A Survey of E-bidding System using Blockchain

Prof S.S.Sambare , Nityam Khandelwal , Mohit Nathwani , Pranjal Munot , Shreyash Patil

santosh.sambare@pccoepune.org , nityamkhandelwal@gmail.com , nathwanimohit15@gmail.com , pranjalmunot19@gmail.com, shreyashpatil2871@gmail.com

Department Of Computer Engineering , Pimpri Chinchwad College of Engineering (PCCOE) , Pune , India

2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) | 978-1-6654-0118-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSSIT53264.2022.9716443

***Abstract*—With the increasing use of the internet, the e-auction system is becoming popular. E-Auction is an efficient e-commerce system that allows buyers and sellers to make a transaction through online platforms. Blockchain technology and smart contracts are being used in an e-auction to make it secure, transparent, and decentralized. In this paper, we use different bidding techniques that use cryptography to ensure security and to keep private information confidential of any participants in the auction. Furthermore, we have explained the concept of public bidding and sealed bidding which will be used in E-auction, we have explained UAE that is used to keep stakeholders identity autonomous, the paper also explains the hash functions which provides the advantage of encryption and decentralization Thus blockchain and smart contracts make it more efficient and secure compared to other traditional and e-auction systems.**

Keywords—blockchain; smart contract; E-bidding; privacy protection.

I. Introduction

The development in internet technology has introduced online platforms for different systems.The constant progress in the block chain technology has made it more and more attractive among a wide range of applications such as the bank transactions, intelligent systems, internet of things based applications , government sectors, industrial sectors etc. for the prevention of the unknown attacks and the hacking of the privacy information[15] . E-auction is one of the most important systems that has been introduced. In E-auction important participants included seller, buyer and third-party as shown in figure 1. Seller is the user who puts an item to sell. Buyers are the users who buy those items. There can be as many as buyers want. Third-party is the person who is intermediate in the process of buying and selling. Third party is an intermediary who connects buyers and sellers. Third parties check the bidding price given by the buyers and the buyer with the highest price gets that item. Third party stores all the important details of the participant. The main problem in the current E-auction system is that there is central authority involved for the communication between seller and buyers. All the personal and transaction records are stored in a database at central authority that may cause privacy leakage.

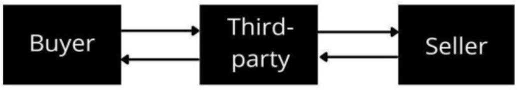

Fig. 1 Participant in E-auction

E-auction is classified in two types: public bid and sealed bid.. In public bidding bidders can raise the price to bid the product.Price continuously increases until no bidder is willing to pay a higher price. If a bidder bids the highest price for a product then he is considered as a winner.Public bid is also called a multi-bidding auction as the bidder can bid a product as many times as he/she wants. In sealed bidding, the bidder encrypts the bill and sends it. It can be sent only once. Then auctioneers check and compare all the bills. The bid with the highest price is the winner of the sealed bid. Sealed bidding is also called a single-bidding auction as bidders can only bid once. All the bidders' prices are sealed until the bid opening deadline. Before the deadline for opening of bids, there are chances of leaking the bid prices by third parties. As a result, malicious bidders may collaborate with bid winners to obtain the best bid price.

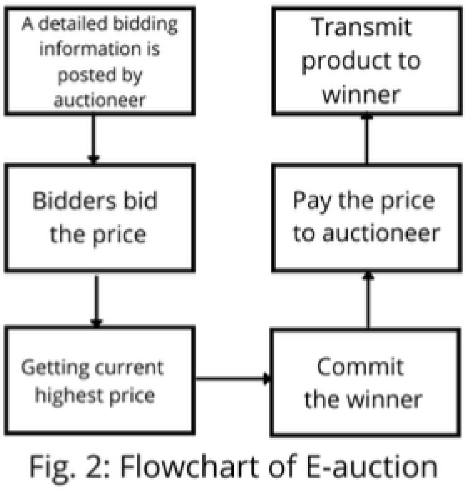
A detailed bidding information is posted by auctioneer
Bidders bid the price
Getting current highest price
Commit the winner
Pay the price to auctioneer
Transmit product to winner

Fig. 2: Flowchart of E-auction

Emerging blockchain technology combined with smart contracts is proposed in this survey paper. Smart contracts are programs stored on blockchain that run when predetermined conditions are met. It could revolutionize the traditional E-bidding system in a decentralized autonomous manner. It creates a way for a secure and immutable E-bidding process. In this paper we have studied the different methods of bidding using blockchain technology. At first different methods of bidding systems are summarized and the most suitable method has been concluded.

