International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Blockchain Based Smart Contract for Sealed--Bid Auction

B L V V Kumar, K Raja Kumar

Abstract: ***In this growing world, Internet has changed so much to an extent that it turned into a powerful tool in every aspects of our lives.E-auction is one of those things which helps the bidders to take part in an auction online over the air. In a sealed bid third parties need to pay an extra cost to help the buyers and sellers carry out their exchange without any hassle. But there can be a breach of trust by the third parties. Owners of the auction or the company that is auctioning can have direct entry to it when the auction is run on a decentralized platform. When the users auction off something on the chain, the smart contract takes control of the auctioned asset and thereafter it manages the bids associated. In this paper, we execute a smart contract for a verifiable sealed-bid auction on the Ethereum blockchain. The type of auction used is sealed-bid in which the bidders submit their bids privately and each bidder can participate only once. As per the biddings received, the highest bidder wins and pays the highest corresponding highest submitted bid. Additionally, before the auction ends the bidder can withdraw the bid after submitting it. In such a case the bidder will have another chance to place the bid. This smart contract implementation abides by the true essence of a sealed-bid, to be precise, no information about the biddings is leaked to the bidders except for the highest bid***

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

I. INTRODUCTION

The principle of Blockchain [1] underlies at the integration of network techniques into the bidding system to reduce the cost of transaction. E-auction system comprises of bidders, third parties and the auctioneers. All the centralized third parties help in providing platform for the bidders and the auctioneers for advertising their products, checking the current highest bidding price etc. Companies like E-bay and Yahoo make revenues out of this kind of bidding system. However E auction has mainly two problems. Firstly, centralized third parties charge a whole lot of money which can increase the transaction cost. Moreover, the privacy of the personal data and transaction history which are supposed to be stored in the database might be at stake. Secondly, in a sealed envelope the bidders have no clue whether the lead bidder is trust worthy. This paper discusses about the application of block chain technique into the E-auction to solve the issues. This technique follows peer to peer access structure which implies each point in the structure can individually communicate, authenticate and transfer data to any other point which is a site in this case without any need for an actual centralized intermediary thereby reducing the transaction cost. On the other hand, a smart contract takes care of a treacherous lead bidder. Some rules are not supposed to be unveiled before the deadline.This paper is organized as follows. Section 2 illustrates the traditional bidding system and the blockchain. Section 3 shows how do we incorporate the blockchain technique into the bidding system. In order to justify the proposed method, we conduct the experiments in Section 4 and we draw our conclusions in Section 5.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Mr B L V Vinay Kumar*, Asst Prof Dept Of CSE Gvp College of Engineering for Women Visakhapatnam.
Dr K RAJA KUMAR, Asst Prof Dept Of CS&SE Andhra University Visakhapatnam

II. E-AUCTION

A. Traditional Bidding System

E-auction [2][11][12] follows the same approach as the traditional manual auction, but as the name suggests it takes place online. So, the assets or goods that to be auctioned are sold through online competitive bidding. The e-auction starts and ends within a given time interval which is managed by the controlling person. Once the e-auction begins, participants must submit their bids within the closing time via the internet. After the e-auction ends, a report is generated and the winners with highest bid are declared. The successful bidders then deposit their bid amount, after which the auctioned item is can be collected from the seller.
E-auction can be divided into two types, namely public bid and sealed bid [3]. Public bid is that in which bidders could increase the price to bid the products. Thus, the bidding price grows continuously till no bidders are interested to pay a greater price. A bidder is declared as a winner if he bids the highest price for such a product. During public bid, bidders can bid many times. Thus, public bid is also called as a multi-bidding auction. Sealed bid is that bidders encrypts the bill and only end the bill once at a time. If there is time, the auctioneer compares the bills. The bidder who bids for the highest price is the winner of the sealed bid. Since bidders only can bid once, it is also called single-bidding auction. In the seal bid, all bidders' costs are sealed until the bid opening date is compared to the costs of all bidders.
There is a common problem in electronic seal ticket auctions i.e.; we cannot make sure if the prices of the other bidders are leaked before the deadline or not.

B. Blockchain

It is a technology [10][13] which accesses, verifies and transmits network data through distributed nodes. It utilizes a peer-to-peer network to gain a decentralized data operation and preservation platform.

