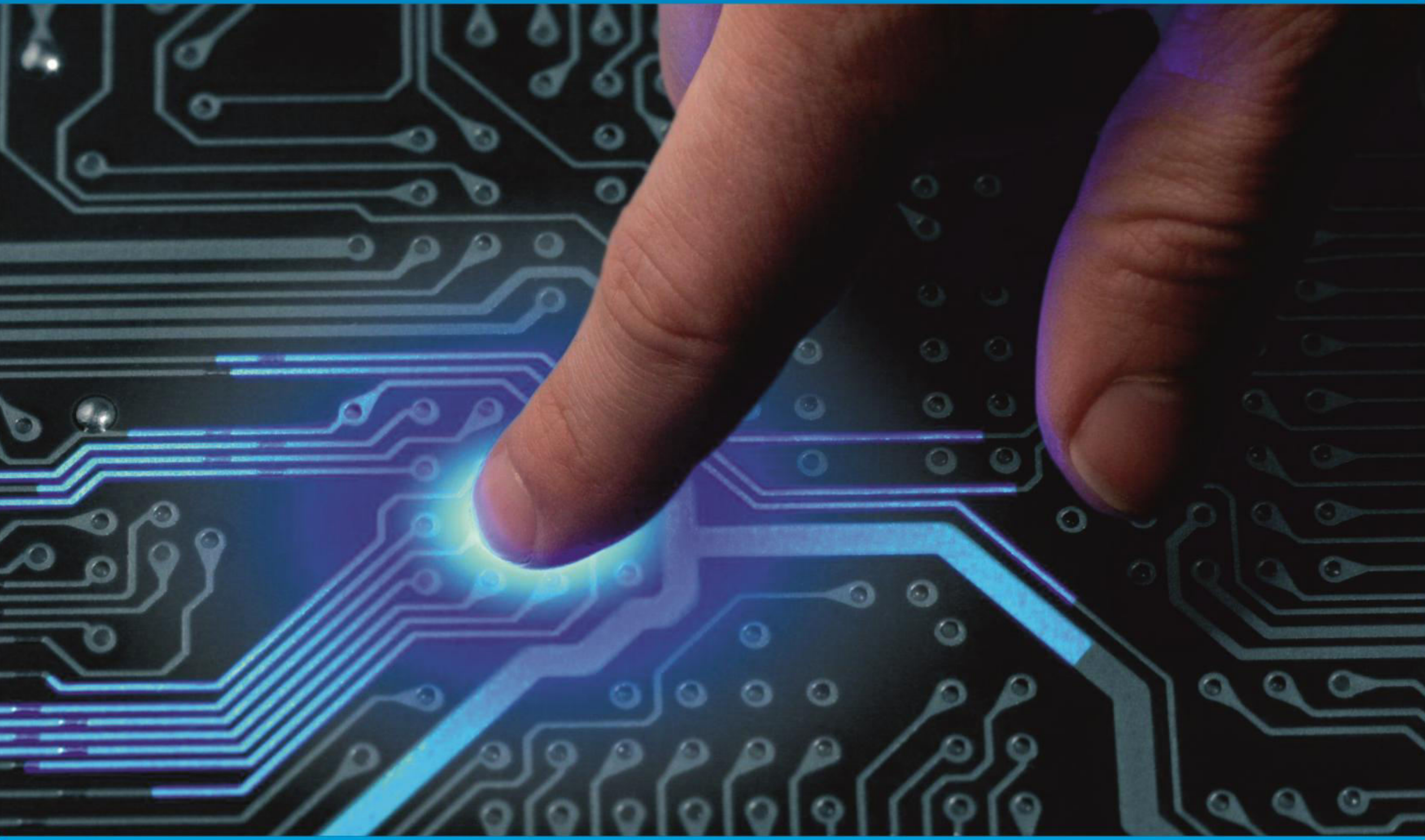
IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| DOI: 10.15680/IJIRCCE.2021.0905237 |

Block-Chain Based Smart Contract for Bidding System

Malatesh.K.R[1], Dr. Ramesh B[2], Dhanush DA[3], Rahul R[4], Santhosh HS[5]

Department of Computer Science and Engineering, Malnad College of Engineering, Hassan, India

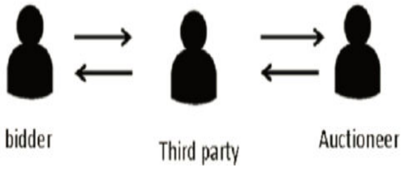
ABSTRACT:- Because of the popularity of the Internet, the integration services have gradually changed people daily life, such as e-commerce activities on transactions, transportation and so on. The E-auction, one of the popular e-commerce activities, allows bidders to directly bid the products over the 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.