II. Literature Survey

[1.]Research on Blockchain-Based E-Bidding System[

This study offers a blockchain-based double-blind E-bidding mechanism. The utilisation of HLF based on consortium blockchain and chaincode for business logic is at the base of the solution. This system satisfies the confidentiality, immutability, and integrity security criteria. A bidding system architecture based on the blockchain technology bidding process is combined with the actual bidding process.In this, a system is created using five types of preliminaries . Consortium Blockchain , Hyperledger Fabric,Smart contract, Idemix, Zero-Knowledge Proof. Consortium blockchain , also known as "permissioned chain," is controlled collaboratively by numerous industrial institutions [1]. Only consortium members have access to read, write, and send any part of the data. All participants must be authorised before they may engage in a blockchain transaction on the HLF platform.SC is a piece of code that runs in a particular habitat, such as virtual machines or containers, and is deployed on the blockchain and kept in the contract address.The consortium blockchain structure is used in the blockchain-based double-blind E-bidding system.

There are five positions in the system: system administrator, supervisor, tenderer, bidder, and review expert, each with many users. There are three stages to the tendering and bidding process: initial preparation, bidding, and review.The tender user logs in to his account and issues a property for bidding as a tender.Then the supervisor ensures the integrity of the tender user and checks all the parameters included by the user which is then verified and bidding is approved.when a bidding user sees such available project in the message board it will issue a tender filling all the necessary parameters required. The supervisor then inspects the qualification of bidding user and after verifying allocates graph and unique string label for the bidding project to be bid.After the approval of bidding user it should download the tender qualification and place a bid .also it needs to invoke SC and prove its authenticity to the system with ZKP technology.After bidding user applies for bid opening, supervisor generates the bid review team.The bid review team shall review the bids according to the bid review tasks.Then the tender user selects the winning bidder based on the review results of the review team and closes the bidding

[2.]Distributed E-Voting and E-Bidding Systems Based on Smart Contract

The study created an electronic bidding system which improves auction efficiency and allows suppliers to get included in the opening phase by introducing a SC with privacy-protection cryptography. Because the blockchain's formation is not biased and is available to the public. Suppliers documents must be absolutely secret before the start of the phase. Moreover, every transmitted data is saved in the SC for additional verification.

A vendor with a bidding qualification is referred to as a vendor. The vendor is charged for the bonds to get a bid bond certificate after undergoing identification verification.The GCA [2] is in charge of confirming vendors' identities and granting company certifications to lawful vendors.The bank comes in to the picture for verifying that the amount collected by bonds; if it is not wrong, then bank will issue a verified certificate. It is the responsibility of Tender authority to write the documents and post them on the website.The TWeb is in charge of transferring vendor deposits to the authority in charge. When bidders finish their bid, the TWeb analyzes and publishes their document papers in the SC.The SC takes the place of a typical bulletin board in terms of functionality. It's dynamic, allows suppliers to double-check their bid information, and boosts the bidding's legitimacy and vendors' confidence.There are seven processes and steps included in the systems .The administration must create their signature key pair before implementing the protocol, with the signing key being the general key required for verification of signature. Vendors must create a key pair for encryption and decryption.The GCA verifies vendors' identities and sends corporate certificates to lawful merchants at this stage. The operations are carried out in a non-interactive mode.The vendor gets the e-identity and gets verified by the GCA in this phase.They can surf through many cases declared by the authority in the system; if they pay the cost of documentation, they can also download and view comprehensive documents. Although the tender materials are secret, suppliers that pay the fee have access to them.They must deposit the amount and acquire a deposit receipt.

