Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

BLOCKCHAIN BASED SMART CONTRACT FOR BIDDING SYSTEM

#1**RAMAKRISHNA VEMULA,** ***Research Scholar,***

#2**Dr. ANOOP SHARMA,** ***Guide,***

Department of Computer Science & Engineering,

UNIVERSITY OF TECHNOLOGY, JAIPUR, RAJASTHAN

Corresponding Author: *Ramakrishna Vemula*, vemula.ramakrishna@yahoo.com

ABSTRACT: Because so many people use the Internet for shopping, transportation, and other purposes, e-commerce and other related services have gradually changed people's life. E-auctions, which allow individuals to bid on items, are a popular way for consumers to buy things online. When hidden bids are used, middlemen that assist buyers and sellers in conducting business at auctions must pay additional transaction fees. Furthermore, there is no guarantee that the third party can be trusted. Blockchain technology is being utilized to develop smart contracts that can manage both open and closed bids at minimal cost in order to tackle the difficulties. Smart contracts, invented in the 1990s and now widely used on the Ethereum platform, keep everything on the same decentralized ledgers. This may safeguard privacy, security, the inability to be amended, and the inability to be retracted. The smart contract contains the address of the auctioneer, the start and end hours, the address of the current winner, and the highest bid. To sign up for a free account, you must have an Ethereum wallet. At the mining gate, you can earn money for the transaction fee associated with the mining stage. The recording process synchronizes all the nodes on the blockchain, which is how smart contracts are created.

Keywords: E-auction, Public Bid, Sealed Bid, Blockchain,Smart Contract

1.INTRODUCTION

E-auctions have grown in popularity in recent years due to their ease of use and efficiency [1, 3, 9, 10, 11, 13]. To lower transaction costs, electronic auction bidding use network technologies. Figure 1 depicts the key E-auction stakeholders as bidders, auctioneers, and a third party. The vast majority of third-party intermediaries help with product posting, tracking the highest offer price, and selecting the winning bidder. Bidding systems on eBay and Yahoo are two examples. Electronic auctions, on the other hand, face two important challenges. In a bidding system, a central mediator is required to promote communication between bidders and auctioneers. The fees charged by the intermediary raise the transaction expenses. The storage of personal and transactional data in a database may also constitute an invasion of privacy. Bidders cannot ensure that the successful bidder will not reveal the value of their sealed proposal.

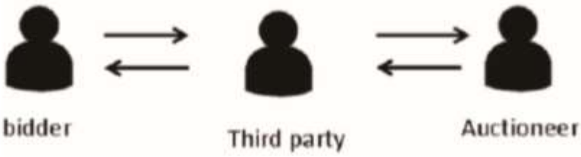


Fig. 1: Capability to conduct online auctions

Blockchain technology is employed in this study to overcome two problems with E-auctions. The blockchain is a decentralized network based on nodes' mutual trust. Every website is capable of securely communicating with other websites, authenticating identities, and transmitting data. Decentralization lowers transaction costs by reducing the requirement for a centralized mediator [7, 15]. A smart contract, on the other hand, forbids the leading purchaser from exposing the offered price. Some smart contract terms are unreachable until a specific date.

The structure of this document is as follows. The following section contrasts blockchain-based auctions with traditional auctions. The third section discusses how blockchain technology can be used to facilitate bidding. Section 4 conducts experiments to support the proposed method, and Section 5 summarizes the results and draws conclusions.

2.RELATED WORKS

Traditional Bidding System

Electronic auctions are classified into two types: open bid and confidential bid. Public bidding enables bidders to present more competitive product ideas. As a result, the auction price climbs until no bidders remain. The bidders who offer the greatest price for a commodity win. During public auctions, many proposals are typically offered, hence the phrase "multi-bidding auction." Bidders must encrypt and email their proposal just once throughout the secret bidding process. All bills received after the deadline are reviewed by the auctioneer. The seal auction winners are those who make the greatest money. In a "single-bid auction," bidders can only submit one proposal. The sealed bid approach conceals bidders' pricing until the bid opening deadline, when they are compared to find the best price. Buying electronic seal tickets is frequently difficult. The bidder cannot guarantee that an external entity, such as the leading bidder, has not disclosed the offer price prior to the start of bidding without authority. As a result, unethical bidders may conspire with the successful bidder to acquire the best offer price.

