IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Special Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

Build an Auction Decentralized Application from Scratch

Said Anisha[1] , Kedari Vaishnavi[2] , Datkhile Janavi[3] , Prof. K. D. Dere[4,*1] ,Prof. S. K. Said[5,*2]

Deptartment of Computer, Jaihind College of Engineering, Kuran, India [1,2,3]

Master in Computer Science Technology, Jaihind College of Engineering, Kuran, India[4]

Assistant Professor, Jaihind College of Engineering, Kuran, India[5]

ABSTRACT: Now a days internet becomes the crucial part of our daily life because of involvement of e-commerce activities on transaction ,transportation etc., The E-auction is very popular e-commerce activity. It allows the bidders to make a bid for the product over the internet. As we know e-Auction can develop or increase the efficiency of bid transaction. However, the bidder's protection, privacy, transaction quality and accuracy , transaction data security, high cost of third-party auction center , and other issues attract our attention. On the basis of transaction process and simple principles of the sealed auction, we explored the problems present in the current sealed-bid e-auction schemes. By using the block-chain technology, we proposed a sealed-bid e-auction scheme with smart contract technology and with the help of Proof of work(POW) algorithm . The smart contract was introduced in 1990 and it can be implemented using Ethereum platform . We developed proposed system which is constructed an auction mechanism without involvement of third-party auctioneer, so as to put a limit on behaviour of auction parties for the purpose of auction security, reliability, accuracy , and privacy protection. As compared to the related sealed e-auction system based on block-chain technologies our system provides the more security and low transaction cost.

KEYWORDS: E-auction, Bid, Smart contract, Block-chain Technology.

I. INTRODUCTION

Block-chain is made up of two words nothing but block and chain. In that number of blocks is connected through the chain. Each block contains the hash value of previous block and it also contains its own hash value. These blocks contain information of various transactions .It combine different database and decentralized record and in that we do not need any verification permission. [2]

In recent year, E-auction is the popular issue and challenges from its efficiency and convenience. We use the E-auction system to integrate the technique of network into bidding System to reduce transaction cost. [1]

The third party allows a platform to help bidders and Auctioneers to post their products, it check the Price of high bidding and committing the winner, like eBay and yahoo bidding system. There are two main problems in E-auction. First, a centralized third party is needed in bidding system that helps interact between bidders and auctioneers. The centralized system required the more transaction fees. [1]

Smart contracts are made form set of codes and digits. Which is implemented in the ethereum platform. Smart - contract is an intelligent agreement .When the time or particular event is activated then only the smart contract started like sending message and handling transaction. We can write the smart contract with the help Solidity Language. [3]

The Auction Decentralized App allows a user to register a "deed" token, that represents some unique assets, such as a house, a car, trademark, etc. Once a token has been registered, the ownership of the token is transferred to the Auction D-App, allowing it to be listed for sale. The Auction D-App list each of the registered tokens, allowing other users to place bids. During each auction, users can join a chat room created specifically for that auction. Once an auction is finalized, the deed token ownership is transferred to the winner of the auction.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

| International Conference on Recent Innovations in Engineering and Technology (ICRIET'23)|

| Sharadchandra Pawar College of Engineering, Pune, India |

|| Volume 11, Special Issue 2, March 2023 ||

MOTIVATION

1. To help people get access to their product.
2. To provide the trust among the user of the block-chain without the third-party involvement.
3. To improve the transaction security.
4. To build the trust among the users while doing transaction and provide security.

II. LITERATURE SURVEY

This section broadly reviews the literature, on block-chain technology application in Eauction. During the last few years auction based theories and models have a large attention from many researchers .In most of the survey auction related topics we can find where they are published before 2017, in the field of economics. Those surveys contain the introduction and comparison of different auction models. As we know block-chain in the other hand newly emerged technology, almost all aspects of block-chain are studied in literature. The survey includes blockchain overview, security and privacy, smart contract, consensus mechanism, models and tools and various block-chain based applications.