The block chain is mainly based on the following technologies as the operating base:

1. Identity identification and security:

Identification and anti-counterfeiting are accomplished using a public key infrastructure. Every account in the block chain has a public key and a private key employed to send and receive the transactions. After the private key encrypts the transaction message, the receiver then utilizes the sender's public key to decrypt the message, and the identity of the sender can be committed.

2. Message delivery and broadcasting:

Message delivery and broadcasting are achieved using a peer-to-peer technique, granting each node to connect and transfer messages with one another. The transactions are saved in the same ledger. Each node in the blockchain can substantiate the transactions using the zero knowledge over the decentralized access structure.

3. Data preservation and linking:

The transaction data that is saved in a block is to produce a hash value and the block is connected to the previous block with the hash values to construct a block chain as shown in Fig. 1. The fields in the block, as shown in Fig. 2, to detail the records of the block such as time-stamp, transaction quantity, hash value, etc.

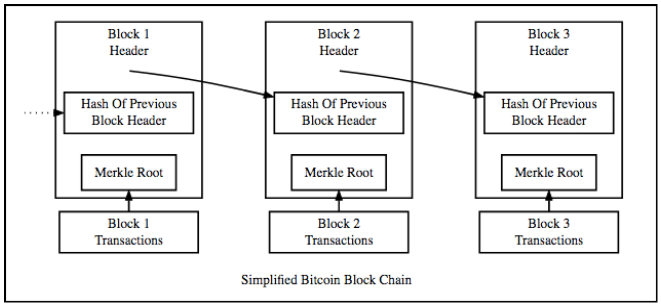

Fig. 1: Blocks architecture in Blockchain

The blockchain is a chain of data blocks and its each block can be considered as a page in a ledger. These individual blocks are composed of several components.
The head of the block [4] is divided into six components:
1.The version number of the software.
2.The hash of the previous block.
3.The root hash of the Merkle tree: All transactions contained in a block can be aggregated in a hash. This is the root hash of the Merkle tree.
4.the time in seconds since 1970–01–01 T00: 00 UTC.
5.The goal of the current difficulty.
6.the nonce: The nonce is the variable incremented by the proof of work. In this way, the miner guesses a valid hash, a hash that is smaller than the target.

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	00000000000000000028c13a4796c74aa31624d99fa4f63c4020b1032178cfe6
Previous Block	00000000000000000256c7224f97c8c508fc8b4bb5537b0d731b7d45741408a
Next Block(s)	
Merkle Root	3ffb92077c5579bb265260bf1ab86376c2e63a9832f393c829dd5f09a3bc58be

Fig: 2: Fields in a block

III. RESEARCH METHOD

The flowchart of E-auction is shown in Fig. 3, the seller posts the bidding information with the product description and starting price at the first phase. Bidders vote the sealed envelope to bid the product with a larger price. After receiving the sealed envelope, the auctioneer announces the highest rate present then. The bidder is as the winner bidder until no one bid the product with the higher price or the deadline is due. The auctioneer can gain the money from winner and sell the product to the bidder. We implement an open bidding system through blockchain technology with smart contracts. Bidders will write the trade contract for the bids into the blockchain. With decentralized access structure, all bidders can bid the product by calling the open contract's trading contract without intermediate brokers[5].

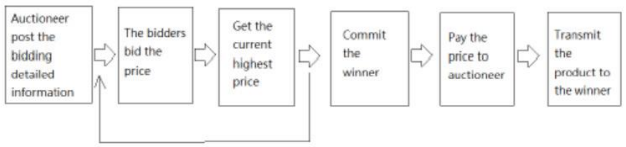

Fig. 3: The flowchart of E-auction

A complete public E-auction[6] system should satisfy the requirements as follows:
1. The identity of the person who is a bidder or winner (successful bidder) is kept anonymous to everyone.

2. The content of seal order cannot be modified during a transaction, and all the people will be able to verify its correctness and completeness.
3. No illegal bidder can pretend the legal one to bid the product. After bidding, no one can deny the bidding if they have ever bided.
4. The successful bidder always has the proof to get the product. The seller can get the money from the successful bidder but not for the other bidder.
5. The sealed envelope must be delivered before the deadline; otherwise, the envelope is invalid. Before the deadline, the sealed envelope is private, and no one can open it.
6. A fair solution is required if the same price is voted by two different bidders.