They next finish the tender document according to the instructions and sign the bidding document with their own private key to confirm that they completed it. The bidder verifies the legitimacy of the documents, the certificate, and the certificate of deposit using the general keys of each vendor, the bank, and the GCA. Vendors begin bidding after proving their legitimacy. Following the bidding, the SC notifies all Vi the bids are recorded.The winner is determined in this phase, and the TA notifies the winner. The seller must accept the electronic notice's outcome in its entirety. If the highest bidder withdraws his or her bid at this time, the TA will seize the bid bond.Except the highest bidder, all other bidders can petition the authority to claim the deposit amount by showing their certificate.

[3.]Blockchain based Smart Contract for Bidding System

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

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 .

[4.]Research on Blockchain Technologies in Bidding Systems

The system proposed two types of bidding systems : public bidding system and sealed bidding system .

Public bidding system :
The proposed system works in a way the bidder announces the bid information the bidder starts the bidding process , the highest bid is announced and the process is continued till the no more bids are placed higher than the biggest bid , The authorities announces the final price of the bid , the winner bidder transfer the funds to the bidder , after the bidder confirms the transaction details the product is sent to the winner . It is a completely transparent system; the name isn't disclosed to both the winning bidder and the bidder .

Sealed bidding system :
The proposed system works in a way the bidder announces the bid details , those who wish to participate in the bid should register with the dedicated authority and one time tenders are placed in the system , after the time expires for placing the bid all the bids are compared and the highest bidder is notified and been called for transaction of funds and product takes place .

[5.] Secure E-Auction System Using Blockchain: UAE

This system was developed by interviewing the people who have previous experience of electronic bidding platforms. The key requirements were to ensure communication channels would keep their stakeholders' identity anonymous. This platform would also eliminate time to re-register for another auction. The bidder should register on the server which would give him a unique key which would be used every time authenticating into his account.

The bidder could also bid for more than one auction which would consume less time . Every time when the bidder participates in an auction a ticket is given to him as a proof of participation. The owner who owns the property should register onto the same platform of blockchain in order to get into transactions. After the registration of the owner to the platform and after uploading all the documents he is provided a safe key which would be used in future reference.

When the owner has the opportunity of making good money he or she can make a request to the auction house for bidding their property. As soon as the listing is done the participants can make their offer. The ledger gets updated as the bidding offer starts and the highest bidder is decided. The main objective of the system was to prevent the violation among the participants. As blockchain is a decentralized system and does not include any third party the needs were fulfilled.

[6.] Land Registry Using Blockchain

The system presented by the paper uses the Django Framework with mysql and blockchain smart contract to ensure secure transactions .Firstly the person having land needs to register his property by visiting the nearest registration office.Then the government officials would take the documents related to the process and encrypt them to ensures security .During the registration the owner has to fill two forms the first consisting of his details and property documents whereas the second the consisting of the parameters such as location, plot number, sector number, etc.

After the verification and registration a mail is sent to the owner. There the details of property and owner are stored into the database encrypted paper into a network which would correspond to a hash value of the file. Using this system of big steps is totally eliminated which consist of collecting the data of owners property and owner details and also verification of his authority. This system enables one to search the property by using property location or by using the owner's name. In order to create a transaction both the buyer and seller are supposed to visit the government office.

There are some steps involved as this system works hand in hand with the current system. As the owner has already registered his property on the platform hence there would be less time taken for the verification. A lawyer could be hired in order to make an agreement for sale which would include some terms and conditions. After the property transfer process the smart contract runs successfully and the property is stored under the buyer's name. Also the previous ownership of the seller is revoked in the blockchain.

Then using the hash that was created in the first step we can concatenate the files hash with the smart contract property which was created now. And hence by executing the smart contract property ,it will map with its corresponding hash value ,which would update the blockchain. The proposed system aims to solve the problems such as frauds and scams by using the new technologies like blockchain which would give advantages such as encryption and decentralization .

[7.]Blockchain based Secure Data Storage and Access Control System

The paper proposed a blockchain based system for cloud data storage and its security . The system mainly focuses on the accessibility of data and also on vulnerability of data issues like data piracy , data breach , data leakage , vulnerability and system security .

The system proposed in like first the data owner uploads the data over the system and encrypts it and obtains a key which will be used to access and decrypt the data . the data owner provides the access key to the person he wants them to access the data . but also accessing the data with a key the user needs to verify himself .