A block-chain provides the decentralized environment to support auction activities, thereby increasing the security and trustworthiness and auctions. [1]

E-auction is classified into two types public bid and sealed bid. Public bid is nothing but bidders have to raise the hand to bid the products in that bidding price is continuously increasing, in that also bidders can bid many times that's why it is called as multi-bidding auction. In sealed bid, bidder encrypts the bill and sends it to the ones that's why it is called as single-bidding auction.

III. BACKGROUND KNOWLEDGE

Block-chain Technology

Block-chain is made up of two words nothing but block and chain . In that number of blocks are connected through the chain .Each block contain the hash value of previous block and it also contain its own hash value. These blocks contain information of various transactions .It combine different database and decentralized record and in that we do not need any verification permission.[2]

Block-chain is a distributed database or ledger which is shared among the nodes of a computer network. Like a database, a block-chain can stores the information in digital format. Block-chains are very popular for their important role in crypto-currency system, for example Bit-coin, it helps in maintaining a secure and decentralized transactions. The blockchain gives guarantee of the security of the data and recorded transactions because of its immutability feature .As we know each block contain the previous block hash value, so if someone tries to hack or ties to misuse of the data for that he/she have to change the all hash values of the blocks and it is very difficult in block- chain technology.

Block-chain Architecture

A block-chain is nothing but sequence of blocks. A block-chain database is distributed, shared; fault tolerance and that maintain the records in block .In block-chain, no one block-chain is user able to delete or altered the blocks. Also, each and every block contains timestamp and a random number for cryptographic operations. Timestamp is nothing but creation of time of block. A block has only one parent block. The first block in the block-chain is called as genesis block which has no parent block and its hash value is entirely zeros eq. (3)

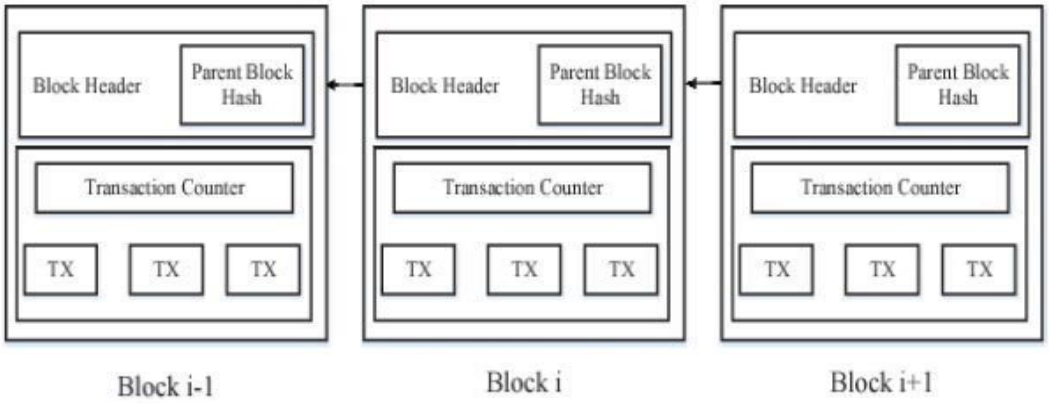

Figure - shows the architecture of block-chain

- Block- A Block Consists Of The Block Header And Block Body. The Block Header Includes: -
- **Block-Version**: It Indicates Which Set Of Block Validation Rules To Follow. ○ **Merkle Tree Root Hash**: The Hash Value of All the Transactions in Block. ○ **Timestamp**: Current Time as Seconds in Universal Time.
- **N-Bits**: It Is A Target Threshold Of A Valid Block Hash.
- **Nonce:** It Is A 4-Byte Field, Which Starts With 0 And Increases For Every Hash Calculation.
- ○ **Parent Block Hash**: 256-Bit Hash Value That Point To Previous Block.[2]

Ethereum Smart-contract

The term smart contract is used to describe a big variety of different things. In the 1990s, cryptographer Nick Szabo discovered this term and defined it as "a set of promises, specified in digital form, and it also including protocols in which the parties perform on the other promises." After that, the concept of smart contracts has developed, especially after the introduction of decentralized block-chain platforms with the invented Bit coin in 2009.

