iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55310

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Smart Blockchain Bidding System

Prof. Dr. Anuradha SG[1], H Vadiraja[2]
Dept. of Computer Science, RYM Engineering College, Ballari, Visvesvaraya Technological University

Abstract: The E-auction is a prevalent e-commerce event that enables bidders to place bids directly on the Internet. Similar to sealed deals, intermediaries are required to facilitate transactions, as third parties play a crucial role in negotiating during the auction between buyers and sellers. However, the trustworthiness of third parties is never guaranteed. This project showcases a bidding framework utilizing blockchain technology. The bidding application is developed using the Advanced Encryption Standard (AES) Algorithm, which specifies the number of transformation **rounds required to convert the input, known as plain text, into the final output, known as cipher text.**

Keywords: Blockchain, Bidding System, AES Algorithm, Plain Text, Cipher Text.

I. INTRODUCTION

by the popularity of the net, the aggregate services have often changed humans daily existence, inclusive of e-commerce sports on transactions, transportation and so forth. the e-public sale, it is the best e-exchange sports, allows bidders to at once bid the goods over the net. as for sealed bid, the greater transaction price is required for the intermediaries due to the fact the 0.33-party is the crucial characteristic the various customers and the dealers help to change each all through the public sale. similarly, it never guarantees whether or not or now not the 1/3-party is believe. to clear up the issues, we advocate the block chain technology with low transaction rate it truly is used to expand the smart settlement of public bid and sealed bid. the clever agreement, made in 1990 and implements thru ethereum platform, can make sure the invoice relaxed, non-public, non-reputability and inalterability due to all of the transactions are recorded within the equal but decentralized ledgers.

The clever settlement includes the deal with of auctioneer, the begin public sale time, reduce-off date, the address of modern winner, the modern highest rate**.**

II. LITERATURE SURVEY AND REVIEW

1) *Paper [1]:* Untrusted practical e-auction bidding technology.

This paper presents a proposed electronic auction scheme that utilizes Bit commitment and blind signature. The proposed scheme possesses a unique characteristic in that it can effectively withstand conspiracy attacks, even in the presence of an untrusted third-party agency.

2) *Paper [2]:* A simple efficient electronic bid technology.

This paper represents the simple and efficient way of auctioning scheme that can be done electronically. And done very clearly and makes the appropriate commands to announce the winner name through the email.

3) *Paper [3]:* User payment choice behaviour in e-auction transactions.

In this paper, a set of criteria which buyers and sellers consider when selecting the payment method is proposed. Analytical Hierarchy Process method is used. Both parties hope to lower the risk by choosing payment method that best safeguards their interest.

4) *Paper [4]:* A sealed-bid electronicauction protocol based on ring signature.

This paper represents a fair electronic auction protocol is proposed which is based on the combination of an efficient group signature scheme relying on the ring signature idea and a public-key cryptosystem of the homomorphic encryption.

5) *Paper [5]:* A model in support of bid evaluation inmulti-attribute e-auction for procurement. In this paper this points on the bid evaluation problem in multi-attribute e-auction for procurement. The proposed model uses an outranking-based multi-attribute decision technique, ELECTRE-III, to calculate the buyer's choices.

6) Paper [6]: A new secure electronic auction scheme.
This paper represents a secure electronic auction scheme is designed improved secure multiparty computation protocol and bit commitment protocol. The scheme is characterized by the fact that all bids of the losing bidders are secret except the winning bidder.

7) Paper [7]: A method of reducing the skew in reducer phase - block chain algorithm.
While processing the Map-Reduce data, skew will occur in both map and less phase. Map skew is easy to reduce therefore for case of reduced phase it may take time to reduce it. So, a methodology is being created to reduce the Reducer side skew and time being compared between the new method and MapReduce to find their efficiency is proposed in this paper.

8) Paper [8]: Responsive signature for confirmation in bitcoin blockchain.
This paper presents a novel system for the precise verification of transactions within a block. The proposed system employs an Interactive Incontestable Signature (IIS) scheme in lieu of the original signature, which facilitates confirmation of transactions between the dealer and owner. Through this signature, the dealer can guarantee the owner that the transaction will be incorporated into the blockchain in a manner that precludes repudiation. The security of the scheme has been established with respect to the unforgeability of the owner and the incontestability of the dealer.

III. PROBLEM FORMULATION

In these recent days security is the most important while any transactions and bidding process, At present days bidding system is become their own game, They are just making someone win which are friends to them or any close relatives or known persons.
This solution helps to give a solution using AES technology, It will calculate user, time, amount and more things to announce the winner.

A. Existing system

Manually saving data provides very little protection, and some data may be lost due to mismanagement. Under the current system, products cannot be properly authorized to be auctioned off. Registration and profile maintenance are insecure. There is no payment and account management system available in this system. It will also provides the external security to the bidding system as not cheating while bidding is live and also end of the bidding there will be chance of humans to interact and change the winner as per many group discussions and also from many of the power people can also participate in this to win the bid and cheat the loyal bidder from another id.
Advantages:

1) Helps to get the high end security for bidding process.
2) It is very efficient and precise; Filtering of winner can be faster.

B. Proposed System

Following are the activities used to develop the web application process based on a database integration approach, as part of the development of this new system.
A secure registration process and profile management are also available in this system, which generates team progress and provides secure user management. A user can select a field to bid on for bids and receive periodic mail alerts if an article goes on auction in that field. On the advice of the administrator, owners may withhold rare articles for auction on the site in special auctions make more the value of the bid.

C. Objective of the project

Decentralizing communication between bidders and auctioneers to reduce the charge fee will help. To very less touch with not legal parties who may not be reliable sources of information, it is not great to engage them. This will make the whole bidding to good level using decentralized communication. This communication helps to get the clear clarity about the internal process of bidding also makes it more precise to decide the winner of the bid. It will directly communicate to the bidder once he won the bid, No third party member will be involved in this bidding procedure

IV. METHODOLOGY FOR THE PROPOSED PROJECT

AES algorithm is the specified algorithm to encrypt the data from the cipher. Cipher is the 128-bit block used to store the data in it. AES is the part of cipher it can hold up to 128,192 and 256 bits of memory.128 bit of time is 10 rounds in the text. Cipher text will be encrypted later it can decrypted.

A. AES Algorithm

The AES Encryption algorithm, also referred to as the Rijndael algorithm, is a equal block program that operates with a block/chunk size of 128 bits. It employs keys of 128, 192, and 256 bits to convert these individual blocks.

Following the encryption of these blocks, they are combined to form the cipher text. The algorithm is founded on a substitution-permutation network, commonly known as an SP network. It comprises a sequence of interconnected operations, including substitutions that replace inputs with specific outputs and permutations that involve bit shuffling.

B. Cipher Text

The term "cipher text" refers to a sequence of seemingly random text that is encrypted and are incomprehensible to human beings. This encryption process involves the advantage of an algorithm that takes a plaintext message as input, applies the program to the message, and generates the corresponding cipher text. Decryption, which is the reverse of encryption, can be employed to convert the cipher text back to its original plaintext form.

C. Encryption and Decryption

Encryption is a fundamental process that involves the conversion of plaintext data into cipher text. Typically, users or systems employ key algorithms to encrypt sensitive information before transmitting it. In certain scenarios, such as when using an automatic teller machine (ATM) or purchasing products online with credit cards, systems automatically encrypt data. Decryption, In second half is the phenomenon of making encrypt text back to plaintext upon receipt. Cipher text is an encoded and indecipherable version of the text that stops illegal people from accessing it. In contrast, plaintext refers to the original format of the data. Once the recipient safely receives the data, they can manually decrypt the cipher text to its readable version. Alternatively, they can use the same key or string of data that was used to encrypt the data for decryption purposes.

V. SYSTEM STRUCTURAL DESIGN

In the context of product development, which combines marketing, design, and manufacturing into a unified approach, design involves taking marketing information and creating a product design for manufacturing. Consequently, systems design involves the definition and development of systems that meet the user's specified requirements.

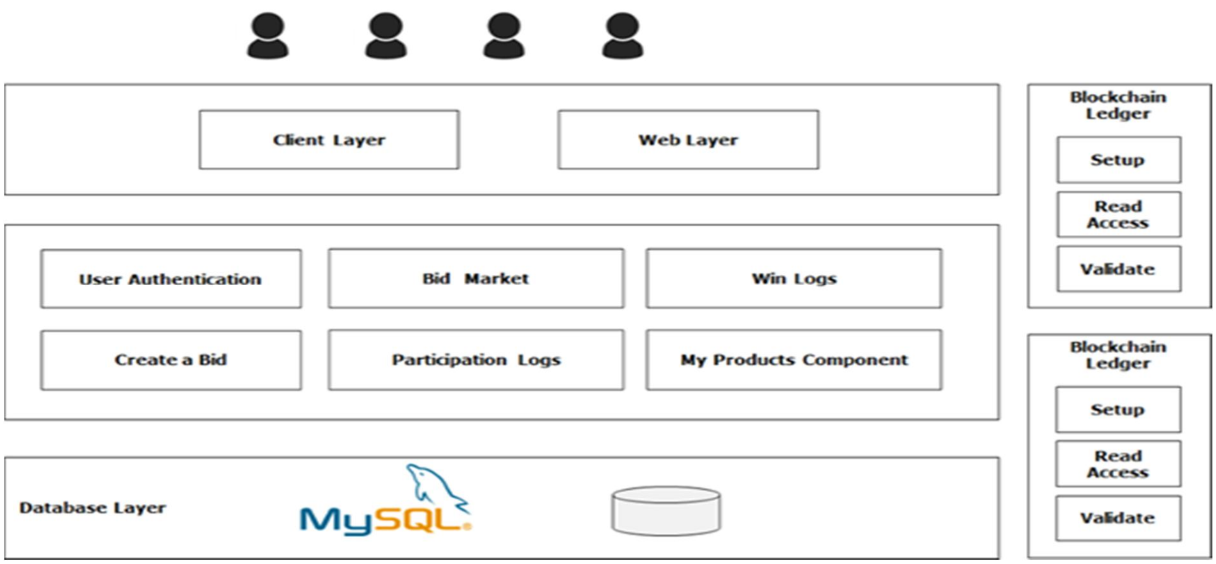


Fig 1: System Architecture

A. Module Discription

Data flow diagrams can serve as it is to furnish the end user with a tangible knowing of the location and impact of the data they input, in relation to the overall system structure. The subsequent section elucidates the data flow diagram on a module-by-module basis.

