International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 04 | April -2019 ISSN: 1847-9790 || p-ISSN: 2395-0126

Secure & Efficient data transmission using Block chain in E-Bidding System

Shreyas S

M.Tech, Information Technology, The National Institute of Engineering, Mysuru.

---***---

Abstract

Because of the popularity of the Internet, the integration services have gradually changed people daily life, such as e-commerce activities on transactions, transportation and so on. The E-auction, one of the popular e-commerce activities, allows bidders to directly bid the products over the Internet. As for sealed bid, the extra transaction cost is required for the intermediaries because the third-party is the important role between the buyers and the sellers help to trade both during the auction.

In addition, it never guarantees whether the third-party is trust. To resolve the problems, we propose the blockchain technology with low transaction cost which is used to develop the smart contract of public bid and sealed bid. The smart contract, proposed in 1990 and implements via Ethereum platform, can ensure the bill secure, private, non-reputability and inalterability owing to all the transactions are recorded in the same but decentralized ledgers. The smart contract is composed of the address of Auctioneer, the start auction time, deadline, the address of current winner, the current highest price.

***Key Words*: E-auction, Public Bid, Sealed Bid, Blockchain.**

1.INTRODUCTION

Third party places a very important role in bidding. It never guarantees whether the third party is trust one. We have to pay extra money to the intermediate because he helps to trade the product between seller & bidder. E-auction has two main problems:

To help bidders & auctioneers intermediary is essential. The charge fees for the centralized intermediary to increase the transaction cost. Besides, the personal data and transaction records are stored in database might cause privacy leakage. In a sealed envelope, bidders have no way to ensure that lead bidder never leaks their bidding price.

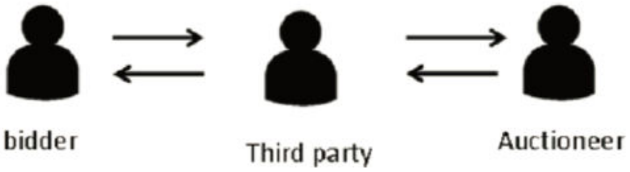


Fig. 1: The role of the E-auction

Nowadays, E-auction can be classified into two types, namely public bid and sealed bid

Public bid is that bidders could raise the price to bid the products. Thus, the bidding price gets increasing continuously until no bidders are willing to pay a higher price. The bidder is as a winner if he bids the highest price for such the product. During public bid, bidders can bid several times; thus, public bid is also called multi-bidding auction

Sealed bid is that bidders encrypts the bill and only send the bill once. If the time is due, the auctioneer compares all of the bills. The bidder who bids for the highest price is the winner of the sealed bid. Due to bidders only can bid once, it is also called single-bidding auction. In the seal bid, all bidders' prices are sealed until the bid opening deadline is compared to the prices of all bidders. There is a common shortcoming in electronic seal ticket auctions. Before the deadline for opening bids, the bidder cannot ensure that the bid price has been leaked by a third party (the principal bidder), resulting in malicious bidders may collaborate with the bid winner to obtain the best bid price.

The blockchain is a technology that accesses, verifies, and transmits network data through distributed nodes. It uses a peer-to-peer network to achieve a decentralized data operation and preservation platform

Marco Iansiti and Karim R Lakhani. "The truth about blockchain"

M Jenifer and B Bharathi. "A method of reducing the skew in reducer phase block chain algorithm"

Yan Zhu, Ruiqi Guo, Guohua Gan, and Wei-Tek Tsai. "Interactive incontestable signature for transactions confirmation in bitcoin blockchain"

The blockchain is mainly based on the following technologies as the operating base

Identity identification and security: Identification and anti-counterfeiting are performed using a public key infrastructure. Each account in the blockchain has a public key and a private key used to send and receive the transactions. After the private key encrypts the transaction message, the receiver then uses the sender's public key to decrypt the message, and the identity of the sender can be confirmed.

Message delivery and broadcasting: Message delivery and broadcasting are performed using a peer-to-peer technique, allowing each node to connect and exchange messages with each other. The transactions are stored in the same ledger. Each node in the blockchain can verify the transactions using the zero knowledge over the decentralized access structure

Data preservation and linking: The transaction data stored in a block to generate a hash value and the block is linked to the previous block with the hash values to construct a blockchain as shown in Fig below.

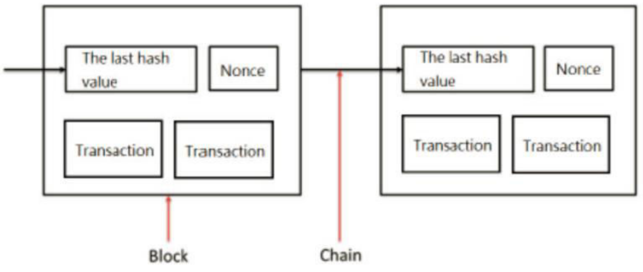
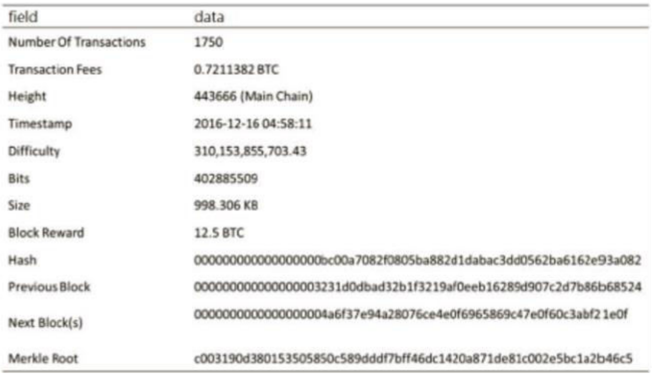


Fig. 2: The relationship between the block and chain

The fields in the block, as shown in Fig below, to detail the records of the block such as time-stamp, transaction quantity, hash value, etc.



field	data
Number Of Transactions	1750
Transaction Fees	0.7211382 BTC
Height	443666 (Main Chain)
Timestamp	2016-12-16 04:58:11
Difficulty	310,153,855,703.43
Bits	402885509
Size	998.306 KB
Block Reward	12.5 BTC
Hash	000000000000000000bc00a7082f0805ba882d1dabac3dd0562ba6162e93a082
Previous Block	000000000000000003231d0dbad32b1f3219af0eeb16289d907c2d7b86b68524
Next Block(s)	0000000000000000004a6f37e94a28076ce4e0f6965869c47e0f60c3abf2 1e0f
Merkle Root	c003190d380153505850c589dddf7bff46dc1420a871de81c002e5bc1a2b46c5

Fig 3: The field name of each block

In the blockchain, there might be different transactions in a block. When a new transaction is just triggered, each node collects unverified transactions to the block to produce a POW (Proof of Work). That is, the node can calculate the Nonce to verify the transaction as soon as possible to get some rewards. If the node completes the proof of work, it broadcast the block to other nodes to verify whether the transaction is valid. If valid, the block is attached to the Blockchain.

2. RELATED WORK

Traditional Bidding System :

Nowadays, E-auction can be classified into two types, namely public bid and sealed bid. Public bid is that bidders could raise the price to bid the products. Thus, the bidding price gets increasing continuously until no bidders are willing to pay a higher price. The bidder is as a winner if he bids the highest price for such the product. During public bid, bidders can bid several times; thus, public bid is also called multi-bidding auction. Sealed bid is that bidders encrypts the bill and only send the bill once. If the time is due, the auctioneer compares all of the bills. The bidder who bids for the highest price is the winner of the sealed bid. Due to bidders only can bid once, it is also called single-bidding auction. In the seal bid, all bidders' prices are sealed until the bid opening deadline is compared to the prices of all bidders. There is a common shortcoming in electronic seal ticket auctions. Before the deadline for opening bids, the bidder cannot ensure that the bid price has been leaked by a third party (the principal bidder), resulting in malicious bidders may collaborate with the bid winner to obtain the best bid price.

3. PROPOSED SYSTEM

This paper applies the blockchain technique into the E-auction to resolve the two main problems in the E-auction that we stated earlier.

The blockchain is peer-to-peer access structure such that points in the structure can trust each other points. Each location can securely communicate, authenticate and transfer data to any of the other sites. Consequently, in the decentralized structure, the centralized intermediary can be removed to reduce the transaction cost.

As for the second problem, the smart contract is used to avoid the bid price leaked by the lead bidder. Some rules are written inside the smart deal which cannot be opened before the deadline.

Advantages:

1.Decentralized structure for communicating between bidders and auctioneers thus reducing the charge fee.

2.Peer to peer access structure to establish the trust thus protecting the personal data and transactional records.

3.The bid price leaked by the lead bidder will be avoided through the smart contract.

Objectives:

To design and implement the blockchain technique into the E-auction.

To design decentralized structure for communicating between bidders and auctioneers to reduce the charge and transactional cost.

To ensure that the personal data of the parties and the transactional records are protected through peer to peer access

To ensure the bid price isn't leaked by the lead bidder by introducing the smart contract between the parties.

To design and develop a simple and efficient user interface for both the bidders and auctioneers to perform their respective functionalities.

4. METHODOLOGY

The flowchart of E-auction is shown in Fig below

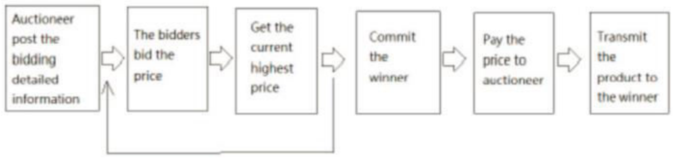

Auctioneer post the bidding detailed information
The bidders bid the price
Get the current highest price
Commit the winner
Pay the price to auctioneer
Transmit the product to the winner

Fig. 4: The flowchart of E-auction

The seller post the bidding information including product description and starting price at the first stage. Bidders vote the sealed envelope to bid the product with a higher price. After receiving the sealed envelope, the auctioneer announces the highest rate right now. 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 get the money from winner and send the product to the bidder. We develop an open bidding system through blockchain with smart contracts. Bidders 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.

A complete public E-auction system must satisfy the following requirements

The identity of the person who is a bidder or winner (successful bidder) is anonymous to everyone.

During a transaction, the content of seal order cannot be modified, and all the people can verify whether its correctness and completeness.

No illegal bidder can impersonate the legal one to bid the product. After bidding, no one can deny the bidding if they have ever bidded.

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

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.

A fair solution is required if the same price is voted by two different bidders.

In an intelligent agreement, the contract is started if the time or event is triggered, such as sending a message, dealing with transactions, terminating the contract. The bytecode of smart contract retrieved with JSON format is used for broadcasting all the nodes of blockchain and wait for verifying. If true, the smart contract is announced with individual contract address and JSON Interface to allow the other person to join in. 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 initialization data, we will announce the following information in advance.

Auctioner: The tenderer address used to record the originating contract.

AuctionStart: Used to announce the start time of the bid.

biddingTime: Used to announce the effective time of the contract.

highestBidder: The address of the bidder who currently bids the product with the highest price.

highestBid: Used to record the current highest price

As for the contract, we define the following function:

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

Bid(): This function can be called by any person to perform 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.

reveal(): Opens the bid by calling this function, and compares the prices of all the tickets to get the final winner.

AuctionEnd(): In this function, AuctionStart and biddingTime are automatically used to determine 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.

withdraw(): Returns the amount of bids tendered by bidders other than the successful bidder

4. CONCLUSIONS

This paper provides an E-auction mechanism based on blockchain to ensure electronic seals confidentiality, non-repudiation, and unchangeability. We expect to encounter potential problems in the implementation of this work. In smart contracts for sealed orders, due to the complexity of the contract, the bidders and bidders come, say may call the wrong contract function. For example, the bidder inadvertently calls Reveal() to open all bids, so that the bidding must be terminated and re-arranged. For this purpose, we will set the authority judgment for different functions and will perform the function before first determine if the caller can perform this function.

ACKNOWLEDGEMENT

I would like to thank Lokesh S, Associate Professor at NIE, Mysore for his guidance and support in doing research of the above paper.

REFERENCES

[1] Decentralizing Ascending Auctions on Blockchain https://medium.com/auctionity/decentralizing-ascending-auctions-on-blockchain-dffab74446c1

[2] Verifiable Sealed-Bid Auction on the Ethereum Blockchain https://eprint.iacr.org/2018/704.pdf

[3] HOW BLOCKCHAIN CAN BE USED IN AUCTIONS? https://www.blockchain-council.org/blockchain/blockchain-can-used-auctions-works/

[4] Christopher K Frantz and Mariusz Nowostawski. From institutions to code: Towards automated generation of smart contracts. In Foundations and Applications of Self* Systems, IEEE International Workshops on, pages 210–215. IEEE, 2016.