RES MILITARIS Social Science Journal

SEALED-BID AUCTIONS REINVENTED: HARNESSING BLOCKCHAIN SMART CONTRACTS FOR TRANSPARENCY AND SECURITY

[#1]GUDELLI ABHISHEK,
[#2]BITLA SHASHIPREETHAM,
[#3]R.HARITHA, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: On the inside and the outside.One of the tools that allows people to bid on auctions online is the e-auction. To facilitate transactions between buyers and sellers in the event of a hidden bid, third parties may be required to pay higher costs. However, you should be aware of the risk of being misled by unreliable sources. An auction's administrator or owner may have unfettered access to the sale when it's hosted on a decentralized platform. A blockchain-based asset's smart contract takes over as owner and oversees the bidding process when it goes up for auction. In this study, we created an Ethereum blockchain-verifiable smart contract for sealed-bid transactions. In a sealed-bid auction, all participants remain anonymous and just one bid is accepted from each buyer. A winner is determined by the largest amount offered in the proposals. Before the auction is over, a bid can be retracted. The buyer will be given a second chance to place a bid in this scenario. This implementation of the smart contract is analogous to a sealed bid in that it reveals just the highest bid. Participants in the bidding process are not given any more information.

KEYWORDS:Blockchain, Ethereum, Metamask, Remix IDE, Smart Contract, Sealed-bid Auction.

1. INTRODUCTION

To cut down on expenses, blockchain is built on the idea of using network-based tendering tactics. Auctioneers, bidders, and others use the electronic bidding approach. The auction website is a collaborative effort between the seller, the buyer, and the third-party organizers, who all have a role in displaying product listings, updating the highest bid, and other features. Companies like eBay and Yahoo benefit from this auction format.

However, there are two common problems with online auctions. To begin, transaction costs may be increased by the high fees charged by centralized third parties. Personal or financial details stored in the database may also be vulnerable to intrusion. Second, the bidder's viability as the frontrunner is not revealed to the other competitors until the envelope is opened. These questions are answered in this essay, which investigates the use of blockchain technology in online auctions. This method uses a decentralized network in which no one entity (here, a website) needs special permission from any other entity to exchange information with, verify information from, or transmit information to itself or any other entity. The associated transaction expenses are decreased. Smart contracts, on the other hand, can deal with a misleading lead offer.

2. E-AUCTION

Traditional Bidding System

E-auctions are a digital version of traditional auctions. To obtain the auctionable items, thus, online bidding tournaments are used. The owner or manager of the sale sets the start and end times. Online bids must be received by the due date once the e-auction has begun. The results of an online auction are made public once the deal has been finalized and a report has been created. After the successful bidders have paid the appropriate deposit, the seller will release the item for pickup.

Online auctions can be either open to the public or private. Those who are interested in buying an item can bid more for it throughout the public proposal process. As a result, the amount being offered for sale goes up until no one is ready to go any higher. The winner of an item is the one who bids the most money for it. Multiple bids are acceptable in an open auction. The term "public offer" can also refer to a public proposal. The

bidders send the encrypted invoice once. A hidden proposition is what you have here. If there's enough time, the auctioneer will compare the two bills side by side. The highest bidder in the clandestine sale was the victor. The auction is sometimes called a "single-bidding sale" to reflect the fact that each bidder is limited to submitting a single offer. Until the proposals are opened and compared, no party knows the other's pricing. Our regular problems with electronic seal ticket auctions stem from the fact that we have no way of knowing whether or not the other bidders' prices were made public before the auction closed.

Blockchain

Data from the network is monitored and validated at many nodes before being transmitted. An autonomous information repository and administration system is built using a P2P network.

The following tools are essential for the operation of a blockchain:

Identity identification and security:

To verify identities and avoid fraud, a public key infrastructure is used. There are two types of keys associated with every blockchain account: public and private. The recipient then uses the sender's public key to decrypt the encrypted transaction message. This proves that the correspondent is who they say they are.