I. INTRODUCTION

In recent years, E-auction is the popular issue since its convenience and efficiency. E-auction integrates the network technique into the bidding system in order to reduce the cost of transactions. The main roles during E-auction include bidders, auctioneers, and the third-party as shown in Fig. 1. Most of the third party is the centralized intermediary to provide a platform to help bidders and auctioneers posting products, checking the highest bidding price and committing the winner, such as eBay and yahoo bidding system. However,

E-auction has two main problems. First, a centralized intermediary is required in bidding system to help communication between bidders and auctioneers. 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. Secondly, in a sealed envelope [8], bidders have no way to ensure that lead bidder never leaks their bidding price. Fig. 1: The role of the E-auction This paper applies the blockchain technique into the E-auction to resolve the two problems. The blockchain [5, 6, 14] 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 [7, 15]. 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 can not be opened before the deadline

In an online biding system, an extra transaction cost is required for the intermediaries because the third-party is an 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 a trusted one.



E-auction has two main problems.

1. First, a centralized intermediary is required in bidding system to help communication between bidders and auctioneers. 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.
2. Secondly, in a sealed envelope, bidders have no way to ensure that lead bidder never leaks their bidding price

II. RELATED WORK

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

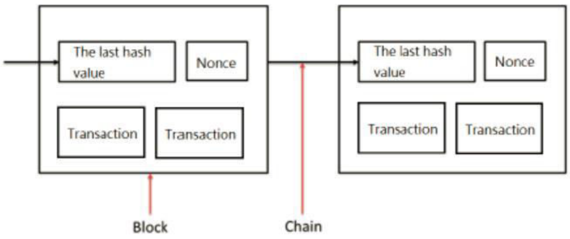
- Marco Iansiti and Karim R Lakhani. "The truth about blockchain"
- M Jenifer and B Bharathi. "A method of reducing the skew in reducer phase block chain algorithm"
- Yan Zhu, Ruiqi Guo, Guohua Gan, and Wei-Tek Tsai. "Interactive incontestable signature for transactions confirmation in bitcoin blockchain"

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

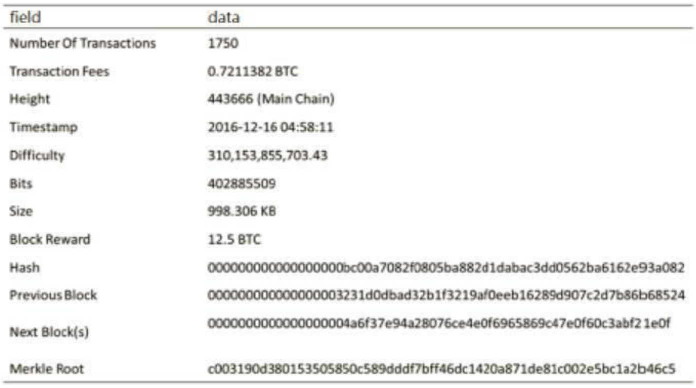
Identity identification and security: Identification and anti-counterfeiting are performed using a public key infrastructure. Each account in the blockchain has a public key and a private key used to send and receive the transactions. After the private key encrypts the transaction message, the receiver 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.



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

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

III. PROPOSED SYSTEM

This project applies the blockchain technique to resolve the main problems

- 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 Some rules are written inside the smart deal which cannot be opened before the deadline.

In the initialization data, we will announce the following information in advance.
The tenderer address used to record the originating contract.
Used to announce the start time.
Used to announce the effective time of the contract.