[8.] Land Registry Using Blockchain - A Survey of existing systems and proposing a feasible solution

The paper proposed a system for a transparent and secure property transaction system . The system consists of an admin section . The admin section will take input for all the necessary details like the login id , password and after that the admin will be able to add land details in the system , then the system will provide a property id and the property verification will take at the back end with the help of aadhar card no .

The users who wanted to buy the property and search the property by using property id or search property using area and location . Then the users propose the buy value in the system and the admin gets notified and the negotiations start between them, once the deal is finalized
, the admin enters the details in the system and a transfer process is started for the property . In this way the system will have a transparent system for property transfer

[9.] Large-scale Election Based On Blockchain

The Paper proposed a system using which the election can happen in a transparent , non-interceptable and secure method with the help of different stages which include different verification processes and casting of votes , verification of symbols of the parties,candidates is done.

However al the voting details like voter credentials , identity is stored in the block chain and if some tampering happens to the data or the process then it can be traceable
, but as a result this will lead to insecurity on the voter and voter identity , to overcome this issue the paper proposed a system in which secrecy of the voter and other end users can be made with the help of

- **unlinkable signature [10] :**is used to protect the receiver of transaction anonymity [10].
- **Ring signature :** helps in keeping the anonymity of the sender.

[10.] Succinctly Verifiable Sealed-Bid Auction Smart Contract

The paper proposed a system for sealed bid auction method with the help of different algorithms , like firstly to find the highest bid from the sealed bids obtained (both highest and second highest bid with their commitment properties . Then the customer verification is done after which the deployment of smart contract is made which and another opportunity is made for bidding and bids are placed again . Then the opening of commitments is done by which the proof of verification takes place , after this the gas analysis takes place by which the actual cost of the property and other details are obtained and then the transfer of property takes place . In this way the auction can happen in a systematic and transparent manner .

[11.] BOREALIS: Building Block for Sealed Bid Auctions on Blockchains

This paper proposed a system which involves multiple seal bids submission i.e. there are more than more stages to submit different sealed bids but without disclosing the current highest bid amount to give multiple chances to the bidders to place bids and also the owner of the property so that he could have a decent profit also .

The system proposed process is the same just like other bidding systems. The difference is that the placement of bids is sealed i.e contract format and the verification is made once all the time of final transfer of the property / product and funds

PAPER NO.	PAPER TITLE	ALGORITHM USED	LIMITATIONS
1	Research on Blockchain-Based E-Bidding System [1] Dan Wang, Jindong Zhao * and Chunxiao Mu Received: 31 March 2021 Accepted: 25 April 2021 Published: 28 April 2021	To develop the bidding process they have used "Permissioned blockchain" such as hyperledger. MSP(Membership Service Provider) and chaincode are used as hyperledger fabric that can control the access of singles at same time and can also set time limits. Hyperledger fabric is an open source block chain framework.	1. Hyper ledger fabric (HLF) is a new technology which is changing rapidly. Adapting such technology is a huge challenge. 2. Maintaining and operating a block chain system needs skilled technical personnel which is also an obstacle.
2	Secure E-Auction System Using Blockchain: UAE Case Study[7] Hani Qusa, Jumana Tarazi, Vishwesh Akre	They presented blockchain e-auction system that can be applied to improve the existing e-auction systems implemented in the UAE. Hyperledger/fabric has been used to solve the security issues in traditional systems. It is an architecture that allows different functions to be combined. That can be used for production of smart contracts that can host any mainstream language	Scalability is real problem in this systemdue complex nature of block chain
3	Distributed E-Voting and E-Bidding Systems Based on Smart Contract [2]Raylin Tso 1,* , Zi-Yuan Liu 1 and Jen-Ho Hsiao 2 Received: 4 March 2019; Accepted: 8 April 2019; Published: 11 April 2019	In the given paper they combine Smart contracts and privacy protection cryptography to create a distributed electronic voting system that enables voters to participate in elections and improves efficiency of the election system.	Apart from privacy and transparency this process is a bit more complex than the existing process.
4	Blockchain based Smart Contract for Bidding System [3] Yi-Hui Chen, Shih-Hsin Chen*, Iuon-Chang Lin	The bidding system uses smart contracts which are implemented using the Ethereum platform. Smart contracts are described by Solidity, Serpent, LLL, and EtherScript. Smart contracts are a set of codes and digits implemented using the Ethereum platform.	This process is longest as well as complex Due to the complexity of this program bidders may call the wrong contract function.

