AUCTION BIDDING BASED ON BLOCKCHAIN

OBJECTIVE

- Introduction
- Sealed bid
- Implementation
- Conclusion
- Future scope
- References

INTRODUCTION

- Blockchain is **a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system**. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.
- Blockchain is a list of records called blocks that store data publicly and in chronological order. The information is encrypted using cryptography to ensure that the privacy of the user is not compromised and data cannot be altered. The information is stored and managed in a decentralised manner hence no central authority is the sole decision maker. Instead, most decisions are based on a consensus of all the participating nodes of the network spread all over the world.

Ethereum

Ethereum is a blockchain-based decentralized platform featuring smart contract functionality. Smart contracts in Ethereum can facilitate and verify the process of a contract, base on the powerful Ethereum virtual machine (EVM). The mechanism supports for Turing–complete scripting, and thus makes it feasible for us to design various applications. Meanwhile, smart contracts also inherit the blockchain's properties on decentralization, immutability, and verifiability. For example, after deployed to Ethereum, the smart contract code cannot be modified by any user even for its creator.

Smart Contract

A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.
Smart contracts are a type of Ethereum account. This means they have a balance and they can send transactions over the network. However they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.

Blockchain e- Auction

e-Auction improves the efficiency of bid transaction. However, the protection of bidders' privacy, transaction fairness and verifiability, transaction data security, high cost of third-party auction center, and other issues have attracted more attention. According to the transaction process and basic principles of the sealed auction, we explored the problems existing in the current sealed-bid e-auction schemes. Based on the blockchain technology, we proposed a sealed-bid e-auction scheme with smart contract technology . We conducted the experiment to show that the proposed scheme protected the bid information from leakage well and successfully verified the winning bid price and the related bidder by all transaction participants without the third-party auctioneer.

Some common types of Auction

- **The English Auction:-** The most common of the auction formats, goods are sold to the highest bidder with bids taking place in ascending order. Frequently, a reserve price must be met. The reserve price is the lowest price at which the auctioneer will sell the goods. This price is sometimes disclosed to the bidders and sometimes not.

- **The Dutch Auction:-** bidding starts at an extremely high price and is progressively lowered until a buyer claims an item by calling “mine,” or by pressing a button that stops an automatic clock. When multiple units are auctioned, normally more takers press the button as price declines. The first winner takes his prize and pays his price and later winners pay less. When the goods are exhausted, the bidding is over.

- **The Vickrey Auction:-** It is also known as the second-price auction. Bids are sealed and the item is awarded to the highest bidder but at a price equal to the second highest bidder's price. If, for example, three bids are received, one for $100, one for $90 and one for $75, the winner will be the $100 bidder. However, the winner will only have to pay $90, the second highest bidder's price.

- **The Sealed Bid Auction:-** As the name implies, this auction uses a sealed bid, where each bidder is allowed to bid only once. Generally, there are two steps to the process. First, the requirements are established by the buyer and, second, the sealed bids are opened. The highest qualified bidder receives the goods or, in the case of a service, the lowest qualified bid wins.

- **The Reverse Auction:-** In a Reverse Auction, the seller provides bids for a seller's requirements. At the end of an allotted period of time, the bid is awarded to the lowest priced, qualified supplier.

SEALED BID AUCTION

- sealed-bid auction is also referred to as a **blind-auction.** This is because the bidders in a sealed bid auction have no knowledge of what the other bidders are submitting. Traditionally, each of the participants will place their bid in a sealed envelope to be opened by the auctioneer. Then the best bid wins.
- A sealed-bid auction is a type of auction in which bids are not viewed until the auction date.
- The bids are sealed, often physically in an envelope, and are all opened at once.

- Sealed-bid auctions are generally used in bidding for government contracts.
- Unlike an open bid, where buyers can make multiple bids and compete against each other actively, in a sealed-bid auction, they only get once chance.

IMPLEMENTATION

- **Remix IDE:-** Remix is most commonly referred to as Remix IDE (Integrated Development Environment), although this is somewhat of a simplification. It is an open-source web and desktop application, a development environment, if you will. It packs a rich set of plugins and fosters a fast development cycle via intuitive GUI. Moreover, Remix IDE is primarily used for the entire process of smart contract development. In addition, it serves as a playground for teaching and learning how to use the Ethereum network.

Functions

1:-placeBid() :- It make sure transfer is done , bid is actually recorded inside our objects and we will map.

2. withdraw() :- Once auction is ended , each person will come in and call this function to withdraw the funds they initially bid and didn't win.

3. reveal() :-Once auction is ended then we pay out whoever needs to be paid but before that we are going to reveal all the bids and reveal what was the highest bid.

4. bid() :- It is used to record the bids that will be placed during the auction **.**

5. auctionEnd() :- This function is called when we auction get to end and then whoever is the beneficiary gets the money after the end of the reveal time.

6. generateBlindedBidByte32() :- when the bidder puts the bid , it returns the hashed value of the bid so that no one can know who made the bid until the reveal period **.**

CONCLUSION

The proposed sealed-bid e-auction scheme showed the following features:

(1)**Sealability -** All information in the auction transaction was encrypted by the public keys of the smart contract, owner, and bidders, which prevented the information from leakage. The bid price was only passed to the smart contract other than published on the blockchain.

(2)**Fairness -** All bidders were equally treated by the smart contract. They got all commitment prices and the winning commitment price . Then, they verified the auction result autonomously. If bidders tried to tamper with the auction result, their auction security would be confiscated and their permissions to the auction transaction were also frozen or cancelled. The punishment was conducted automatically by the smart contract.

(3) **Cost-Effective** - The scheme was free of the cost of the third-party auctioneer, which made the biggest benefits of all auction parties.

(4)**Validity** - The smart contract selected the winning bid price and the related bidder as the auction result, which obeyed the basic rule of the first-price sealed auction.

(5)**Nonrepudiation** - All information in the auction transaction was saved in the blockchain and can never be denied under the consensus mechanism of blockchains.

(6)**Decentralized Verification** - All bidders can verify and prove the auction result with zero-knowledge proof protocol .None of them can deny the bid price.

FUTURE SCOPE

In this project, accuracy is a great point of concern. There are many areas where we can improve our system. Few of them are listed below.

•We can implement other different types of auction using solidity language and its oops concepts.

•More security can be provided in terms of auction bidding to ensure smooth and fair bidding.

•Frontend part can be added to take input from it and show output on it and not all functionalities need to run by us.

REFERENCES

1. Verifiable Sealed-Bid Auction on the Ethereum Blockchain by Hisham S. Galal and Amr M. Youssef Concordia from Institute for Information Systems Engineering, Concordia University, Montr´eal, Queb´ec, Canada

2. Designing smart-contract based auctions by Chiara Braghin1 , Stelvio Cimato1 , Ernesto Damiani1,2 , and Michael Baronchelli . Centre on Cyber-Physical Systems, Khalifa University, Abu Dhabi, UAE

3. https://cloudname.com/en/what-is-metamask/

4. https://moralis.io/remix-explained-what-is-remix/

Thank You

Anurag Upadhyay

Aman Singh

Anshuman Bhargava

Dikshita Bhatia