Blockchain

Blockchain technology facilitates network data access, verification, and transmission through decentralized nodes [5, 6, 14]. To run and store data, the system employs a decentralized peer-to-peer network. The fundamental blockchain technology are as follows:

This conversation is about identification and security. The use of public key infrastructure allows for the detection and prevention of counterfeiting. For transaction transmission and receipt, each blockchain account has a public and private cryptographic key. The recipient decrypts the transaction message using the originator's public key after encrypting it with the private key. Message and data distribution across numerous channels and platforms. Nodes can exchange messages and communicate with one another using peer-to-peer communication. A centralized ledger is used to record transactions. Each node in a decentralized access hierarchy verifies blockchain transactions using a zero-knowledge protocol.From block transaction data, a unique hash value is generated during the data preservation and linkage process. Figure 2 demonstrates how hash values link this block to the prior block via the preceding block in order to build a blockchain. Figure 3 shows the records of the block, which include the time stamp, the number of transactions, the hash value, and other information.

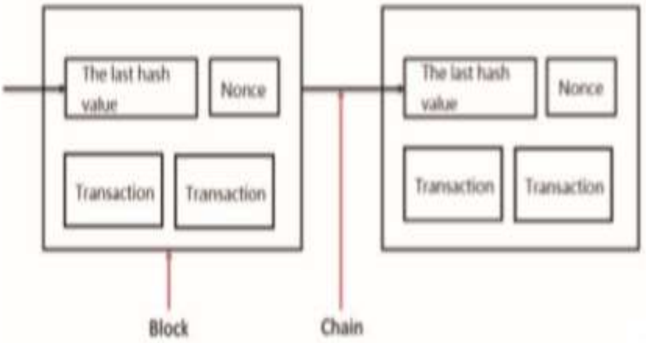
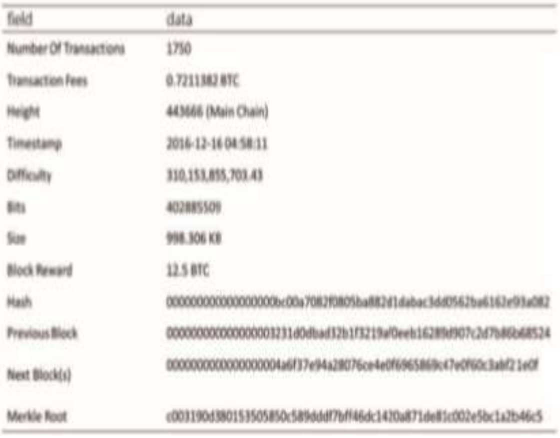


Fig. 2: Transactional association in the blockchain



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	0000000000000000003231d0dbad32b1f3219af0eeb16289d907c2d7b86b68524
Next Block(s)	0000000000000000004a6f37e94a28076ce4e0f6965869c47e0f60c3abf21e0f
Merkle Root	c003190d380153505850c589dddf7bff46dc1420a871de81c002e5bc1a2b46c5

Fig. 3: Unit identification

Blocks can include a large number of transactions when using blockchain technology. By consolidating unconfirmed transactions into a block, each node in the network creates a Proof of Work for each new transaction. To authenticate the transaction and gain incentives, the node can quickly calculate the Nonce. Following completion of the proof of work, the node sends the block to other nodes for validation. The block is sent to the blockchain when it has been validated.

3.Research Method

A flowchart of the E-auction procedure is shown in Figure 4. Bidding details such as the product description and opening bid are initially published by the vendor. Bidders vote on price increases by mailing product proposals in sealed envelopes. The auctioneer reveals the highest bid after opening the sealed envelope. A bidder is not considered successful until no other bidders outbid them or the bidding period expires. The auctioneer can collect payment and manage delivery from winning bidders. A public procurement procedure is established using blockchain and smart contracts. Bidders use blockchain to register trade contracts. All purchasers can bid directly on a product utilizing the open contract's trade contract in a decentralized access structure, removing the need for intermediaries.