Message delivery and broadcasting:

Each server can connect to the network and have conversations with other nodes thanks to the use of peer-to-peer technology for the transmission and distribution of messages. A single file is used to record all financial dealings. Each node in the blockchain may verify events, even if its users don't understand the decentralized access structure

.**Data preservation and linking:**

Block chains are seen in construction in Figure 1. Each block is connected to the one before it using the hash values calculated from the transaction data contained in that block. The characteristics of the block are shown in Figure 2. A hash value, the number of transactions, a timestamp, etc. are all examples of the types of data that make up a block's records.

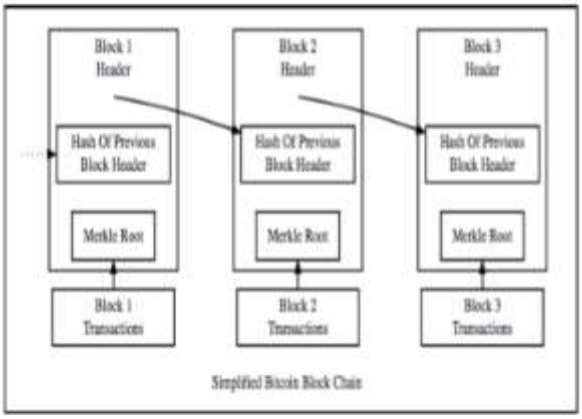

Fig. 1: Blockchain block structure design

There are six parts that make up the block's brain: The version number of the program. Reference to the section number up top. A block's worth of transactions can be used to derive the Merkle tree's root hash. It looks like the illustrated hash for the Merkle tree's root.

Total elapsed time since midnight, January 1, 1970 UTC.

The goal of this work.

The proof of work is complete when the nonce changes. A valid hash is estimated by the miner to be less than the target hash in this process.

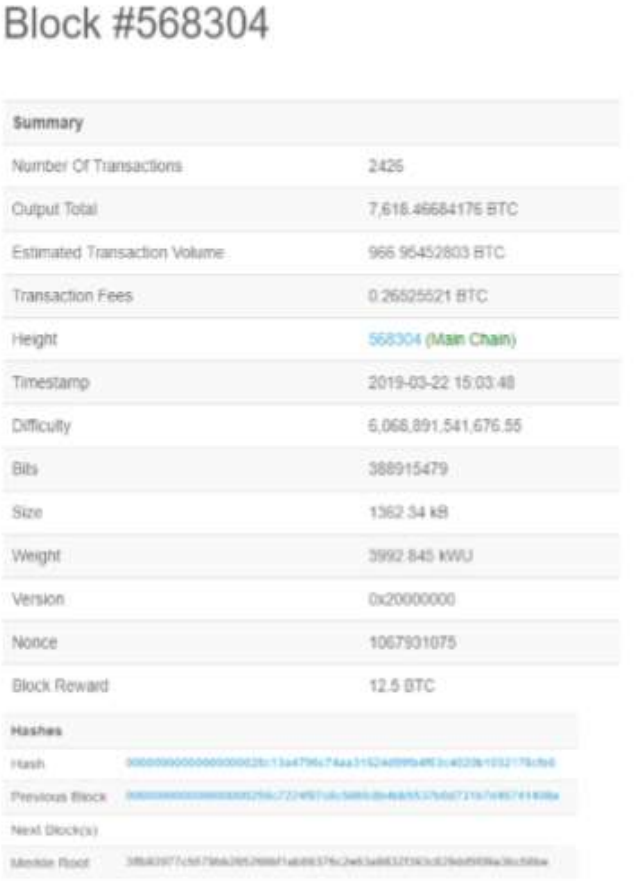

Fig: 2: Fields in a block

3. RESEARCH METHOD

The supplier puts forth bid details, including a description of the product and an initial offer price. Votes for the unopened package are highest among those who want to buy the more expensive item. After removing the lid, the auctioneer announces the highest bid. When the maximum bid is achieved or a higher bid is received, the highest bidder wins. The auctioneer will be compensated if the item is purchased from them. To create a transparent bidding process, we use blockchain and smart contracts. The trade agreement for the candidates' proposals will be recorded on the blockchain. Any interested party can place a bid on the goods by invoking the trade contract of the open contract thanks to the decentralized access mechanism.