B. Account Access Layer

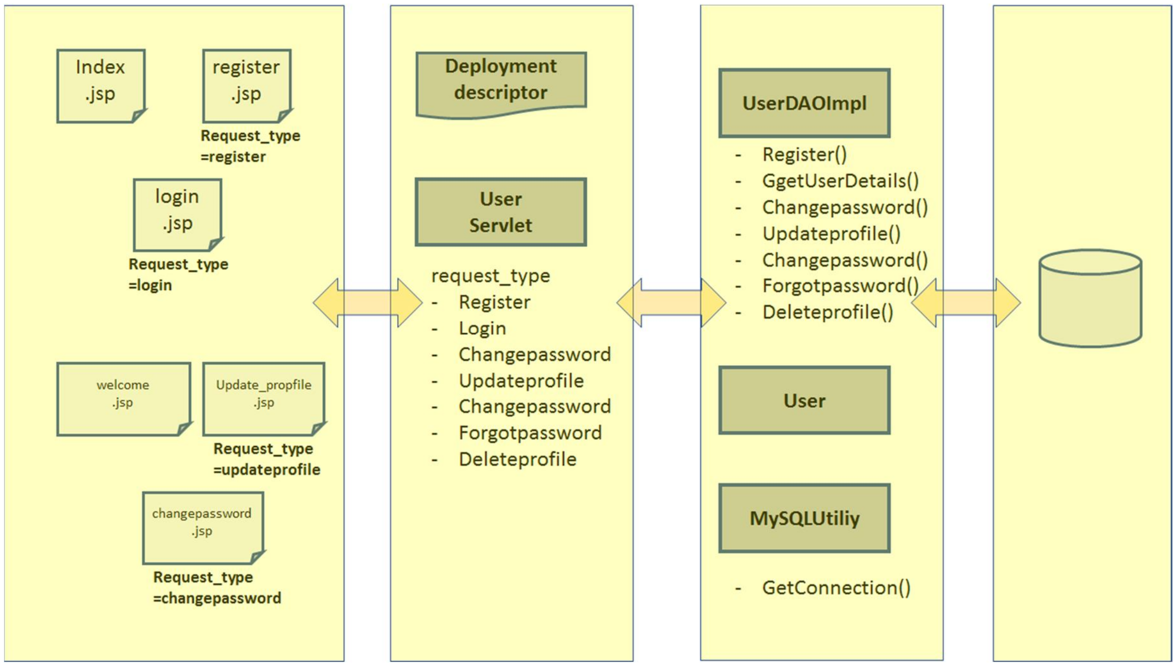


Fig 2: Layer of account access

The account operations module shall utilize the DAO layer to furnish the aforementioned functionalities. The DAO layer serves as the service layer that offers database CRUD (create, update, read, and delete) services to the other layers. It shall comprise of POJO classes that facilitate the mapping of database tables into Java objects. Additionally, it shall encompass Util classes that manage the database connections..

C. Implementation of Node

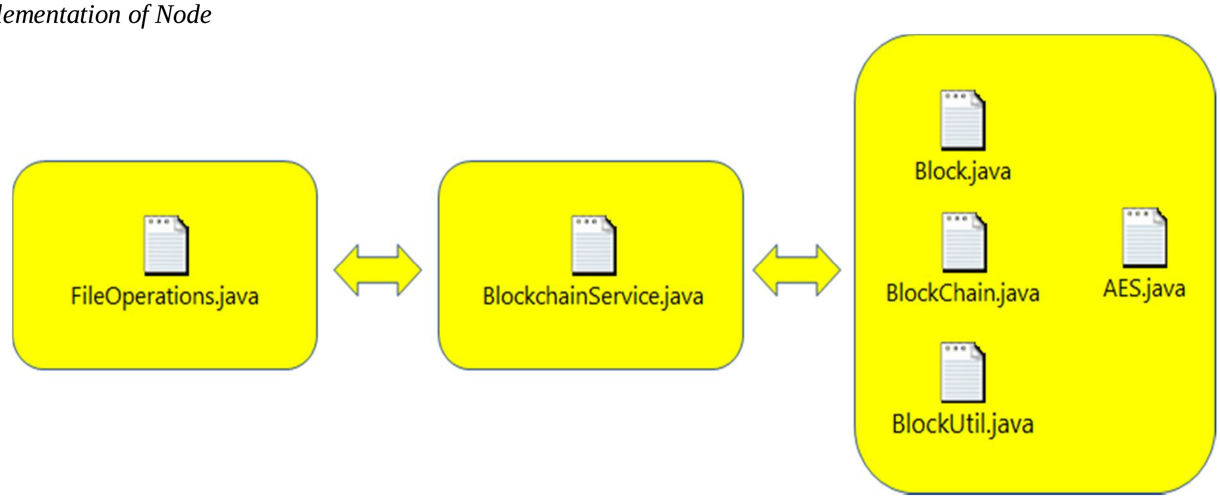


Fig 3:Implementation of Node

In this module, we shall proceed with the implementation of the blockchain network by creating a set of distributed ledger nodes. Each node will possess the capability to execute various operations, including receiving the blockchain data once the transaction in the blockchain has been committed and the block is mined. Additionally, each node will perform block validation by comparing the hash codes of the current block and the hash codes of the previous blocks.

D. Products Addition Node:

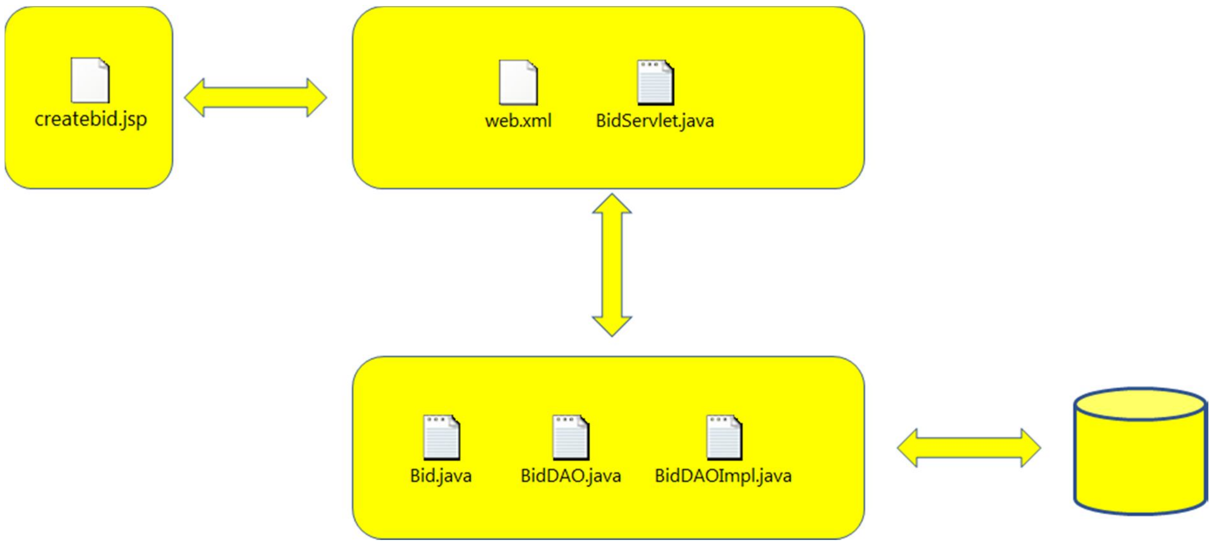


Fig 3: Products Addition Node

In this module or node, products can be added to the backend of the website. Admin will be having the all the access to add the products to the data base. It is directly visible to the users who are using the bidding website.

E. Block chain participation layer:

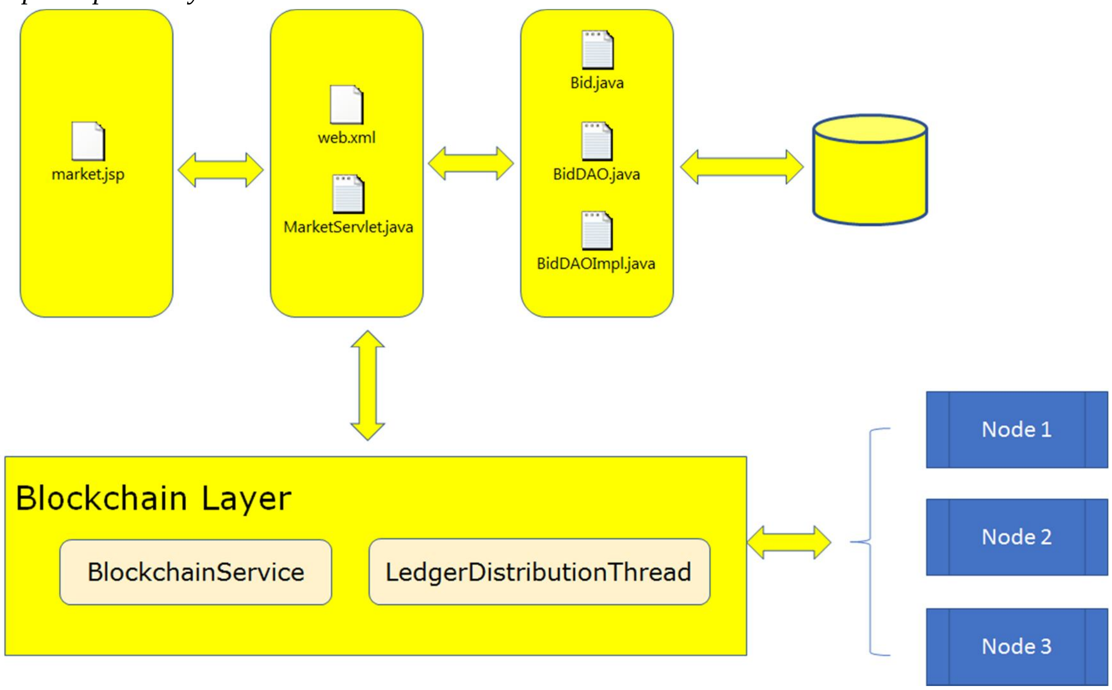


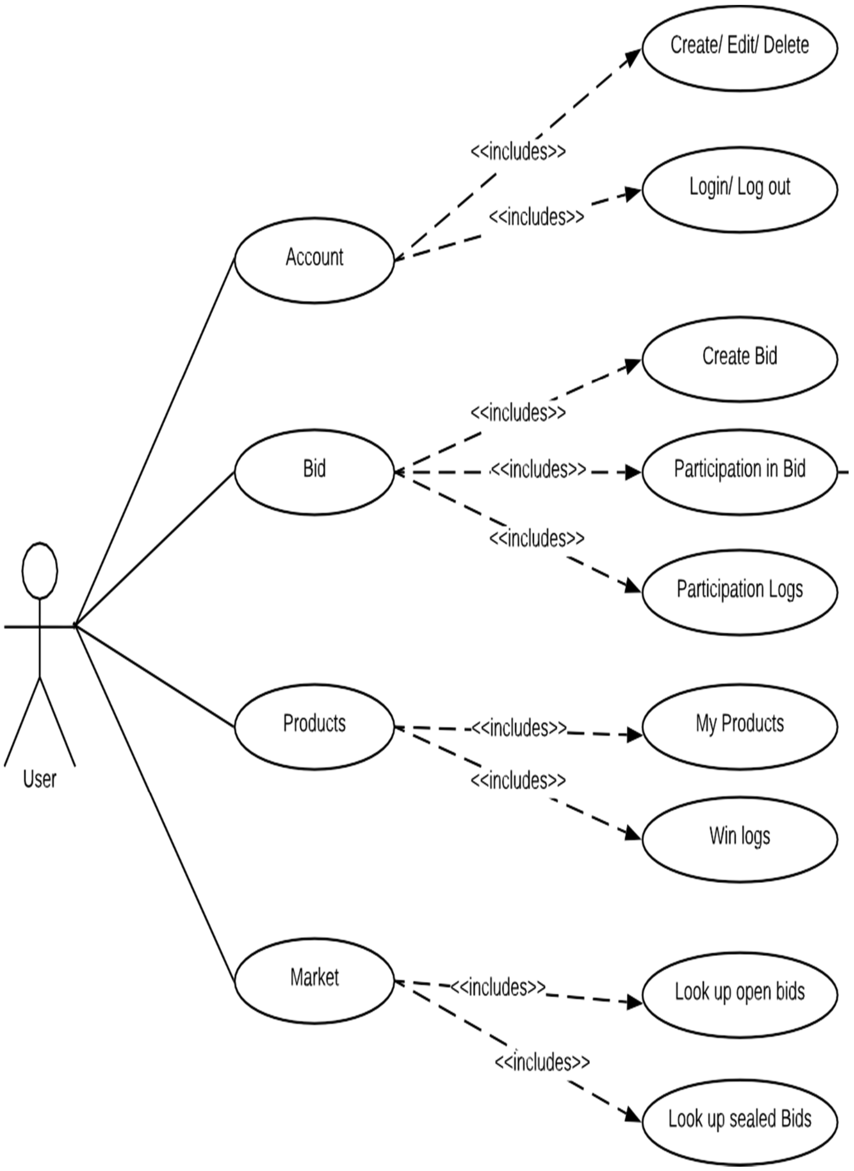
Fig 4: Block chain participation layer

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

In this module, user can participate to the bidding, this module helps to get the market and web files to be linked via internet. Bid java files will be saved in container. Different nodes will be connected to the block chain layer from this.

