ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

SMART CONTRACT AND BLOCKCHAIN-BASED TRADING SYSTEM

[#1]**Mr.BOLLI RAMESH,** *Assistant Professor*

[#2]**Mr.KANDUKURI CHANDRA SENA CHARY,** *Assistant Professor*

Department of Computer Science and Engineering,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Because the Internet is so widely used, integration services such as e-commerce for shopping, transportation, and other activities have gradually changed people's lives. E-auctions are a well-known sort of e-commerce in which consumers can bid on items via the Internet. When sealed bids are used, middlemen must pay additional transaction fees since they assist buyers and sellers in conducting business at auctions. Furthermore, there is no guarantee that the third party can be trusted. To address the challenges, blockchain technology is used to create smart contracts with cheap processing costs for both open and private bids. Smart contracts, which were developed in the 1990s and are currently employed on the Ethereum platform, may preserve privacy, security, non-repudiability, and immutability by keeping everything on the same decentralized ledgers. The smart contract contains the address of the auctioneer, the start and end hours, the address of the current winner, and the highest price. An Ethereum wallet is required to create a free account. The mining Gate is used to collect funds for the mining stage's transaction fee. The blockchain nodes are brought into sync during the recording process, which results in smart contracts.

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 effectiveness [1, 3, 9, 10, 11, 13]. To reduce transaction costs, network technology is used in electronic auction bidding. Figure 1 depicts the primary stakeholders in an E-auction: bidders, auctioneers, and a third party. Most third-party intermediaries help with product posting, tracking the highest bid price, and selecting the successful bidder. Bidding systems on eBay and Yahoo are two examples. Electronic auctions, on the other hand, face two major obstacles. A central mediator is required in a bidding system to assist bidders and auctioneers in communicating. The fees charged by the centralized intermediary enhance transaction expenses. Personal and transaction records saved in a database may also infringe privacy. Bidders cannot ensure that the winning bidder would not reveal the amount of their proposal in a sealed envelope.

Fig. 1: Online auction function

In this study, blockchain technology solves two E-auction problems. The blockchain is a decentralized network in which nodes trust one another. Every site may securely communicate

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

with another site, authenticate identities, and send data. Decentralization reduces transaction costs by eliminating the requirement for a centralized mediator [7, 15]. A smart contract, on the other hand, forbids the lead bidder from disclosing the offered price. Some smart contract clauses are inaccessible until a specific date.

The following is the structure of this document. This section contrasts blockchain bidding with traditional bidding. The third section explains how blockchain can be used in bidding. Section 4 conducts experiments to support the proposed method, and Section 5 summarizes the findings and provides conclusions.

2.RELATED WORKS

Traditional Bidding System

There are two types of E-auctions: open bid and confidential bid. Bidders can use public bidding to present competitively higher product bids. As a result, the auction price climbs until no bids are received. Winners are the bidders who offer the highest price for a commodity. Bidders frequently place multiple bids during public bidding, hence the term "multi-bidding auction." Bidders must encrypt and email their proposal once throughout the private bid process. The auctioneer compares all invoices beyond the deadline. The seal bidding winners are those who make the most money. Bidders in a "single-bidding auction" can submit only one proposal. The sealed bid technique conceals bidders' pricing until the bid opening deadline, at which point it is compared to establish the best price. Purchases of electronic seal tickets frequently have issues. The bidder cannot guarantee that an external entity, such as the lead bidder, has not released the offer price without permission before bidding begins. As a result, unethical bidders may work with the winning bidder to obtain the best offer price.

Blockchain

Through decentralized nodes, blockchain technology simplifies network data access, verification, and transfer [5, 6, 14]. The system uses a peer-to-peer network to run and store data decentralized. The following are the blockchain's fundamental technologies:

This discussion focuses on identity and security. Using 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 with the originator's public key after encrypting it with the private key. Message and data distribution over multiple channels and platforms. Peer-to-peer communication allows nodes to communicate with one another and share messages. The transactions are recorded in a common ledger. Each node in a decentralized access hierarchy validates blockchain transactions with a zero-knowledge protocol.From block transaction data, data preservation and linkage generates a unique hash value. Figure 2 depicts how hash values link this block to the previous block in order to construct a blockchain. Figure 3 depicts the block's records, which include the time stamp, transaction quantity, hash value, and other information.

