their intentions or valuation publicly, which can be especially important in sensitive or high-value auctions.
  Increased Participation: Blind auctions can attract more participants, as bidders may be more willing to engage in an auction where their bids are confidential. This increased participation can lead to more competitive pricing.
  Fairness and Equal Opportunity: Blind auctions promote fairness by ensuring that all bidders have an equal opportunity to participate and win without being influenced by the actions or knowledge of other bidders.

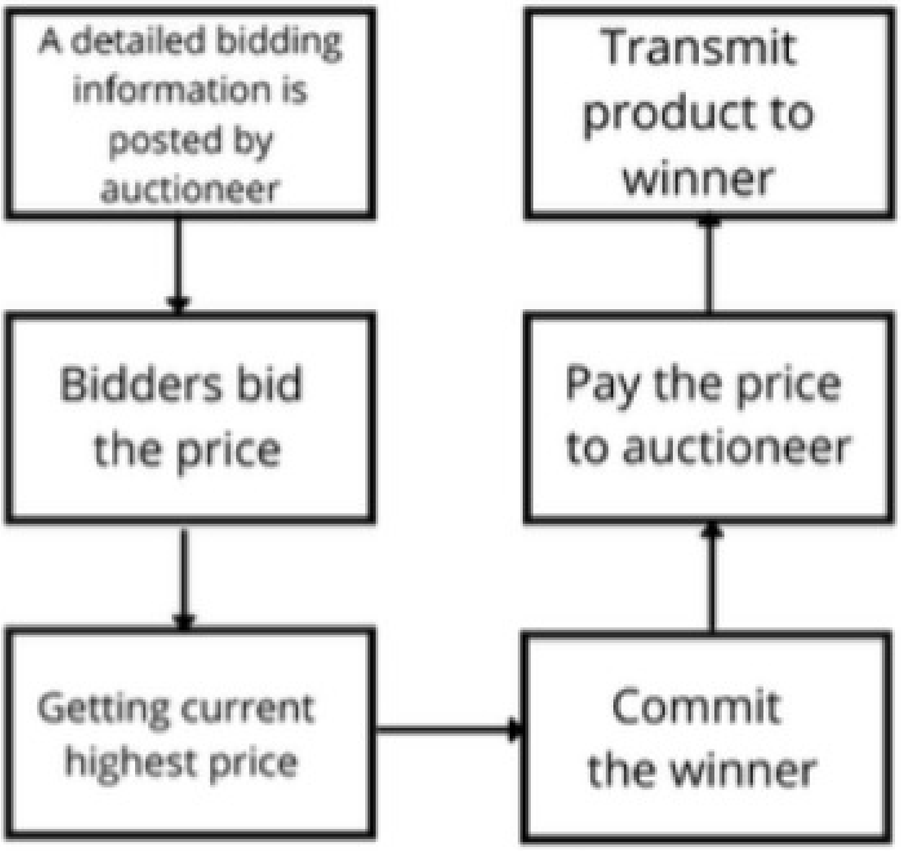

A detailed bidding information is posted by auctioneer
Bidders bid the price
Getting current highest price
Commit the winner
Pay the price to auctioneer
Transmit product to winner

Fig. 2: Flowchart of E-auction

Figure 3.2.1: Blockchain Architecture

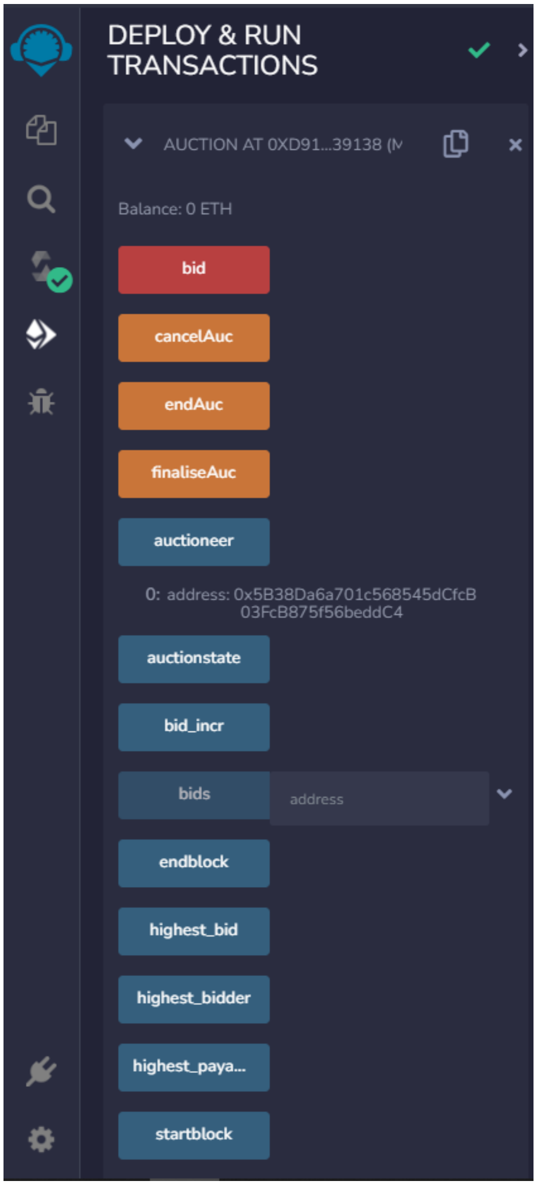
CHAPTER 4

RESULTS AND ANALYSIS

4.1 Key Findings

The developed ”Blockchain-based Auction System” project has yielded promising results, showcasing the potential for enhancing security and data integrity. The key achievements and findings of this project include:

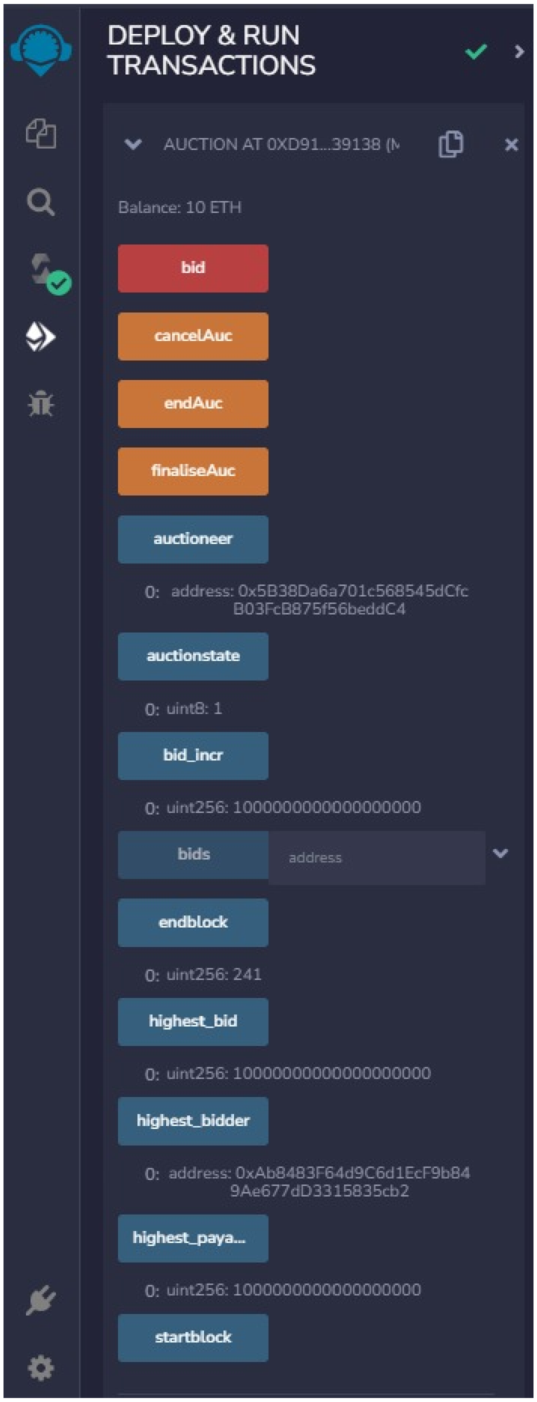
The use of blockchain technology in auctions can offer several advantages and improvements to the traditional auction process. We Implemented a auction system in which users can bid and buy the required products in a very transparent and secure system. We built smart contracts for the bidding, finalising and withdrawing processes, which automates various aspects of the auction process, such as bid verification, countdown timers and payment release upon successful bids. We also implemented a special novel blind auction in which users will not be knowing the highest bid and will bid without the competition prices. They will also profit the auctioneer with the more highest bid-prices.



Balance: 0 ETH

```
0: address: 0x5B38Da6a701c568545dCfcB
            03FcB875f56beddC4
```