F. Use case diagram

Below is the use case diagram of this project helps to understand the complete project and easy to maintain the whole diagram. We can also call it as blue print of the software and the project. Bylooking at this anyone from the institute and outside of the institute.



Includes -→ Blockchain network

Fig 5: Block chain participation layer

G. SEQUENCE DIAGRAMS

A Unified Modelling Language (UML) sequence diagram is an interaction diagram that depicts the manner where things communicate with everyone they occur. It illustrates the participants involved in the interaction and the sequence of messages exchanged between them, with each participant being allocated a column in a table. The following section presents the sequence diagrams utilized in this application.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

1) Account operation and Bidding

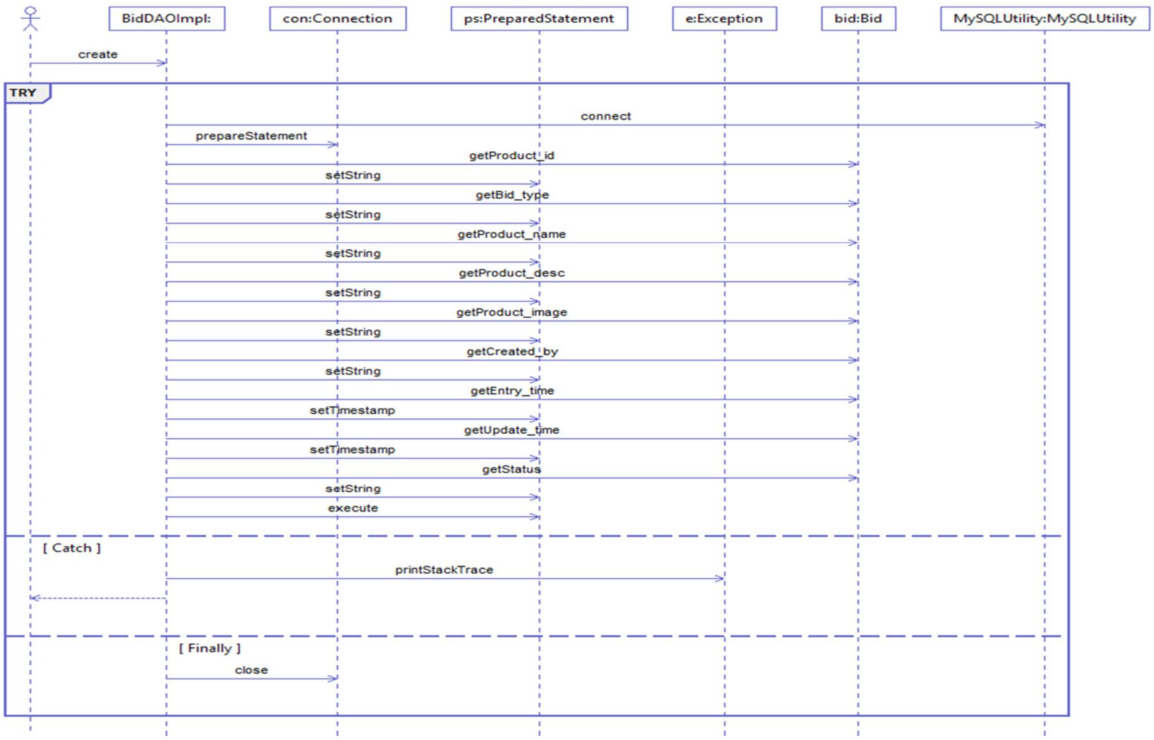


Fig 5.7.1: Sequence diagram of Account operation and Bidding

2) Node implementation

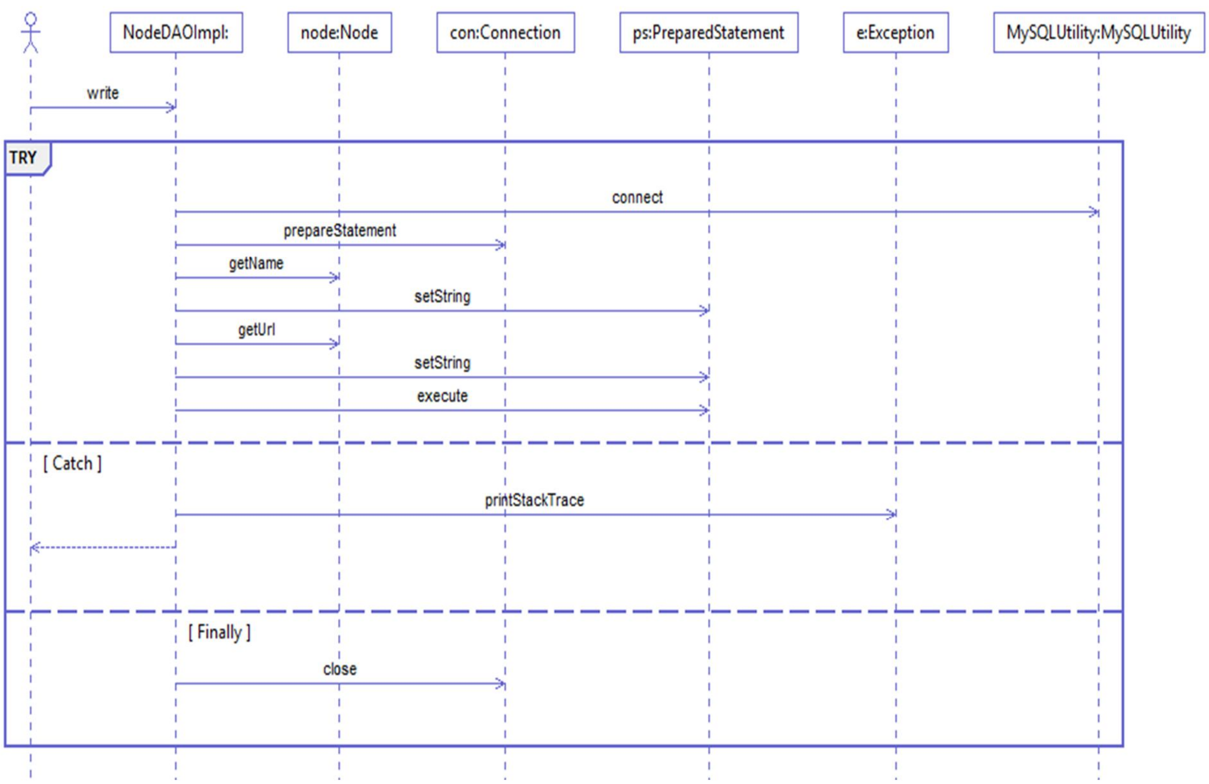


Fig 5.7.2: Sequence diagram of Node Implementation

3) Transaction

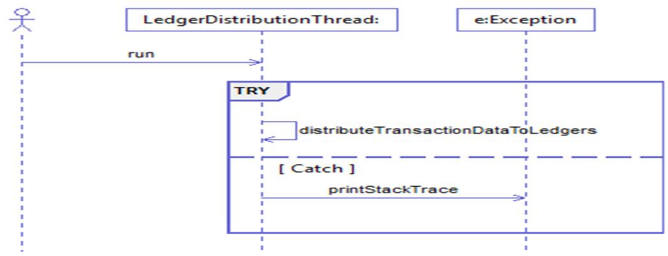


Fig 5.7.3: Sequence diagram of Transaction

4) Bid Market and Participation Using Blockchain

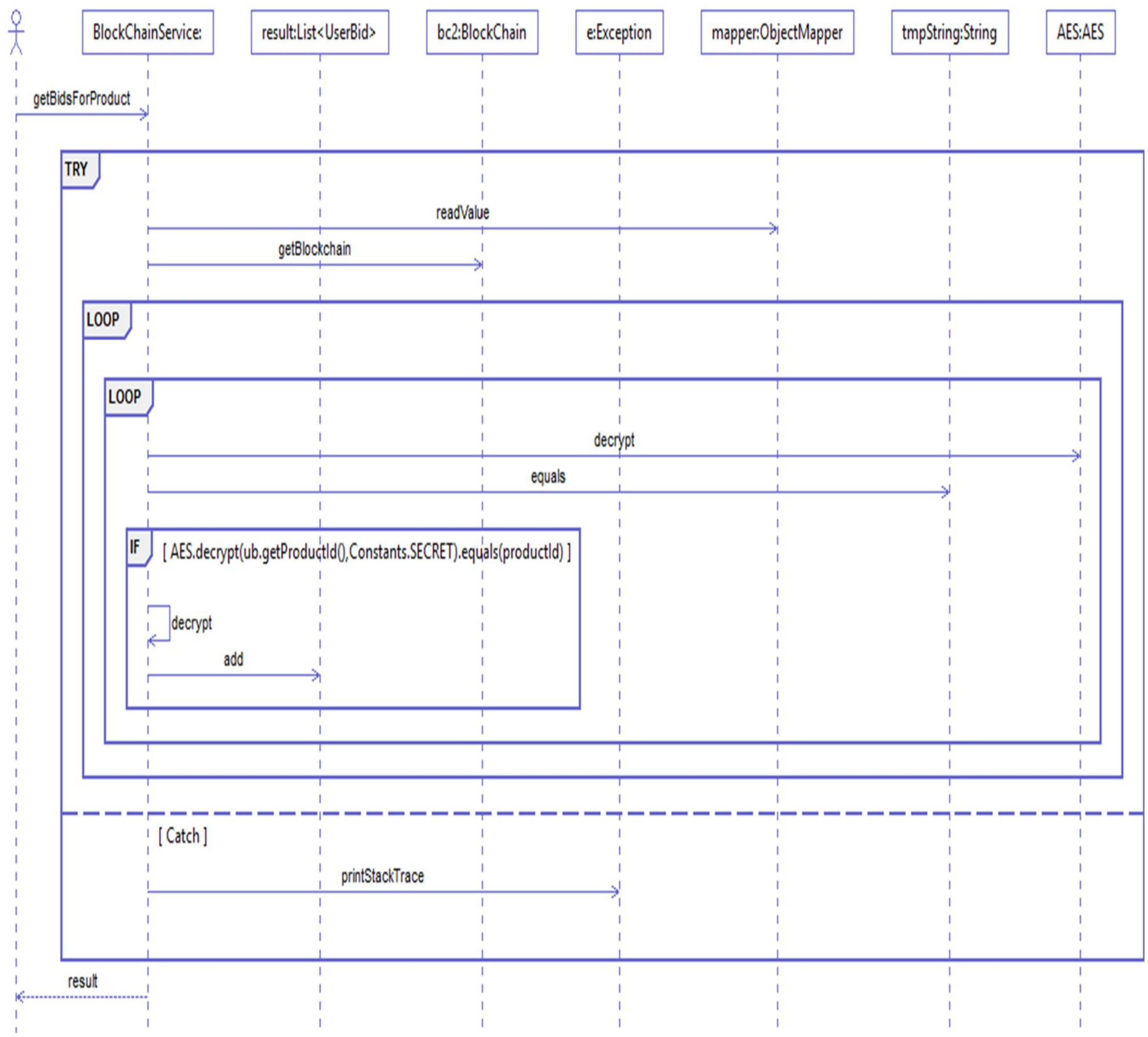


Fig 5.7.4: Sequence diagram of Bidding using Blockchain

5) Super Admin Configuration

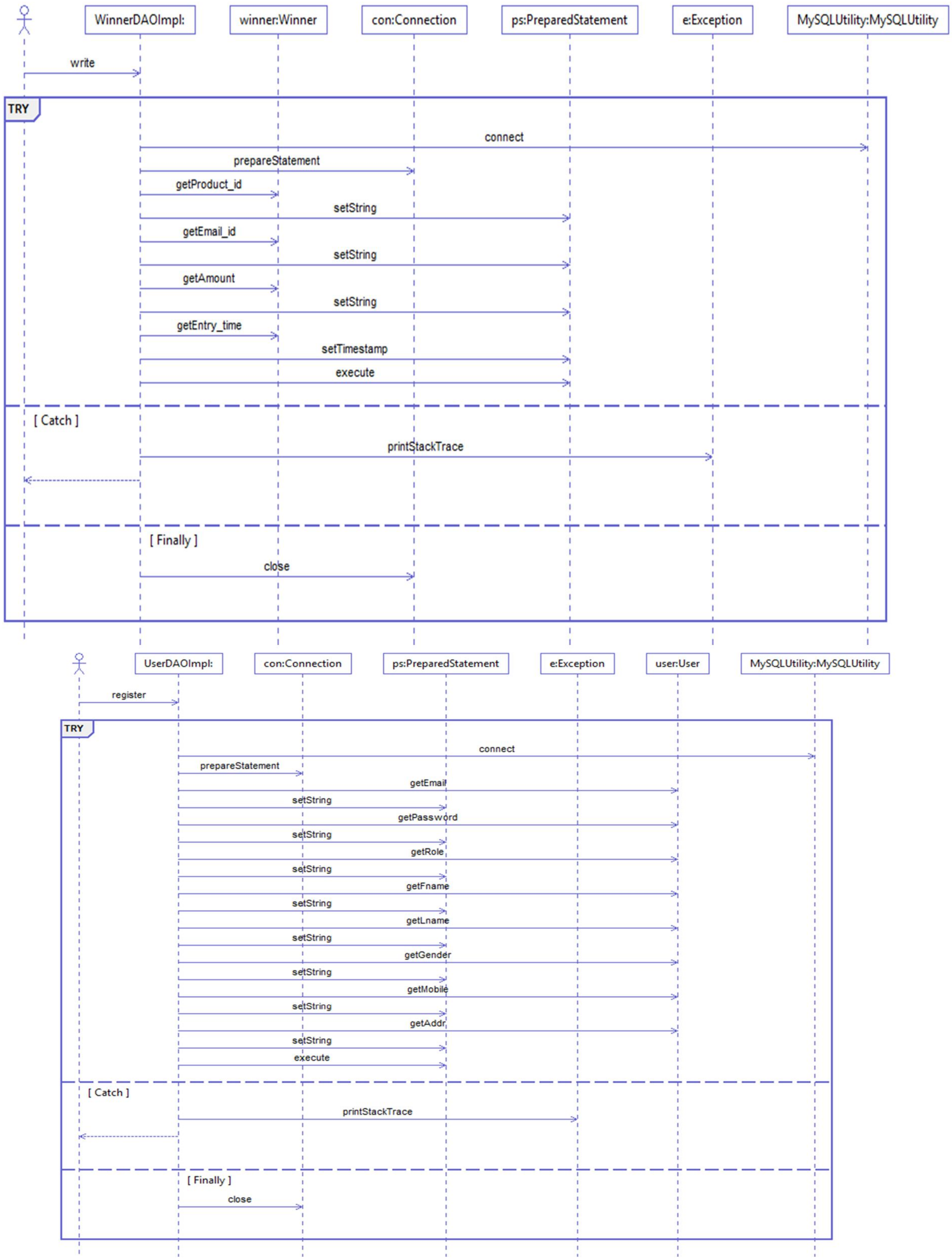


Fig 5.7.5: Sequence diagram of Super Admin Configuration

H. Class Diagrams

According to the Unified Modeling Language (UML), a class diagram is a static structure diagram that shows the classes, attributes, operations (or methods), and relationships between the classes to show how a system is structured. The class diagram is the primary building block of the object-oriented modeling process and is used both for technical modeling that converts models into programming code as well as for general conceptual modeling of the application's systematics. The class diagrams for the application are shown in the next section.