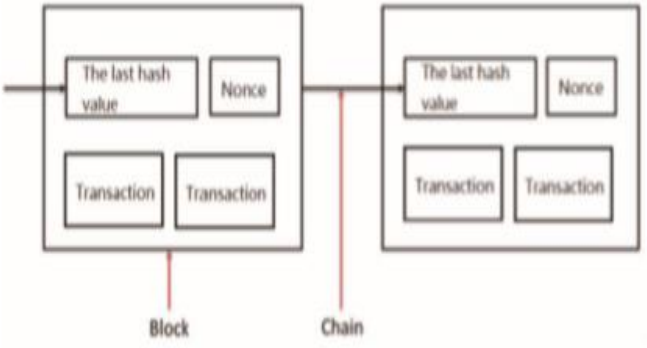

Fig. 2: Association of blockchain blocks

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

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	0000000000000000bc00a7082f0805ba882d1dabac3dd0562ba6162e93a082
Previous Block	0000000000000000323 1d0dbad32b1f3219af0eeb16289fd907c2d7b86b68524
Next Block(s)	000000000000000004a6f37e94a28076ce4e0f6965869c47e0f60c3abf21e0f
Merkle Root	c003190d38015350585 0c589dddf7bff46dc1420a871de81c002e5bc1a2b46c5

Fig. 3: Unit identification

Blockchain technology enables blocks to contain a large number of transactions. For each new transaction, each node in the network generates a Proof of Work by combining unconfirmed transactions into a block. The node can compute the Nonce quickly in order to authenticate the transaction and obtain incentives. After finishing the proof of work, the node sends the block to other nodes for verification. The block is added to the blockchain when it has been validated.

3.Research Method

The flowchart of the E-auction process is shown in Figure 4. Initially, the seller posts bidding information such as product description and starting price. Bidders vote to boost the price by mailing sealed envelopes containing product proposals. The auctioneer announces the highest offer after opening the sealed envelope. Until no one else bids higher or the bidding period closes, a bidder is considered successful. Auctioneers can collect payment from winning bidders and arrange delivery. A public tendering process is created by blockchain and smart contracts. Bidders use blockchain to record trade contracts. In a decentralized access structure, all purchasers can directly bid on a product using the open contract's trade contract, removing the need for middlemen.

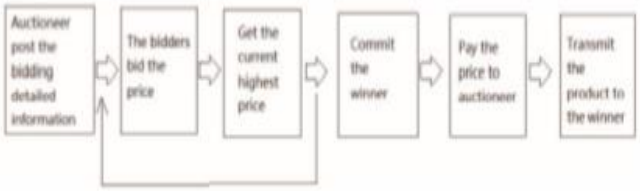

Fig. 4: Diagram of the electronic auction procedure and decision points.

- A complete public electronic auction system must secure the identity of bids and winners.
- During a transaction, seal orders cannot be modified, and all parties may verify their authenticity and completeness.
- An unauthorized bidder may not bid on a commodity by impersonating a lawful bidder. A proposal cannot be contested after it has been filed.
- The successful bidder always has the required proof.
- The vendor can only be paid by the winning bidder.
- The sealed envelope must be delivered before the deadline or it will be considered null and invalid.
- Sealing the envelope before the deadline ensures that it remains private.
- When two offers have the same price, a reasonable solution is required.
- Smart contracts implemented on Ethereum [4, 12] include computer instructions as well as numerical values. A well-informed contract begins when a message is sent, transactions are completed, or the contract expires. Solidity, Serpent, LLL, and EtherScript are the languages used to create smart contracts. Solidity is used in this article. A smart contract's JSON-formatted bytecode is delivered to all blockchain nodes for verification. Validated smart contracts publish their contract address and JSON interface, making it possible for others to participate. Watch Contracts are used by Ethereum Wallet to invite participants. Before the deadline, all

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

qualifying vendors can submit updated pricing in a sealed envelope. Each envelope is opened at the appropriate time. The envelope with the highest value wins.

- We will provide future information in the form of preliminary data.
- The auctioneer's address establishes the contract's origin.
- The bidding process is initiated by pressing the "Auction Start" button.
- "Bidding Time" signals the commencement of the contract.
- The top bidder is the individual or organization who has placed the highest bid on a product.
- "Highest Bid" refers to the current highest price.
- The following function is specified in the contract:
- The contract is initiated by the Blind Auction() method, and the auction Start and bidding End variables provide the start and end timestamps.
- "Bid()" can be used by anyone to begin bidding. Before completing the function, the contract's expiration status is determined by the "Auction Start" and "Bidding Time" fields. If the bidder's price is higher than the highest price, they may submit the bid envelope. Using the highest proposal and highest bidder processes, the contract management system will record the highest price and bidder's address.
- The "Reveal()" function initiates bidding and compares ticket prices to determine the winner.
- The "Auction End()" function calculates contract validity automatically based on the "Auction Start" and "Bidding Time" parameters. After the effective period, the address and highest price of the winning bidder will be communicated promptly. Redundancy is avoided by deactivating the function.
- The "Withdraw()" function returns the bids of unsuccessful bidders.

4.EMPIRICAL RESULTS

To test and execute bidding transactions, the researchers employed two Ethereum Wallet-based blockchain accounts. As demonstrated, we mine data and earn cryptocurrency for transaction fees using command-line and Miner Gate software. Figure 6 depicts the command-line interface for verifying the progress of blockchain block transactions. A smart contract is written, compiled, and advertised using the Solidity programming language. Bytecode is generated by the Solidity real-time compiler. Figure 5 shows how the interface is developed using the Solidity runtime. Figure 7 depicts the Ethereum Wallet's ability to publish the smart contract to the blockchain. During testing, the smart contract's address is determined by checking it. Solidity and Interface in the second account may aid in the addition of contract proposals.

Interface, smart contract, and bytecode.

Fig. 5 Interface, smart contract, and bytecode.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

Fig. 6: Complexity of smart contracts.

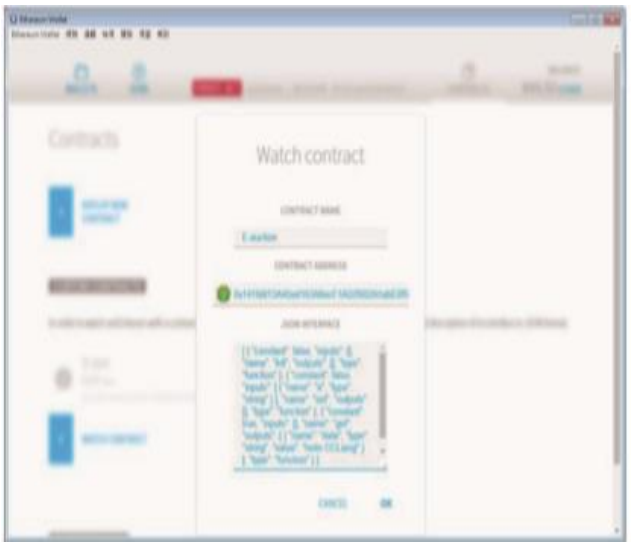

Fig. 7: This is a formal announcement about the deployment of smart contracts.

5.CONCLUSIONS

This article discusses a revolutionary E-auction approach that uses blockchain technology to assure electronic seal confidentiality, non-repudiation, and immutability. It is expected that probable impediments would occur throughout the execution of this project. It is vital to highlight that the intricacy of smart contracts for confidential orders may result in both bids and bidders mistakenly calling the erroneous contract function. As an example, suppose a bidder unintentionally runs the Reveal() function, revealing all bids. As a result, the tendering process must be terminated and reorganized. To accomplish our goal, we will evaluate the authority applicable to various functions, and we will only execute the function after a prior verification of 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.

ISSN2454-9940
www.ijsem.org
Vol 13, Issuse.3 Aug 2019

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.