2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)
Manipal University Jaipur, Sep 28-29, 2019

Blockchain-Based Smart Contract for E-Bidding System

Praveensankar Manimaran
PG Scholar
Department of Computer Science and Engineering
National Institute of Technology Puducherry, Karaikal, India
praveensankar1995@gmail.com

Dr. R. Dhanalakshmi,
Associate Professor
Department of Computer Science and Engineering
National Institute of Technology Puducherry, Karaikal, India
dhanalakshmi@nitpy.ac.in

***Abstract* — Electronic bidding systems have become widespread since the advent of the internet and mobile phones. In the Electronic bidding systems, the seller will sell an item and many buyers will bid for that item and the highest bidder will get the item. One of the main issue with this E-Bidding system is the introduction of third-party mainly a company or set of companies which will develop and host either the website or smartphone application. The Buyers and the Sellers have to trust this company because all the bidding process will be handled by the company. The company can manipulate the bidding process if it wants. So to avoid the trust issues blockchain based electronic bidding system is introduced in this paper. In this model, there is no need for third party. Smart Contract will handle all the bidding transactions. Since blockchains are known for its integrity this system makes sure that the integrity of the bidding process is preserved.**

Keywords* — *Bidding, Blockchain, Smart Contract

I. INTRODUCTION

E-Auction systems are using encryption, hash function, blind signature and various other cryptographic mechanisms to maintain integrity and confidentiality.[1] Main participants of the E-Auction system are Buyer, Seller and the third-party. Seller is the one who is selling the item. Buyers are the users who are trying to buy the item. The third party is responsible for creating the auction and managing the auction. This is shown in Figure 1. In the E-Auction systems, the third party will store all the details on its own server. The details may be the buyer's details or the seller's details. The main important detail which is stored by the third-party is bidding amounts chosen by the buyers for an item which is being sold by the sellers. This detail can be tampered by the attackers. The third-party can manipulate the bidding process if it wants. The third-party can reveal the bidding amount given by the buyers to some selected buyer so that the selected buyer can win the auction. This entire E-Auction System is not trustworthy and it relies heavily on the third-party. Since this is a centralized process the buyers and the sellers will have to pay transaction fees to the centralized entity which is third-party. The centralized entity has to protect the privacy of the buyers and sellers.

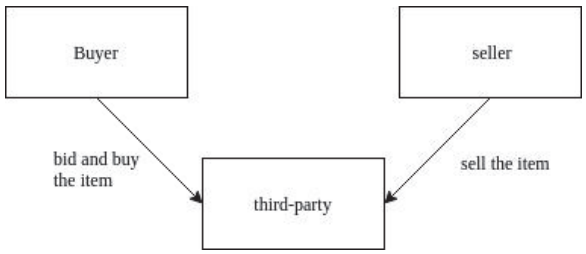

Fig. 1: Participants in E-Auction

This paper presents a blockchain based solution for the E-Bidding system. Blockchain is a decentralized network in which unreliable peers interact among themselves and perform transactions. In blockchain based system there is no need for third-party. So all the data and bidding amounts will be stored in the peer nodes. This architecture uses public-key cryptography, so the privacy of the data is maintained. Blockchain is known for its tamper-proof mechanism, so no attacker can manipulate the data.It maintains integrity. In the traditional system, if the third-party is down, the whole bidding process will collapse. In blockchain based network even if one node is down, others will hold the data and it will make sure that the bidding process will be available all the time.

This rest of this paper is structured as follows. Section II gives a detailed overview of the blockchain technology and smart contracts. Section III explains the existing blockchain based solution for E-Bidding System. Section IV explains the new solution and advantages of it over the existing one. Section V concludes this paper.