1) User Operation

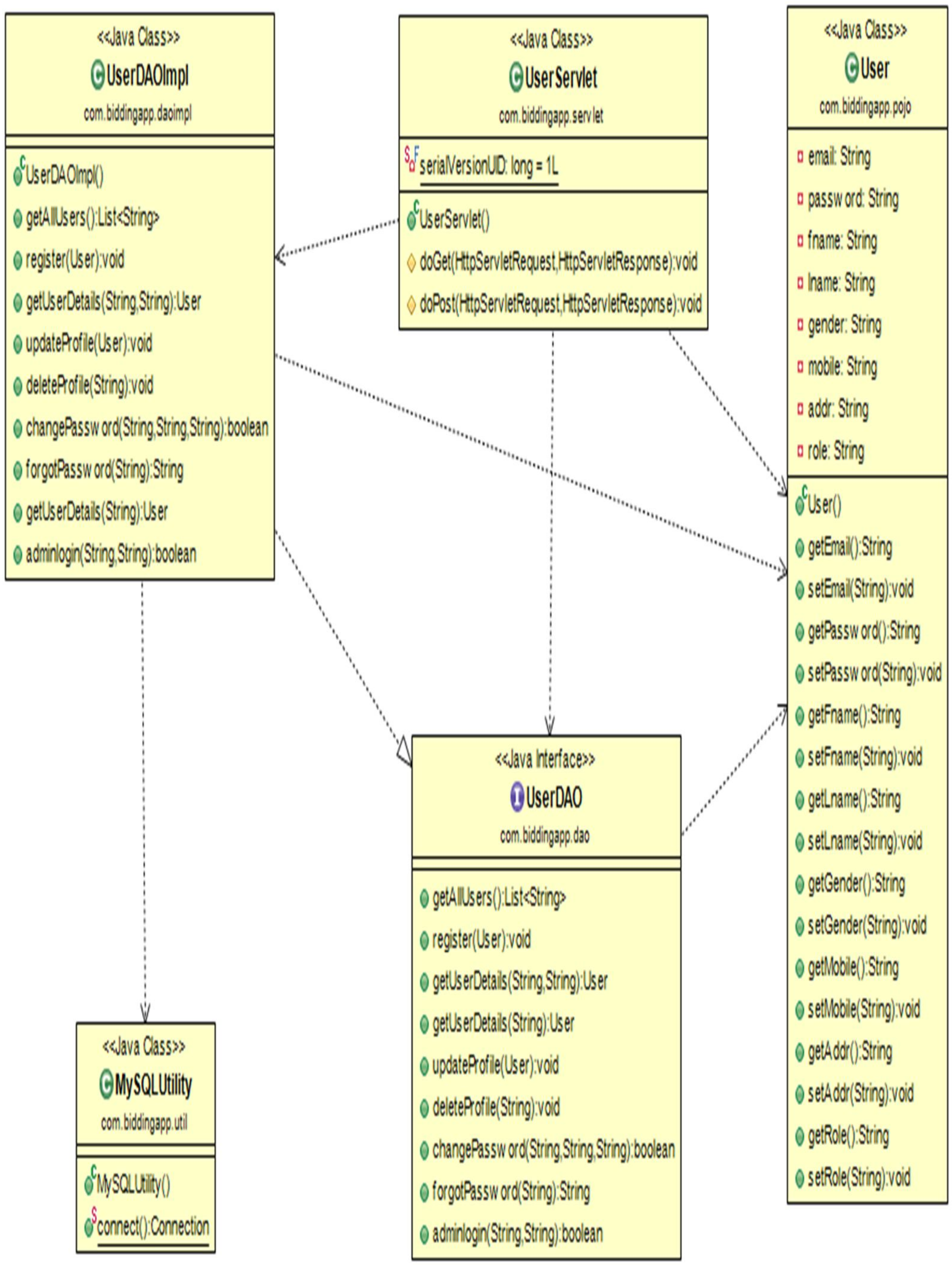


Fig 5.8.1: Class diagram of User Operation

2) *Creating and Updating bid*

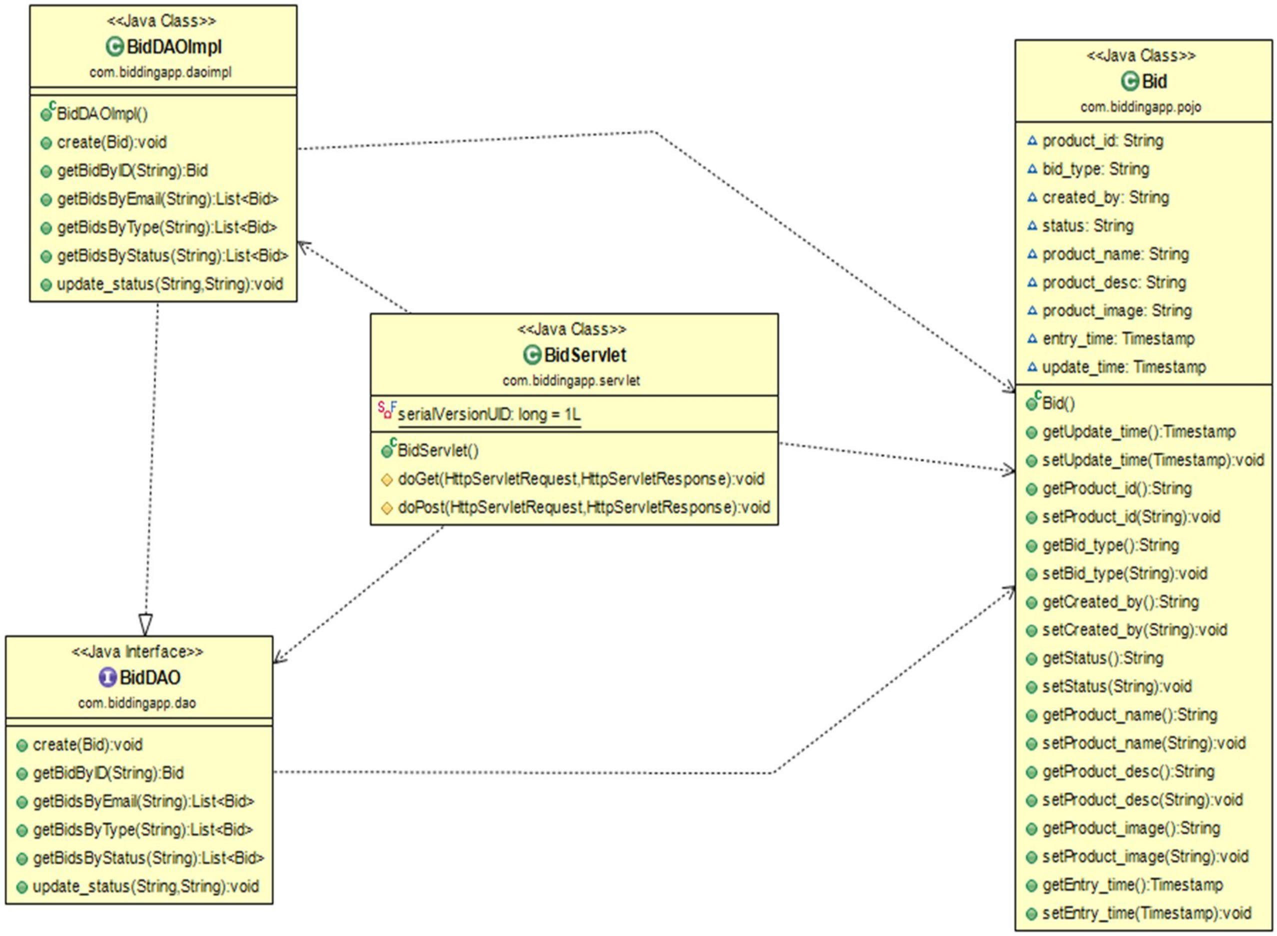


Fig 5.8.2: Class diagram of Creating and Updating Bid

3) *Node Operation*

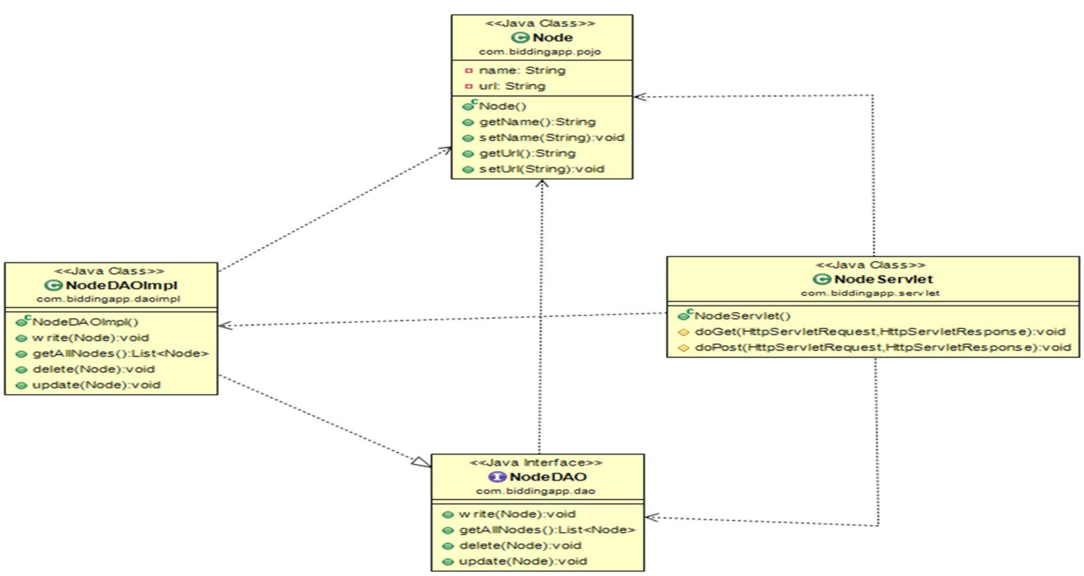


Fig 5.8.3: Class diagram of Node Operation

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

4) Blockchain Service

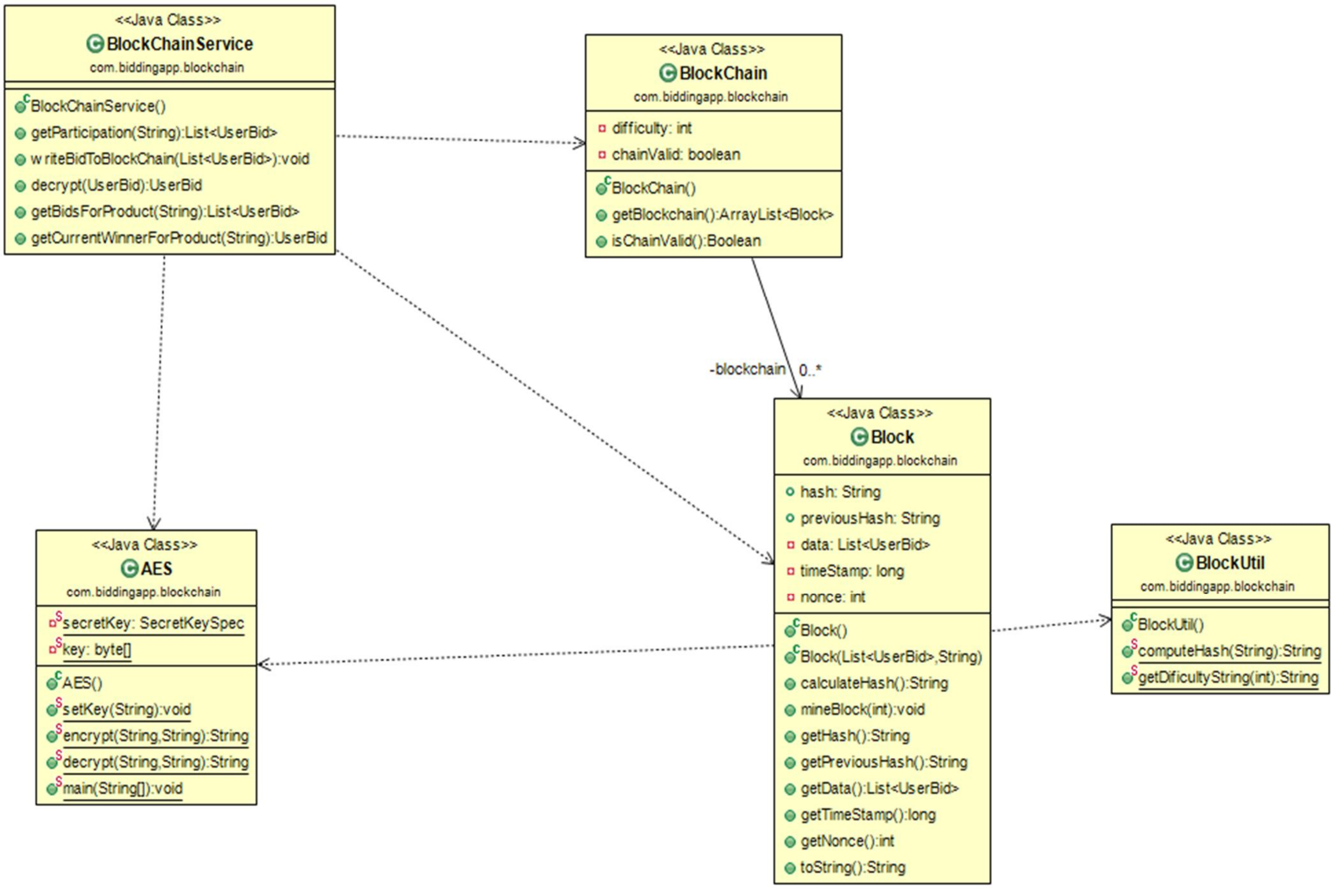


Fig 5.8.4: Class diagram of Blockchain Service

VI. SOFTWARE REQUIREMENTS SPECIFICATION

A. Functional Requirements

1) To layout and put in force the block chain technology into a web bidding gadget
2) To layout and increase the decentralized machine for making the entire database owned by way of many customers.
3) To make certain the cheating resources of the database manipulation is reduced via the concept of block chain and design the solution in any such way that it is easy and feasible to update the traditional bidding system
4) To make sure the results of the bidding are available to each consumers and sellers at any instance of the time

B. Non-Functional Requirements

1) Performance: The device ought to be easier to get entry to from the various browsers available.
2) Scalability: response time of the applications ought to replicate the actual time observations.
3) Maintainability: The set of rules must by no means fail in any of the test cases during trying out of software.
4) Safety: There shouldn't be any security issues on the merged information.
5) Usability: each user's pastime ought to be separated from the opposite consumer's sports.

VII. MOTIVATION/SCOPE OF THE PROJECT

This software or the project will help the whole bidding world to get them in a right direction. After this project no human interaction will be taken. This motivates to bid online over the internet and gives all the safety measures to make every transaction done completely and hassle free. Using block chain technology as a block, it will store the whole information in blocks and it will be encoded and decoded only once the bidding has been done over the bidding software.

VIII. MODULE

A. Account Access Module

In this module it is helpful to register the user and the people who wants to create themselves for the software, user can able to open their accounts, update accounts and delete the accounts. Log in and log off from the account. User can edit the profiles from this module.

B. Node Module

In this module, There is group of other nodes work with each other to communicate among them. They will receive data of the block chain only when transaction is committed by the block. Later it will perform the validation it will checks hash codes by comparing with another blocks. It is only read only access for clients so it is very secure.

C. Super Admin Module

In this super admin module, Admin can add all the products to the software using this super admin module. Super admin will be the product owner.

D. Product Module

Addition of all the products and removal which are planned for selling can be seen from this module. There will be direct html access where products are shown from database. It will be in photo form and information format. Where high size photos are not valid due to some restrictions.

IX. SYSTEM TESTING

The objective of the check is to identify and rectify any issues. A comprehensive assessment is conducted to detect any possible flaws or vulnerabilities in a completed work within the stipulated timeframe. This uncomplicated procedure can be employed to checks feasibility of assemblies, sub-assemblies, and entire product. The code of a package is utilized to examine its similarity with standards and the expectations of its users, ensuring that it meets both requirements satisfactorily. Different kind of examinations are available, each designed to cater a particular assessment.

A. Types Of Tests

1) Unit Testing

When a program is executed, the inputs and outputs undergo verification to guarantee the correctness reason on a property of the underlying program logic. This process is commonly referred to as unit testing. It is vital call branching and internal code flow are valid on all call levels. A visual inspection of the appliance's individual packaging components may be necessary to achieve this. Such an inspection can be carried out upon completion of the individual part, prior to integration. Alternatively, a structured check that is dependent on knowledge about the creation of the check and is offensive in its nature may be employed. Unit tests, also known as unit checks, are duplicate tests performed at the unit level on a particular business procedure, application, and/or system configuration. For the method to be considered successful, every individual approach of the business process must perform perfectly according to the requirements stated and contain clearly defined inputs and anticipated outputs.

2) Integration Testing

The primary objective of conducting integration tests is to assess the compatibility of diverse software system components, with the aim of determining their effectiveness when working in tandem. The testing process is triggered by specific events and primarily centers on the initial identification and interpretation of screens or fields. Although the individual components may meet the required standards, the triple-crown unit analysis is essential in verifying the suitability and consistency of the combined parts. The integration test is designed to highlight the questions asked after adding dissimilar elements.