The smart contract is a pack of codes and digits implemented via Ethereum platform. In a smart agreement, the contract is started if the time or event is being triggered, like sending a message, dealing with transactions, ending the contract. The smart contract is described by Solidity, Serpent, LLL and Ether Script. The bytecode of smart contract redeemed with JSON format is utilized for broadcasting all the nodes of blockchain and then wait for verifying. If it is true, the intelligent contract is with individual contract address and JSON Interface to allow the other person to get in. Over Ethereum Wallet, we use Watch Contract to invite other people to join. Before the deadline, all the legal bidders can send the sealed envelope to renew the price. All the sealed envelopes are opened when the time is due. The highest price on the sealed envelope is the final winner. In the beginning data, we will announce the following information in advance.[7]

(1) Auctioneer: The tenderer address is used to record the beginning contract.

(2) AuctionStart: Used to announce the start time of the bid

(3) biddingTime: Used to announce the effective time of the contract

(4) highestBidder: The address of the bidder who is operating currently, bids the product with the highest price.

(5) highestBid: Used to save the current highest price.

As for the contract, we define the functions below:

(1) blindAuction(): Activate the contract by calling this function, and use the auctionStart and biddingEnd to record the start and end time

(2) Bid(): This function can be called by anyone to initialize the bidding action. Before the function is executed, AuctionStart and biddingTime are used to judge whether the contract is expired. If not, the bidder can send the bid envelope if the price is greater than the current highest price. The contract system will use highestBid and highestBidder to record the current highest price and the corresponding bidder's address

(3) revealwinners(): Checks and compares the prices of all the tickets to attain the final winner when the Auction is closed

(4) AuctionClose(): In this function, AuctionStart and biddingTime are automatically used to compute 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.

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

IV. EMPIRICAL RESULTS

In the experiments, we strive to create two blockchain accounts using Metamask for testing and bidding transactions. We can use the console in Remix IDE to keep a check on the transaction status for the details of blocks in blockchain as shown in Fig. 4. In smart contract creation, three stages are present, namely writing, compiling, and announcing by using Solidity programming. The bytecode is originated by Remix IDE compiler. The Remix IDE is used to generate the Interface as shown in Fig. 5. Finally, we can see how the Ethereum Wallet is used to announce the smart contract to the blockchain as shown in Fig. 6 and Fig. 7.

In the testing phase, the smart contract[8] is verified to get the address of the contract. The second account can add the new bidding to the contract by using Remix IDE[9] and Interface.

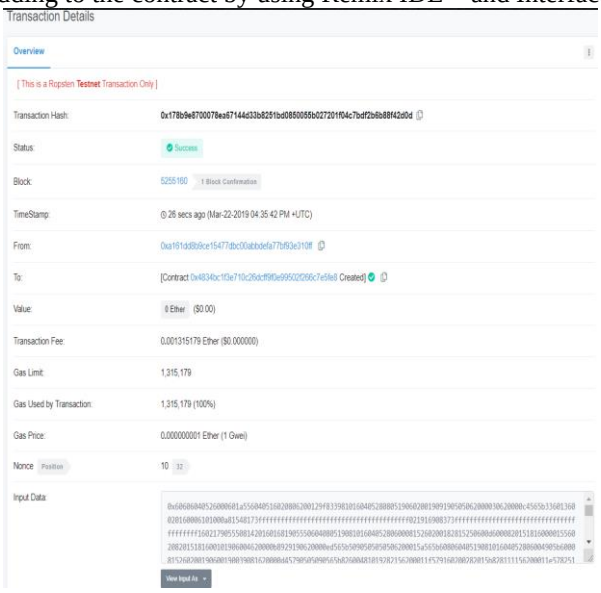

Fig. 4: The details of a smart contract transaction.

