ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.2 May 2019

SEALED BID AUCTION: A SMART CONTRACT ON THE BLOCKCHAIN

[#1]**Ms.NALLAGONI RENUKA,** *Assistant Professor*
[#2]**Mr.BOLLI RAMESH,** *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Both within and without our being. E-auction is one of the tools that helps people bid in online public auctions. Third parties must pay additional costs if there is a hidden bid to ensure that buyers and sellers may readily trade things. However, there is a chance that third parties will mislead you. When an auction is hosted on a decentralized site, the auction's owner or the organization in charge of it may have direct access to it. When a blockchain object is auctioned off, the smart contract takes ownership and oversees the bids. We designed a smart contract for a sealed-bid transaction that can be confirmed on the Ethereum blockchain in this work. A sealed-bid auction is held, in which each bidder can participate only once, and ideas are presented anonymously. The highest bidder wins and pays the highest bid amount based on the received bids. A proposal may also be withdrawn prior to the auction's conclusion. In this case, the buyer will be given a second chance to submit a proposal. Because it only reveals the highest proposal, this smart contract implementation works similarly to a sealed bid. Bidders are not shown any extra information about the bidding.

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

1. INTRODUCTION

Blockchain's basic concept is that network-based tendering approaches can be utilized to cut transaction costs. Auctioneers, bidders, and others are among those who use the electronic bidding method. All organized third parties participate to the auction website, which allows bidders and auctioneers to post adverts for their products, view the current highest bid price, and conduct other duties. This type of auction structure benefits companies like eBay and Yahoo.

E-auctions, on the other hand, are often beset by two problems. For starters, centralized third parties demand significant fees, which can raise transaction costs. Furthermore, the database may not be safe for sensitive personal information or transaction records. Second, the sealed envelope keeps the other bidders from understanding whether the leading bidder is reliable. The concerns are addressed in this essay, which examines incorporating blockchain technology into online auctions. This technique uses a peer-to-peer access structure, which means that any node, in this case a website, can communicate, verify, and transmit data to any other node without requiring a central authority.

This lowers the transaction expenses. A smart contract, on the other hand, deals with a dishonest lead offer.

2. E-AUCTION

Traditional Bidding System

E-auctions function similarly to traditional auctions but take place online. As a result, online bidding competitions are used to acquire the goods that will be auctioned. The start and end times of the sale are set by the person in charge. After the e-auction begins, bids must be filed online by the deadline. The e-auction winners are revealed when the sale has completed and a report has been compiled. The vendor will allow the successful bidders to collect the item once they have paid the appropriate deposit.

E-auctions are classified into two types: public bid and covert bid. There is a public proposal when those who want to buy something can raise their offer price. As a result, bid prices rise until no one is willing to pay any more. The winner is determined by the highest bidder on an item. A public auction allows for several bids. A public offer is also known as a multi-bid sale. Bidders encrypt and only finish the invoice once. This is referred to as a hidden offer. The auctioneer compares the two banknotes side by side if time allows. The bidder who provided the highest money won the secret auction. Because individuals are confined to submitting a single bid, the auction is sometimes known as a "single-bidding" sale. The bidders' prices are kept secret until the sealed proposals are unsealed and compared. We frequently run into problems with electronic seal ticket auctions since we can't tell if the other bidders' prices were made public before the auction ended.

Blockchain

This approach use distributed nodes to monitor, validate, and send network data. To create a decentralized data management and storage tool, a peer-to-peer network is used.

The following tools are necessary for the block chain to function:

Identity identification and security:

To identify persons and prevent forgeries, a public key system is utilized. For sending and receiving funds, each account on the block chain has both a public and a private key. The recipient decrypts the transaction message using the originator's public key after the private key has encrypted it. This confirms the correspondent's identity.

Message delivery and broadcasting:

For message transit and dissemination, peer-to-peer technology is utilized, which allows each server to join and communicate with other nodes. Every transaction is saved in the same file. Every node in the blockchain is capable of confirming events, even if they are uninformed of the decentralized access structure.

Data preservation and linking:

Figure 1 shows how a block chain is built. The hash values obtained from the transaction data contained in each block connect each block to the previous block. Figure 2 displays the attributes of the block. These pieces include information about the records in the block, such as a hash value, the number of transactions, a time stamp, and so on.