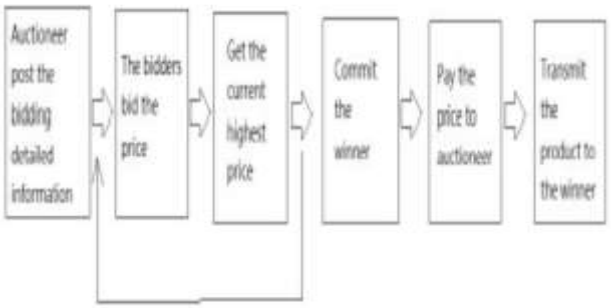

Fig. 3: The flowchart of E-auction

- The following requirements must be met by any public E-auction platform: The winner (the highest bidder) is a secret.
- The accuracy and completeness of the seal order can be independently checked by all parties involved in a transaction.
- Those who aren't supposed to be bidding on the item shouldn't make it look like they are. An accepted offer is final and cannot be revoked.
- All necessary paperwork is in the possession of the auction winner at all times. The supplier is only obligated to take the higher of the two bids.The envelope is invalid if it is not received by the specified date. The contents of the sealed envelope are secret and must remain so until the deadline has passed. If two suppliers provide the same price, a fair solution must be found.
- A smart contract is a data set and set of algorithms built on the Ethereum platform. When a certain condition is met, such as the exchange of information or the passing of time, the smart agreement begins to take effect. Solidity, Serpent, LLL, and Ether Script are all valid contracting languages. A smart contract's JSON-redeemed bytecode is used to send a message to every node on the blockchain and then wait for proof. If the precondition is met, the smart contract will be accessible via a JSON interface and a specific contract address. Our method of inviting others to join is the Watch Contract over Ethereum Wallet setup. Anyone with a valid proposal who submits their sealed envelope by the due date will receive the same pricing. Each sealed package is opened at the right time. The person whose sealed envelope holds the most money is the winner. The following details will be released ahead of time in the initial data.
- **Auctioneer:** The location of the bidder is used to secure the initial contract.
- **Auction Start:** When the proposal will commence is specified.
- **Bidding Time:** used to specify when the agreement will become law
- **highest Bidder:** The most expensive item for sale is placed at the current highest bidder's location.
- **Highest Bid:** Used to keep the most recent values. The following obligations are specified in the contract:
- **blind Auction():**
- The bidding and bargaining now begin. The start and end times will be recorded using the final methods after using this function.
- **Bid():**

Anyone can start the bidding process by invoking this mechanism. In the absence of a defined auction Start and bidding Time, the function will not be carried out until the corresponding contract has been satisfied. If the bidder's offer is higher than the current highest price, they may submit their bid by mail. To maintain track of the current highest price and the contact information for the highest bidder, the contract system will use the fields highest Bid and highest Bidder.

- **Reveal winners**

- Once the sale is over, all the ticket prices should be checked and double checked to see who got the best deal.
- **Auction Close ():**

Starting the Auction and Placing Bids Time is the mechanism by which the term of the agreement is calculated. If the deadline is missed, the bidder will be notified of the successful bidder's address and the current highest bid. This feature will be disabled so that it cannot be activated again.

- **With draw():**

The total number of proposals submitted by everyone other than the winner is given.

4. EMPIRICAL RESULTS

We plan to use Metamask to set up two blockchain accounts to use for research-related testing and speculation. As seen in Figure 4, the Remix IDE interface can be used to track a block's transaction status in the blockchain. Creating a smart contract in Solidity entails just three simple steps: coding, building, and releasing it to the public. The Remix IDE's assembler was responsible for producing the bytecode. The Remix IDE was used to generate Figure 5. The smart contract is deployed to the blockchain via the Ethereum Wallet (Figures 6 and 7).