Fig. 5: The smart contract's bytecode and interface

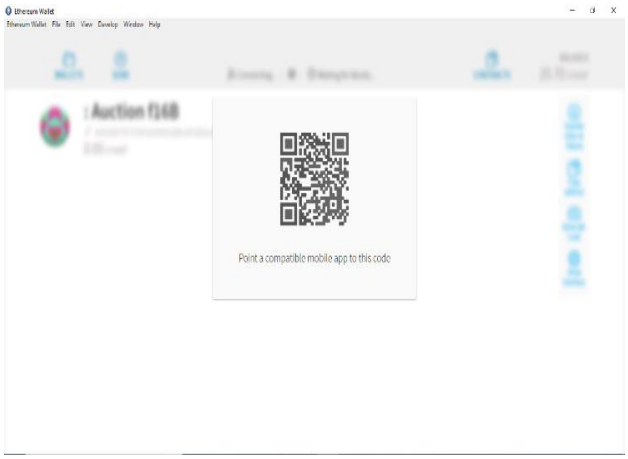

Fig 6: Contract's QR Code

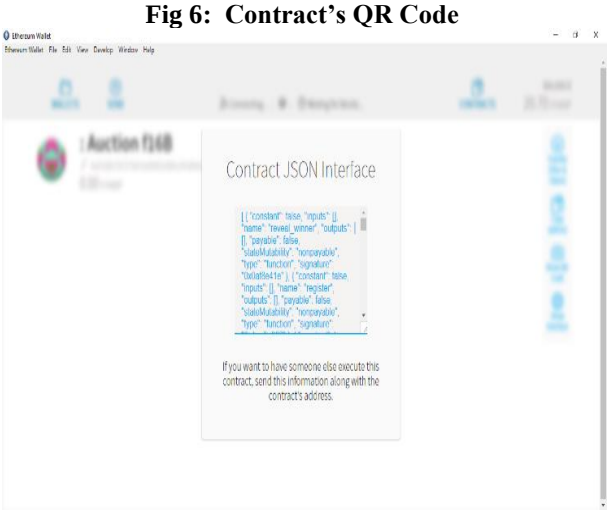

FIG 7: CONTRACT JSON

V. CONCLUSION

In this paper, we administered a smart contract for organizing a verifiable sealed-bid on the Ethereum blockchain. It proposes an approach for e-auction which abides by the confidentiality, immutability and traditional auction rules and regulations. This contract maintains the privacy the bids placed such that the corresponding details are not learnt by other bidders. Moreover, this approach requires simple interactions from the bidders, which include bidders registering and submitting their bids. The participation in this e-auction is also direct by simply using the contract's deployed address or the corresponding QR code.

REFERENCES

1. www.blockchain-council.org
2. "Financial Cryptography and Data Security", Spring Nature, 2019.
3. "*Writing a Sealed-Bid Auction Contract", by Todd Proebsting* https://programtheblockchain.com/posts/2018/03/27/writing-a-sealed-bid-auction-contract/
4. https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373
5. "Verifiable Sealed-Bid Auction on the Ethereum Blockchain", Hisham S. Galal and Amr M. Youssef
6. "An Introduction to Auction Theory: Blockchain Edition" by JinglanWang.https://medium.com/crypto-economics/an-introduction-to-auction-theory-blockchain-edition-cf09b005b1cc
7. [7] "Decentralizing Ascending Auctions on Blockchain" by Toraider teamhttps://medium.com/auctionity/decentralizing-ascending-auctions-on-blockchain-dffab74446c1
8. "Solidity" https://solidity.readthedocs.io/en/v0.4.24/
9. "Blockchain based smart contract for Bidding System", Yi-Hui Chen ; Shih-Hsin Chen ; Iuon-Chang Lin.
10. Marco Iansiti and Karim R Lakhani. The truth about blockchain. *Harvard Business Review*, 95(1):118–127, 2017
11. 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
12. 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.
13. 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.

AUTHORS PROFILE

Mr B L V Vinay Kumar Working As Asst Prof Dept Of CSE Gvp College of Engineering for Women Visakhapatnam. His Research Interest Include Blockchain ,Cryptography and Network security.His Publication include "Penetration testing using Linux tools" and "Evaluation of Optimised Apriori Algorithm on HDFS using MapReduce in Hadoop Distributed Mode" He has been certified as resource person for "Wipro Project Based learning" from Wipro Technologies Pvt Ltd Bengaluru

Dr K RAJA KUMAR Working As Asst Prof Dept Of CS&SE Andhra University Visakhapatnam Received Phd(COMPUTER SCIENCE AND SYSTEMS ENGG) For Work On AN EMBEDDED COMPUTER BASED DIGITAL SOUND PROCESSOR WITH IMPLANTABLE RECEIVER STIMULATOR FOR PROFOUNDLY DEAF PEOPLE - COCHLEAR IMPLANT SYSTEM His Research Interests Include Blockchain, Authentication, Embedded Systems And Vehicular Networks His Publications Include "Clinical Programming Software To Manage Patient's Data With A Cochlear Implantat" In 0163-5948 ACM SIGSOFT Software Engineering Notes" Co-Authored Byv. Bhujanga Rao,P. Seetha Ramaiah He Recieved RAJIV GANDHI NATIONAL FELLOWSHIP By UGC , 2006.