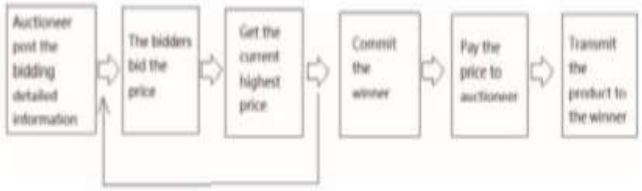

Auctioneer post the bidding detailed information
The bidders bid the price
Get the current highest price
Commit the winner
Pay the price to auctioneer
Transmit the product to the winner

Fig. 4: The electronic auction process and decision points are depicted in this diagram.

- A complete public electronic auction system must safeguard the identity of bids and winners.
- Seal orders cannot be changed during a transaction, and all parties may authenticate their legitimacy and completeness.
- In order to put an offer on a commodity, an unauthorized bidder may not mimic a legal bidder. A suggestion cannot be challenged after it has been filed.
- The winning bidder always has the requisite evidence.
- Only the winning bidder is permitted to pay the seller.
- The envelope shall be considered null and void if it is not delivered by the deadline.
- Sealing the envelope before the deadline assures that the contents remain private.
- When two plans have equal prices, a reasonable solution must be discovered.
- Smart contracts developed on Ethereum [4, 12] involve computer instructions in addition to numerical data. A well-informed contract begins when a message is sent, transactions are completed, or the contract expires. Smart contracts are written in the programming languages Solidity, Serpent, LLL, and EtherScript. This article makes use of robustness. For verification, all blockchain nodes receive the JSON-formatted output of a smart contract. Validated smart contracts make their contract address and JSON interface visible to others, allowing them to participate. Watch Contracts are used by Ethereum Wallet to summon participants. Before the deadline, all eligible vendors may submit updated price in a sealed envelope. Each envelope is opened at the appropriate time. The envelope with the highest value wins.
- Preliminary data will be used to present future information.
- The auctioneer's address identifies the contract's origin.
- When the "Auction Start" option is selected, the bidding process begins, and "Bidding Time" marks the start of the contract.
- The top vendor is the person or organization

that made the most competitive bid for a commodity.

- The term "Highest Bid" refers to the highest price currently being offered.
- The following function is specified in the contract: The contract is initiated using the Blind Auction() method, and the auction Start and bidding End variables supply the start and end timestamps.
- "Bid()" can be used by anyone to start a negotiation. The "Auction Start" and "Bidding Time" parameters define the contract's expiration status before ending the function. The bid envelope may be filed if the bidder's price is higher than the highest price. Using the highest proposal and highest bidder processes, the contract management system will record the highest price and bidder's address.
- The "Reveal()" function starts bidding and compares ticket prices to identify the winner.
- Using the "Auction Start" and "Bidding Time" options, the "Auction End()" function automatically calculates contract validity. After the validity period has expired, the winning bidder's address and highest bid will be communicated as soon as possible. By deactivating the function, redundancy is avoided.
- The "Withdraw()" function retrieves the offers of unsuccessful respondents.

4.EMPIRICAL RESULTS

The researchers used two Ethereum Wallet-based blockchain accounts to test and implement bidding transactions. As illustrated, we mine data and earn cryptocurrency for transaction fees using command-line and Miner Gate software. The command-line interface for monitoring blockchain block transaction status is shown in Figure 6. Smart contracts are created, compiled, and marketed using the Solidity programming language. The real-time compiler in Solidity generates bytecode. Figure 5 demonstrates the interface creation using the Solidity runtime. Figure 7 depicts the Ethereum Wallet's ability to publish the smart contract to the blockchain. The address of the smart contract is determined during testing by confirming it. The Solidity and Interface of the second account may make it easier to incorporate contract proposals.

A programming language's three components are the interface, smart contract, and payload.

