IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

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

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

Agriculture Supply Chain Management Using Blockchain Technology

Saykar Punam Mahadev, Unde Vaishnavi Babasaheb, Jawale Dipali Rajendra, Takle Khushboo Rajesh, Prof.Avhad P.S

Department of Computer Engineering, Shri Chhatrapati Shivaji Maharaj College of Engineering, Nepti, Ahmednagar, India

ABSTRACT: Block chains are now firmly established as a digital technology that combines cryptographic, data management, networking, and incentive mechanisms to support the verification, execution, and recording of transactions between parties. While block chain technologies were originally intended to support new forms of digital currency for easier and secure payments, they now hold great promise as a new foundation for all forms of transactions. Agribusiness stands to become a key beneficiary of this technology as a platform to execute 'smart contracts' for transactions, particularly for high-value produce.

First it is important to distinguish between private digital currencies and the distributed ledger and block chain technologies that underlie them. The distributed and cross-border nature of digital currencies like Bit coin means that regulation of the core protocols of these systems by central banks is unlikely to be effective. Monetary authorities are focused more on understanding 'on-ramps' and 'off-ramps' that constitute the links to the traditional payment's system rather than being able to monitor and regulate the currency itself. In contrast to the digital currency feature of block chain, the distributed ledger feature has the potential for widespread use in agribusiness and trade financing, especially where workflows involve many different parties with no trusted central entity.

I. OVERVIEW

An increasing demand in society for greater information about food reflects the need for more transparency and the lack of trust. At the same time, more and more food products and beverages are branded and accompanied by a variety of certification schemes, with an increasing risk of fraud (selling unqualified product with high- quality labels or claims) and adulteration. In the current situation, much of the com- pliance data and information is audited by trusted third parties and stored either on paper or in a centralized database and these approaches are known to suffer from many informational problems such as the high cost and inefficiency of paper-based processes and fraud, corruption and error both on paper and in IT systems. These information problems, indicating that current transparency and trust systems have not been able to solve or at times even have exacerbated the problems of low trans- parency and trust in agrifood chains, pose a severe threat to food safety, food quality, and sustainability. In particular, food integrity has become a major concern. Food integrity refers to the fairness and authenticity of food in food value chains both at the physical layer and the digital layer, where the digital layer should provide reliable and trustworthy information on the origin and provenance of food products in the physical layer. Blockchain technology provides a means to ensure permanence of records and potentially to facilitate the sharing of data between disparate actors in a food value chain. This potential may lead to an exciting paradigm shift facilitating transparency and trust in food chains that ensures food integrity.

II. MOTIVATION

The last three years have seen an explosion of interest in Blockchain Technology (BCT) with a great many companies and research institutions focusing on potential applications of this technology across a range of financial, industrial and social sectors. However, the technology has also been surrounded by a great deal of exag- geration and hype resulting in misplaced expectations and misunderstandings. BCT is still in an early stage of development, with considerable potential for real-life com- mercial applications. Innovation in blockchain architectures, applications and busi- ness concepts is happening at a fast pace; it is often characterized by decentralized, open-source development, and it is perceived as being disruptive to traditional play- ers in many industries.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

III. PROBLEM DEFINITION AND OBJECTIVES

Objectives:

1. To implement a java-based web application.
2. To implement AES.
3. To implement visual cryptography.
4. To implement block chain.
5. To implement distributed database system using WLAN.

PROJECT SCOPE AND LIMITATIONS

Project will be developed as a prototype model using JSP and servlet technology. It will run as a local host. System will be communicate through wireless local area network. System communication will be limited in the wireless local area network, but in future if we will host the project using WAN , it can communicate worldwide.

IV. METHODOLOGIES OF PROBLEM SOLVING

BCT Agricultural products are the foundation of the people's survival, and the qual- ity of agricultural products has always been the focus of attention of society and the government; the original agricultural product traceability system is too difficult to tamper with data due to the excessive concentration of data storage, it faces the challenge of fraudulent data tracing, and it is difficult for consumers to trust such traceability results. Moreover, the centralized storage method is not conducive to the centralized management of traceable data from many enterprises, and there will be problems of low traceability and difficulty in government supervision. The emergence of blockchain technology provides a new solution for data security problems of food traceability, its decentralization, anti-tampering and other characteristics and data encryption technology improve the difficulty of data fraud and ensure data security. If the blockchain is combined with the traceability of agricultural products, the safety of traceable data and the tampering of data can be guaranteed to the greatest extent, the producer's production behavior can be regulated, and consumers' confidence in food quality can be improved. This project mainly proposes a framework of agricultural product traceability system based on blockchain technology, it uses blockchain to store the traceability data of agricultural products safely, and proposes a traceability model of agricultural products, which can cover the entire industrial chain of agricultural products, and consumers can query the authentic source of traceability of agricultural products

SYSTEM ARCHITECTURE

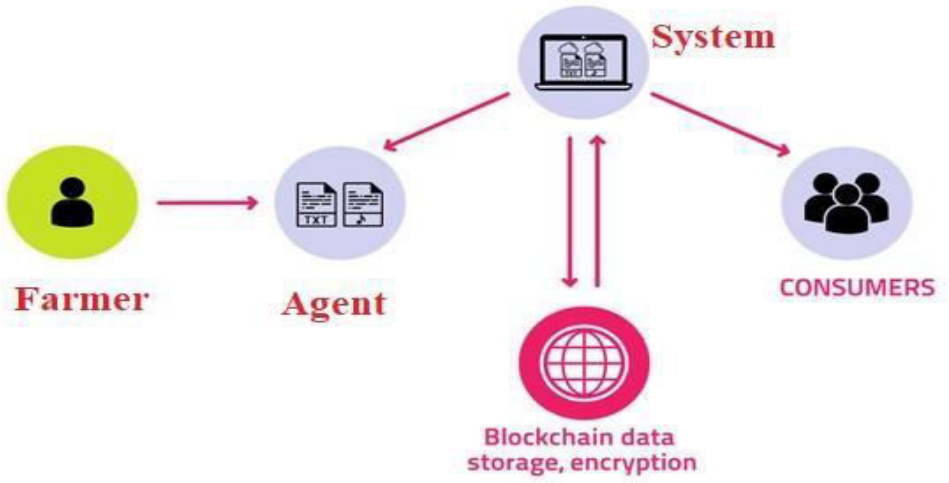

Figure 1: System Architecture

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

Whenever any transaction will occur in the system , the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the block's hash must be changed . Such multiple copies are maintained at different servers , which will assure the data security and confidentiality. As everything is

through application interface, it will maintain the transparency in the agricultural supply chain management.

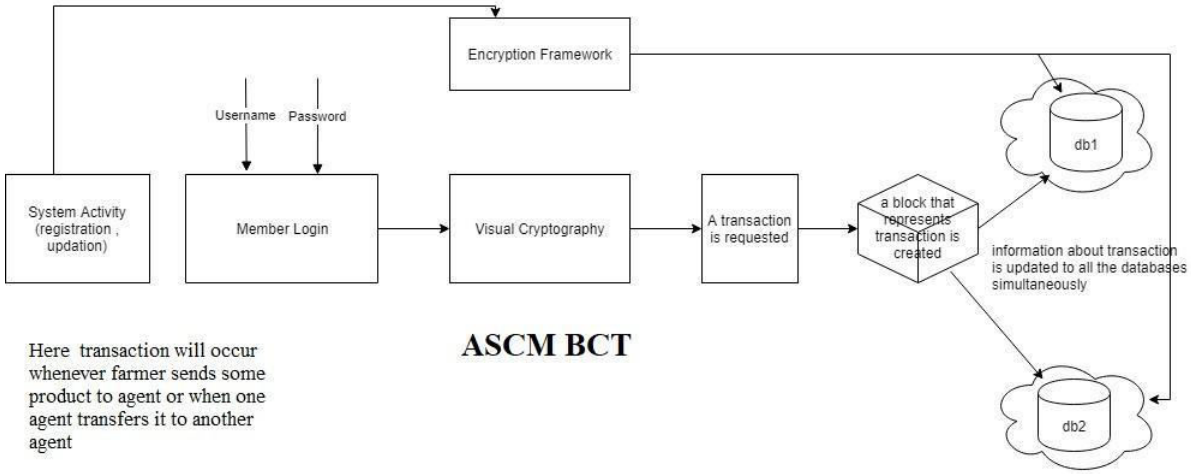

Figure 2: System Flow

V. OVERVIEW OF PROJECT MODULES

BCT: First and foremost, blockchain is a public electronic ledger built around a P2P system that can be openly shared among disparate users to create an unchangeable record of transactions, each time-stamped and linked to the previous one. Every time a set of transactions is added, that data becomes another block in the chain (hence, the name). Blockchain can only be updated by consensus between participants in the system, and once new data is entered it can never be erased. It is a write-once, append-many technologies, making it a verifiable and auditable record of each and every transaction. Famer will transfer the products to the agent through the application interface, agent in turn will transfer any product to another agent through application interface only. Also, the record of each and every transaction will be maintained at different places which will maintain transparency also the database is secured through AES. System login is secured through visual cryptography.

TOOLS AND TECHNOLOGIES USED:

JDK 1.8 Installation
1. Double click jdk-8-ea-bin-b32-windows-i586 to run the installation program. JDK License dialog displayed. Accept the license in order to install JDK.
2. The JRE Custom setup dialog enables you to choose a custom directory for JRE Files.
3. The complete dialog indicates a successful installation.
Net Beans IDE 7.3.1 Installation To install the software:
1. After the download completes, run the installer. For Windows, the installer executable file has the .exe extension. Double-click the installer file to run it. 2. If you downloaded the All bundle, you can customize your installation. Perform the following steps at the Welcome page of the installation wizard: a. Click Customize.
b. In the Customize Installation dialog box, make your selections.

- At the Welcome page of the installation wizard, click Next. At the License agreement page, review the license agreement, click the acceptance check box, and click Next. At the JUnit License Agreement page, decide if you want to install JUnit and click the appropriate option, click Next. At the NetBeans IDE installation page, do the following: • Accept the default installation directory for the NetBeans IDE or specify another directory. Note: The installation directory must be empty and the user profile you are using to run the installer must have read/ write permissions for this

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

directory. • Accept the default JDK installation to use with the NetBeans IDE or select a different installation from the drop-down list. If the installation wizard did not find a compatible JDK installation to use with the Net-Beans IDE, your JDK is not installed in the default location. In this case, specify the path to an installed JDK and click Next, or cancel the current installation. After installing the required JDK version you can restart the installation.

- If you are installing Apache Tomcat, on its installation page, accept the default installation directory or specify another installation location. Click Next.
- At the Summary page, verify that the list of components to be installed is correct and that you have adequate space on your system for the installation. • Click Install to begin the installation. • At the Setup Complete page, provide anonymous usage data if desired, and click Finish.

MySQL Database

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications which may run either on the same computer or on another computer across a network (including the Internet). Microsoft markets at least a dozen different editions of Microsoft SQL Server, aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concur- rent users.

ALGORITHM DETAILS:

Algorithm:

1. AES is used to encrypt the database.

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

STEPS:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation
- Copy the final state array out as the encrypted data (ciphertext).

SHA 256:Hash Function

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash func- tion with digest length of 256 bits. It is a keyless hash function; that is, an MDC

(Manipulation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds A cryptographic hash (sometimes called ‘digest’) is a kind of ‘signature’ for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. A hash is not ‘encryption’ – it cannot be decrypted back to the original text (it is a ‘one-way’ cryptographic func- tion, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare ‘hashed’ versions of texts, as opposed to decrypting the text to obtain the original version.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

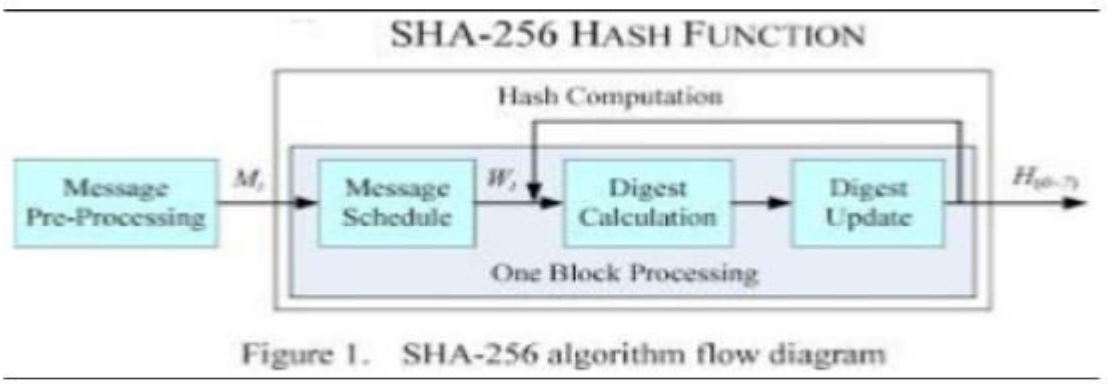

Figure 3: SHA 256 Diagram

VI. RESULTS

Transparent supply chain due to use of BCT, block chain of every transaction is maintained and can be tracked in future.

SCREENSHOTS

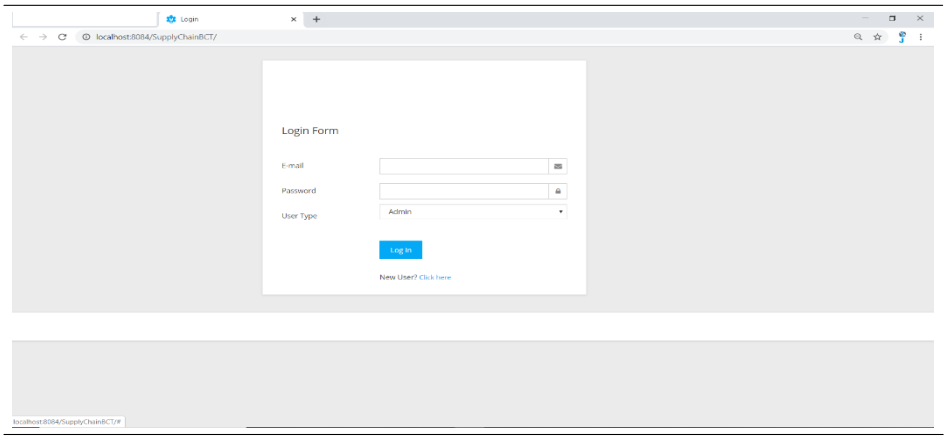

Figure 4: Login Page

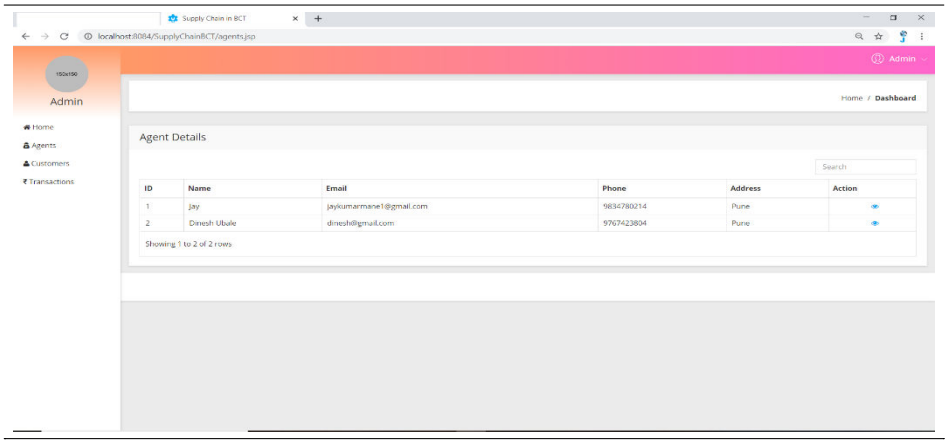

Figure 5: Admin View Agents

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

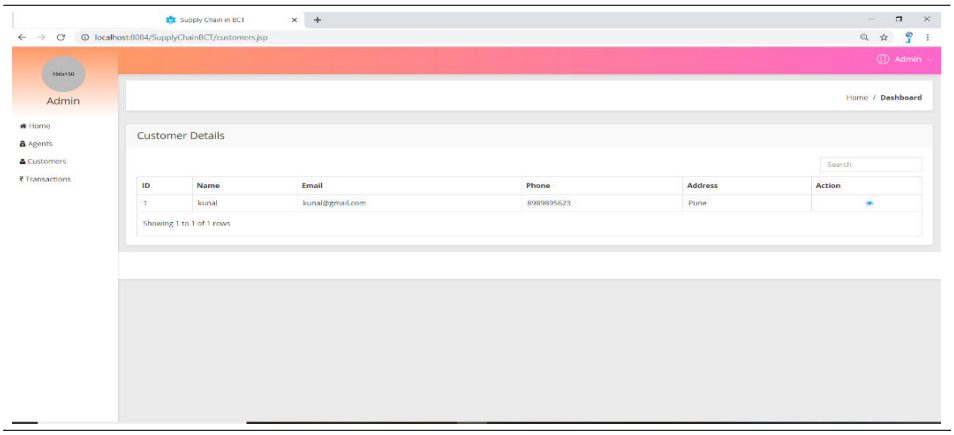

Figure 6: Admin View Costumers

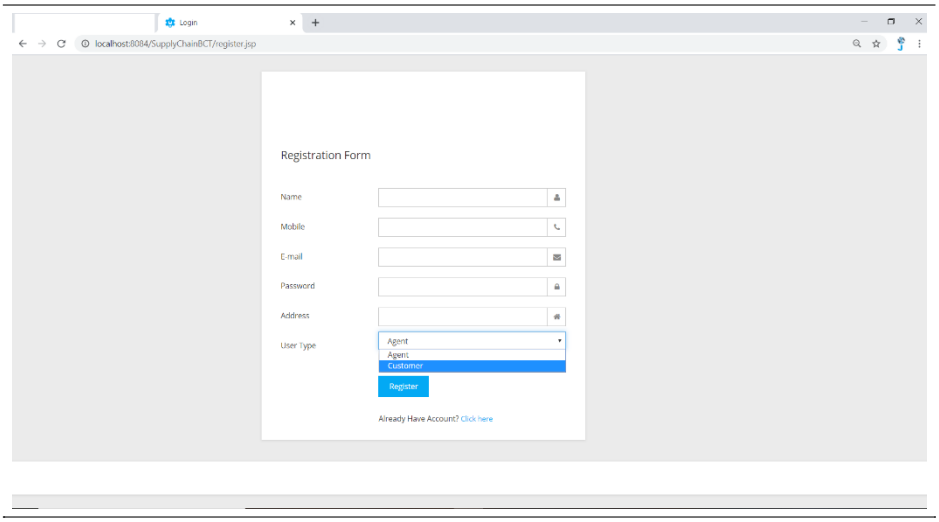

Figure 7: User Registration

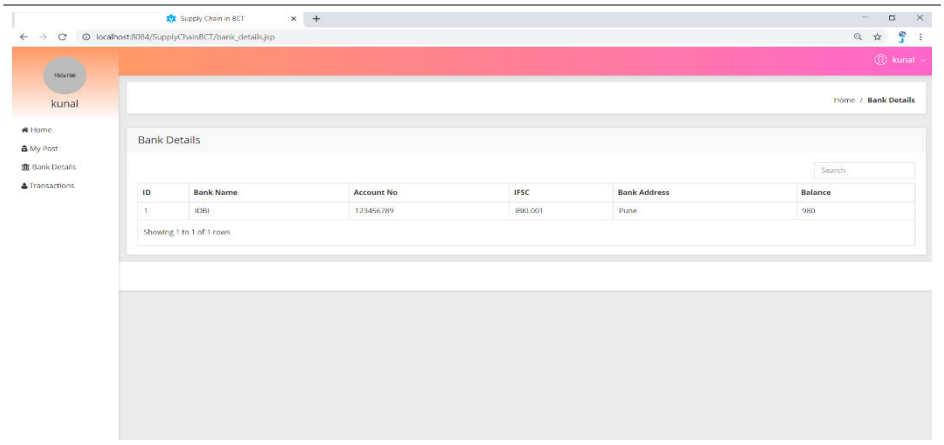

Figure 8: Costumer Bank Details

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

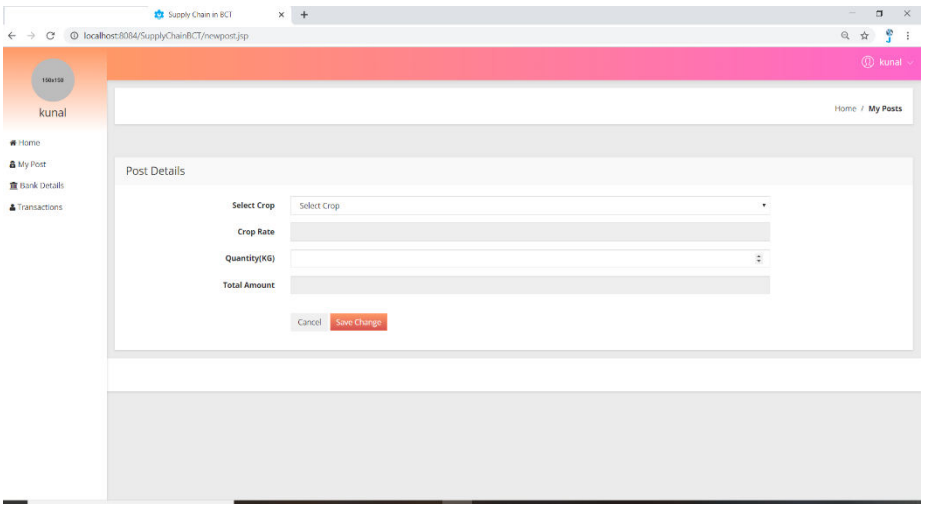

Figure 9: Farmer Add Post

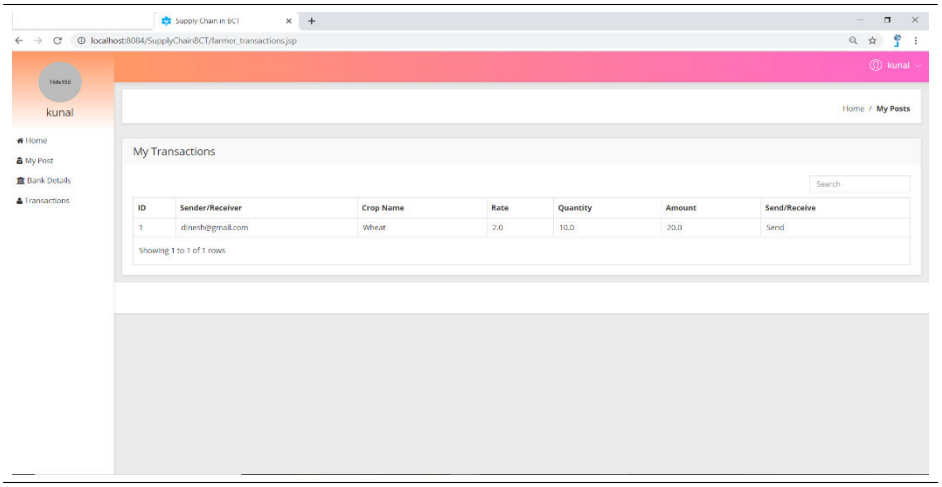

Figure 10: Farmer Transaction

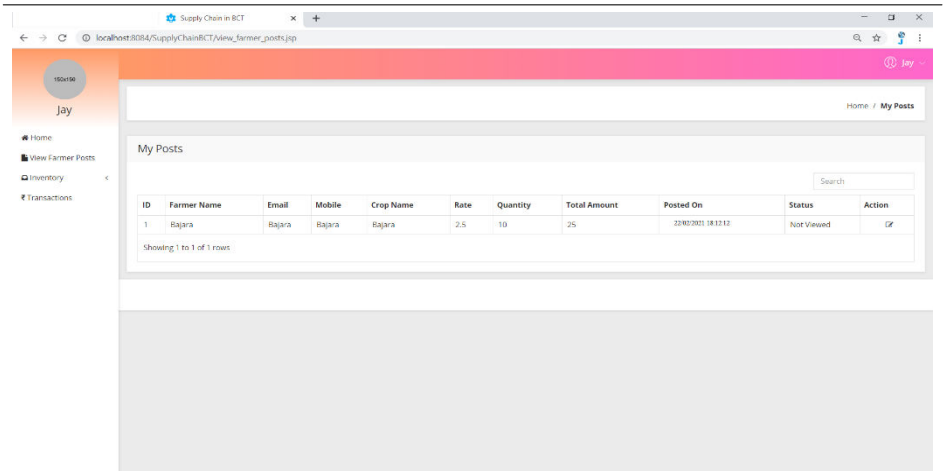

Figure 11: Agent View Farmer Post

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

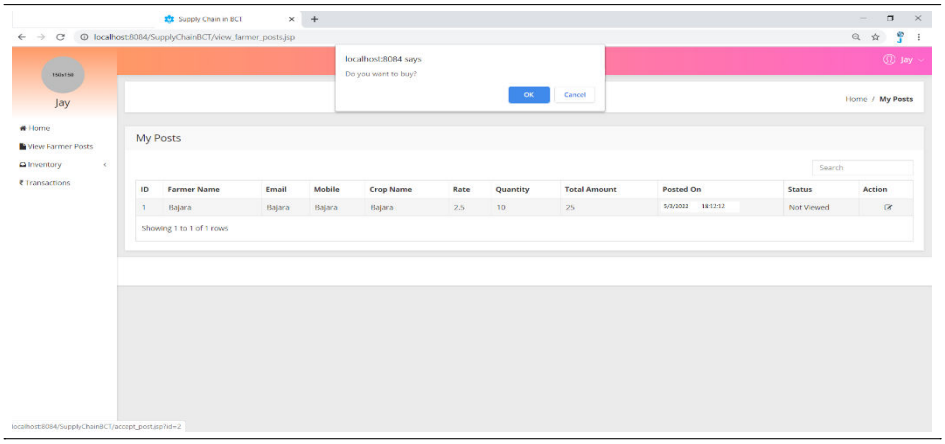

Figure 12: Buy Famer Product

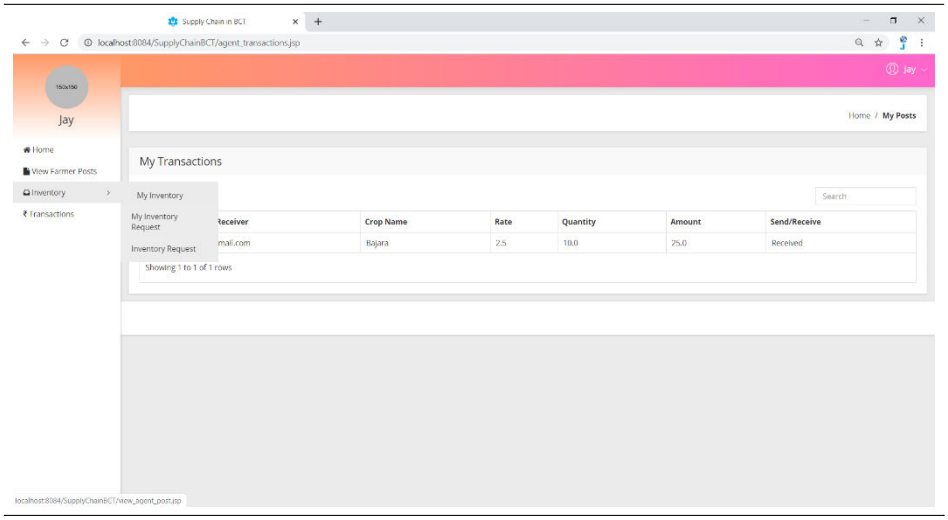

Figure 13: Agent Inventory

VII. CONCLUSION

Thus, we are have implemented a prototype web based software application in Java for application of BCT in supply chain management . We have implemented block chain features such as: 1. Decentralization 2. Visual Cryptography 3. Hash Algorithm 4. Encrypted Database. Thus, it is possible to track agricultural supply chain and to give minimum price for agricultural products.

VIII. FUTURE SCOPE

In future we will try for sponsorship from government and will implement a project on large scale with some domain and hosting space online.

APPLICATIONS

1. Farmers
2. Government Organizations
3. Banking Sector

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105297 |

REFERENCES

1. L. Guo, C. Zhang, J. Sun, Y. Fang. “A privacy-preserving attribute-based authentication System for Mobile Health Networks”, IEEE Transactions on Mobile Computing, 2014.
2. A. Abbas, S. Khan, “ A review on the state-of-the-art privacy preserving approaches in e-health clouds”, IEEE Journal of Biomedical Health Informatics, 2014.
3. J. Yang, J. Li, Y. Niu, “ A hybrid solution for privacy preserving medical data sharing in the cloud environment ”, Future Generation Computer Systems, 2015.
4. V. Goyal, O. Pandey, A. Sahai, B. Waters, “ Attribute-based encryption for fine-grained access control of encrypted data ”, Proc. 13thm ACM Conf. Computer and Comm. Security (CCS06), 2006.
5. R. Ostrovsky, A. Sahai, B.Waters, “ Attribute-based encryption with non- monotonic access structures ”, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007.
6. J. Han, W. Susilo, Y. Mu. “ Improving privacy and security in decentralized cipher text-policy attribute-based encryption ”, IEEE Transactions on on In- formation Forensics and Security, 2015.
7. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, “ Scalable and secure sharing of personal health records in cloud computing using attribute based encryption ”, IEEE transactions on parallel and distributed systems, 2013.
8. M. Green, S. Hohenberger, B. Waters, “ Outsourcing the decryption of ABE ciphertexts ”, in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.
9. J. Lai, R. H. Deng, C. Guan, J. Weng, “Attribute-based encryption with verifiable outsourced decryption ”, IEEE Trans. Inf. Forensics Security, Aug. 2013.
10. B. Qin, R. H. Deng, S. Liu, S. Ma, “Attribute-based encryption with efficient verifiable outsourced decryption ”, IEEE Trans. Inf. Forensics Security, JULY. 2015.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details