Activate the contract by calling this function, and use the Start and smart contract End to record the start and end time. This function can be called by any person to perform the smart contract. Before the function is executed, and smart contract Time are used to judge whether the contract is expired. If not, the smart contract can send the smart contract envelope if the price is greater than the current highest price. The contract system will use highest Smart contract and highest Smart contract to record the current highest price and the corresponding smart contract's address.

Opens the smart contract by calling this function, and compares the prices of all the tickets to get the final winner.
In this function, Auction Start and smart contract Time are automatically used to determine the contract validity time. If the effective time ends, the successful smart contract's Address and the current highest price will be automatically sent to the tenderer. This function will be disabled to avoid repeated execution.
Returns the amount of smart contracts tendered by smart contracts other than the successful smart contract.

Data flow diagram

A data flow diagram is the graphical representation of the flow of data through an information system. DFD is very useful in understanding a system and can be efficiently used during analysis.

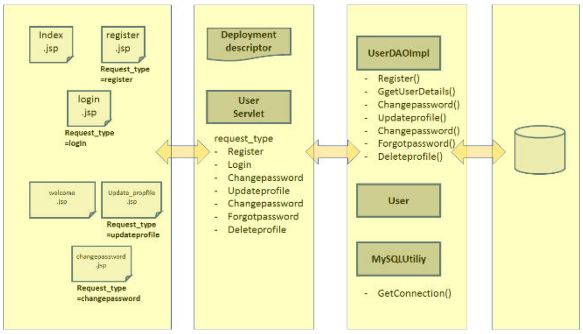
A DFD shows the flow of data through a system. It view a system as a function that transforms the inputs into desired outputs. Any complex systems will not perform this transformation in a single step and a data will typically undergo a series of transformations before it becomes the output.

With a data flow diagram, users are able to visualize how the system will operate that the system will accomplish and how the system will be implemented, old system data flow diagrams can be drawn up and compared with a new systems data flow diagram to draw comparisons to implement a more efficient system.

Data flow diagrams can be used to provide the end user with a physical idea of where the data they input, ultimately as an effect upon the structure of the whole system.

Below section explains the module wise data flow diagram

Module 1: Account Access Layer



Account operations module provides the following functionalities to the end users of our project.

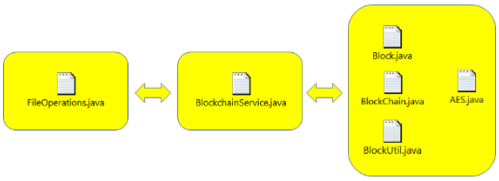
- Register a new seller/ buyer account
- Login to an existing account
- Logout from the session
- Edit the existing Profile
- Change Password for security issues
- Forgot Password and receive the current password over an email
- Delete an existing Account

Account operations module will be re-using the DAO layer to provide the above functionalities.

The DAO layer is the service layer which provides database CRUD (create, update, read, and delete) services to the other layers.

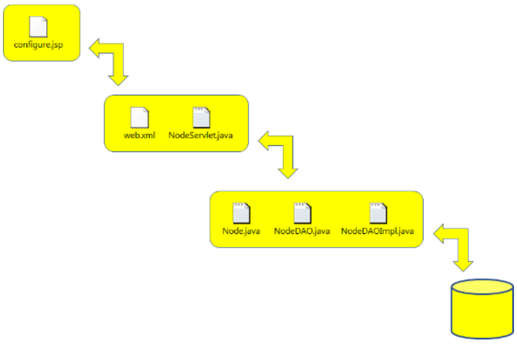
It will contain the POJO classes to map the database tables into java object. It will also contain the Util classes to manage the database connections.

Module 2: Node Implementation



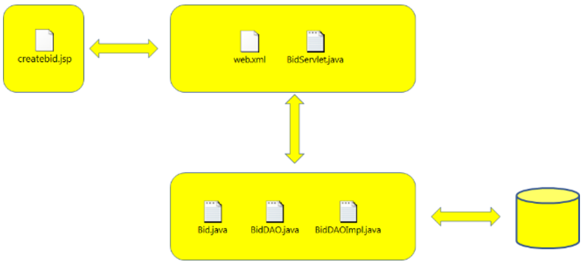
- In this module we will be implementing the blockchain network by creating our set of distributed ledger nodes.
- Each node will be able to perform various operations
  - Receive the blockchain data once the transaction in the blockchain has been committed and the block is mined.
  - Perform block validation by comparing the hashcodes of the current block and the hash codes of the previous blocks
  - Provide a readonly access to the clients on that node for visualizing the number of blocks and the type of data being stored
  - Provide the block chain data to the bidding application once requested.
- Each node will be deployed in its own platform over the cloud infrastructure. For this purpose, we make use of Digital ocean cloud service proider