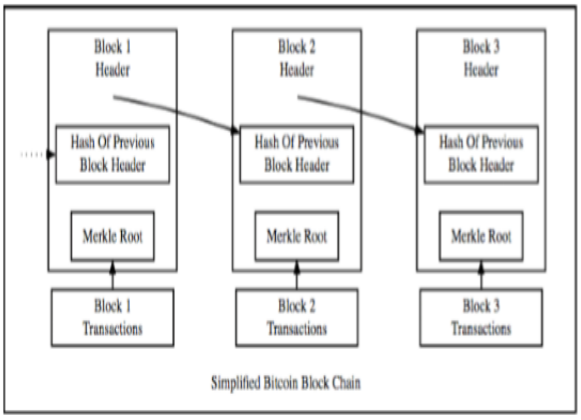
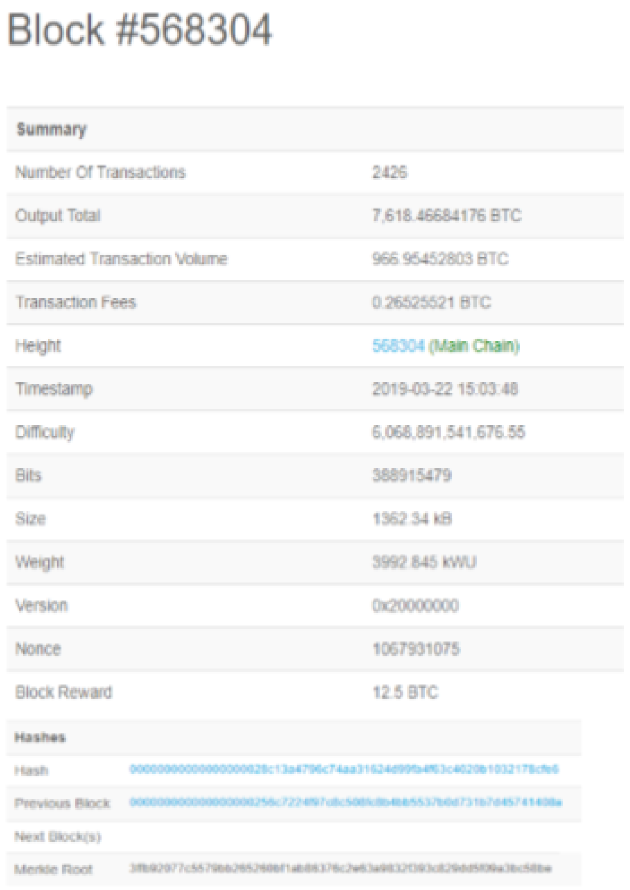


Fig. 1: Blockchain block structure design

- The block's head is made up of six elements, which are as follows: The application's version number. The previous section's number. By aggregating all transactions in a block, the Merkle tree's root hash may be computed. The Merkle tree's root hash appears as illustrated.
- The amount of time that has passed since 0:00:00 UTC on January 1, 1970.
- What the goal of this work is.
- The variable that changes when the proof of work is complete is the nonce. In this method, the miner attempts to estimate a valid hash that is smaller than the target hash.



Block #568304

Summary	
Number Of Transactions	2426
Output Total	7,618.46684176 BTC
Estimated Transaction Volume	966.95452803 BTC
Transaction Fees	0.26525521 BTC
Height	568304 (Main Chain)
Timestamp	2019-03-22 15:03:48
Difficulty	6,068,891,541,676.55
Bits	388915479
Size	1362.34 kB
Weight	3992.845 kWU
Version	0x20000000
Nonce	1067931075
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000000028c13a4796c74aa31624d99b4f63c4020b1032178cfe6
Previous Block	0000000000000000000256c7224f97c8c508fc8b4bb5537b6d731b7d457414 08a
Next Block(s)	
Merkle Root	3ffb92077c5579bb2652608f1ab88376c2e63a9832f393c829dd5f09a3bc58be

Fig: 2: Fields in a block

3. RESEARCH METHOD

Figure 3 depicts the E-auction. As the first phase, the vendor submits bid information, as well as a description of the item and a starting price. Those who want to buy the more expensive item cast the most votes for the sealed package. The auctioneer declares the greatest price now acceptable after removing the sealed package. The highest bidder is the winner until another bidder outbids them or the bidding limit is reached. Bidders may acquire the item from the auctioneer, who will be rewarded. To create an open tendering system, we leverage smart contracts and blockchain technology. The trade agreement for the bidders' proposals will be recorded on the blockchain. Anyone who wants to bid on the products can do so directly by invoking the open contract's trade contract, thanks to a decentralized access mechanism.

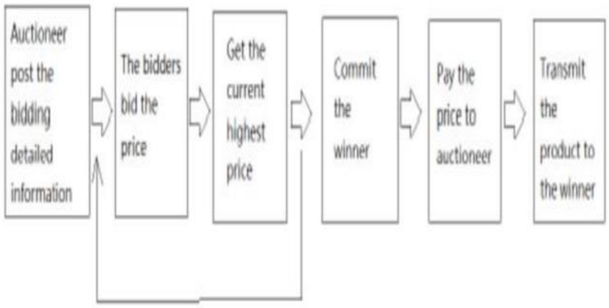

Auctioneer post the bidding detailed information
The bidders bid the price
Get the current highest price
Commit the winner
Pay the price to auctioneer
Transmit the product to the winner

Fig. 3: The flowchart of E-auction

- Each public E-auction system must meet the following criteria: Nobody knows who the winner (highest bidder) is.
- During a transaction, the content of the seal order cannot be changed, and everyone can establish that it is accurate and complete.
- No one who is not allowed to bid on the item may appear to be so. Once an offer has been approved, no bidder can withdraw it.
- The auction winner always has the proper papers to get the item. The vendor may accept the winning bid but not the losing bid.
- The envelope is no longer valid if it is not delivered by the due date. The sealed envelope is private and must not be opened before the deadline. If two vendors submit the same price, a fair resolution must be reached.