3) Functional Test

Technical and business things, and person who owner guides are all utilized to showcase the availability of tested functions. Functional checking can be systematic validation of this. In this case, practical testing focuses on below aspects:

Valid Input: The system should receive valid input from established categories of valid input.
Revised: make enough and maintain accuracy and efficiency, it is imperative to reject any invalid input that falls within recognized categories of invalid input. Furthermore, it is crucial to subject known functions to rigorous testing. To enhance performance, recognized categories of software results thoroughly exercised. The activation of interface systems or processes is a necessary step in this process. The structure and preparation of task tests must be tailored to the demands of the organization, important functions, or specific circumstances under examination. Additionally, the test plan should encompass a systematic scope of typical business method flows, knowledge domains, specified processes, and consecutive processes. Prior to concluding the practical examination, the results of further tests must be evaluated to determine their effectiveness.

4) System Testing

The finding of system testing is guarantee that the product meets the system's criteria as a whole. This test validates well-known and certain results. For instance, system testing for an Associate in Nursing may include configuration-based system integration testing. Method descriptions and flows, as well as pre-run method links and integration points, are critical components of system testing.

5) Validation Testing

Upon completion of black box testing, the software is fully assembled and interfacing errors have been identified. The final series of tests, known as validation tests, are then initiated. Validation testing is defined as successful when the software functions in a manner that is deemed reasonable by the customer.

6) Output Testing

Following validation testing, the next step is to conduct output testing of the proposed system. As the system's usefulness is dependent on its ability to produce the required output, the user is consulted regarding the format in which the system is required to operate. The output displayed or generated by the system is then tested, with consideration given to both on-screen and printed formats. The on-screen format is verified to be correct and in accordance with user needs, while the hard copy output adheres to the user's requested specifications. Output testing does not result in any system corrections

7) User acceptance Testing

User acceptance testing is a critical factor in the success of the system. The system is tested for user acceptance by maintaining constant communication with the prospective system during development and making necessary changes as required. This includes input screen design and output screen design.

8) GUI Testing

GUI testing is utilized to ensure the visual clarity, flexibility, and user-friendliness of the system. The various components that are tested include relative layout, various links, and buttons.