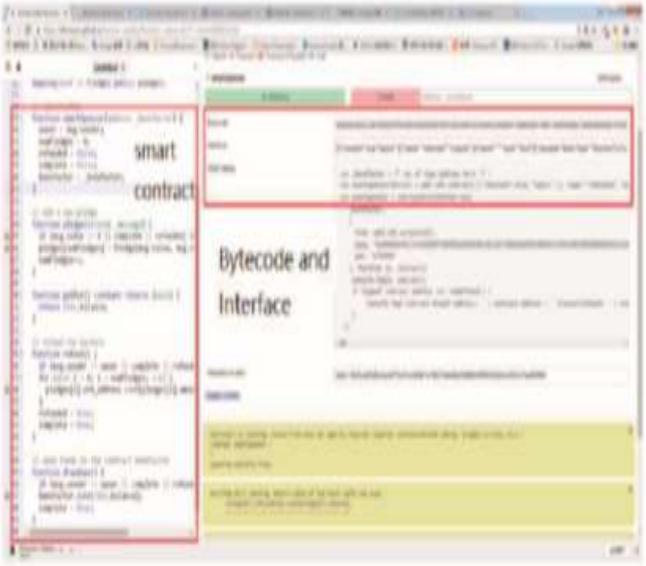


Fig. 5 A programming language's three components are the interface, smart contract, and payload..

Fig. 6: Complexity of smart contracts.

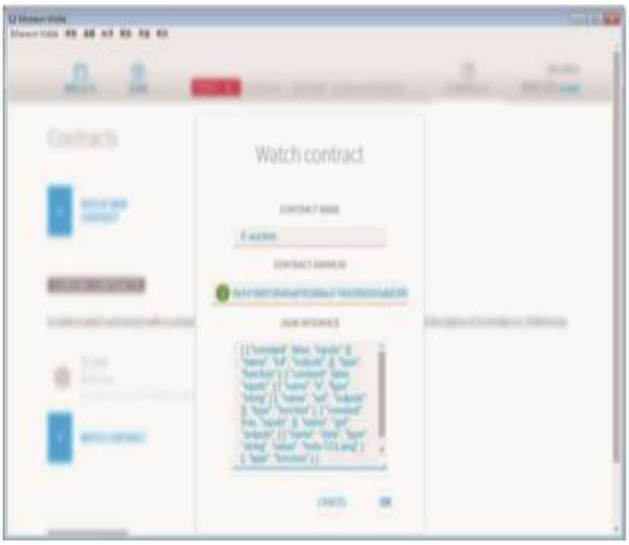


Fig. 7: This is an official announcement about the deployment of smart contracts..

5.CONCLUSIONS

This article covers a groundbreaking E-auction technique that uses blockchain technology to ensure electronic seal confidentiality, non-repudiation, and immutability. It is expected that difficulties would develop throughout the execution of this project. It is critical to note that due to the intricacy of smart contracts for confidential orders, bids and bidders may mistakenly call the erroneous contract function. Consider the case where a bidder unintentionally calls the Reveal() function, revealing all bids. As a result, the bidding process must be cancelled and restructured. To accomplish our goal, we will analyze the authority relevant to various functions and will only run the function after confirming the caller's capability to perform the function.

REFERENCES

1. Gang Cao and Jie Chen. Practical electronic auction scheme based on untrusted third-party. In Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, pages 493–496. IEEE, 2013.
2. 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.
3. M Jenifer and B Bharathi. A method of reducing the skew in reducer phase?block chain algorithm. In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on, pages 1–4. IEEE, 2016.
4. Junichi Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, and Akihiko Akutsu. The blockchain-based digital content distribution system. In Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on, pages 187–190. IEEE, 2015.
5. Wenbo Shi, Injoo Jang, and Hyeong Seon Yoo. A sealed-bid electronic marketplace bidding auction protocol by using ring signature. In Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on, pages 1005–1009. IEEE, 2009.
6. Wee-Kheng Tan and Yung-Lun Chung. User payment choice behavior 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.
7. Hu Xiong, Zhiguang Qin, Fengli Zhang, Yong Yang, and Yang Zhao. A sealed-bid electronic auction protocol based on ring signature. In Communications, Circuits and Systems, 2007. ICCCAS 2007. International Conference on, pages 480–483. IEEE, 2007.
8. 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.
9. Fangguo Zhang, Qiongfang Li, and Yumin Wang. A new secure electronic auction scheme. In EUROCOMM 2000. Information

Systems for Enhanced Public Safety and Security. IEEE/AFCEA, pages 54–56. IEEE, 2000.

10. Yan Zhu, Ruiqi Guo, Guohua Gan, and Wei-Tek Tsai. Interactive incontestable signature for transactions confirmation in bitcoin blockchain. In Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual, volume 1, pages 443–448. IEEE, 2016.