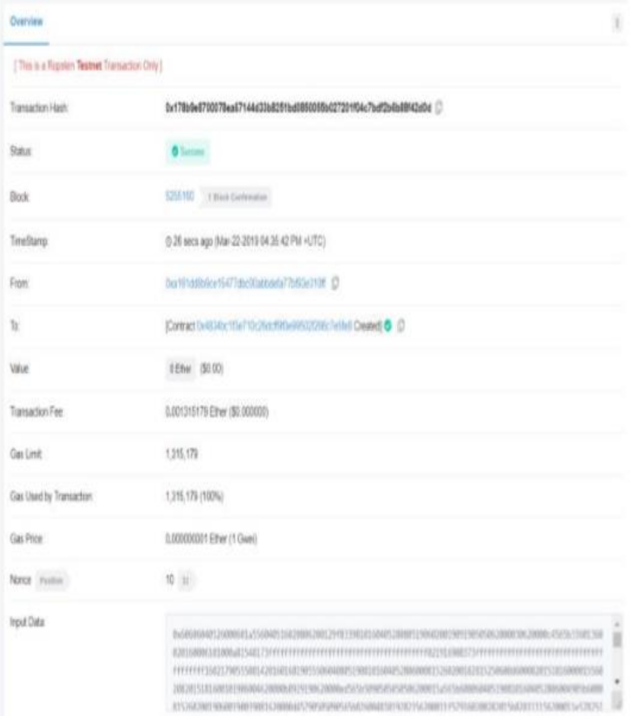
A smart contract is a set of algorithms and numbers that were created on the Ethereum platform. When a certain time or event occurs, such as when a message is sent, a transaction is concluded, or the contract expires, a smart agreement begins. The smart contract can be written in Solidity, Serpent, LLL, or Ether Script. A smart contract's JSON-redeemed bytecode is used to send a message to all blockchain nodes and then wait for proof. If the condition is met, the smart contract has a JSON interface and a unique contract address that allows the other party access. The Watch Contract over Ethereum Wallet approach is how we invite others. Anyone with a valid proposal who mails the sealed envelope before the deadline can repeat the pricing. At the right time, each sealed package is unsealed. The person whose sealed envelope holds the most cash is declared the winner. The following information will be made public 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 auction and negotiations begin. After using this function, the start and end times will be recorded using final methods.
- **Bid():**This method can be called by anyone to start bidding. If auction Start and bidding Time are not set, the function will not be called until the contract is completed. If the bid is higher than the highest price currently being offered, the bidder may mail the bid envelope. The contract system will employ highest Bid and highest Bidder to keep track of the most recent highest price and the bidder's address.
- **Reveal winners ():**After the sale has ended, compare and verify all ticket prices to identify the winner.
- **Auction Close ():** Auction Start and bidding Time are automatically used to determine the duration of the contract in this function. If the time restriction expires, the successful bidder's address and the most recent maximum price will be promptly forwarded to the tenderer. This function will be disabled so that it does not run again and again.
- **With draw():**The total number of proposals made by all participants, excluding the winner, is provided.

4. EMPIRICAL RESULTS

We intend to construct two blockchain accounts with Metamask for testing and wagering on research-related transactions. Figure 4 depicts how the interface of the Remix IDE may be used to track the status of blockchain transactions for certain blocks. Using the Solidity program, a smart contract may be developed in three steps: writing, compiling, and publishing. The bytecode was created by the Remix IDE's assembler. The layout presented in Figure 5 was produced using the Remix IDE. In this case, the Ethereum Wallet is used to publish the smart contract to the blockchain (Figures 6 and 7).

The smart contract is validated during the phase of validating the contract address. The second account can include the new offer into the transaction by utilizing the Remix IDE and Interface.



[This is a Ropsten **Testnet** Transaction Only]

Transaction Hash:	0x178b9e8700078ea57144d33b8251bd0850058b027201f04c7bdf2b4b8f42d0d
Status:	Success
Block:	5255160 1 Block Confirmation
TimeStamp:	26 secs ago (Mar-22-2019 04:35:42 PM +UTC)
From:	0xa191dd8b6ce15477dbc90abbdefa77b60e210f
To:	[Contract [illegible] Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.001315179 Ether ($0.000000)
Gas Limit:	1,315,179
Gas Used by Transaction:	1,315,179 (100%)
Gas Price:	0.000000001 Ether (1 Gwei)
Nonce Position	10 11
Input Data:	[illegible]

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

To manage a protected, validated proposal, we created a smart contract on the Ethereum blockchain. The goal is to hold an electronic auction in accordance with traditional auction principles, such as keeping information secret and preventing it from being altered. This agreement protects the secrecy of offer information, preventing other bidders from accessing it. For this technique to work, bidders just need to register and submit their proposals, which are two simple procedures. You can also participate in this e-auction directly by entering the contract's launched address 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/crypto economics/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/v 0.4.24/

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.