Figure 4.1.1: Auction Deploy



Balance: 10 ETH

auctioneer: 0: address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

auctionstate: 0: uint8: 1

bid_incr: 0: uint256: 1000000000000000000

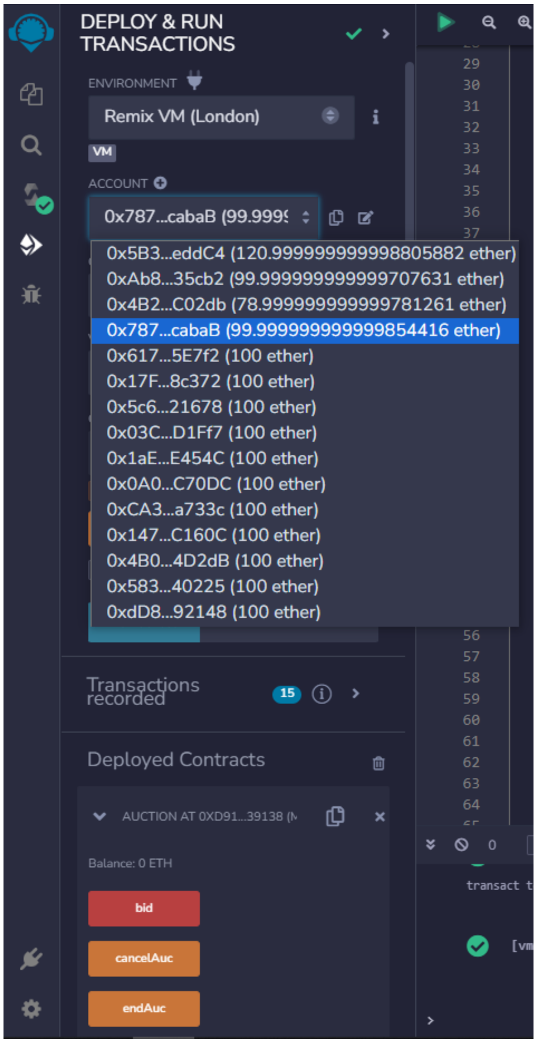
endblock: 0: uint256: 241

highest_bid: 0: uint256: 10000000000000000000

highest_bidder: 0: address: 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

highest_paya...: 0: uint256: 1000000000000000000

Figure 4.1.2: User Bidding



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Remix VM (London)

VM

ACCOUNT

0x787...cabaB (99.9999

```
0x5B3...eddC4 (120.999999999998805882 ether)
0xAb8...35cb2 (99.999999999999707631 ether)
0x4B2...C02db (78.999999999999781261 ether)
0x787...cabaB (99.999999999999854416 ether)
0x617...5E7f2 (100 ether)
0x17F...8c372 (100 ether)
0x5c6...21678 (100 ether)
0x03C...D1Ff7 (100 ether)
0x1aE...E454C (100 ether)
0x0A0...C70DC (100 ether)
0xCA3...a733c (100 ether)
0x147...C160C (100 ether)
0x4B0...4D2dB (100 ether)
0x583...40225 (100 ether)
0xdD8...92148 (100 ether)
```

Transactions recorded 15

Deployed Contracts

AUCTION AT 0XD91...39138 (M

Balance: 0 ETH

Figure 4.1.3: Final Balances after auction

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

In conclusion, our ”Blockchain-Based Auction Platform” has ushered in a new era of innovation within the auction industry by seamlessly integrating Blind Auctions and blockchain technology. This successful project has realized our objectives of enhancing auction privacy, promoting fairness, ensuring transparency, and improving user experience, reaffirming the transformative potential of this initiative.

The introduction of Blind Auctions, where concealed bids are submitted, has effectively addressed longstanding challenges, fostering an authentic and secure auction environment. Blockchain technology has played a pivotal role in ensuring transparency, immutability, and enhanced security. The user-centric design, marked by a user-friendly interface, has elevated the overall auction experience.

Beyond the immediate project scope, this innovation has the potential to inspire a broader industry shift, encouraging the adoption of similar technological advancements that prioritize trust, fairness, and user satisfaction.

Looking to the future, our project's continuation will involve exploring additional auction formats, expanding cryptocurrency support, and enhancing scalability to accommodate a growing user base. User experience refinements, gamification, and heightened security measures will remain central to our development efforts. Collaborations with industry stakeholders and regulatory bodies will further solidify our compliance with evolving auction regulations. The trajectory of our blockchain-based auction platform is defined by ongoing innovation, ensuring it remains at the vanguard of the dynamic online auction landscape.

REFERENCES

[1] Jindong Zhao Dan Wang and Chunxiao. Research on blockchain-based e-bidding system. MDPI Journal, 2021.

[2] Vishwesh Akre Hani Qusa, Jumana Tarazi. Secure e-auction system using blockchain: Uae case study. 2020 Advances in Science and Engineering Technology International Conferences (ASET), 2020.

[3] Jen-Ho Hsiao Raylin Tso, Zi-Yuan Liu. Distributed e-voting and e-bidding systems based on smart contract. MDPI Journal, 2019.

[4] Yi-Hui Chen; Shih-Hsin Chen; Iuon-Chang Lin. Blockchain based smart contract for bidding system. 2018 IEEE International Conference on Applied System Invention (ICASI), 2018.

[5] Paola Grosso-Zhiming Zhao Zeshun Shi, Cees de Laat. Integration of blockchain and auction models: A survey, some applications, and challenges. Nov 2022.

[6] Wei Weng Zongli. Ye. An anonymous and fair auction system based on blockchain. Sept 2022.

[7] Prashant Kumbharkar; Nagarjuna Balla; Vaibhav More; Adarsh Choudhar. Secure online e-auction system using blockchain technology. 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 2023.

[8] Po-Chu Hsu; Atsuko Miyaji. Blockchain based m+1st-price auction with exponential bid upper bound. IEEE Journals, 2023.