Module 3: Super Admin configuration



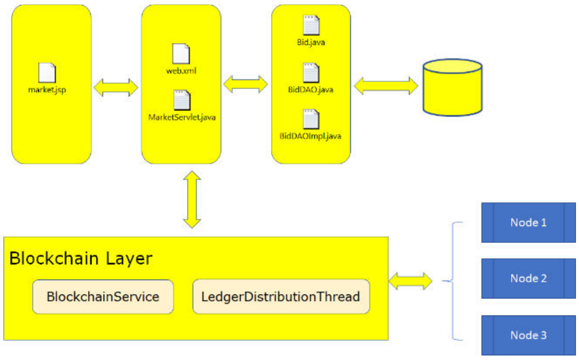
- This feature is made available only the super admin of the project.
- The super admin of the project essentially will be the product owners himself/herself.
- Through this feature, the super admin of the project will be able to perform nodes addition, nodes deletion, and nodes visualization operation from the front end user interfaces provided to him/her
- This feature will be secured and nobody else apart from the super admin will be able to get access to.
- More the number of nodes, stronger the security measures provided by the blockchain bidding application
- Hence, it is recommended to add as many nodes as possible.

Module 4: Product addition



- In this module the seller of the product in our portal will be given an HTML interface through which he/she can add the product which he/she is planning to sell.
- The seller will have to provide some basic information about the product like the name, description, and the URL to the actual product
- All the above fields are mandatory to be provided by the seller.
- The product once added, it will immediately be shown up in the market where the users can start bidding for it.
- The end users will not be given a luxury to upload the products images due to the limitations in the cloud storage space. Instead, the sellers must be specifying the URL to the image of the product from google drive or any other hosting sites.

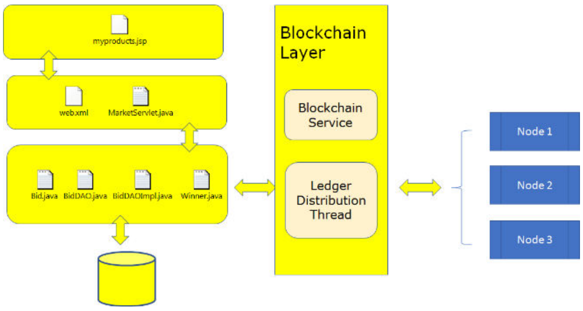
Module 5: Bid Market and Participation



- The product once added by the seller, it will immediately be shown up in the market where the users can start bidding for it.

- The user must be entering the amount in the textbox provided against the product of interest.
- The amount bid by the buyers along with the unique identifier for the product will be stored in the blockchain network
- There will be a blockchain service class which does the operation of writing and reading to and from blockchain network.
- This blockchain service class will make use of the Ledger Distribution Thread to write to numerous blockchain network concurrently

Module 6: My Products and Win Logs



- This portal enables the seller of the product to see the status of their products and the bidders details for their product
- At any point of time, the seller can close the bid window and declare the buyer with highest bid as the winner
- An email communication will be sent to both buyer and seller once the bidding window has been closed
- The buyer details and the log of the total bidders will always be there at this portal so that the seller can have an access to this data at any point of time

IV. CONCLUSION

- This project provides an E-auction mechanism based on blockchain to ensure electronic seals confidentiality, non-repudiation, and unchangeability.
- 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
- In future, we would be working towards scaling our project to enormous amounts of users and come up with an efficient algorithm for balancing the load across them.

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] llichetty S Chandrashekar, Y Narahari, Charles H Rosa, Devadatta M Kulkarni, Jeffrey D Tew, and Pankaj Dayama. Auction-based mechanisms for electronic 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. 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.

[7]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.

[8]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.

[9] 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.

[10] 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.