Table 1: comparison table

III. Outcome Of Survey

After going through different research papers and a bit of survey we obtained an idea to create a land registry and bidding system using ethereum blockchain . through which we can make the bidding system for land totally transparent and transfer of property can also be made a digital record without interaction of paper . Our system will give opportunities to both the types of owners who want to give their land for auction and for those who are forced to sell the land due to personal circumstances .

our system will consist of both sealed and open bidding systems .

IV. Conclusion

Blockchain is a revolutionary technology that has gained tremendous attention in recent years. E-auction is one of the applications of block chain. As blockchain technology is used to eliminate the middleman in the electronic bidding system. And the systems we studied are pretty powerful and more secure compared to traditional systems. We can bring integrity and confidentiality to the bidding process using block chain. In this paper we have influenced different methods in the E- bidding system. After a survey of different papers we came to the conclusion that "Blockchain based Smart Contract for bidding system" [3]. is more suitable for developing systems since the process flow is simple and easily understandable. This process requires less interaction of different parties which results in transparency of process . Also, less time is required for completion. That's why we found it more efficient.

V. References

[1.]Yantai University, 2021 , “Research on Blockchain-Based E-Bidding System” ,doi.org/10.3390/app11094011

[2.] Tso , Liu and Hsiao , 2019 ,”Distributed E-Voting and E-Bidding Systems Based on Smart Contract” doi:10.3390/electronics8040422

[3.] Meen, Prior & Lam (Eds) , 2018 , “ Blockchain based Smart Contract for Bidding System” , In Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018

[4.] Sun , Yao , Wang & Wu , 2019 ,”Blockchain Based Secure Data Storage and Access Control System using IPFS” , DOI:10.1109/ACCESS.2020.2982964

[5.] Desai , Deshmukh , Shelke , Choudhary , 2019 , “Blockchain based Secure Data Storage and Access Control System”, 10.1109/ICCUBEA47591.2019.9129015

[6.] Shinde , Padekar , Raut & Wasay , 2019 , ”Land Registry Using Blockchain - A Survey of existing systems and proposing a feasible solution” , DOI:10.1109/ICCUBEA47591.2019.9129289

[7.] Qusa , Tarazi & Akre , 2020 , “Secure E-Auction System Using Blockchain: UAE Case Study “, DOI:10.1109/ASET48392.2020.9118213

[8.] Wang , Sun , He & Pang , 2018 , “Large-scale Election Based on Blockchain” , DOI:10.1016/j.procs.2018.03.063

[9.] Galal And Youssef , 2018 , “Succinctly Verifiable Sealed-Bid Auction Smart Contract” , DOI:10.1007/978-3-030-00305-0_1

[10.] Blass & Kerschbaum , 2020, “BOREALIS: Building Block for Sealed Bid Auctions on Blockchains “ , DOI:10.1145/3320269.3384752

[11.] Sarfarz & Chakrabortty , 2021 , “A tree structure-based improved blockchain framework for a secure online bidding system “ , DOI:10.1016/j.cose.2020.102147

[12.] Chen , Chen & Lin , 2018 , “Blockchain-Based Smart Contract for E-Bidding System” , DOI:10.1109/ICASI.2018.8394569

[13.] Syms & Wang , 2021 , “Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework” , doi.org/10.36548/jaicn.2021.2.002

[14.] Vijesh & Raj , 2021 , “Deniable Authentication Encryption for Privacy Protection using Blockchain.” , doi:10.36548/jaicn.2021.3.008

[15.] Dr. V. Suma , 2019 , “Security and Privacy Mechanism Using Blockchain “ , doi.org/10.36548/jucct.2019.1.005

[16.] Shuaib , Daud , Alam & Khan , 2020 , "Blockchain-based framework for secure and reliable land registry system“ , DOI:10.12928/telkomnika.v18i5.15787

[17.]Shaji , Rony , Kuriakose & Rawther , 2019 , Decentralized Land Lending System using Blockchain ,doi.org/10.30534/ijiscs/2019/14822019