VISVESVARAYA TECHONOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi, Karnataka 590018

A Project Report
on

"BLOCKCHAIN BASED SMART CONTRACT FOR BIDDING SYSTEM"

Submitted in the partial fulfilment for the academic year 2018-2019

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE & ENGINEERING

Submitted by:

CHAITHRA H	**4BW15CS012**
CHAITHRA R	**4BW15CS014**
POORNIMA G	**4BW15CS049**
PRABHAVATHI S	**4BW15CS050**

Under the Guidance of
Mrs. PALLAVI N R
Asst. Prof, Dept. of CSE
BGSIT, BG Nagar

Shashikar
H O D
Dept. of Computer Science & Engg.
BGS Institute of Technology,
B.G. Nagar - 571 448
Dist: Mandya (INDIA)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
BGS INSTITUTE OF TECHNOLOGY
B G NAGAR-571 448
2018-2019

BGS INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University, Belagavi)

DEPARTMENT OF COMPUTER SCIENEC AND ENGINEERING

CERTIFICATE

This is to Certify that the Project entitled **"BLOCKCHAIN BASED SMART CONTRACT FOR BIDDING SYSTEM"** carried out by **Chaithra H (4BW15CS012), Chaithra R (4BW15CS014), Poornima G (4BW15CS049), Prabhavathi S (4BW15CS050)** a bonified students of **BGS Institute of Technology, B.G Nagara** in partial fulfilment of the award of Bachelor of Engineering in Computer Science & Engineering under Visvesvaraya Technological University, Belagavi during the year 2018-2019. It is certified that all corrections/suggestions indicated for the internal assessment have been incorporated in the report deposited in the department library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Technology.

Signature of Guide:	**Signature of HOD:**	**Signature of Principal:**
Pallavi 17/05/19	Shashikala 17/6/19	Narendra
Mrs. PALLAVI N R	**Mrs. SHASHIKALA S V**	**Dr. B K NARENDRA**
Asst. Prof,	**HOD & Prof.**	**Principal**
Dept. of CSE, BGSIT	**Dept. of CSE, BGSIT**	**BGSIT, B G NAGAR**

Name of the Examiners:

1. Swetha K.R
2. Ravikumar

Date and Signature:

Swetha KR 13/6/19

Ravi 13/06/19

ACKNOWLEDGEMENT

We take this opportunity to acknowledge all those who guided, supported and encouraged to emerge successful in completion of this project.

We have immense pleasure in expressing our thanks to **Dr. B K NARENDRA, Principal,** BGSIT, B G Nagar for having supported us in in academic endeavors and for providing all the facilities for the successful completion of mini project.

Our heartful thanks to **Mrs. SHASHIKALA S V, Prof. and head of the Department** for **Computer science and Engineering**, for her valuable suggestions and for helping us to complete our project.

We own deep sense of gratitude to our guide **Mrs. PALLAVI N R, Asst. Professor, Dept. of CSE** for her kind and able guidance. We are grateful for her help in the preparation. We take this opportunity to acknowledge all those who have of this manuscript.

We own deep sense of gratitude to our Coordinator **Mrs. ARPITHA K, Asst. Professor, Dept. of ISE** for her kind and able guidance. We are grateful for her help in the preparation. We take this opportunity to acknowledge all those who have of this manuscript.

Last but not the least, we extend sincere thanks to our beloved friends, teaching and non-teaching staff during the course of this work.

CHAITHRA H (4BW15CS012)

CHAITHRA R (4BW15CS014)

POORNIMA G (4BW15CS049)

PRABHAVATHI S (4BW15CS050)

Shashikala

H O D
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology
B.G. Nagar 571 448
Nagamangala Tq. Mandya Dist
Karnataka (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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic_hash of the previous block, a timestamp, and transaction data.

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

- Don & Alex Tapscott, authors Blockchain Revolution (2016)

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. The result is a robust workflow where participants uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. Blockchains have been described as a value-exchange protocol. This blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional

systems. A blockchain can assign title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

1.1Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Because blockchains are typically built to add the score of new blocks onto old blocks and because there are incentives to work only on extending with new blocks rather than overwriting old blocks, the probability of an entry becoming superseded goes down exponentiallyas more blocks are built on top of it, eventually becoming very low.

For example, in a blockchain using the proof-of-work system, the chain with the most cumulative proof-of-work is always considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

1.2 Block time

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five

seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions. The block time for Ethereum is set to between 14 and 15 seconds, while for bitcoin it is 10 minutes.

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. 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 , bidders have no way to ensure that lead bidder never leaks their bidding price.

This paper applies the blockchain technique into the E-auction to resolve the two 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 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 cannot be opened before the deadline.

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.

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.

1.3 Objective

- To design and implement the blockchain technique into the E-auction.
- To design decentralized structure for communicating between bidders and auctioneers to reduce the charge and transactional cost.
- To ensure that the personal data of the parties and the transactional records are protected through peer to peer access
- To ensure the bid price isn't leaked by the lead bidder by introducing the smart contract between the parties
- To design and develop a simple and efficient user interface for both the bidders and auctioneers to perform their respective functionalities.

1.4 Problem statement

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.

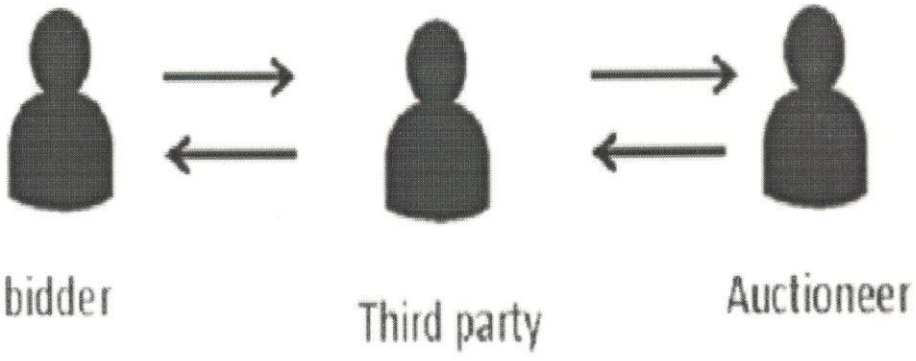

Fig 1.1: The role of the E-auction

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

CHAPTER 2
LITERTATURE SURVEY

[1] Paper Name : The truth about blockchain.

Authors: Marco Iansiti and Karim R Lakhani

Paper id: 95(1):118–127

Year: 2017

Contracts, transactions, and the records of them are among the defining structures in our economic, legal, and political systems. They protect assets and set organizational boundaries. They establish and verify identities and chronicle events. They govern interactions among nations, organizations, communities, and individuals. And yet these critical tools and the bureaucracies formed to manage them have not kept up with the economy's digital transformation.

Blockchain promises to solve this problem. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

Blockchain contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain.

Advantages:

- Secret bidding prices
- Unforgeability

Disadvantages:

- Privacy issues: Piracy refers to the unauthorized duplication of copyrighted content that is then sold at substantially lower prices. The ease of access to technology has meant that over the years, piracy has become more rampant.

[2] Paper Name: An online identity and smart contract management system

Authors: Affan Yasin and Lin Liu.

Paper id: 874-1-7852-0.

Year:2016

In today's online environment, people attend various kinds of activities, exhibit different digital presence, build personal digital reputations, issuing and receiving feedbacks.

From online communities being involved with. These diverse information sources once aggregatedcan provide a valuable future reference for personal online digital identity and credits check. The primary objective of this paper is to propose a systematic framework for aggregating online identity and reputation information, to providea holistic approach to personal online behavioral ratings. Major contributions include: An identity aggregation mechanism based on social dependency network is proposed, a smart contract management framework referring to personal online ratings based on the aggregated digital identity, an experiment implementation based on blockchain technology, with illustrative examples and theoretical evaluations to the proposed approach.

Advantages:

- With a decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data should be simpler.
- Moreover, laws and regulations could be programmed into the blockchain itself, so that they are enforced automatically

Disadvantages:

- This limits the domain of possible bidders
- The problem with both the English and Dutch auctions is that the bidding participants must be present at the auction.

[3] Paper Name: Decentralizing privacy: Using blockchain to protect personal data.

Authors: Guy Zyskind, Oz Nathan.

Paper id: 978-1-4799-9933-0.

Year: 2015

The recent increase in reported incidents of surveillance and security breaches compromising users privacy call into question the current model, in which third-parties collect and control massive amounts of personal data.

Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data.

We implement a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. Unlike Bitcoin, transactions in our system are not strictly financial – they are used to carry instructions, such as storing, querying and sharing data.

Finally, we discuss possible future extensions to blockchains that could harness them into a well-rounded solution for trusted computing problems in society.

Advantages:

- Users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used.
- Companies can focus on utilizing data without being overly concerned about properly securing and compartmentalizing them.
- A decentralized personal data management system that ensures users own and control their data

Disadvantages:

- They would need to increase the usefulness of the platform presented earlier.
- The blockchain recognizes the users as the owners of their personal data

[4] Paper Name: Practical electronic auction scheme based on untrusted third-party.

Authors: Gang Cao and Jie Chen.

Paper id:978-0-7695-5004-6.

Year: 2013

Most electronic auction schemes need assistance of third-party arbitration institution. If the third-party agency conspires with seller or buyer, buyer's bid price and seller's trade secret would be betrayed. Based on the Bit commitment and blind signature, an electronic auction scheme is proposed.

The peculiar feature of the proposed scheme is that the third-party agency can be untrusted, namely, the scheme can resist conspiracy attack effectively. Anonymity and security of all bidders, including lose bidder, have the same and important position in the proposed scheme, and are satisfied well too. Moreover, the proposed scheme has additional characteristics such as unforgeability, strong verifiability, non-repudiation, time limitation, fairness and high effectiveness.

Advantages:

The proposed scheme can be widely applied in any sensitive auction (e.g., auctions of cosmetics, medical services, etc.).

Moreover, the proposed scheme also satisfies the following requirements:

- Bidding privacy
- Strong anonymity
- Unforgeability
- Strong verifiability

Disadvantages:

- This scheme could not withstand the man-in-the-middle attacks, where man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other

[5] Paper Name: User payment choice behavior in e-auction transactions.

Authors: Wee-Kheng Tan and Yung-Lun Chung.

Paper id: 874-0-7584-5744-4

Year: 2010

Payment is an inborn part in any e-transaction. Risk is also prevalent in e-auction. Payment methods, e.g. online specialized C2C payment services and ATM transfer are used to address such fear. This research uses the buyers and sellers of e-auction as the subjects of investigation. A set of criteria which buyers and sellers consider when selecting the payment method is proposed.

Since no single criterion can adequately explain their choice, Analytical Hierarchy Process method is used. Research shows that buyers' and sellers' final choice of the payment method is a multi-criteria consideration and the relative importance of the criteria is a reflection of their risk perception. Both parties hope to lower the risk by choosing payment method that best safeguards their interest. However, such concern, especially for buyers, is moderated if the payment method is already widely used.

Advantages:

- Verifiability
- Non-repudiation
- Traceability
- One-time registration
- Easy revocation

Disadvantages:

- This scheme was unable to achieve
- Strong anonymity
- Bidding privacy
- Secret bidding prices for sealed-bids

[6] Paper Name: A sealed-bid electronic marketplace bidding auction protocol by using ring signature.

Authors: Wenbo Shi, Injoo Jang, and Hyeong SeonYoo.

Paper id: 854-1-5454-2587-25.

Year: 2009

We modified the multi-agent negotiation test-bed auction scheme which was proposed by Collins et al. In 2004, Jaiswal et al. have modified Collins's scheme, but Jaiswal's scheme still has some security weaknesses: such as replay data attack and DOS (denial-of-service) attack, collision between customers and a certain supplier. So the proposed protocol tries to reduce DOS attack and avoid replay data attack by using improved ring signature scheme, also it achieves perfect anonymity.

And it publishes an interpolating polynomial for sharing the determination process data and avoids collusion between a customer and a certain supplier. Furthermore, the proposed scheme relaxes the trust assumptions for three-party in Jaiswal's scheme. According to comparison and analysis with other protocols, our proposed protocol shows good security.

Advantages:

- Reasonable security and simplicity can be realized
- The auctioneer can authenticate the real identity of the winner at the end of the protocol without additional interactions with the winning bidder even though all the bidders bid anonymously

Disadvantages:

- This causes the game of hide-and-seek between the encryption technology and illegal decrypt or get-out of the protection.
- There are some security weaknesses: such as replay data attack and DOS (denial-of-service) attack, collision between customers and a certain supplier.

[7] Paper Name: A sealed-bid electronic auction protocol based on ring signature.

Authors: Hu Xiong, Zhiguang Qin, Fengli Zhang, Yong Yang, and Yang Zhao.

Paper id: 974-0-2857-4445-2

Year: 2009

The blockchain-based digital content distribution system was developed. Decentralized and pear-to-pear authentication mechanism can be considered as the ideal rights management mechanism. The blockchain has the potential to realize this ideal content distribution system. This is the successful model of the Super distribution concept which was announced almost 30 years ago. The proposed system was demonstrated and got a lot of feedback for the future practical system

Advantages:

- The content owner can control easily and always. This means owner can control everything. To realize this concept, simple and easy operation would be required.

Disadvantages:

- The problem of these system is the pirate attacking. There are so many attacks to decrypt or steal the key for taking the content without the legal procedure.

[8] Paper Name: A model in support of bid evaluation in multi-attribute e-auction for procurement.

Authors: Shengbao Yao, Wan-An Cui, and Zhenqian Wang.

Paper id: 997-0-8154-8521-0.

Year: 2008

Bid evaluation is an important but complex problem in multi-attribute auction. Management science techniques might be helpful tools for this kind of decision making problems. This paper focuses 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 evaluate the buyer's preferences. It is shown by means of a bid evaluation example that the presented

approach may be well suited as a decision-making tool for multi-attribute e-procurement.

Advantages:

- A study conducted by the Center for Advanced Purchasing Studies [14] shows that more than a third of the firms interviewed by them are procuring goods in excess of $ 100 million through electronic procurement auctions.

Disadvantages:

- Strategic Complexity
- Winner Determination

[9] Paper Name: Auction-based mechanisms for electronic procurement.

Authors: llichetty S Chandrashekar, Y Narahari, Charles H Rosa, Devadatta M Kulkarni, Jeffrey D Tew, and Pankaj Dayama.

Paper id: 985-1-5478-7457-5.

Year: 2007

Auction-based mechanisms are extremely relevant in modern day electronic procurement systems since they enable a promising way of automating negotiations with suppliers and achieve the ideal goals of procurement efficiency and cost minimization. This paper surveys recent research and current art in the area of auction-based mechanisms for e-procurement. The survey delineates different representative scenarios in e-procurement where auctions can be deployed and describes the conceptual and mathematical aspects of different categories of procurement auctions.

Advantages:

- Many large corporations have now either used or are in the process of using automated auction-based negotiation methods for their procurement operations.

- General Electric has adopted on-line auctions for many of its procurement operations, procuring more than $6 billion worth of goods and services in on-line auctions in 2000.

Disadvantages:

- Valuation Complexity
- Communication complexity

[10] Paper Name: A new secure electronic auction scheme.

Authors: Fangguo Zhang, Qiongfang Li, and Yumin Wang.

Paper id: 0-7803-6323-X.

Year: 2000.

With the advance of science and technology, many human procedures have been replaced by electronic ones among which is electronic auction. Auction is one of the most important financial transactions for setting price. The Internet provides an unique distributed environment allowing distributed Internet electronic auction which offers an unique opportunity to reach a large bidding population.

An electronic auction scheme is viewed as a set of electronic protocols which allow a collection of bidders to buy a thing at an auction with the low price as possible, while a seller puts a thing up for auction and wants the bidders to buy his goods with the high price as possible.

The two most common auctions are the English auction where bidders bid up the price, and the Dutch auction where the price starts out high, and is lowered until a bidder claims the item at the current price. The problem with both the English and Dutch auctions is that the bidding participants must be present at the auction. This limits the domain of possible bidders. The solution is the sealed bid auction(or secure auction).

Advantages:

- This paper presented an electronic auction scheme based on an improved secure multiparty computation protocol and bit commitment protocol, in which all prices of bidders except the winning bidder are secret.
- This scheme includes many computations, but in reality, the value of price can be in smaller range.

Disadvantages:

- The problem with both the English and Dutch auctions is that the bidding participants must be present at the auction.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

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.

Disadvantages

- Centralized intermediary is required whose charge fees increases the transaction cost.
- It also involves data security risk.
- In a sealed envelope, bidders have no way to ensure that lead bidder never leaks their bidding price.

3.2 Proposed System

This project applies the blockchain technique into the E-auction to resolve the two main problems in the E-auction that we stated earlier. 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 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 cannot be opened before the deadline.

Advantages

- Decentralized structure for communicating between bidders and auctioneers thus reducing the charge fee.
- Peer to peer access structure to establish the trust thus protecting the personal data and transactional records.
- The bid price leaked by the lead bidder will be avoided through the smart contract.

3.3 Application

Cyber security

- Guardtime – This company is creating "keyless" signature systems using blockchain which is currently used to secure the health records of one million Estonian citizens.

Healthcare

- Gem – This startup is working with the Centre for Disease Control to put disease outbreak data onto a blockchain which it says will increase effectiveness of disaster relief and response.

- MedRec – An MIT project involving blockchain electronic medical records designed to manage authentication, confidentiality and data sharing.

Government

- Estonia – The Estonian government has partnered with Ericsson on an initiative involving creating a new data center to move public records onto the blockchain.

- South Korea – Samsung is creating blockchain solutions for the South Korean government which will be put to use in public safety and transport applications.

Real Estate

- Ubiquity – This startup is creating a blockchain-driven system for tracking the complicated legal process which creates friction and expense in real estate transfer.

3.4 System Requirements

3.4.1 Hardware requirements

• Processor	Intel Core i5 or AMD FX 8 core series with clock speed of 2.4 GHz or above
• RAM	2GB or above
• Hard disk	40 GB or above
• Input device	Keyboard or mouse or compatible pointing devices
• Display	XGA (1024*768 pixels) or higher resolution monitor with 32bitcolor settings
• Miscellaneus	USB Interface, Power adapter, etc

3.4.2 Software Requirements

• Operating System	Windows
• Programming Language – Backend	Core Java, Advanced Java, J2EE, Map Reduce Framework, MVC Framework
• Programming language - Frontend	Bootstrap Framework, HTML, CSS, JavaScript, Ajax, JQuery
• Development environment	Eclipse Oxygen IDE
• Application Server	Apache Tomcat v9.0
• Database	MySQL

CHAPTER 4

SYSTEM DESIGN

4.1 Architecture of Blockchain Bidding System

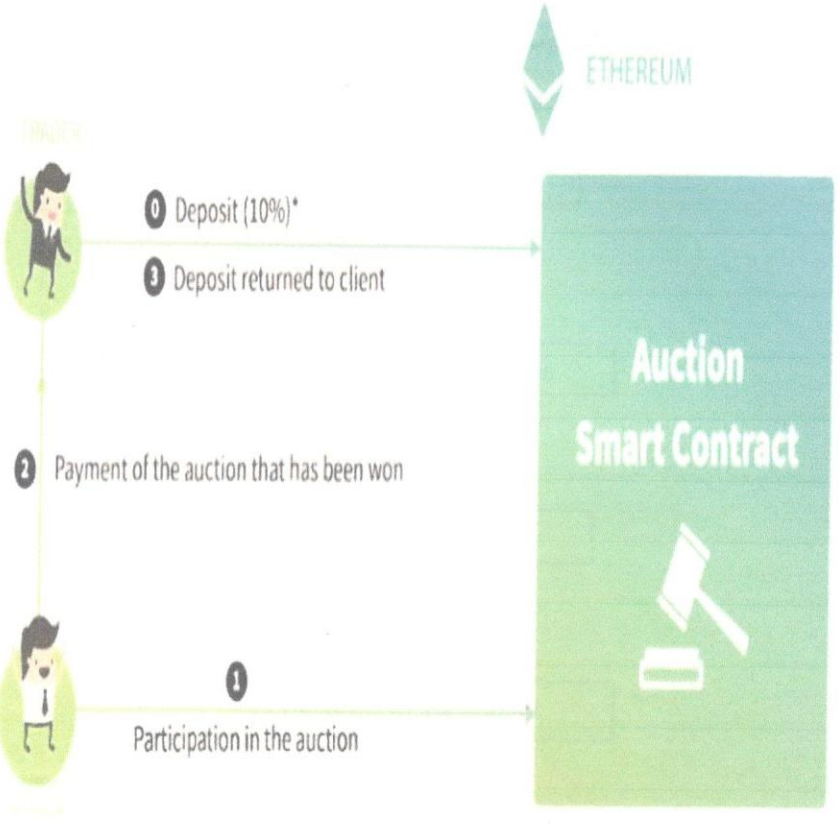

Fig 4.1: Architecture of Blockchain Bidding System

As shown in Fig 4.1 Architecture of Blockchain Bidding System the seller upload the information to the auction database then bidder prepare for the auction if he won the auction process he will get the product.

4.2 Flow Chart

In the below Fig 4.2 Flow chart of Blockchain Bidding System, in the first stage auctioneer post the details about the product, in the next stage bidder bid the product, in the next stage current highest price processed. These stapes will be repeated until due time will encountered. After the due time highest bidding will be displayed. And bidder

with highest price pay the price to auctioneer. Auctioneer will transmit the product to the winner.

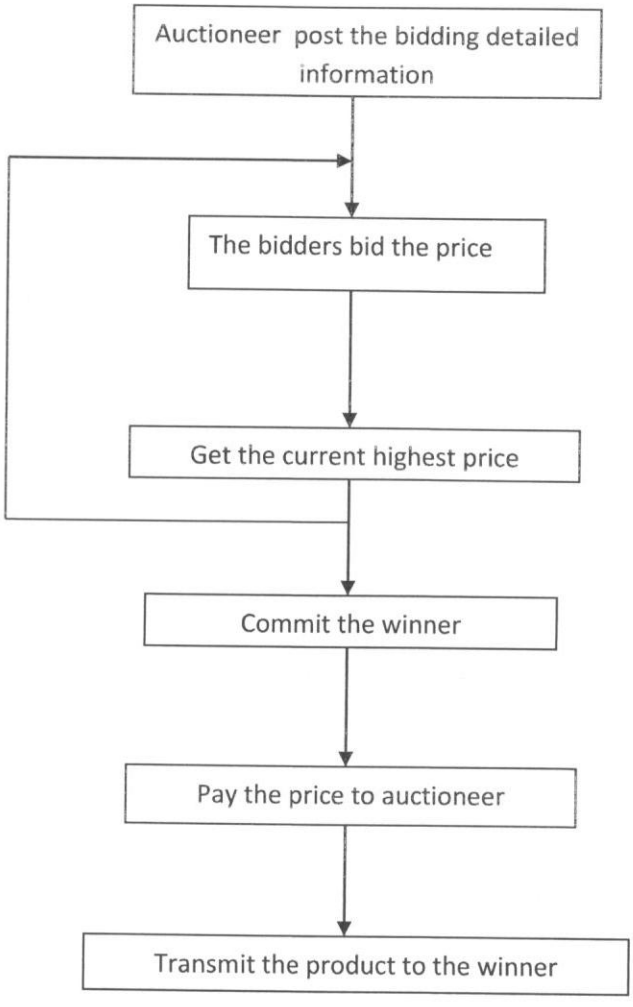

Fig 4.2 Flow chart of Blockchain Bidding System

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.

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. 4.3. The fields in the block, as shown in Fig. 4.4, to detail the records of the block such as time-stamp, transaction quantity, hash value, etc

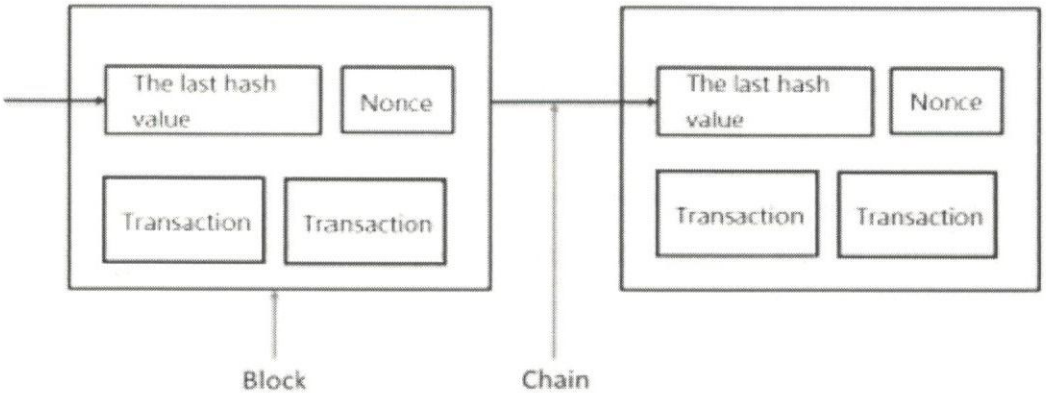

Fig. 4.3: The relationship between the block and chain

The fields in the block, as shown in Fig 4.4 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)	000000000000000004a6f37e94a28076ce4e0f6965869c47e0f60c3abf21e0f
Merkle Root	c003190d380153505850c589dddf7bff46dc1420a871de81c002e5bc1a2b46c5

Fig. 4.4: The field names of each block

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.

The seller posts the bidding information including product description and starting price at the first stage. Bidders vote the sealed envelope to bid the product with a higher price. After receiving the sealed envelope, the auctioneer announces the highest

rate right now. The bidder is as the winner bidder until no one bid the product with the higher price or the deadline is due. The auctioneer can get the money from winner and send the product to the bidder. We develop an open bidding system through blockchain with smart contracts. Bidders write the trade contract for the bids into the blockchain. With decentralized access structure, all bidders can bid the product by calling the open contract's trading contract without intermediate brokers.

A complete public E-auction system must satisfy the following requirements

- The identity of the person who is a bidder or winner (successful bidder) is anonymous to everyone.
- During a transaction, the content of seal order cannot be modified, and all the people can verify whether its correctness and completeness.
- No illegal bidder can impersonate the legal one to bid the product. After bidding, no one can deny the bidding if they have ever bidded.
- The successful bidder always has the proof to get the product.
- The seller can get the money from the successful bidder but not for the other bidder
- The sealed envelope must be delivered before the deadline; otherwise, the envelope is invalid.
- Before the deadline, the sealed envelope is private, and no one can open it.
- A fair solution is required if the same price is voted by two different bidders.

In an intelligent agreement, the contract is started if the time or event is triggered, such as sending a message, dealing with transactions, terminating the contract. The bytecode of smart contract retrieved with JSON format is used for broadcasting all the nodes of blockchain and wait for verifying. If true, the smart contract is announced with individual contract address and JSON Interface to allow the other person to join in. Before the deadline, all the legal bidders can send the sealed envelope to renew the price. All the sealed envelopes are opened when the time is due. The highest price on the sealed envelope is the final winner.

In the initialization data, we will announce the following information in advance.

- Auctioner: The tenderer address used to record the originating contract.
- AuctionStart: Used to announce the start time of the bid.
- biddingTime: Used to announce the effective time of the contract.
- highestBidder: The address of the bidder who currently bids the product with the highest price.
- highestBid: Used to record the current highest price

As for the contract, we define the following function:

- blindAuction(): Activate the contract by calling this function, and use the auctionStart and biddingEnd to record the start and end time.
- Bid(): This function can be called by any person to perform the bidding action. Before the function is executed, AuctionStart and biddingTime are used to judge whether the contract is expired. If not, the bidder can send the bid envelope if the price is greater than the current highest price. The contract system will use highestBid and highestBidder to record the current highest price and the corresponding bidder's address.
- reveal(): Opens the bid by calling this function, and compares the prices of all the tickets to get the final winner.
- AuctionEnd(): In this function, AuctionStart and biddingTime are automatically used to determine the contract validity time. If the effective time ends, the successful bidder's Address and the current highest price will be automatically sent to the tenderer. This function will be disabled to avoid repeated execution.
- withdraw(): Returns the amount of bids tendered by bidders other than the successful bidder.

4.3 Data Flow diagram of Blockchain Bidding System

4.3.1 Data Flow diagram of Seller

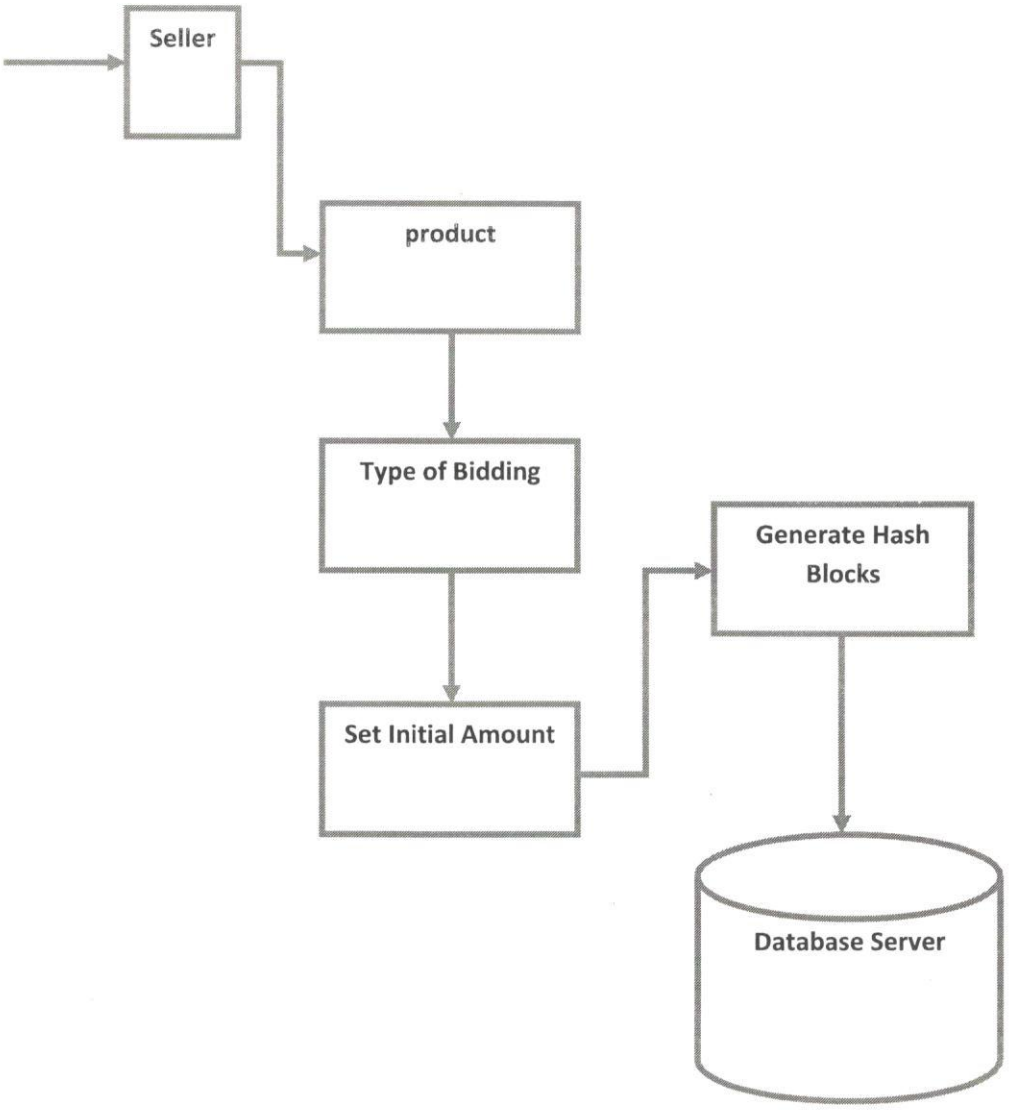

Fig 4.5: Data Flow diagram of Seller

As shown in above Fig 4.5 Data Flow diagram of Seller, it is the part of Dataflow diagram of Blockchain based bidding system, it consists of product details items and type of bidding which the seller wants to sell. Seller can also set the initial price of the items and which interns generates the hash blocks they are stored in the database server.

4.3.2 Data Flow diagram of Bidder

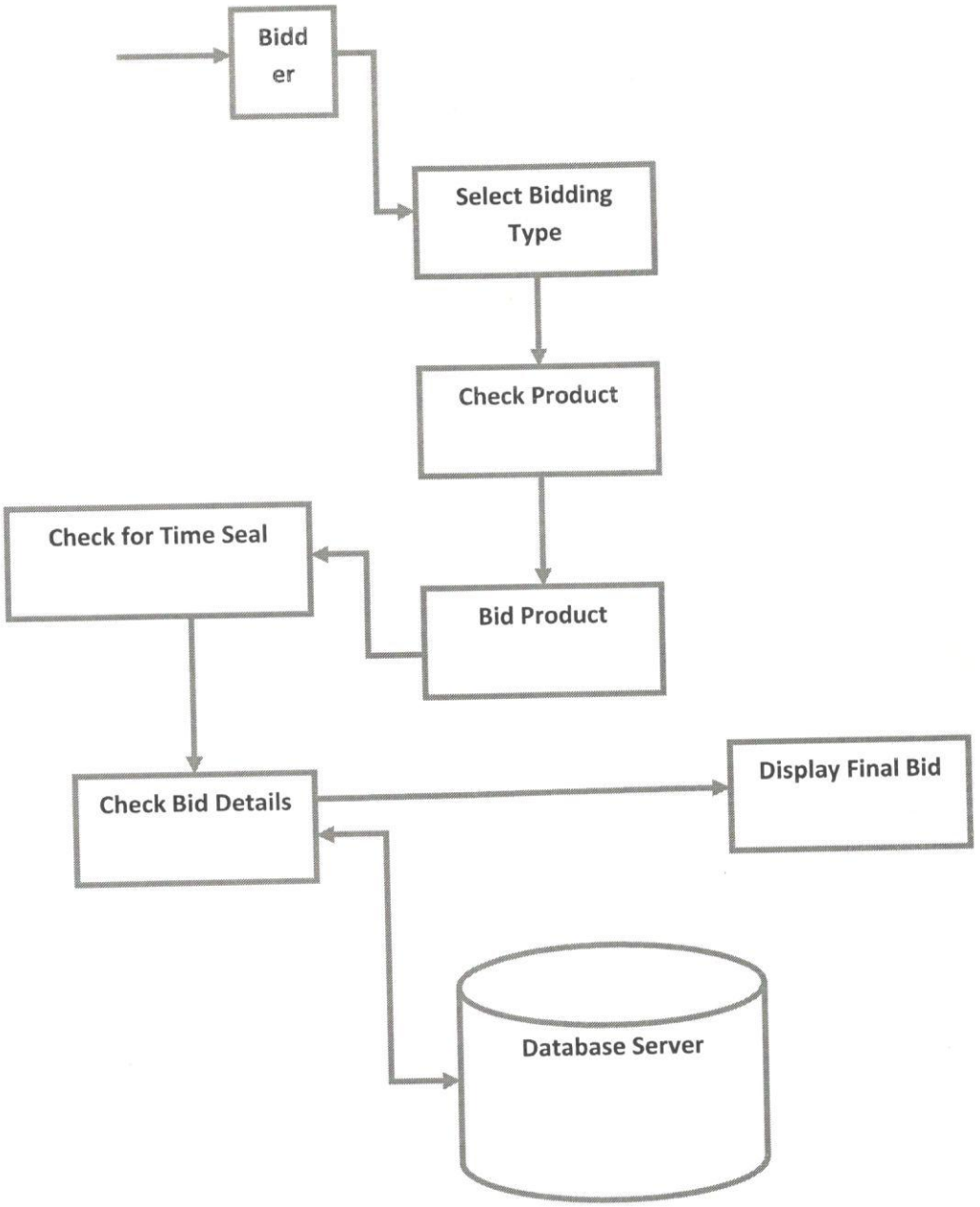

Fig 4.6: Data Flow diagram of Bidder

As shown in Fig 4.6 Data Flow diagram of Bidder, it consists of Bidder, type of bidding where bidder can select the type of bidding, he can bid the product and he can also check the sealed time. Bidder can check the bid details and these datas are stored in database.

4.3.3 Use Case diagram of Blockchain Bidding System

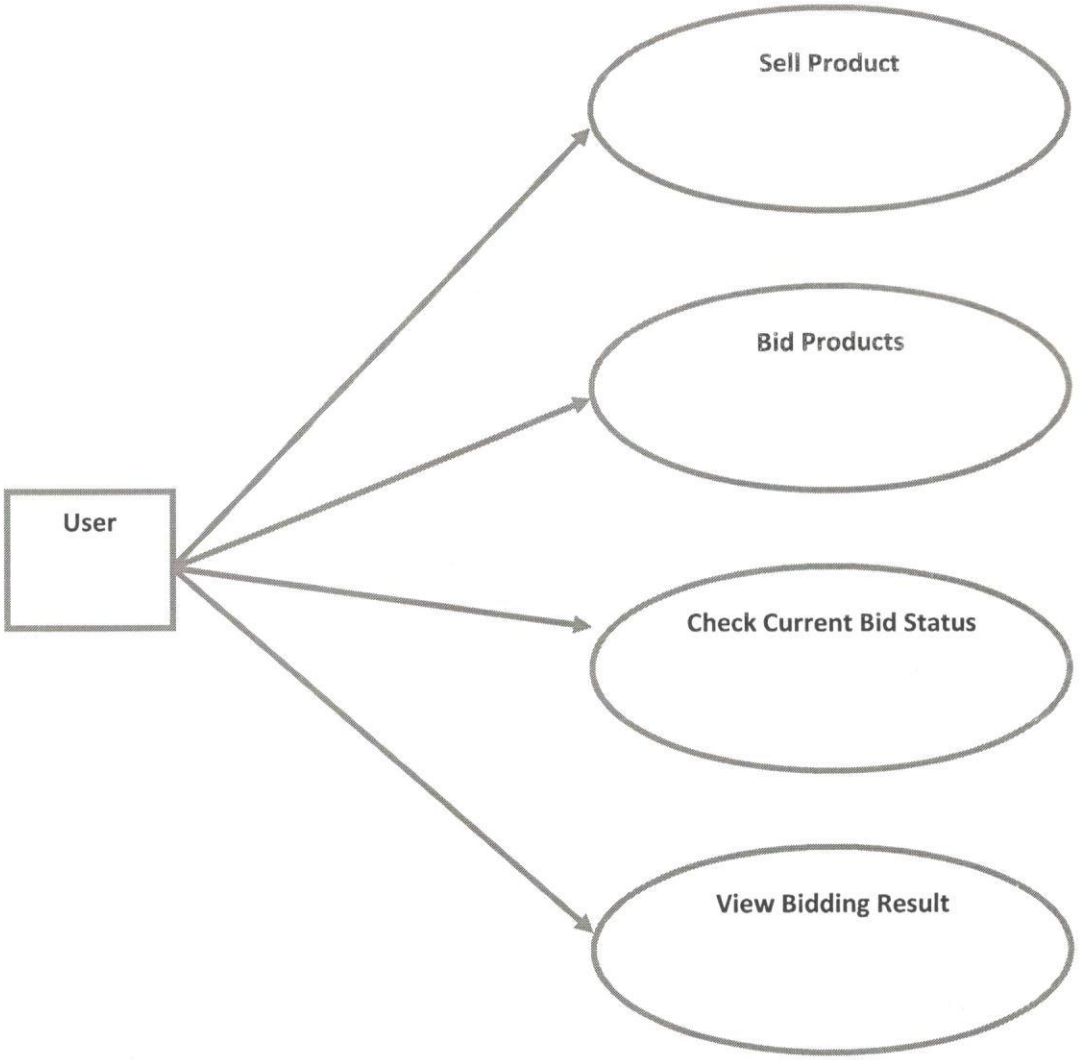

Fig 4.7: Use Case diagram of Blockchain Bidding System

As shown in above Fig 4.7 Use Case diagram of Blockchain Bidding System, here user may be the seller or bidder. User can sell the products by giving the description of items and bidding type. Bidder bid the product according to the type of bid and initial bid price, and also by checking the bid status. At the end time Bidder and seller view the results. Finally, seller sells the product to the bidder.

4.3.4 Sequence diagram of Blockchain Bidding System

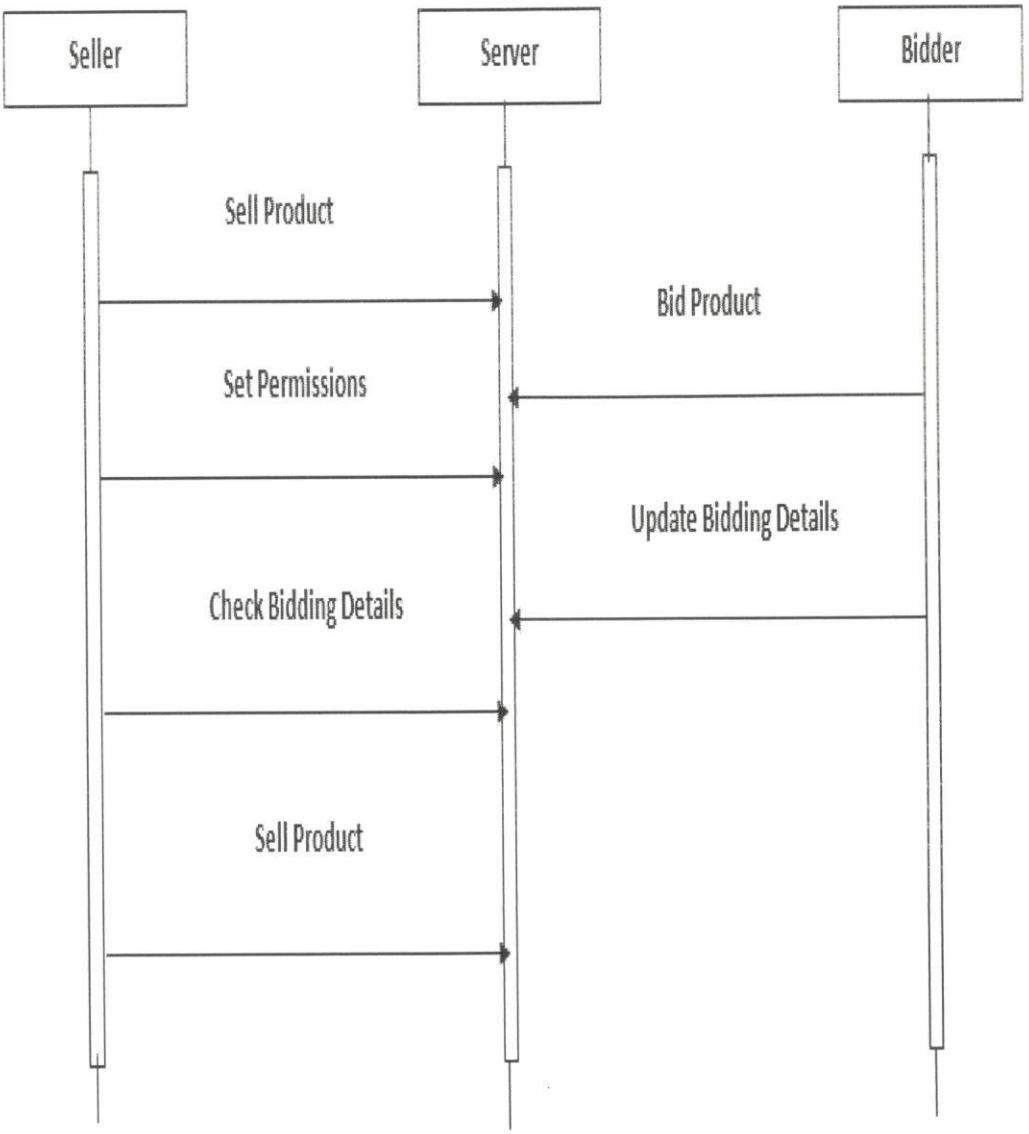

Fig 4.8: Sequence diagram of Blockchain Bidding System

As shown in above Fig 4.8 Sequence diagram of Blockchain Bidding System, If seller wants the products he approach the server. After successful uploading of product details, he set the type of bidding. Bidder bid the products and information are stored in server. Seller set the permission so that only once bidder can bid the products in sealed bid. But in Public bid, bidder can bid on the products several times by updating bidding details. Seller check the bidding details to check who is the winner in bidding. And seller sells product to bidder, all these data are maintained in the server.

Chapter 5

IMPLEMENTATION

5.1 Java Technology

Java technology is both a programming language and a platform. The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.

5.2 The Java Platform

A platform is the hardware or software environment in which a program runs. We've already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the

operating system and hardware. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other hardware-based platforms.

The Java platform has two components:

- The Java Virtual Machine (Java VM)
- TheJava Application Programming Interface (Java API)

You've already been introduced to the Java VM. It's the base for the Java platform and is ported onto various hardware-based platforms.

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as packages. The next section, What Can Java Technology Do? Highlights what functionality some of the packages in the Java API provide.

5.3 Project Modules

5.3.1 Module 1: Generate Blocks

```
package BlackChain;

import java.io.File;

import java.io.FileWriter;

import java.sql.Connection;

import java.sql.Statement;

import com.artgallery.model.dbc;

public class GenBlackChainData {

        public void genData(String productid,String name,String address,String
amount,String email,String contact,String path){

        try{

                String fname = productid+contact;

                String data =
productid+","+name+","+address+","+amount+","+email+","+contact;

                FileWriter fw = new FileWriter(path+"/Document/"+fname+".txt");
```

```
                fw.write(data);
                fw.flush();
                fw.close();
                new split();
                split.splitData(path+"/Document/",fname,path);
                String hash = new FileSHA1Code().genHash(path,fname);
                Connection con = new dbc().connect();
                Statement st = con.createStatement();
                st.executeUpdate("insert into blackdetails
values('"+productid+"','"+name+"','"+address+"','"+amount+"','"+email+"','"+contact+"','
"+fname+"','"+hash+"')");
        }
        catch(Exception e){
                e.printStackTrace();
        }
}
}
```

5.3.2 Module 2: Split Blocks

```
package BlackChain;
import java.io.*;
import java.util.Scanner;
public class split {
public static void splitData(String filepath,String fname,String mypath)
{
 try{
  // Reading file and getting no. of files to be generated
  String inputfile = filepath+fname+".txt"; //  Source File Name.
  double nol = 1.0; //  No. of lines to be split and saved in each output file.
```

```
File file = new File(inputfile);
Scanner scanner = new Scanner(file);
int count = 0;
while (scanner.hasNextLine())
{
 scanner.nextLine();
 count++;
}
System.out.println("Lines in the file: " + count);     // Displays no. of lines in the input file.
double temp = (count/nol);
int temp1=(int)temp;
int nof=0;
if(temp1==temp)
{
 nof=temp1;
}
else
{
 nof=temp1+1;
}
System.out.println("No. of files to be generated :"+nof); // Displays no. of files to be generated.
// Actual splitting of file into smaller files
FileInputStream fstream = new FileInputStream(inputfile); DataInputStream in = new DataInputStream(fstream);
BufferedReader br = new BufferedReader(new InputStreamReader(in)); String strLine;
for (int j=1;j<=nof;j++)
```

```
{
FileWriter fstream1 = new FileWriter(mypath+"/SplitFiles/"+fname+j+".txt");
BufferedWriter out = new BufferedWriter(fstream1);
for (int i=1;i<=nol;i++)
{
strLine = br.readLine();
if (strLine!= null)
{
out.write(strLine);
if(i!=nol)
{
out.newLine();
}
}
}
out.close();
}
in.close();
}catch (Exception e)
{
System.err.println("Error: " + e.getMessage());
}
}
}
```

5.3.3 Module 3:Merge file

```
package BlackChain;
import java.io.File;
```

```
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.util.ArrayList;
import java.util.List;
public class MergeFileExample {
        private static String FILE_NAME = "test123.txt";
        public static void main(String[] args) {
                File ofile = new File(FILE_NAME);
                FileOutputStream fos;
                FileInputStream fis;
                File f = new File("C:/New Folder/");
                String totalFiles[] =f.list();
                byte[] fileBytes;
                int bytesRead = 0;
                int j=1;
                List<File> list = new ArrayList<File>();
                for(int i=0;i<=totalFiles.length;i++){
                        if(j==6){
                                break;
                        }
                        else{
                                list.add(new File("C:/New Folder/File"+j+".txt"));
                                j++;
                        }
                }
                try {
                   fos = new FileOutputStream(ofile,true);
                   for (File file : list) {
                      fis = new FileInputStream(file);
                      fileBytes = new byte[(int) file.length()];
                      bytesRead = fis.read(fileBytes, 0,(int)  file.length());
                      assert(bytesRead == fileBytes.length);
                      assert(bytesRead == (int) file.length());
                      fos.write(fileBytes);
```

```
                    fos.flush();
                    fileBytes = null;
                    fis.close();
                    fis = null;
                }
                fos.close();
                fos = null;
            }catch (Exception exception){
                    exception.printStackTrace();
            }
        }
}
```

5.3.4 Module 4:Bidding History

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
  pageEncoding="ISO-8859-1"%>
  <%@page import="java.sql.*" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Online Bidding</title>
  <link rel="stylesheet" href="css/bootstrap.min.css">
      <script src="js/jquery.min.js"></script>
      <script src="js/bootstrap.min.js"></script>
</head>
<body Style="background-color:">
      <nav class="navbar navbar-inverse" style="background-color:#1C2833;">
 <div class="container-fluid">
  <div class="navbar-header">
```

```
    <button type="button" class="navbar-toggle" data-toggle="collapse" data-
target="#myNavbar">
      <span class="icon-bar"></span>
      <span class="icon-bar"></span>
      <span class="icon-bar"></span>
    </button>
    <a class="navbar-brand" href="#"style="margin-left:20px;">Online Bidding</a>
   </div>
   <div class="collapse navbar-collapse" id="myNavbar">
    <ul class="nav navbar-nav" style="margin-left:288px;">
      <li class="active"><a href="bidderacc.jsp">Create Account</a></li>
      <li><a href="viewbidderacc.jsp">Account Detail</a></li>
      <li><a href="bidtype.jsp">Bid Product</a></li>
     <li><a href="biddinghistry.jsp">Bidding History</a></li>
    </ul>
    <ul class="nav navbar-nav navbar-right">
     <li><a href="index.jsp"><span class="glyphicon glyphicon-log-out"></span>
LOGOUT</a></li>
    </ul>
   </div>
  </div>
</nav>
<%
String urs = (String)session.getAttribute("user");
%>
<h5 style="color:blue;font-weight:bold;margin-left:200px">Welcome <span
style="color:brown"><%=urs %></span></h5>
<center>
```

```
<div class="container">
<center><h3 style="color:red;font-weight:bold">Bidding Details</h3></center>
<table class="table table-bordered table-hover" style="width:80%";>
<thead style="color: #ff6666;">
<tr style="font-weight:bolder">
<th>product id</th>
<th>Name</th>
<th>Address</th>
<th>Amount</th>
<th>seller mail</th>
</tr>
</thead>
<tbody>
<%
String email=(String)session.getAttribute("user1");
String type=request.getParameter("id");
try{
        Class.forName("com.mysql.jdbc.Driver");
        Connection
con=DriverManager.getConnection("jdbc:mysql://localhost/bidding","root","root");
        Statement st=con.createStatement();
        ResultSet rs=st.executeQuery("select*from bidderamount where
email='"+email+"' and type='"+type+"'");
        while(rs.next()){
                Class.forName("com.mysql.jdbc.Driver");
                Connection
con1=DriverManager.getConnection("jdbc:mysql://localhost/bidding","root","root");
                Statement st1=con.createStatement();
```

```
                ResultSet rs1=st1.executeQuery("select*from signup where
emailid='"+rs.getString(8)+"'");
                rs1.next();
                String name = rs1.getString(1);
                String adds = rs1.getString(5);
                %>
                <tr style="font-weight:bolder">
                <td ><%=rs.getString(1) %></td>
                <td><%=name %></td>
                <td><%=adds %></td>
                <td><%=rs.getString(4) %></td>
                <td><%=rs.getString(8) %></td>
                </tr>
                <%
        }
}
catch(Exception e){
        e.printStackTrace();
}
%>
</tbody>
</table>
</div>
</center>
</body>
</html>
```

CHAPTER 6

SOFTWARE TESTING

In software development life cycle, software testing is one of the significant phases. In software testing phase, verification and validation of the project under development are performed with respect to requirements mentioned. In this project, Unit testing of main modules, Integration testing of different modules and complete System testing functionality along with the GUI testing is performed.

6.1 Test Environment

This project was tested on the following platforms

Software Platform :

Software used for testing is given below

Operating System	:	Windows XP or Windows 7
Tool / IDE	:	Eclipse Juno 4.2 with Tomcat Server
Visual Interface	:	Java Server Pages, Servlets
Database	:	MySQL 5.0

Hardware Platform :

Processor	:	Intel Pentium 4 or more
Memory	:	1GB RAM or more
Harddisk	:	40GB or more with 5400 rpm

6.2 Unit Testing of Main modules

The whole application is made up of different modules. Unit testing focuses on each sub module, independent of one another, to locate errors. This enables the programmer to detect errors. Individual modules or functions are tested under Unit testing. This method of testing is also called as White Box Testing. Independently, different modules are tested here and their functionality is checked. Each of these modules of Unit testing is explained below.

Sl No of Test Case	UTC-1
Name of Test Case	Test case to verify Registration Page
Feature being Tested	Registration details
Description	User should provide details like Name, Email Id, Mobile Number
Sample Input	Email Id, Mobile Number, Username Password
Expected Output	Registration Successful message should be displayed
Actual Output	As expected
Remarks	Passed

Table 6.1 Unit Test Case 1 for Registration Page

The Table 6.1 shows Unit Test Case 1(UTC-1) to verify whether user interface accepts registration details of sender and receiver. During the registration phase accept the information like email id, phone number and password. If it is a valid registered user it will display message.

Sl No of Test Case	UTC-2
Name of Test Case	Test Message Post
Feature being Tested	Messages have been posted
Description	Store in database
Sample Input	Text
Expected Output	Message posted
Actual Output	Device is ready to use
Remarks	Passed

Table 6.2 Unit Test Case 2 for Message Post

The Table 6.2 shows Unit Test Case 2(UTC-2). Here we are testing that message have been posted or not. Here we are sending text message and it will store in a

database. The expected output is message posted or not. If it is valid the device is ready to use

6.3 Integration Testing

Two or more modules are combined together to check for Integration testing. Integration Testing purpose is to check whether the integrated modules are performing as expected.

Integrated testing is to test the system, when all the modules and its sub modules are integrated. This testing is done to ensure that all the modules, work correctly when independent, without any discrepancies when integrated. System testing ensures that the related modules work together to achieve the main objective of the application. The project was tested with all its modules integrated and ensured that there were no errors. Samples of data were keyed into the application. It has been seen the application is working perfectly, to the satisfactory of the user.

6.4 System testing

System testing can be defined in many ways, but a simple definition is that the validation succeeds when the system function in a manner that reasonably expected by the user. Validation testing provides the final assurance that the system meets all the functional, behavioural and performance requirements.

The project was tested with all its modules and ensured that there were no errors. It has been seen that the system is working perfectly, to the satisfaction of the user meeting all the requirement of user. System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

CHAPTER 7

RESULTS

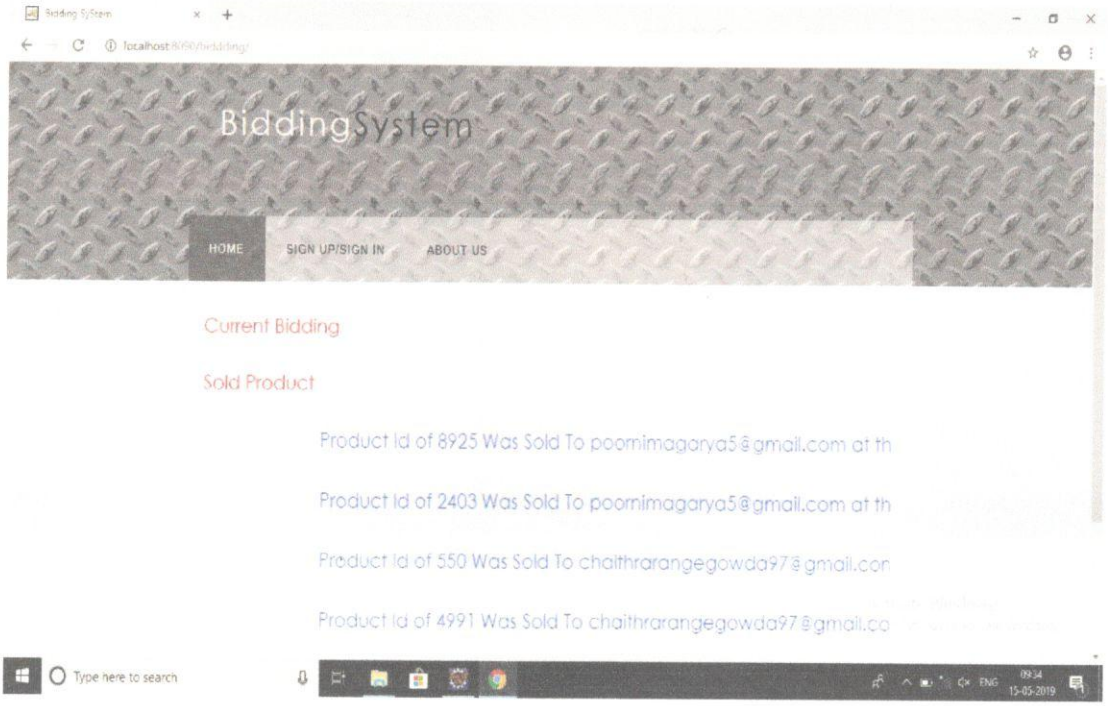

Fig 7.1: Home Page

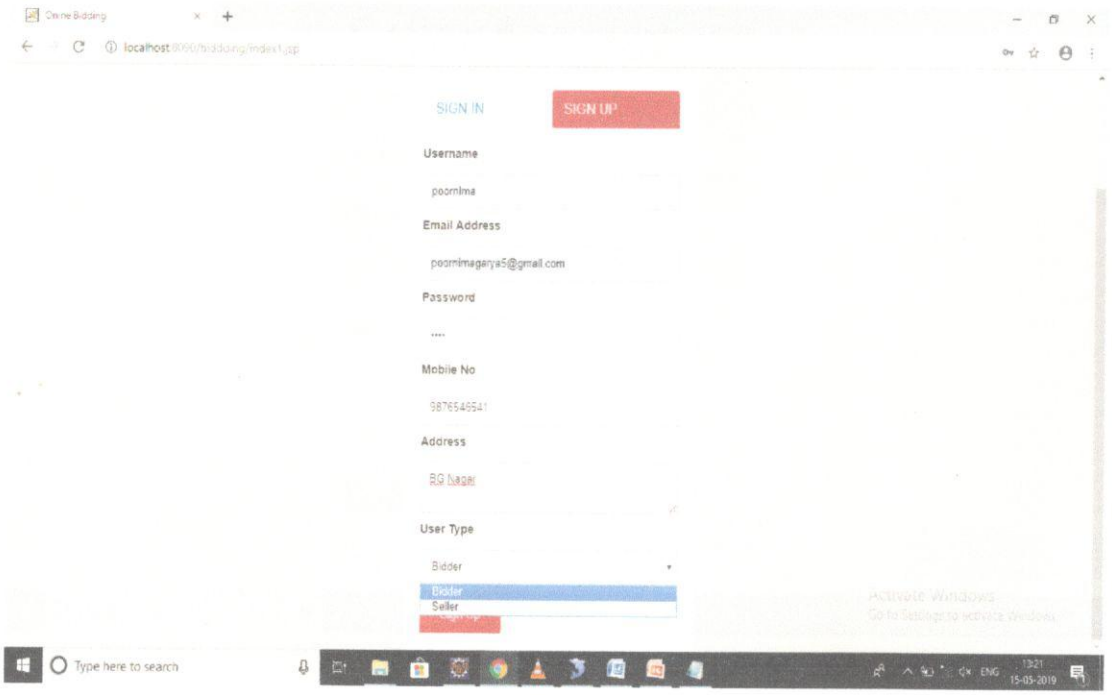

Fig 7.2: Sign up page

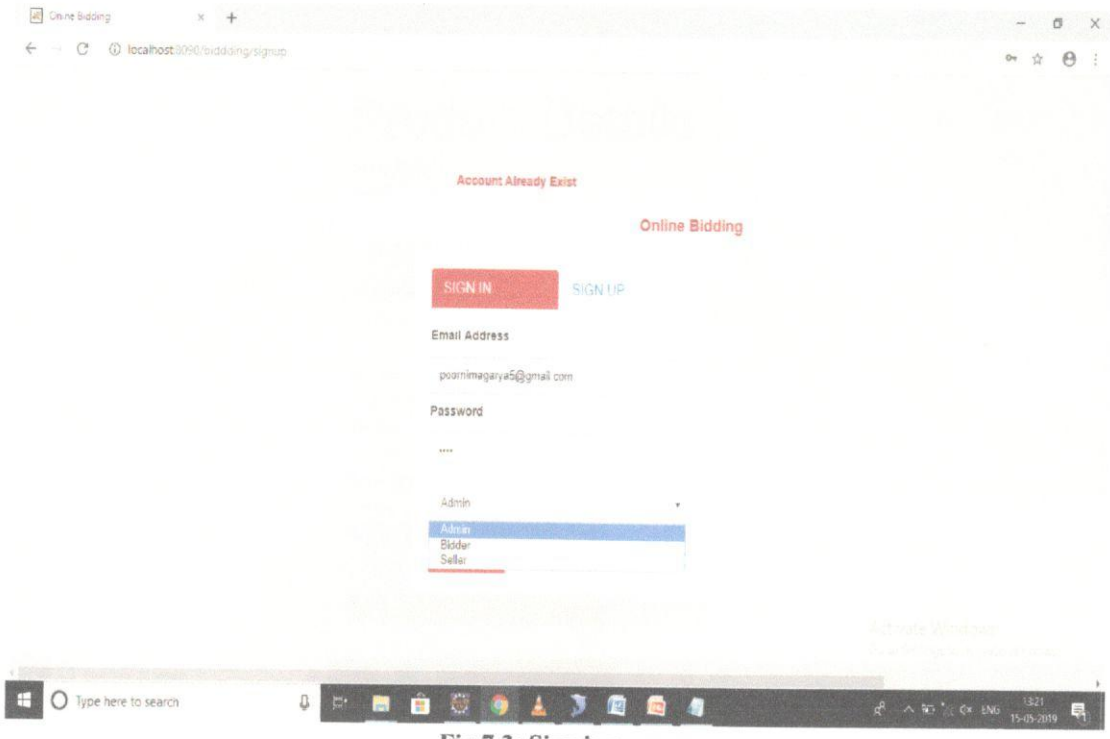

Fig 7.3: Sign in page

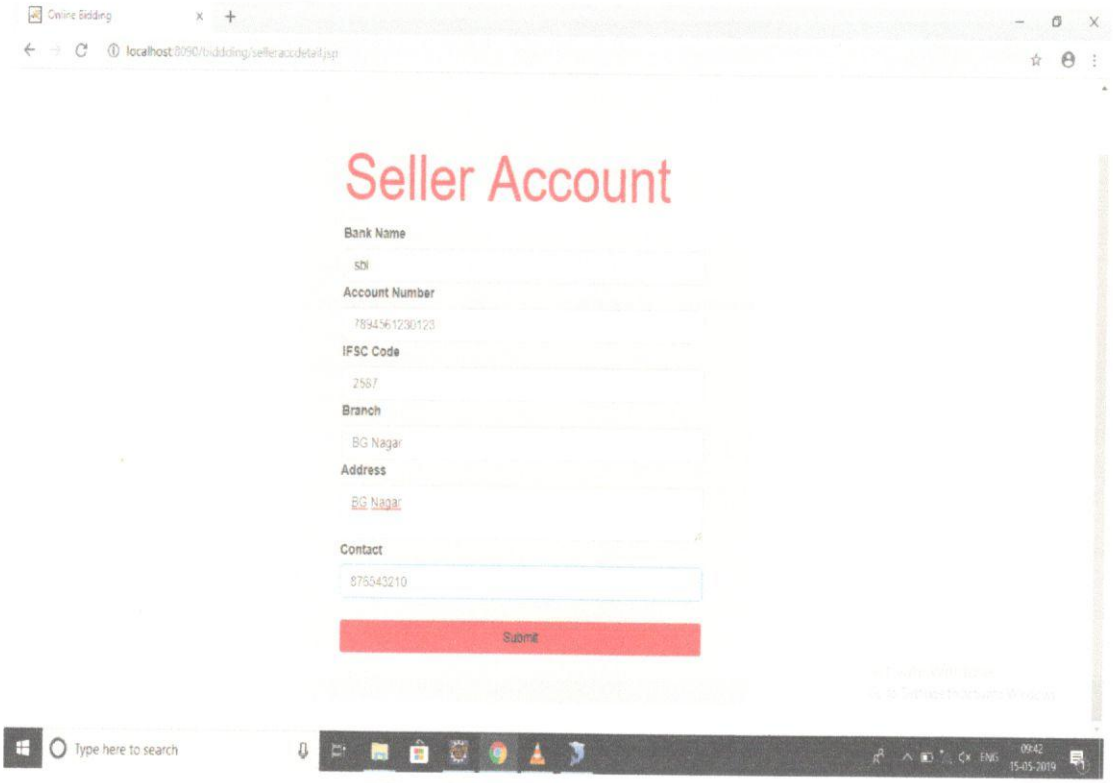

Fig 7.4: Creating seller account

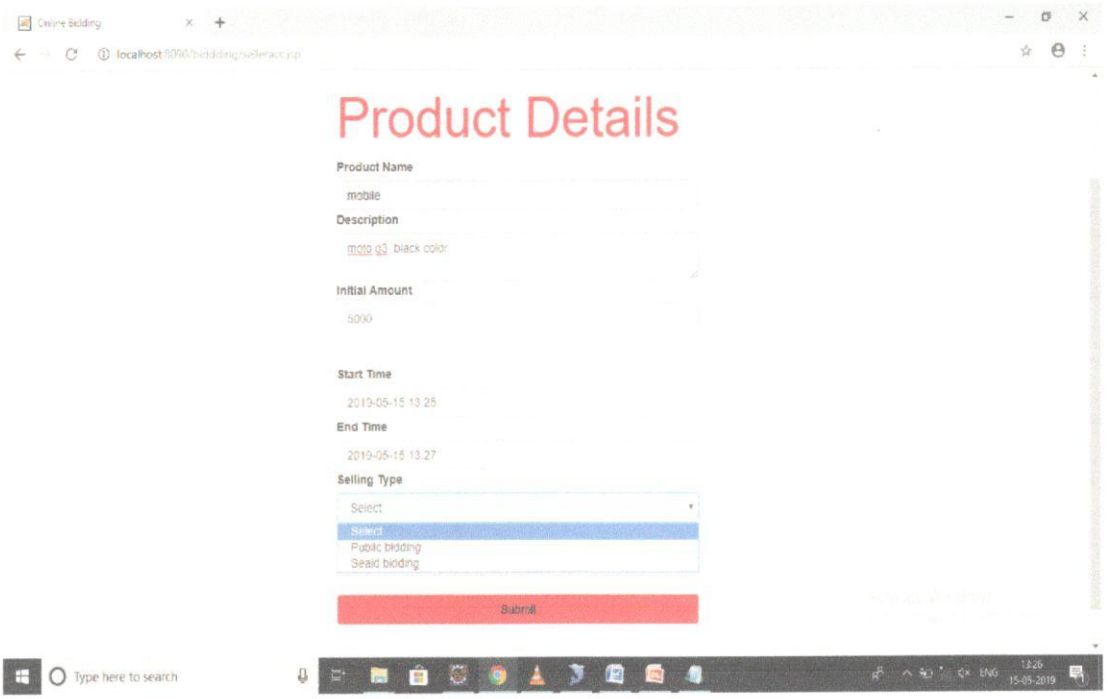

Fig 7.5: Product details

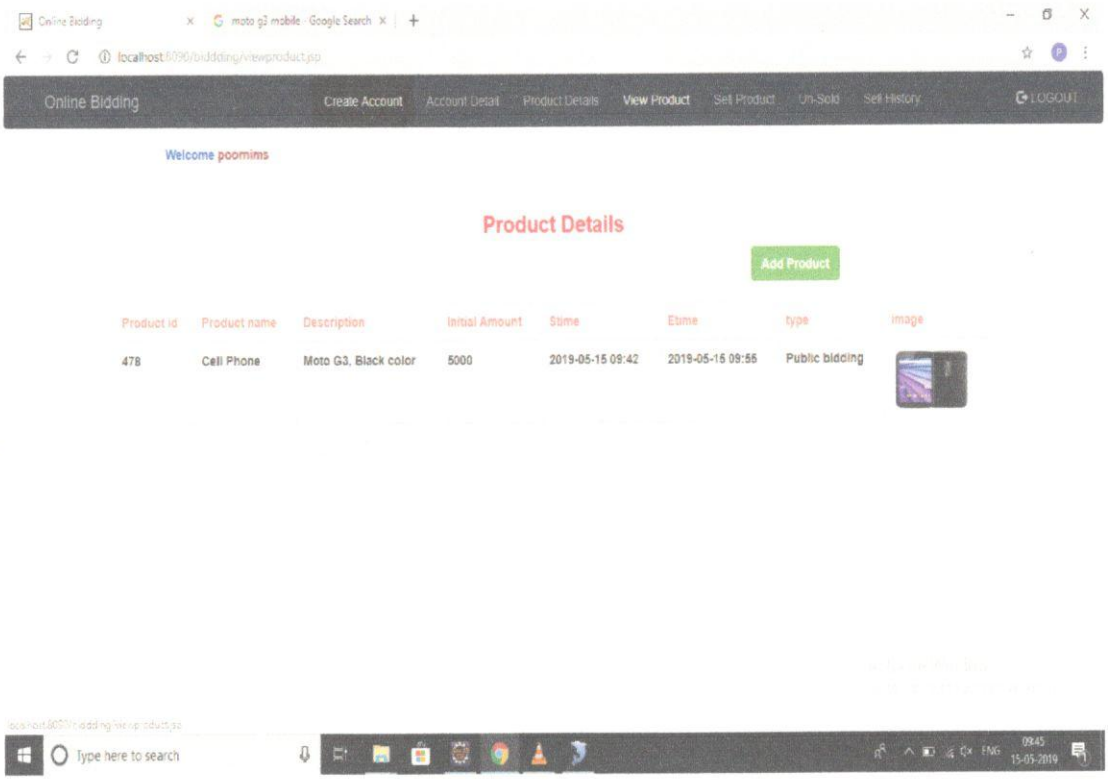

Fig 7.6: Viewing product details

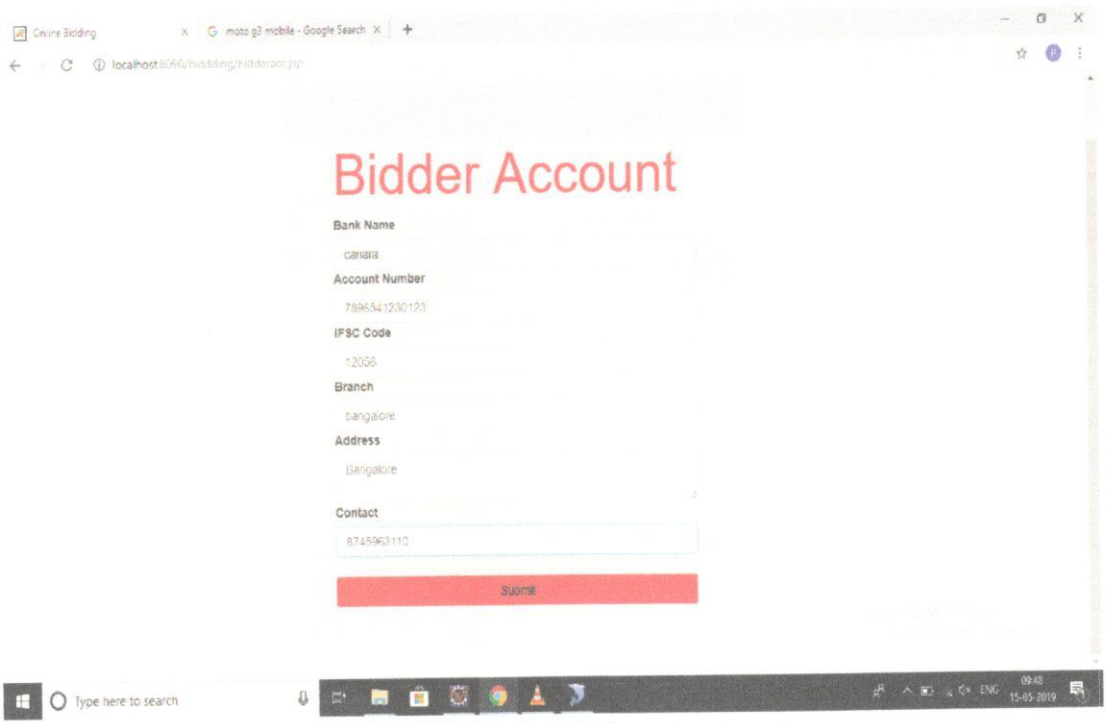

Fig 7.7: Creating bidder account

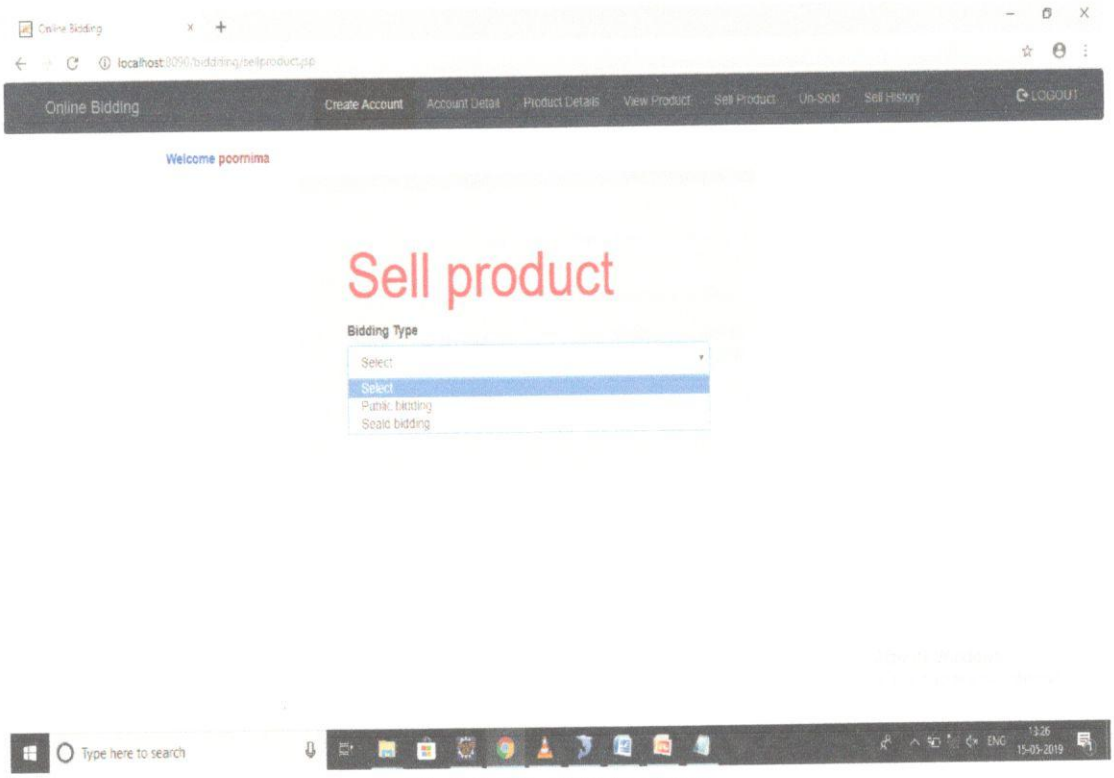

Fig 7.8: Select bidding type

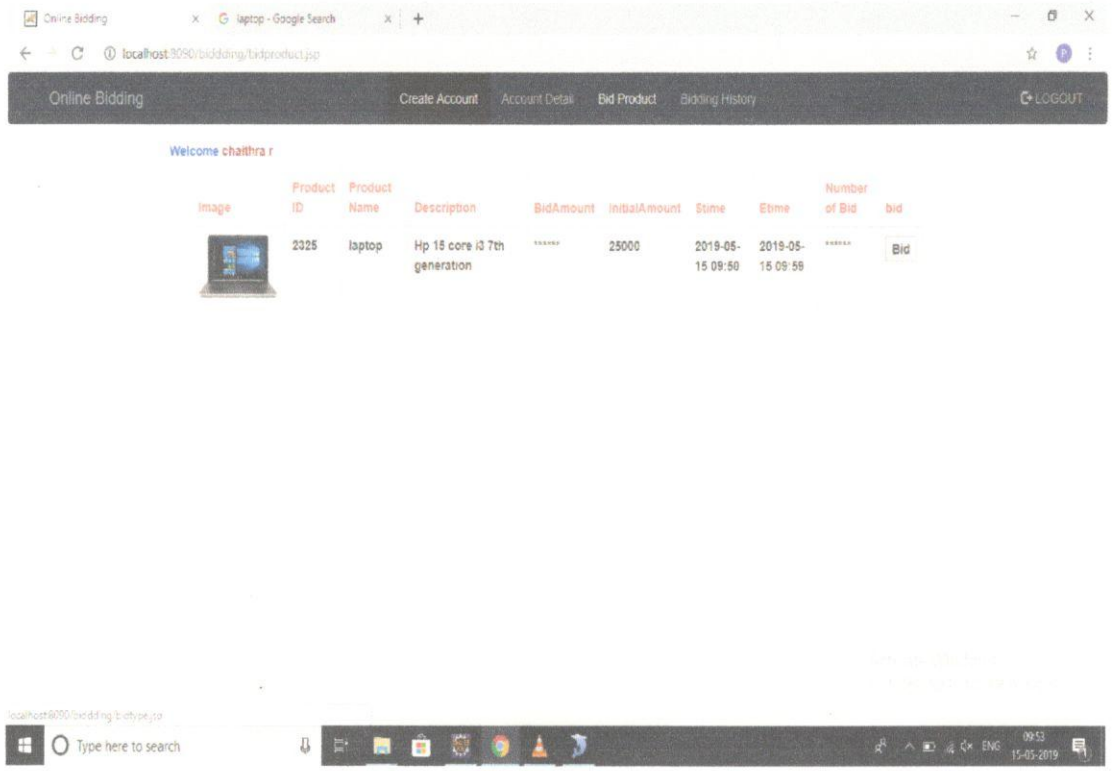

Fig 7.9: Sealed bidding

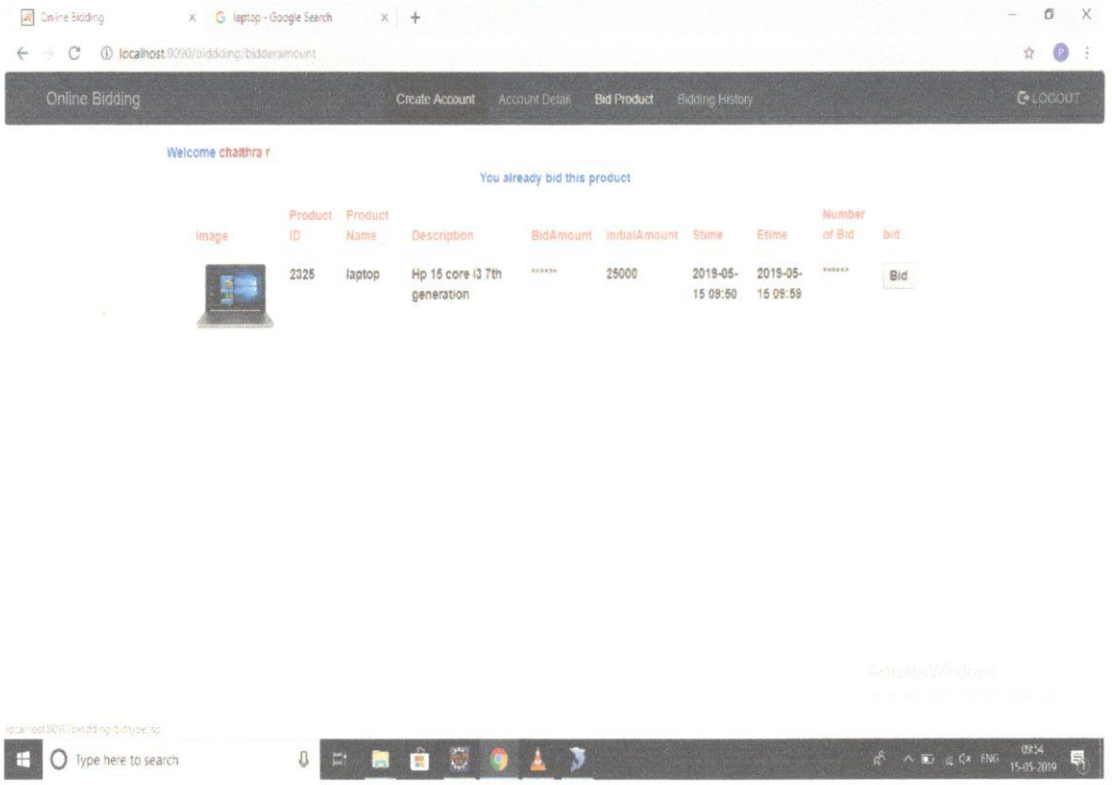

Fig 7.10: One time bidding in sealed bid

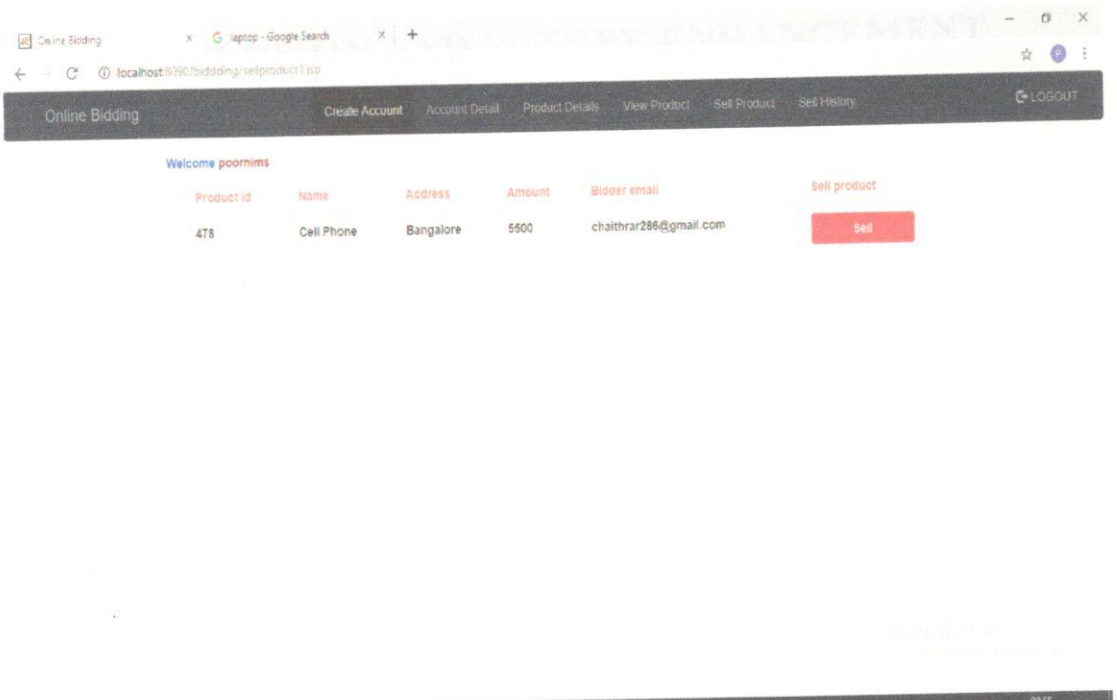

Fig 7.11: After bidding time over

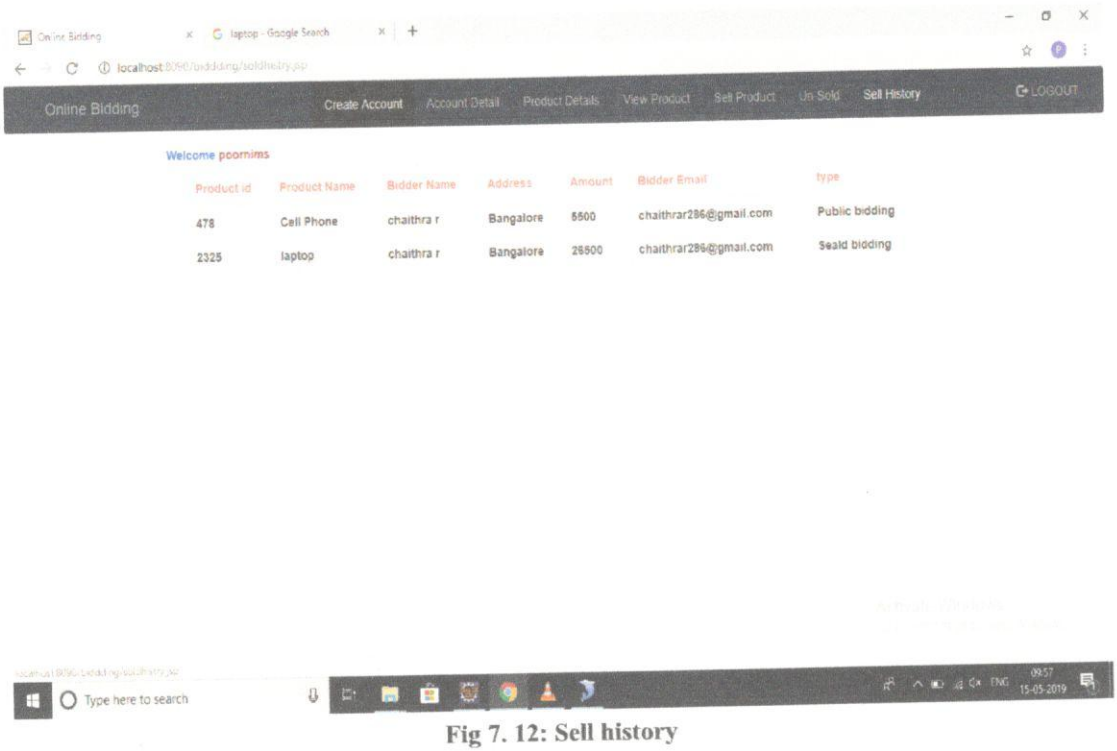

Fig 7. 12: Sell history

CONCLUSION AND FUTURE ENHANCEMENT

This project provides an E-auction mechanism based on blockchain to ensure electronic seals confidentiality, non-repudiation, and unchangeability. We expect to encounter potential problems in the implementation of this work.

The future plan of this project is to improve design, implementation and documentation in such a way that anyone can use this project for better perform. In future we will add the following module for better improvement of the project.

- Online account verification
- More user friendly system.

REFERENCES

[1] Gang Cao and Jie Chen. Practical electronic auction schemebased on untrusted third-party. In Computational andInformation Sciences (ICCIS), 2013 Fifth InternationalConference on, pages 493–496. IEEE, 2013.

[2] Ilichetty S Chandrashekar, Y Narahari, Charles H Rosa, DevadattaM Kulkarni, Jeffrey D Tew, and Pankaj Dayama. Auction-basedmechanisms for electronic procurement. IEEE Transactions onAutomation Science and Engineering, 4(3):297–321, 2007.

[3] Wen Chen and Feiyu Lei. A simple efficient electronic auctionscheme. In Parallel and Distributed Computing, Applicationsand Technologies, 2007. PDCAT'07. Eighth InternationalConference on, pages 173–174. IEEE, 2007.

[4] Christopher K Frantz and Mariusz Nowostawski. Frominstitutions to code: Towards automated generation of smartcontracts. 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 inreducer phase??block chain algorithm. In Circuit, Power andComputing Technologies (ICCPCT), 2016 InternationalConference on, pages 1–4. IEEE, 2016.

[7]JunichiKishigami, Shigeru Fujimura, Hiroki Watanabe, AtsushiNakadaira, and Akihiko Akutsu. The blockchain-based digitalcontent distribution system. In Big Data and Cloud Computing(BDCloud), 2015 IEEE Fifth International Conference on, pages187–190. IEEE, 2015.

[8]Wenbo Shi, Injoo Jang, and Hyeong SeonYoo. A sealed-bidelectronic marketplace bidding auction protocol by using ringsignature. In Computer Sciences and Convergence InformationTechnology, 2009. ICCIT'09. Fourth International Conferenceon, pages 1005–1009. IEEE, 2009.

[9] Wee-Kheng Tan and Yung-Lun Chung. User payment choicebehavior in e-auction transactions. In e-Education, e-Business,e-Management, and e-Learning, 2010. IC4E'10. InternationalConference on, pages 183–187. IEEE, 2010.

[10] Hu Xiong, Zhiguang Qin, Fengli Zhang, Yong Yang, and YangZhao. A sealed-bid electronic auction protocol based on ringsignature. 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 insupport of bid evaluation in multi-attribute e-auction forprocurement. In Wireless Communications, Networking andMobile Computing, 2008. WiCOM'08. 4th InternationalConference on, pages 1–4. IEEE, 2008.

[12] Affan Yasin and Lin Liu. An online identity and smart contractmanagement system. In Computer Software and ApplicationsConference (COMPSAC), 2016 IEEE 40th Annual, volume 2,pages 192–198. IEEE, 2016.

[13] Fangguo Zhang, Qiongfang Li, and Yumin Wang. A new secureelectronic auction scheme. In EUROCOMM 2000. InformationSystems 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 confirmationin bitcoin blockchain. In Computer Software and ApplicationsConference (COMPSAC), 2016 IEEE 40th Annual, volume 1,pages 443–448. IEEE, 2016.

[15] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Usingblockchain to protect personal data. In Security and PrivacyWorkshops (SPW), 2015 IEEE, pages 180–184. IEEE, 2015.

BAHUBALI COLLEGE OF ENGINEERING

Gommatanagara, Shravanabelagola 573 135, Hassan District, Karnataka

ISTE Students Chapter

FIESTA'19

Come, drive into the fest with us

A NATIONAL LEVEL CONFERENCE & TECHNICAL FEST FOR UG STUDENTS ON 25th & 26th APRIL 2019

Certificate of Participation

This is to certify that ~~Mr.~~ / Ms. CHAITHRA . H

of BGSIT B.G NAGAR has actively participated in the below mentioned events of FIESTA'19 held on 25th & 26th April 2019.

- ✓ Paper Presentation entitled Blockchain Based Smart Contract for bidding System

COLLAGE | PASSWORD HUNT | POSTER PRESENTATION | CODETHAN | CAD MODELING | CIRCUITRIX | QUICK SURVEY | PHOTOGRAPHY | ROBOTICS | GAMING

Prof. Baban P. Dathwade
Co-convener

Prof. Manjunath N.
Convener

Dr. Gomatesh M. Ravanavar
Principal

S.S.D.J.J.P. Sangha's (Regd.)

BAHUBALI COLLEGE OF ENGINEERING

Gommatanagara, Shravanabelagola 573 135, Hassan District, Karnataka

ISTE Students Chapter

FIESTA'19

Come, drive into the fest with us

A NATIONAL LEVEL CONFERENCE & TECHNICAL FEST FOR UG STUDENTS
ON 25th & 26th APRIL 2019

Certificate of Participation

This is to certify that ~~Mr.~~ / Ms. CHAITHRA . R

of BGSIT B.G NAGAR *has actively participated in the below mentioned events of* **FIESTA'19** *held on 25th & 26th April 2019.*

☑ *Paper Presentation entitled* Blockchain Based Smart Contract for Bidding System

COLLAGE | PASSWORD HUNT | POSTER PRESENTATION | CODETHAN | CAD MODELING | CIRCUITRIX | QUICK SURVEY | PHOTOGRAPHY | ROBOTICS | GAMING

Prof. Baban P. Dathwade

Prof. Manjunath N.

Dr. Gomatesh M. Ravanavar

S.S.D.J.J.P. Sangha's (Regd.)

BAHUBALI COLLEGE OF ENGINEERING

Gommatanagara, Shravanabelagola 573 135, Hassan District, Karnataka

ISTE Students Chapter

FIESTA'19

Come, drive into the fest with us

A NATIONAL LEVEL CONFERENCE & TECHNICAL FEST FOR UG STUDENTS
ON 25th & 26th APRIL 2019

Certificate of Participation

This is to certify that ~~Mr.~~ / Ms. POORNIMA . G

of BGSIT B.G NAGAR *has actively participated in the below mentioned events of* **FIESTA'19** *held on 25th & 26th April 2019.*

☑ *Paper Presentation entitled* Blockchain Based Smart Contract for bidding System

COLLAGE | PASSWORD HUNT | POSTER PRESENTATION | CODETHAN | CAD MODELING | CIRCUITRIX | QUICK SURVEY | PHOTOGRAPHY | ROBOTICS | GAMING

Prof. Baban P. Dathwade

Prof. Manjunath N.

Dr. Gomatesh M. Ravanavar

S.S.D.J.J.P. Sangha's (Regd.)

BAHUBALI COLLEGE OF ENGINEERING

Gommatanagara, Shravanabelagola 573 135, Hassan District, Karnataka

ISTE Students Chapter

FIESTA'19

Come, drive into the fest with us

A NATIONAL LEVEL CONFERENCE & TECHNICAL FEST FOR UG STUDENTS ON 25th & 26th APRIL 2019

Certificate of Participation

This is to certify that ~~Mr.~~ / Ms. PRABHAVATHI .S

of BGSIT B.G NAGAR *has actively participated in the below mentioned events of* **FIESTA'19** *held on 25th & 26th April 2019.*

✓ *Paper Presentation entitled* Blockchain Based smart contract for bidding System

COLLAGE | PASSWORD HUNT | POSTER PRESENTATION | CODETHAN | CAD MODELING | CIRCUITRIX | QUICK SURVEY | PHOTOGRAPHY | ROBOTICS | GAMING

Prof. Baban P. Dathwade

Prof. Manjunath N.

Dr. Gomatesh M. Ravanavar