II. BLOCKCHAIN

A. Blockchain Overview

Blockchain is a distributed ledger [14] where ledger contains a list of blocks and each block will contain a set of transactions and hash value of the previous block [2] as shown in Fig. 2. All network participants will have a copy of the blockchain. The first blockchain technology which is developed to solve the double-spending problem is Bitcoin [3]. The first block is called genesis block. It initializes the

978-1-7281-1711-9/19/$31.00 ©2019 IEEE

ledger. Subsequent blocks will contain transactions and the hash value of the previous blocks.

The definition of the transactions will vary greatly depending on the blockchain architecture. In Ethereum [4] blockchain transactions are used to either create a contract or to transfer ether from one account to another account. In hyperledger fabric [5] the ledger state can contain different values at different times. The world state represents the current value of the ledger states. The transaction changes the current world state value to new value and the blockchain stores all these transactions.

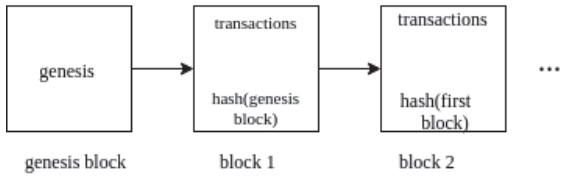

Fig. 2: Blockchain architecture

B. Consensus

Transactions are added to the block based on the consensus protocol defined in the blockchain. Each peer will use a set of private and public keys. When a peer creates a transaction, the private key of the peer is used to digitally sign the transaction. The other peers can use the public key of the peer to verify the authenticity of the transaction. When many peers are trying to append a transaction in the same block, the consensus protocol is used by the blockchain network to choose a transaction out of all transactions and that transaction will be added in the block and broadcasted to all the nodes in the blockchain. The peers will verify the validity of the transaction and if it is valid it will be added to the local blockchain copies of the respective peers. [6] The Consensus protocol will determine the validity of the transaction and the order of transaction. Different blockchain architectures use different consensus mechanisms. Blockchain ledgers will be kept in a consistent state by the consensus protocol which chooses the order of transaction for each new block. The basic consensus mechanism is such that it goes with the majority. Whatever order is decided by the majority of the nodes, it will be followed in the whole blockchain network. But the main issue with that approach is if the malicious peer can join the network with multiple identities then it can manipulate the whole consensus process. This type of attack is called "Sybil Attack" [7]. In Bitcoin mining new node that will be mined is CPU intensive and expensive, so it avoids this attack. That consensus algorithm is called "Proof-Of-Work"(POW) [8]. In POW based blockchains to mine the new block (add the next block to the blockchain) all the nodes will race to get a solution for a cryptographic problem based on the current block. Whichever node solves the problem at first will get the right to mine the block. This mechanism eliminates the possibility of the Sybil attack in bitcoin-based blockchains. Ethereum uses "Proof-Of-Stake" (POS) consensus protocol [9]. In POS whichever nodes want to participate in the mining operation will stake a specified amount of cryptocurrency. The nodes can stake from a minimum amount to the maximum amount. The node to mine the next block will be chosen randomly from those nodes. The probability for the particular node to be chosen is based on the amount of cryptocurrency it staked. In hyperledger fabric the consensus mechanism is pluggable. Currently, it supports solo, raft and kafka protocols [5]. Raft and Kafka are based on the Byzantine fault tolerant algorithms [10].

C. Smart Contract

The definition for Smart Contract is "a computerized transaction protocol that executes the terms of a contract" given by Nick Szabo [11]. Smart Contracts are self-executing scripts which are stored in the blockchain [6]. Smart Contracts reduce the need for the middleman since it can perform all the transactions autonomously and still provide the kind of services given by the middleman. Business logic can be expressed using smart contracts in the blockchain network. Smart contracts are distributed applications and it is secure because it is stored in the blockchain [5]. Smart Contracts can be hosted by all the peer nodes in the blockchain network or by some specified set of peer nodes.

D.Blockchain Characteristics

The important characteristics of the blockchain are given below:

Decentralization. By using smart contracts and consensus protocols all the transactions can be executed, verified and validated by the peers participating in the blockchain network. This basically eliminates the centralized authority.

Integrity. Only the authorized peers can perform the transactions. All the transactions will be verified by the other peers. So no one other than authorized peers can modify the data.

Anonymity. Since public-key cryptography is used for identification, all the peers will use its private key to sign the transactions and its public key will be used for signature verification.

Auditability. All the transactions that have been executed in the blockchain network will be stored in the blockchain. So all the transactions can be traced back to its origin and can be verified.

E. Blockchain Taxonomy

The blockchain networks can be classified into three types: private, public blockchain and consortium blockchain. Usually, a single organization will govern and control the private blockchain. Multichain [12] is an example for private blockchain. In public blockchain, all the peers can view the transactions and perform the transactions and all the peers can mine the new block. Bitcoin [3] is an example of a public blockchain. In consortium blockchain, a group of organizations controls the blockchain network. Consensus mechanisms are handled by the selected nodes from these group of organizations. Hyperledger fabric [5] is an example for this type of blockchain.

III. RELATED WORK

A. Electronic Auction

There are 2 types of bidding systems available. One is public bid and the another one is sealed bid [13]. In public bid, the bidders will raise the amount to bid for the bidding item. Whoever is bidding the highest amount will be the winner. At a time anyone can see the bids of the bidders and the current highest bid. Bidders can bid incrementally to win the auction. In sealed bid, the bidders will put their bid in the sealed envelope. Once the deadline is passed the auctioneer will open all the sealed envelopes and check the bidding amounts. Whoever has given the highest bid will be announced as a winner. In sealed bid, the bidders can bid only once. The main issues with this traditional bidding systems are bid leakage in case of sealed bid and manipulation of bid amounts in both public bid and sealed bid. In both of these bidding systems, the transaction fees for the third-party is also a big drawback. So blockchain based solutions can be used to avoid these problems.

B. Public Blockchain-Based E-Auction

Smart contracts for the public bid is proposed by Chen *et al* [13]. This smart contract is implemented via the Ethereum [4] platform using the programming language solidity. In Ethereum blockchain all the users will have an address and all the smart contracts will have an address associated with it. At the starting stage, the smart contract will be initialized with an address of the seller, auction start time and auction end time. It will contain the fields for storing the highest bidder address and highest bidding amount.

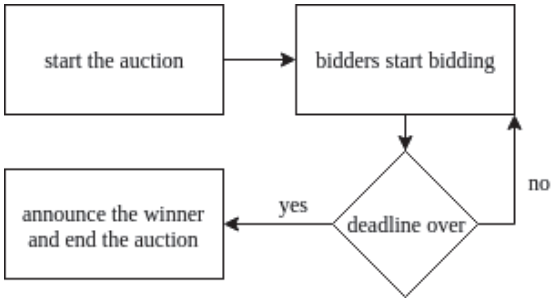

Fig. 3: Bidding System Workflow

The workflow of the solution proposed by Chen *et al* is explained in Fig. 3. The auctioneer will start the auction. Once the auction is started the bidders will start bidding for an item. Once the deadline is over the winner will be announced and the winner will get the item and the bidding amount will be transferred from the bidders account to the seller's account. Only the public address of the bidders and sellers will be used throughout the process. No one will know the real identity of the buyer or seller. The smart contract contains the following functions: BlindAuction, Bid, Reveal, Withdraw and AuctionEnd [13].BlindAuction function will initialize the smart contract. Bid function can be called by the bidders to do the bidding. Reveal function will announce the highest bidder. AuctionEnd function will end the auction and send the bid amount to the seller. Withdraw function will return bids to the bidders who couldn't win the auction. This method makes sure that confidentiality and non-repudiation are preserved. The main issue with this smart contract is the access control mechanism which is not implemented properly. If the bidder calls the Reveal function before the deadline then it will reveal the highest bidder and finish the auction. In this implementation sealed bidding is not implemented. The bidders can bid any number of time before the deadline. Since it is implemented in the Ethereum blockchain it can be viewed by anyone because Ethereum blockchain is a public blockchain and anyone can participate in it. It is not suitable for business to business auctions or highly confidential auctions where other than bidders and sellers no one should know about the auction.

IV. BLOCKCHAIN BASED SMART BIDDING SYSTEM

A. Smart Contract for Bidding System

The flowchart for the Smart Bidding system is shown in Fig. 4. When the smart contract is installed and instantiated the following arguments will be passed to the smart contract.The item name which is going to be auctioned, the public address of the seller, the validity of the smart contract which is essentially the duration of the whole auction and type of auction whether it is public bid or sealed bid.

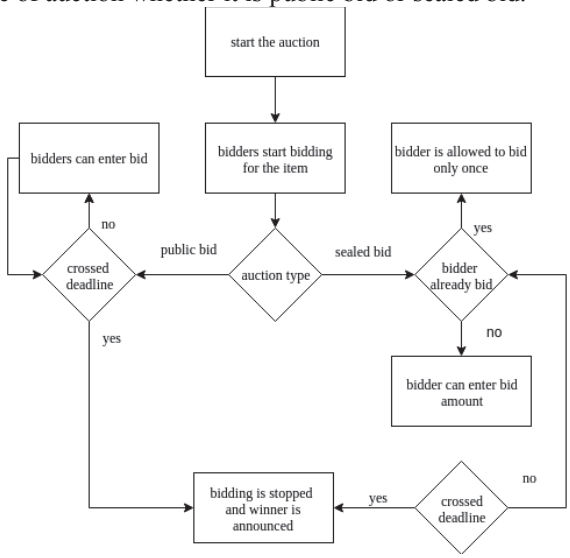

Fig. 4: The flowchart for the bidding system

Once the smart contract is instantiated the buyers can call the smart contract functions using the libraries provided by the hyperledger fabric platform.

The buyers will start the bidding next. They are allowed to bid until the deadline. If the auction type is public bidding, then the buyers can bid any number of time until the deadline is reached. The buyers can see the current highest bidder and the current highest bidding amount at any time. The buyers can verify his or her bid amount at any

time. If the auction type is sealed bid, then the buyers will be allowed to bid only once. The buyer can't see who is the highest bidder or what is the highest bidding amount. The only thing the buyers can do before the deadline is bid for the item only once and verify their bid. Once the deadline is passed the highest bidding amount and the highest bidder details can be seen by everyone in the blockchain network. The buyers can get details about the auction at any point in time.

Functions provided by the smart contract to the buyers and sellers are listed below.

instantiate: This function will be executed when the smart contract is instantiated for the first time. This function will assign bidding item name, seller public address, starting time of the auction, deadline of the auction and the auction bidding to the smart contract. The Deadline is passed as number of seconds to the instantiate function. The auction type can be either 'public' for public bid or 'sealed' for sealed bid.

Bid: This function will append the Bid amount provided by the buyer to the blockchain ledger. Before adding the bid to the ledger this function will check whether the deadline is passed or not. If the deadline is passed error message will be shown to the buyer. If the auction type is sealed then the buyers can bid only once. This function will check this condition. If the auction type is public then the buyers can bid any number of times. The algorithm is given in algorithm 1.

getDetails: This function will return the item name for which the auction is going on, the public address of the seller, the starting time of the auction, the ending of the auction and the auction type.

getBidByBidder: This function will return the bid amount given by the user. algorithm is given.

getAllBids: This function will return all the bids that have been given until now along with the associated bidder public address. If the auction type is sealed then this function will return these details only after the deadline is passed.

getHighestBid: This function will return the current highest bid amount. If the auction type is sealed bid then it will reveal the highest bid only after the deadline is passed.

getHighestBidder: This function will return the current highest bidder's public address. If the auction type is sealed bid then this will give the winner's address only after the deadline.

There is no function to end the auction. Once the deadline is crossed the bidding process will be stopped automatically and the winner will be announced.

Algorithm 1 Bid

```
Input: bidder_id, price
Output: bool
if bidType = 'sealed' then
  if getBidByBidder(bidder_id) != null then
    throw;
  end
  else
    putState(bidder_id, price);
    return;
  end
end
if bidType = 'public' then
  putState(bidder_id, price);
  return;
end
```

Algorithm 2 getBidByBidder

```
Input: bidder_id
Output: price
Bid ← getState(bidder_id)
if Bid != null then
  return Bid;
end
else
  throw
end
```

B. Advantages of this system

This system is better than the previous one because it is implemented using hyperledger fabric which is a permissioned blockchain. Hyperledger fabric can be used for open biddings where anyone can participate and confidential bidding where the bidding process should be known only to the participants. This smart contract provides an option for both public bid and sealed bid. The work done by Chen *et al* [13] didn't implement sealed bid. For auctions conducted by defence agencies and other similar agencies where the auction should be kept secret, this implementation will work since it provides integrity and confidentiality to the bidding process.

C. Drawbacks of this system

This implementation used the consensus mechanism 'solo' [5] which is suitable for proof of concepts but not suitable for production systems. Other consensus mechanisms such as 'kafka' or 'raft' can be used to overcome this issue. Since all the peers will have a copy of the blockchain, it will create a lot of issues when peers are in high numbers, so to avoid inconsistency and redundancy, Decentralized and distributed storage mechanism should be introduced for storing the blockchain. In this way, all the peers will need not store the same copy of the blockchain but at the same time, it will give immutability of the blockchain technology.

V. CONCLUSION

The proposed blockchain based Smart Bidding System for the E-Auction system is pretty powerful and secure compared to the normal web-based E-Auction system. The blockchain technology brings in confidentiality and integrity to the auction process which makes it possible to perform the auction even though some of the buyers are not trustworthy. This approach can be extended to other electronic-based systems such as electronic voting. Thus the blockchain technology is used to eliminate the middleman in the electronic bidding system. It eliminates the transaction fees given to the middleman because smart contract performs the functions of the middleman.

REFERENCES

[1] G. Cao and J. Chen, "Practical Electronic Auction Scheme Based on Untrusted Third-Party," *2013 International Conference on Computational and Information Sciences*, Shiyang, 2013, pp. 493-496.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[3] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf.

[4] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", *Ethereum Project Yellow Paper*, vol. 151, pp. 1-32, 2014.

[5] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Mu-ralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains", *Proceedings of the 13th ACM SIGOPS European Conference on Computer Systems*, 2018.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[7] J. R. Douceur, "The Sybil attack" in Peer-to-Peer Systems, Berlin, Germany: Springer, pp. 251-260, Mar. 2002, [online] Available:http://link.springer.com/chapter/10.1007/3-540-45748-8_24.

[8] Jakobsson, Markus & Juels, Ari. (1999). Proofs of Work and Bread Pudding Protocols.. Communications and Multimedia Security. 258-272. 10.1007/978-0-387-35568-9_18.

[9] S. King, S. Nadal, Ppcoin: Peer-to-peer crypto-currency with proof-of-stake self-published paper, August 2012.

[10] J. Sousa, A. Bessani and M. Vukolic, "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform," *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Luxembourg City, 2018, pp. 51-58.

[11] N. Szabo, Smart Contracts, 1994, [online] Available: http://szabo.best.vwh.net/smart.contracts.html.

[12] Gideon Greenspan, "MultiChain Private Blockchain" ,[online] Available:https://www.multichain.com/download/MultiChain-White-Paper.pdf.

[13] Y. Chen, S. Chen and I. Lin, "Blockchain based smart contract for bidding system," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 208-211.

[14] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in *IEEE Access*, vol. 6, pp. 32979-33001, 2018.