X. RESULTS

A. Home/Index Page

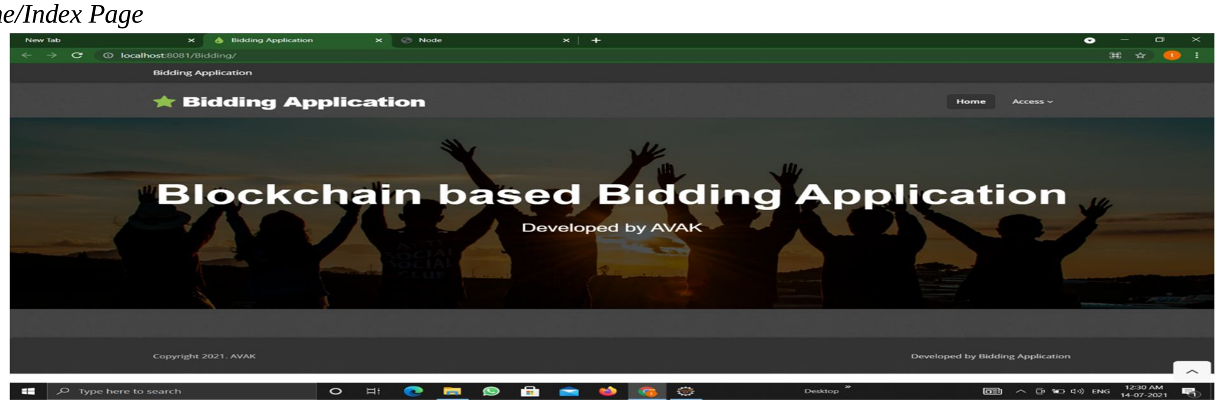


Fig 10.1: Home/Index page

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

B. New User Registration Page

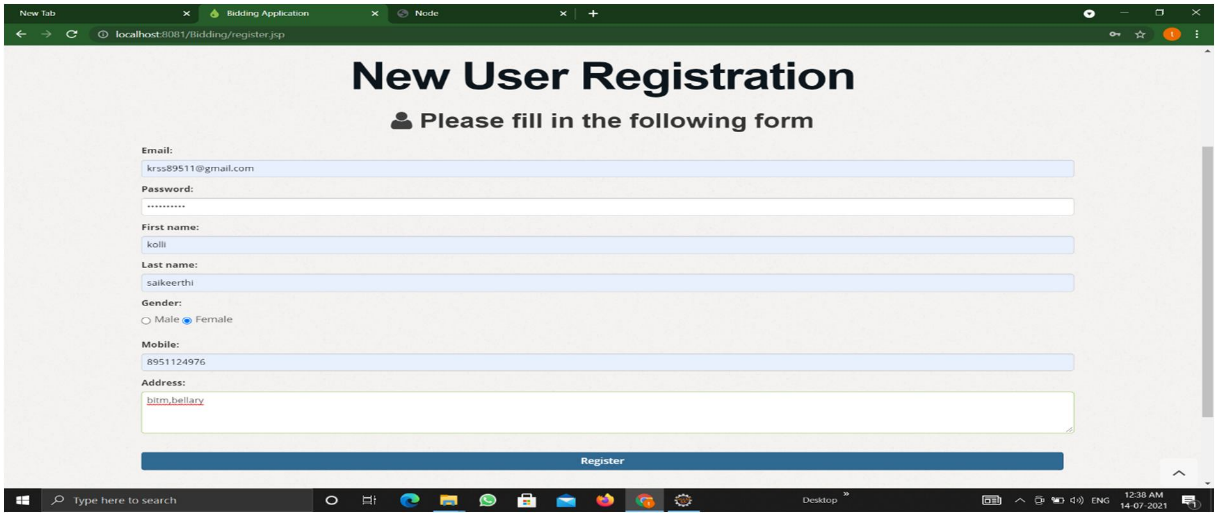


Fig 10.2: New User Registration page

C. New User Welcome Page

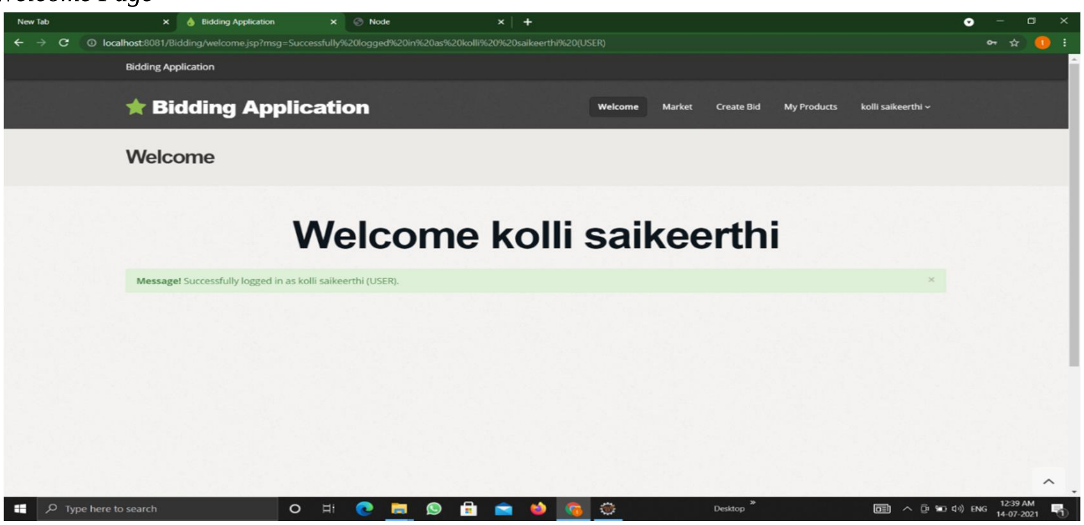


Fig 10.3: New User Welcome page

D. Creating New Bid Page

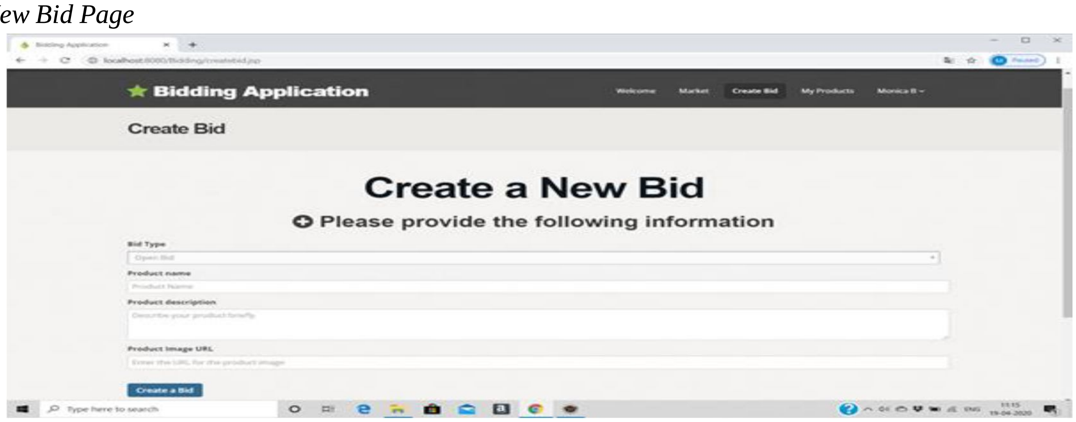


Fig 10.4: New User Welcome page

E. New Bid Created Successfully

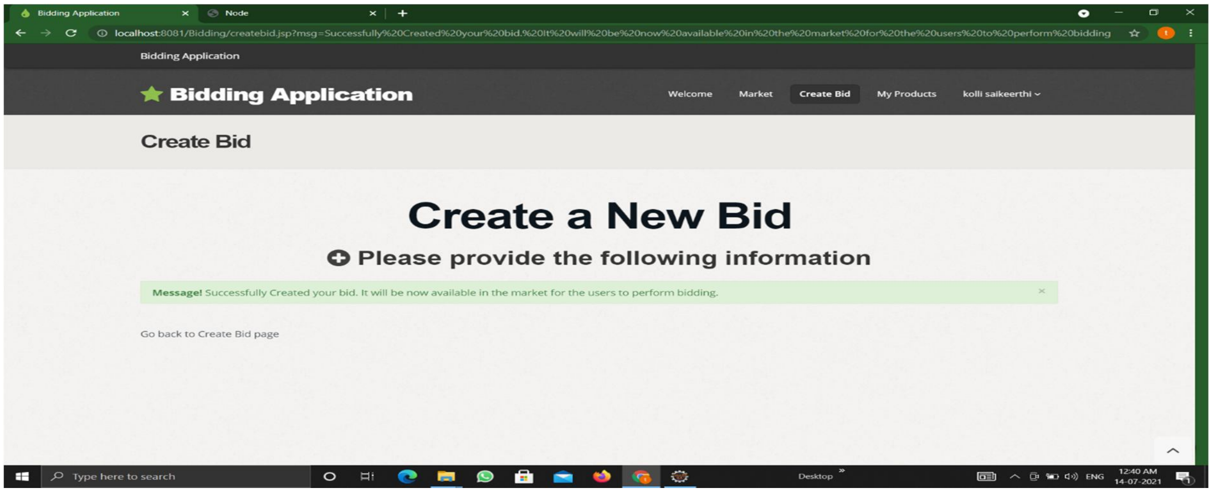


Fig 10.5: New Bid Created Successfully

F. My Product Page of the Seller

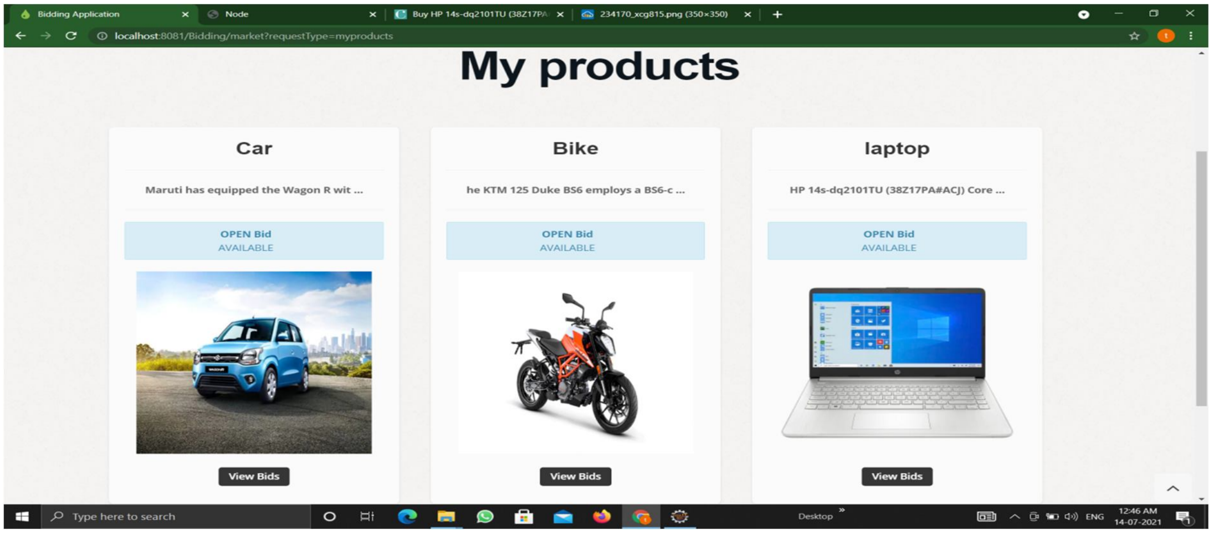


Fig 10.6: My Product page of Seller

G. Successfully Placed a Bid from Buyer.

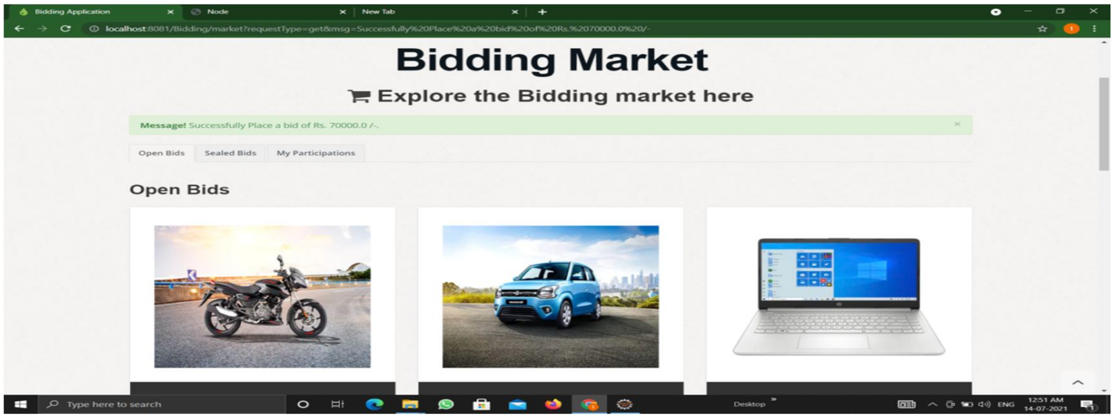


Fig 10.7: Successfully Placed a Bid from Buyer.