During this step, the smart contract's contract address is verified. The second account can use the Remix IDE and Interface to add the updated offer to the process.

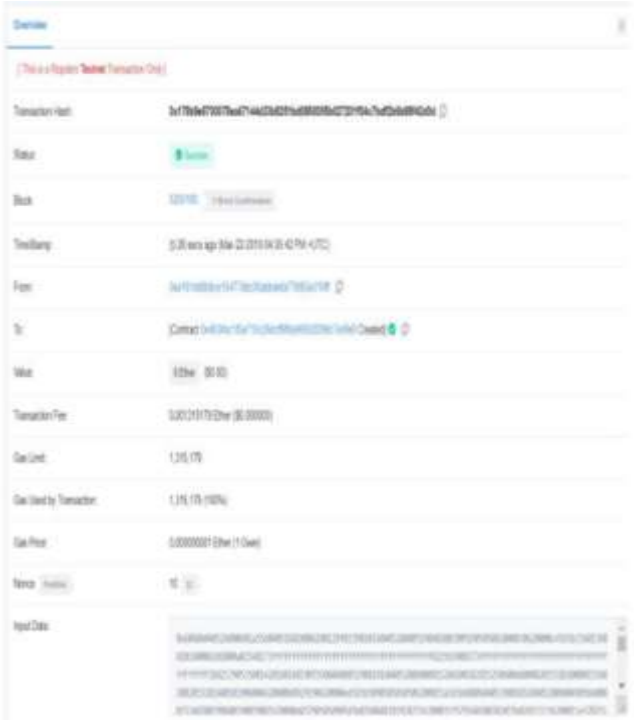

Fig. 4: Specifics about a smart contract transaction.

Fig. 5: Where the smart contract's code and interface are stored.

Fig 6: Contract's QR Code

FIG 7: CONTRACT JSON

5. CONCLUSION

We built a smart contract on the Ethereum blockchain to manage a secure, verified proposal. The goal is to hold an electronic auction in accordance with the principles of a conventional auction, such as protecting the privacy of bidders and preventing data from being tampered with. This contract ensures that all information on the offer is kept private and is not shared with any other candidates. Bidder registration and proposal submission are the only two required steps for this approach to work. Direct participation in this online auction is also possible through the use of the contract's unique URL or QR code.

REFERENCES

1. "Financial Cryptography and Data Security", Spring Nature, 2019.
2. "Verifiable Sealed-Bid Auction on the Ethereum Blockchain", Hisham S. Galal and Amr M. Youssef.
3. "An Introduction to Auction Theory: Blockchain Edition" by JinglanWang.https://medium.com/cryptoeconomics/an-introduction-to-auction-theory blockchain-edition-cf09b005b1cc
4. "Decentralizing Ascending Auctions on Blockchain" by Toraider teamhttps://medium.com/auctionity/decentralizing-ascending-auctions-on-blockchain-dffab74446c1
5. "Solidity"https://solidity.readthedocs.io/en/v0.4.24/
6. "Blockchain based smart contract for Bidding System", Yi-Hui Chen ; Shih-Hsin Chen ; Iuon-Chang Lin.
7. Marco Iansiti and Karim R Lakhani. The truth about blockchain.
Harvard Business Review, 95(1):118–127, 2017
8. Shengbao Yao, Wan-An Cui, and Zhenqian Wang. A model in support of bid evaluation in multi-attribute e-auction for procurement. In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on, pages 1–4. IEEE, 2008
9. Wee-Kheng Tan and Yung-Lun Chung. User payment choice behaviour in e-auction transactions. In e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E'10. International Conference on, pages 183–187. IEEE, 2010.
10. Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE, pages 180–184. IEEE, 2015.