In the context of Ethereum, the term is actually a bit of inaccurate name; given Ethereum smart contracts are neither smart nor legal contracts. In this system we use the term "smart contracts" to refer to immutable computer programs that run deterministically in the Ethereum Virtual Machine as part of the Ethereum network protocol—i.e., on the decentralized Ethereum world computer.

- **Computer programs**

Smart contracts are computer programs. The word "contract" has no legal meaning in this context.

- **Immutable**

Immutable means once we develop, the code of a smart contract then it cannot be changed. In traditional System there are chances of losing the data or transaction because of central authority.

- **EVM context**

Smart contracts work with a very limited execution context. They are able to access their own state, the condition of the transaction that called them, and some information about the most recent blocks.

- **Decentralized world computer**

As we know the Decentralized means the there is no central authority. In block-chain, decentralization is the transformation of control and decision-making from a centralized entity to a distributed network. Decentralized networks are used to reduce the level of trust that participants must have in one another, and put of their ability to apply authority or control over one another in ways that decrease the functionality of the network.

Auction

An Auction is a sale activity in that the potential buyers create competitive bid for the particular objects or service. Generally there are many fundamental elements present in auction:

1. Seller – Who wants to sell their product by using auction.
2. Bidder – There are many bidders, who want to buy the objects by using auction.
3. Auction Object – The object that traded between the Seller and Buyer.
4. An Auctioneer – Who works as an intermediary like an agent to conduct and control the auction process.

Auction Types	Alternative Name	Auction Mechanism
English Auction	Open –outcry ascending –price auction	As buyers bid the price starts from low and increases . The auction will continues until we don't received higher bids .
Dutch Auction	Clock auction ;Open – outcry descending price auction	Auctioneer start auction with higher price. The price reduced until one bidder accepts.
Vickery Auction	Second-price sealed – bid auction	All bidders submit sealed bid . The highest bidder win the auction but only pay the second highest bid.
Double Auction	Double –sided auction	There are multiple sellers and buyers submit their bids/offers.
Combinatorial Auction	Multi-lot auction	It have many homogeneous items are sold . In this bidders can make bids on combinations of items
Uniform price Auction	Clearing price Auction	Multiple homogeneous items are sold . Winner have to pay the same price regardless of their actual bid.
Pay – as bid auction.	Discriminatory price auction	Multiple similar items are sold . Winner have to pay bid according to their items owns
All –Pay attribute Auction	-	Each and every bidder has to pay regardless of whether they win or not.

Table -1: Summary of Representative Auction Types [1]

Methodology

In this system we will start building an example of Decentralized App, to increase the various decentralization tools.

Our D-App will implement a decentralized auction.

The Auction D-App allows a user to register a "deed" token that shows some unique asset, like a house, a car, a trademark, etc. Once a token is registered, the ownership of the token is send towards the Auction D-App, and allows it to be listed for sale. The Auction DApp shows each registered tokens, and it allows other users to make bids. At the time of each auction, in that users have to join a chat room which is created specifically for that auction. Once an auction is finalized, the deed token ownership is send to the winner of the auction.

The main components of our Auction D-App are:

- The smart contract implements the ERC721 non-fungible "deed" tokens.
- A smart contract implements an auction to sell the deeds.
- A web frontend is created using the Vie/Verify JavaScript framework.
- The web3.js library is used to connect to Ethereum chains (via Meta-Mask or other clients)
- A Swarm client is used to store resources such as images
- A Whisper client is used to create per-auction chat rooms for all participants