H. My Participation Page

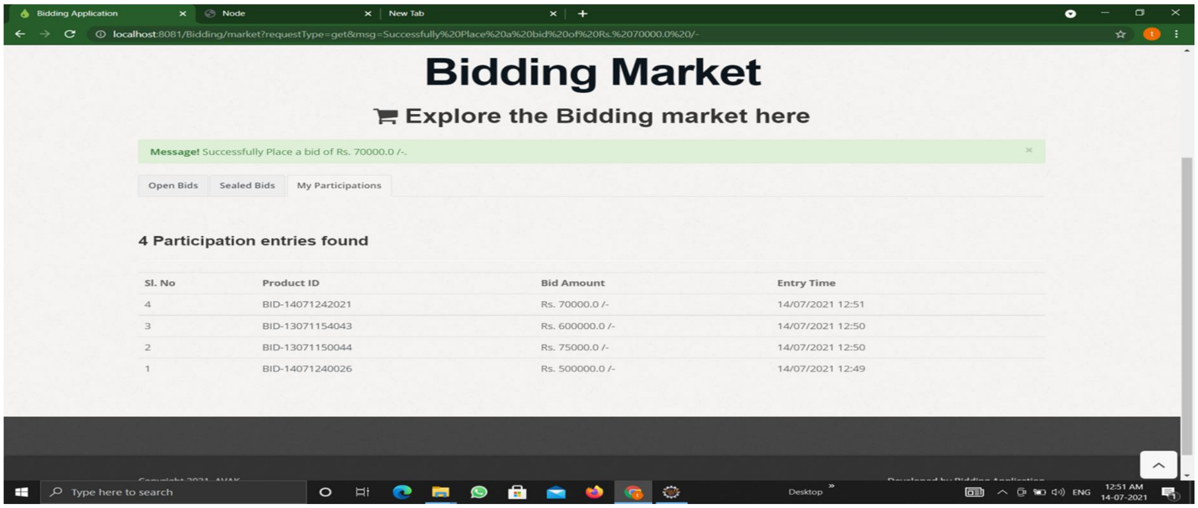


Fig 10.8: My Participation Page

I. Closing Bid by the Seller Page

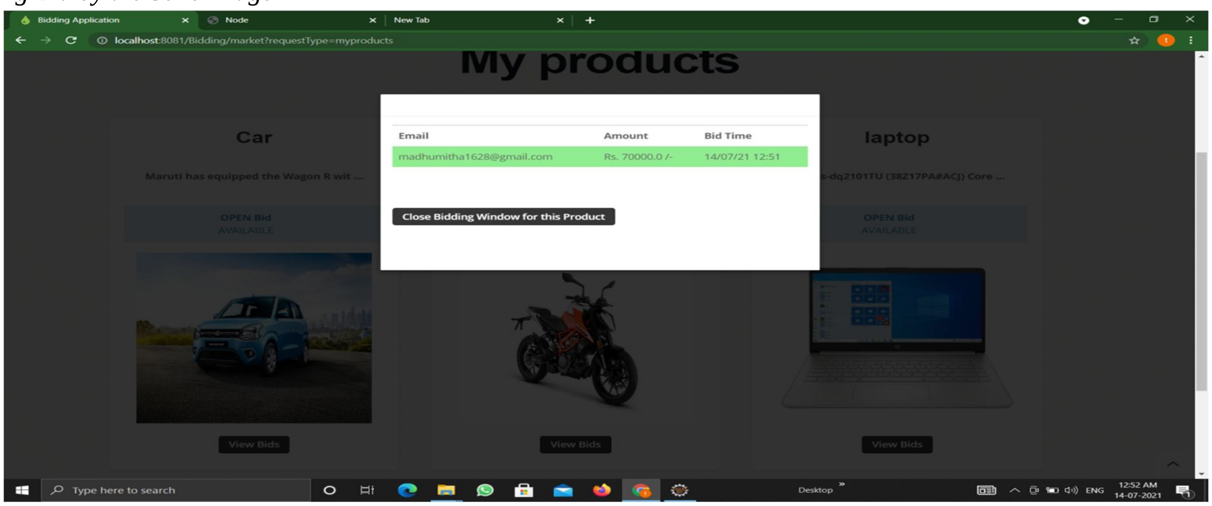


Fig 10.9: Closing Bid by the Seller Page

J. Page after Closing Bid by the Seller

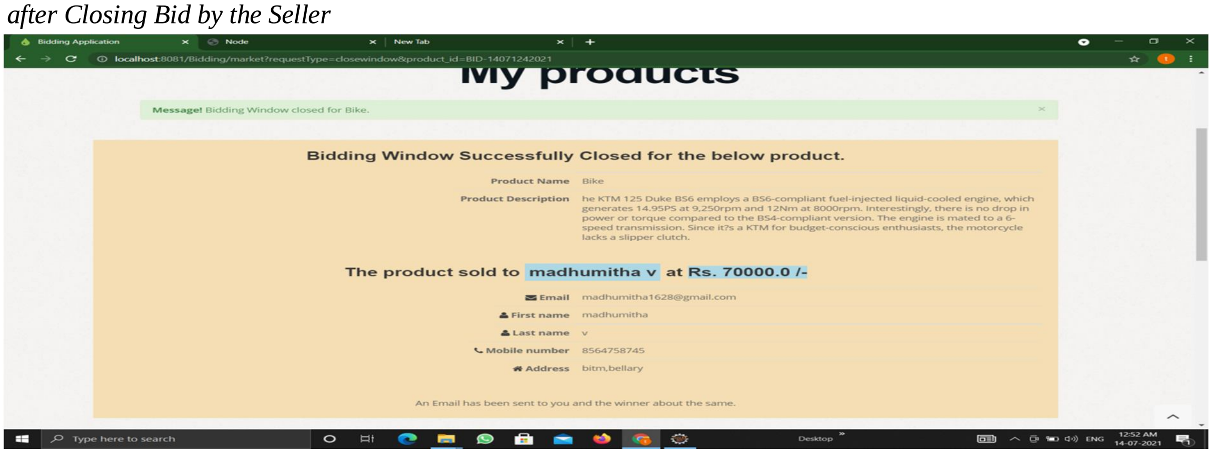


Fig 10.10: Page after Closing Bid by the Seller

K. E-mail sent to the Seller Page

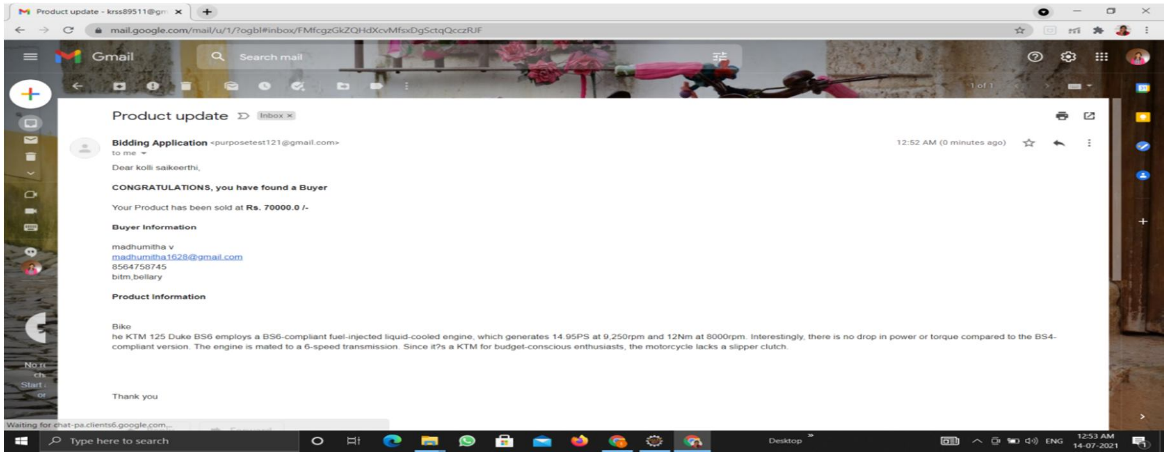


Fig 10.12: E-mail sent to the Seller Page

L. E-mail sent to the Winner Page

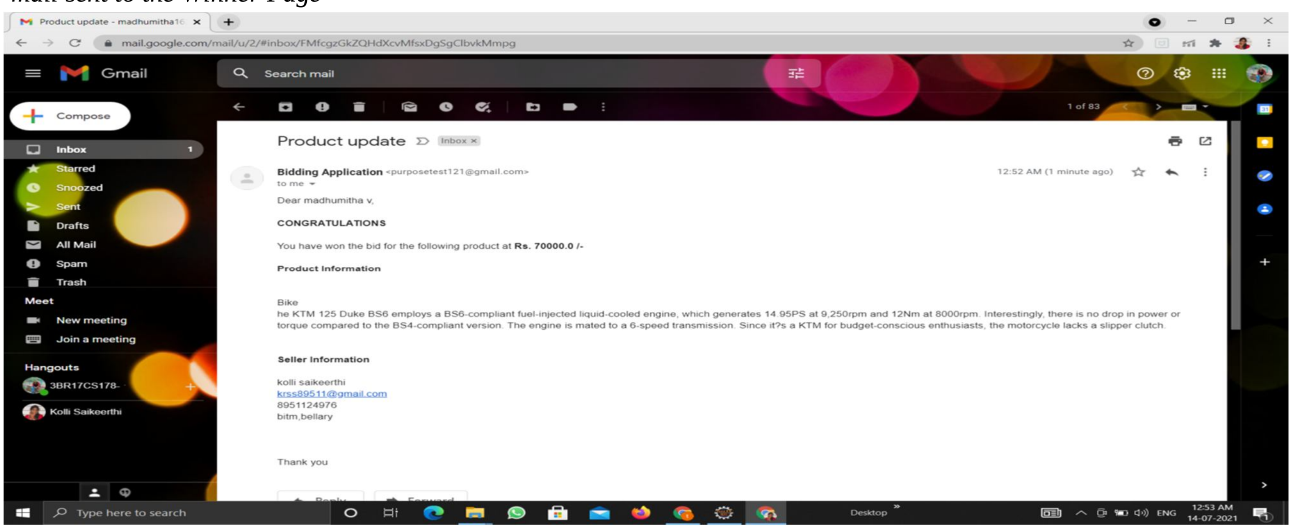


Fig 10.13: E-mail sent to the Winner Page

M. Winner Details in the Application

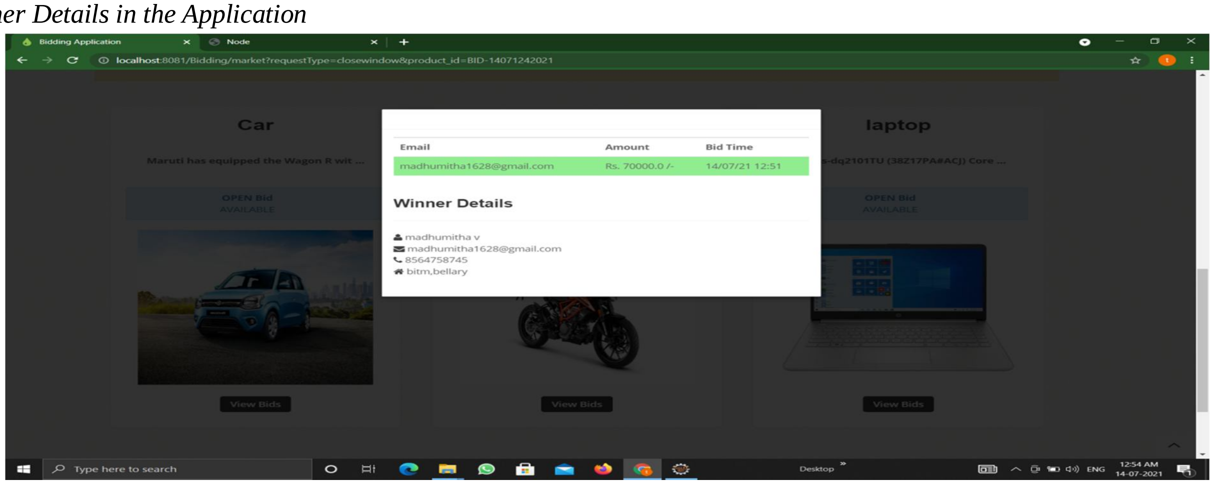


Fig 10.14: Winner Details in the Application

N. Products Won by the Buyer Page

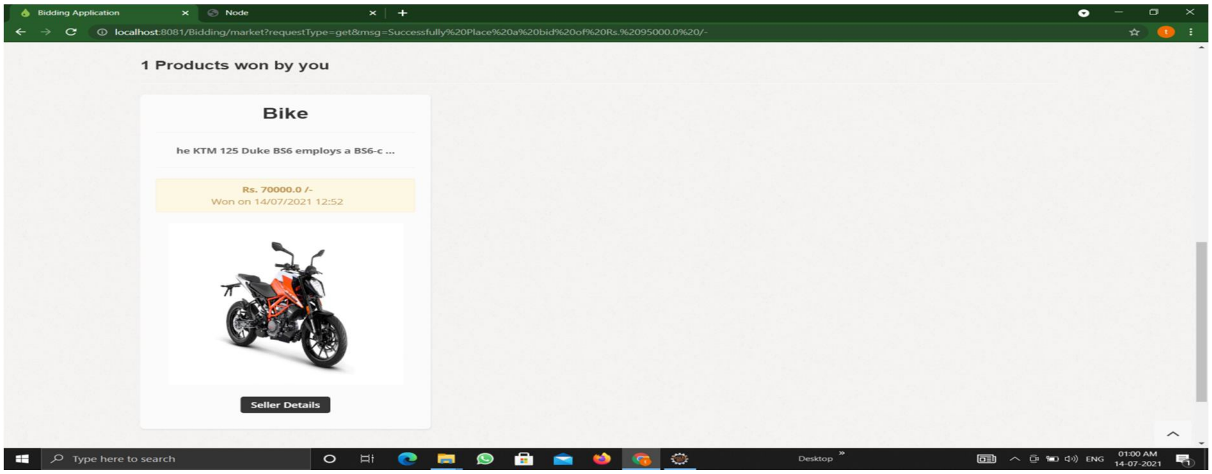


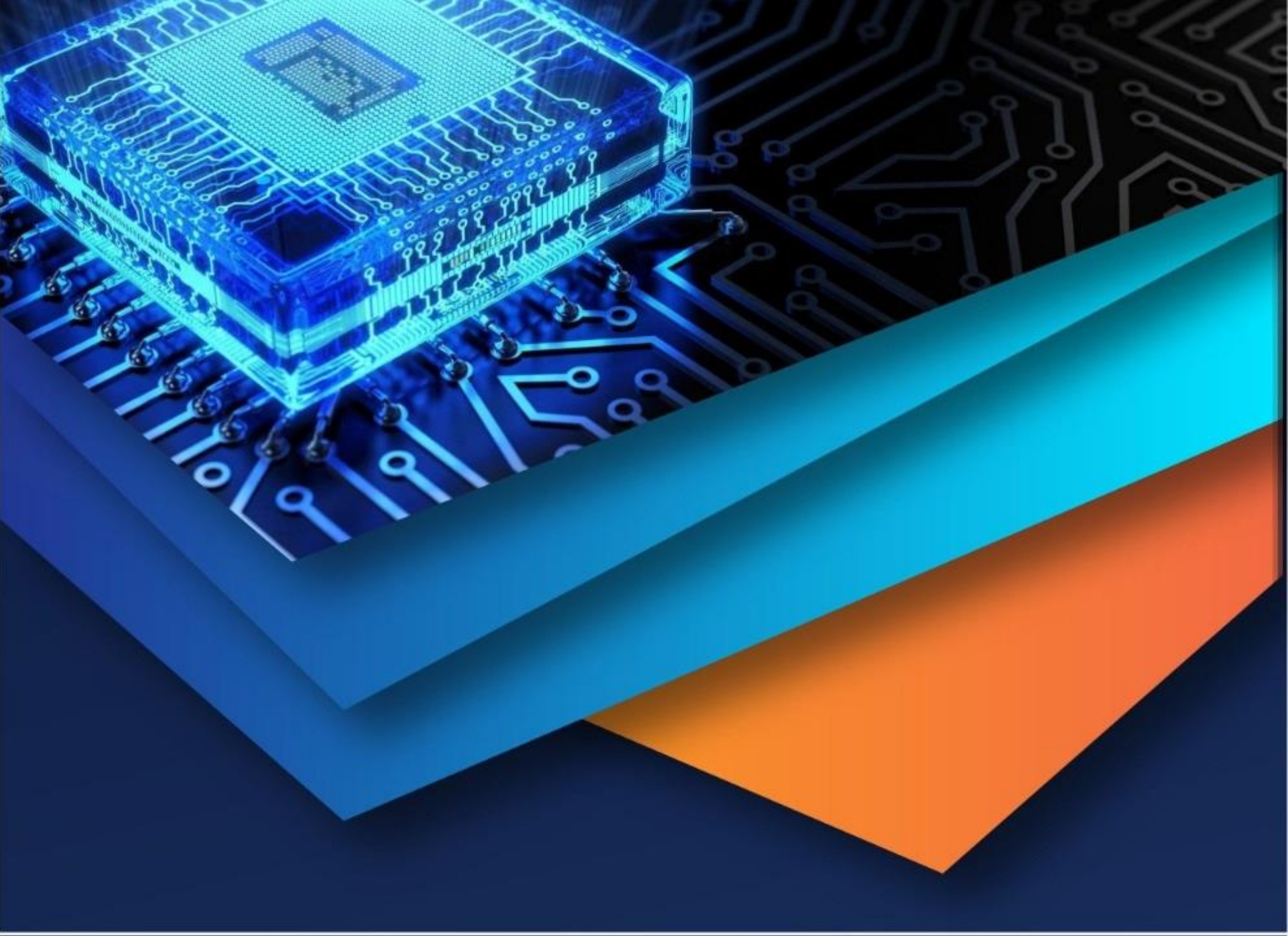
Fig 10.15: Products Won by the Buyer Page

XI. CONCLUSION

This project presents an electronic auction mechanism based on block chain technology, which guarantees the confidentiality, non-repudiation, and immutability of electronic seals. Our proposal utilizes block chain technology with low transaction costs to develop a smart contract for public and sealed bids. The smart contract, first introduced in 1990 and implemented through the Ethereum platform, ensures the security, privacy, non-repudiation, and immutability of bills by recording all transactions on the same decentralized ledger. The smart contract comprises the Auctioneer's address, the start and deadline of the auction, the current winner's address, and the current highest price.

REFERENCES

[1] Gang Cao and Jie Chen. Practical electronic auction scheme based on untrusted third-party. Computational and information and science IEEE, 2013
[2] llichetty S Pankaj Dayama. Auction-based mechanisms for electronic procurement. 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.
[11] 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.
[12] Affan Yasin and Lin Liu. An online identity and smart contract management system. In Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual, volume 2, pages 192–198. IEEE, 2016.
[13] 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.
[14] 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.
[15] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE, pages 180–184. IEEE, 2015.



10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

SJIFactor

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY