IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10220

BLOCKCHAIN BASED SMART CONTRACT FOR BIDDING SYSTEM

Mr. Raghavendraachar S[1], Amogha H S[2], Adith Karthik Raju[3], Gagan Reddy S[4], Talluru Maurya[5]

Assistant Professor, Dept of Computer Science, K S Institute of Technology, Bengaluru, Karnataka[1]

Dept of Computer Science, K S Institute of Technology, Bengaluru, Karnataka[2-5]

Abstract: Due to the widespread use of the Internet, integration services have steadily transformed how people live their daily lives,including how they conduct business online, travel, and other things. One of the most well- liked forms of online commerce is the E-auction,which enables bidders to place direct bids onthings. Regarding sealed bids, an additional transaction fee is necessary for the middlemen because they play a crucial role in facilitating trade between the buyers and sellers throughout the auction. Furthermore, it never guarantees the dependability of the third party. In order to resolve the concerns, we propose leveraging blockchain technology, which has low transaction costs, to develop smart contracts for open and sealed bids. The smart contract, first conceived in 1990 and implemented via the Ethereum system, may guarantee the bill is secure, private, unreliable, and unalterable because all transactions are recorded in the samebut decentralized ledgers. The smart contract contains the following information: the address of the auctioneer, the start and end times of theauction, the deadline, the location of the currentwinner, and the most recent price

I. INTRODUCTION

Trillions of dollars have been exchanged for goods and services through online auctions in recentdecades, which has benefited the global economy. Asa means for the vendor to publicize the sale of their assets, buyers participate in auctions by submitting competitive bids that signify the greatest amountsthey are glad to pay. Practically speaking, bidding encourages a variety of financial advantages for the efficient exchange of goods and services. Trillions ofdollars have been exchanged for economic consumption through online auctions in recent decades, which benefited the global economy. Buyers participate in auctions by submittingcompetitive bids that represent the highest amounts they are ready to pay as a way for sellers to publicize the sale of their goods. Practically speaking, auctions promote a variety of financial upper hands for the efficient exchange of goods and services. With the inconsistencies of the vanquisher paying the second-top most, it is comparable to FPSBA (Vickrey auctions). Escalating bid open auctions (English auctions). A bidder will cease bidding and make greater offers if they are unwilling to pay more thanthe highest offer that has already been made. Descending bid open auctions. The cost is initially set high by the barker and then gradually brought down to a decision to buy at the present price. One could contend that the main advantage of sealed- bid auctions is that no bidder learns about the other bids. Therefore, bidders are asked to submit proposals that accurately depict the asset's financialvalue to them. However, a deal between the barker and a dishonest bidder could nullify the advantage. In other words, there is a conflict between maintaining the privacy of the bids and trusting the auctioneer to select the winning bid. In order to achieve publicly verifiable correctness sealed bid online auctions while maintaining the bidders' privacy, cryptographic techniques can be implemented. According to a recent magazine report, the Ukrainian justice ministry conducted theexamination on top of the blockchain auctions in aneffort to boost the transparency of governmental operations. The main goal is to improve the security and openness of the auction system so that anybody may access the information and look for fraud.

II. LITERATURE REVIEW

Nowadays, E-auctions can be classified into two types: public bids and sealed bids.A public bid is when bidders could raise the priceto bid on the products. Thus, the bidding price gets increasing continuously until no bidders are willing to pay a higher price. The bidder is a winner if he bids the highest price for such a product. Duringpublic bids, bidders can bid several times; thus, the public bid is also called a multi-bidding auction.

A sealed bid is when bidders encrypt 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 alsocalled a single-bidding auction. In the sealed 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

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10220

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 aboutblockchain” M Jenifer and B Bharathi. "A method of reducing the skew in reducer phase blockchain 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 followingtechnologies as the operating base identity identification and security: Identification and anti-counterfeiting are performed using the public keyinfrastructure. Each account in the blockchain has a public key and a private key used to send and receivetransactions. After the private key encrypts the transaction message, the receiver then uses the sender’s public key to decrypt the message, and theidentity 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. Eachnode in the blockchain can verify the transactions using the zero-knowledge of the decentralized access structure.

Data preservation and linking:
The transaction data is stored in a block to generatea hash value and the block is linked to the previous block with the hash values to construct a blockchain 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. Inthe 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 Nonceto 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 verifywhether the transaction is valid. If valid, the blockis attached to the blockchain

2.1 Election and Blockchain Technology
E-voting is currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting [A. Barnes, C. Brake, and T. Perry, “Digital Voting with the use of Blockchain Technology"] Since then, a legally binding online voting systemhas been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on [T. Martens, “Verifiable Internet Voting inEstonia,”] But it still has considerable security issues and the selection is often canceled.

Although gettinga lot of attention, the online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated. The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transactionthat can be created into a blockchain that can work totrack voice counting. In this way, everyone can approve the final calculation because of the openblockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.

III. OBJECTIVES

With the use of blockchain technology, many things can be done better, more securely, and in a transparent manner, and a regular person caninfluence some portions of its future developments in our case, this would be changing the auctionmarket and business for the better. For the endbidder/buyer and the seller. In this paper, we propose a system in which coins are used to complete transactions between agents.

The coin represents a part of the device and acts as proof of ownership. For building blockchain-basedapplications, some factors have to be taken intoconsideration. Building a blockchain from scratchis a complex task. There are multiple platformsavailable for creating blockchain-based applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10220

IV. METHODOLOGY

The seller post the bidding information including the product description and starting price at the firststage. Bidders vote on the sealed envelope to bid onthe product with a higher price. After receiving the sealed envelope, the auctioneer announces the highest rate right now. The bidder is the winning bidder until no one bids on the product with the higher price or the deadline is due. The auctioneer can get the money from the 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 theblockchain. With a decentralized access structure, all bidders can bid on the product by calling the open contract's trading contract without intermediate brokers. A complete public E-auction system must satisfy the following requirements:

a) The identity of the person who is a bidder or winner (successful bidder) is anonymous to everyone. During a transaction, the content of the seal order cannot be modified, and all the people can verify whether its correctness and completeness.
b) No illegal bidder can impersonate the legal one tobid on the product. After bidding, no one can deny the bidding if they have ever bedded.
c) The successful bidder always has the proof to get the product.
d) The seller can get the money from the successful bidder but not from the other bidder.
e) The sealed envelope must be delivered before the deadline; otherwise, the envelope is invalid.
f) The sealed envelope is private before the deadline,and no one can open it.

In an intelligent agreement, the contract is started if the time or event is triggered, such as sending amessage, dealing with transactions, or terminatingthe contract. The bytecode of the smart contract retrieved with JSON format is used for broadcasting all the nodes of the blockchain and waiting for verification. If true, the smart contract is announced with an individual contract address and JSONInterface 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 envelopesare 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.

a) **Auctioneer:** The tenderer address used to recordthe originating contract.
b) **Auction Start:** Used to announce the start timeof the bid.
c) **Bidding time:** Used to announce the effectivetime of the contract.
d) **Highest bidder:** The address of the bidder who currently bids on the product with the highest price.
e) **Highest bid:** Used to record the current highest price.

As for the contract, we define the following function:

a) **blind Auction():** Activate the contract by calling this function, and use the auction start and bidding End to record the start and end time.
b) **Bid():** This function can be called by any personto perform the bidding action. Before the function is executed, Auction Start and bidding time areused to judge whether the contract is expired. If not, the bidder can send the bid envelope if theprice is greater than the current highest price. The contract system will use the highest bid and highestbidder to record the current highest price and the corresponding bidder's address.
c) **reveal():** Opens the bid by calling this function, and compares the prices of all the tickets to get the final winner.
d) **Auction End():** In this function, Auction Start and bidding time are automatically used to determine the contract validity time. If the effectivetime ends, the successful bidder's Address and the current highest price will be automatically sent to the tenderer. This function will be disabled to avoidrepeated execution.
e) **withdraw():** Returns the number of bids tendered by bidders other than the successful bidder

V. CONCLUSION

In order to ensure the unchangeability, non-repudiation, and confidentiality of electronic seals, this project provides a blockchain-based E-auctiontechnique. We propose to develop sealed-bid and open-bid smart contracts utilizing low-cost blockchain technology. Because all transactions are recorded in the same but decentralized ledgers, the smart contract, initially proposed in 1990 and implemented via the Ethereum platform, may ensure that the bill is secure, private, unreliable, and unalterable. The smart contract contains thefollowing information: the address of the auctioneer, the start and end times of the auction, the deadline, the address of the current winner, and the most recent price.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10220

REFERENCES

[1] Gang Cao and Jie Chen. Practical electronic auction scheme based on untrusted third-party. InComputational and Information Sciences (ICCIS), 2013 Fifth International Conference on, pages 493–496. IEEE, 2013.

[2] llichetty S Chandrashekar, Y Narahari, Charles HRosa, Devadatta M Kulkarni, Jeffrey D Tew, andPankaj Dayama. Auction-based mechanisms forelectronic procurement. IEEE Transactions on Automation Science and Engineering, 4(3):297–321, 2007.

[3] Wen Chen and Feiyu Lei. A simple efficient electronic auction scheme. In Parallel and Distributed Computing, Applications and Technologies, 2007. PDCAT'07. Eighth International Conference on pages 173–174. IEEE,2007.

[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.

[5] Marco Iansiti and Karim R Lakhani. The truth about blockchain. Harvard Business Review, 95(1):118– 127, 2017. [6] M. Jenifer and B. Bharathi, in a technique for decreasing the skew in the blockchain algorithm's reducer phase. International Conference on Circuit, Power, and Computing Technologies (ICCPCT), pages 1-4. IEEE, 2016