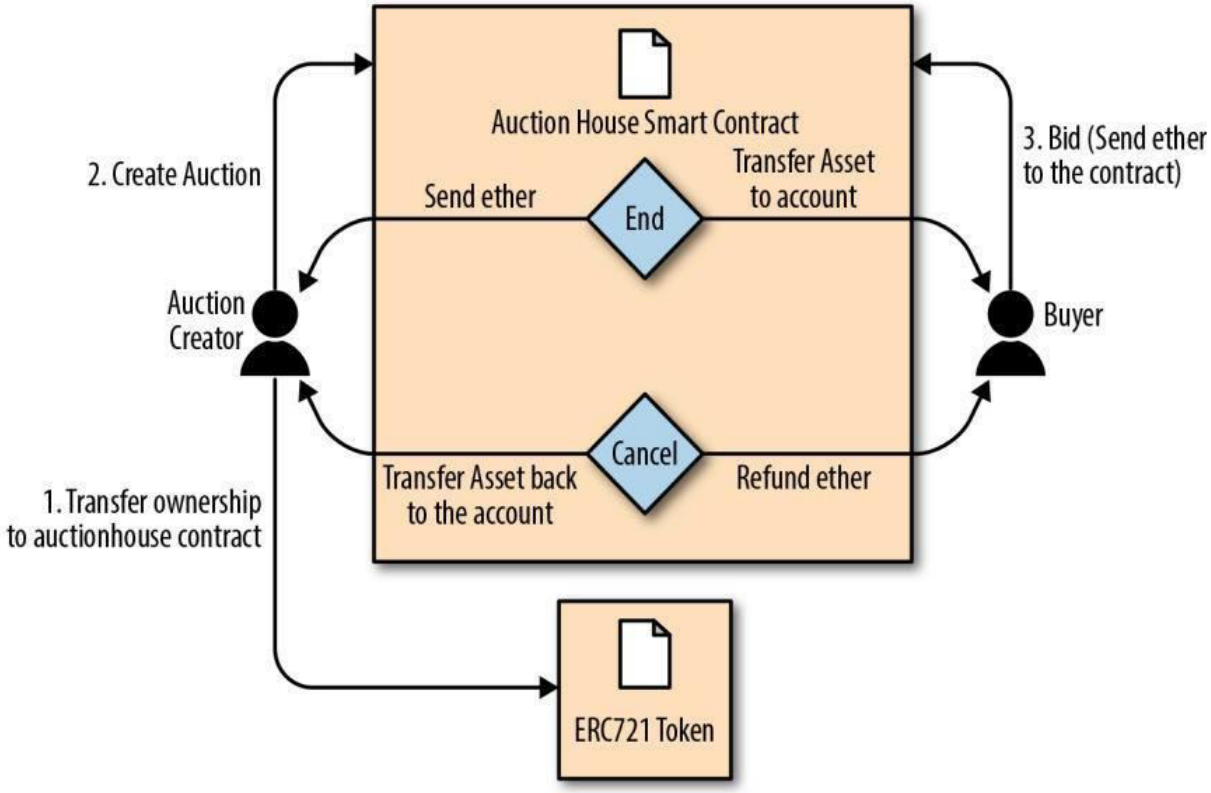

Fig -1: System Architecture of Forward Auction

REFERENCES

[1] https://cypherpunks-core.github.io/ethereumbook/07smart-contracts-solidity.html

[2] https://www.jdsupra.com/legalnews/distinguish-smart-contract-from-5791475
[3]https://www.researchgate.net/publication/348127582_A_Brief_Analysis_of_Blockchain_Algori thms_and_Its_Challenges
[4]https://www.academia.edu/en/67712495/A_Brief_Analysis_of_Blockchain_Algorithms_and_Its _Challenges [5] https://ieeexplore.ieee.org/document/6643395
[6] https://www.computer.org/csdl/proceedings-article/pdcat/2007/30490173/12OmNwdtw5E

[7] https://ieeexplore.ieee.org/document/8394569
[8]https://www.researchgate.net/publication/350368224_PeertoPeer_Energy_Trading_in_Smart_Grid_Through_Blockchain_A_Double_AuctionBased_Game_ Theoretic_Approach

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details