

1. Introduction

- **Blockchain-** Blockchain is a technology that utilizes distributed systems to store data. Each individual block in a blockchain contains its hash, the hash of the previous block, data and the functions that it uses and stores. The hash of a block is calculated when a new block is created. Through this way, the blocks together form a chain starting from the first block.

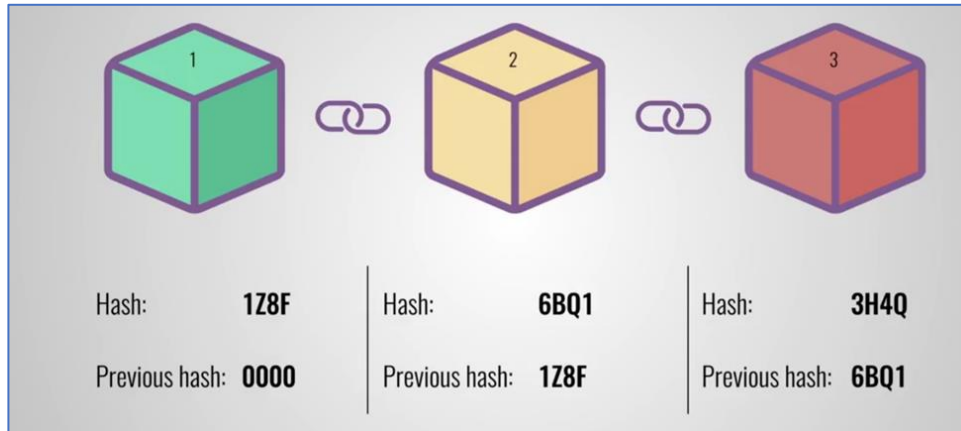


Figure 1: Formation of a blockchain by the links through hash values.

Figure 1 explains the formation of a blockchain. Each block points to its previous blocks and so on.

It is also a distributed ledger which means that the entire blockchain is not in the control of a single entity but every user has its own copy. To add a new block to the blockchain, we will have to compute the hash of our block, then we will have to tell about the change to everyone in the blockchain system after giving them a proof of elapsed time. After this, every system using the chain update their blockchain and we have a valid system again. This feature makes blockchain very much secure. To change a single block, we will have to take control of more than 50% of the users' systems as we will have to change the blockchain of the more than 50% systems to achieve a majority. We will have to change the hash of the following blocks after our block in which we intend to make a change. This is because once our block is changed, its hash also changes because of the functions and the programs stored in the block and once the hash changes, the following block no longer points to our intended block, even if we change its hash also, the next one doesn't and the process goes on to the very last block in the chain. This will require a lot of computing power since a hash is calculated through a lot of complex mathematical calculations. Also, the proof of work makes the creation of new blocks slower to protect this tampering of the blockchain. So, this makes the tampering of the blockchain a long, expensive and tiresome process. This makes blockchain an extremely secure technology.

- **Blockchain in Agriculture**

It can be used in agriculture to maintain land records, crop records, the information about the quality of the soil, etc. In this project, our main focus will be on the land records and the crop records. The land records will contain the location, the area, the assigned number, the neighboring land pieces and the ownership records. In terms of crop records, the data will include things like the crop grown at the present time, the availability of water and past performances of the crops on the land. These will be stored in the blocks. Also, further data fields can be added to the block data type to store more varied information about any land piece in the blockchain.

2. Background Study

To implement the system, we have referred some research papers and noted the merits and the demerits of the current blockchain-based systems in development. The summarizations of the research papers are as follows:

- **Blockchain: The Evolutionary Next Step for ICT E-Agriculture [1]**

Authors: Yu-Pin Lin, Joy R. Petway, Johnathen Anthony, Hussnain Mukhtar, Shih-Wei Liao, Cheng-Fu Chou and Yi-Fong Ho

The paper discusses the potential uses of blockchain as an Information and Communications Technology (ICT) that will enhance the notion of trust among the various related groups. Right now, the agricultural record systems use a centralized database for all the records that include the ownership details, the crop details and the irrigation details. Security has always been a major concern in all these systems as they are susceptible to manipulation by not only the external entities like hackers trying to cause disturbance but also by various stakeholders and the policymakers. Many a time these records are modified and even deleted in the light of a political agenda. Sometimes other people that are involved in the whole industry also cause problems in order to gain more profits. Since blockchain-based ICT systems will be a distributed database, they will provide controlled access to all the parties involved and the records will be immutable since no particular entity will control all the records. Also, the international standards can be implemented in such records in a better way as the blockchain will always have credible data. This further enhances the credibility of the entire record system as everyone shall know that the blockchain is immutable and there are multiple copies of the record that have been verified. Data on the farms can be collected via the smartphones or the wireless sensor networks and the authorized node can add a record as a block to the complete chain after mining. The major enhancement that such a system brings about is the notion of trust and providing cleaner and quality data for everyone.

Advantages:

- Such a system improves the trust among the various entities involved in the agricultural industry by providing immutable data and also by ensuring the quality standards.
- Such systems provide credibility to the data as the various international standards can be implemented easily.
- Such systems also prevent the censorship of the data by any single party involved in the process.
- An evaluation tool has also been proposed in the paper that can help anyone decide whether such a system will be suitable in the context of a particular region for which the system is to be decided upon. It takes into account the suitability of the blockchain-based system in terms of the environmental, social and technical context.

Disadvantages:

- Scalability remains a very large issue in such a system as the transaction processing rates are highly limited due to the block sizes and the block intervals.
- Also, the transaction processing times in a blockchain-based systems are slower than that of a centralized database system and to decrease that time, more centralized processing is needed in the blockchain that results in compromise on one key component, i.e, security of the entire blockchain system.

- **Food Safety Traceability System based Blockchain and EPCIS [2]**

Authors- Qijun Lin, Huaizhen Wang, Xiaofu Pie, Junyu Wang

The paper describes a system as a hybrid of the blockchain and the EPICS(Electronic Product Code Information Services).It also proposes the management architecture of on-chain & off-chain data, through which the traceability system can improve in the food supply chain. The enterprise-level smart contract is designed to prevent data tampering and sensitive information disclosure during information interaction among participants. The existing traceability systems adopt either of the two architectures: Centralized traceability system is managed and maintained by an authoritative third party. It may suffer a single node attack and has higher risk of data tampering and information disclosure. Distributed traceability system, such as the EPCIS-based distributed traceability system, can facilitate the creation and sharing of visibility event data concerning physical or digital objects both within and across enterprises. The EPCIS specification defines four different events—ObjectEvent, AggregationEvent, QuantityEvent, TransactionEvent, which is good for the scalability of traceability system but couldn't solve data tampering and information disclosure issues. The current researches mainly work in two directions: One is to redesign the whole blockchain system from underlying architecture to meet the requirements of the

application in supply chain management. The other is to make use of the existing mainstream blockchain architectures to optimize system security and solve some pain points of the supply chain management.

Items	Centralized system	EPCIS-based system	Blockchain-based system	This work
Information Traceability	Yes	Yes	Yes	Yes
Tamper-proof Ability	Low	Low	High	High
Privacy Protection	No	No	Yes	Yes
Degree Of The Decentralization	No	Low	High	High
Amount of on-chain data	/	/	high	low

Figure 2: Advantages of the given system over other systems

Advantages:

- **Higher Degree of Decentralization:** The system is completely decentralized with a removed centralized server, which can avoid the monopoly and improve the credibility of the system.
- **Stronger System Robustness:** Blockchain-based design and Collaborative Data Management Model of On-chain and Off-chain Data guarantee a tamperproof system.
- **Higher Security of Data Interaction:** Only companies belonging to the same supply chain can share event data with each other. In this way, sensitive business data will not be easily divulged.

Limitations: The off-chain and the on-chain interaction of data can lead to more delays. Also, the system only talks about the traceability of the food items but the complete land records and farm records are more difficult to process and store as on-chain and off-chain data.

- **Ensure Traceability in European Food Supply Chain by using blockchain System [3]**

Authors: Gavina Baralla, Andrea Pinna, Giacomo Corrias

In this paper, the authors have put forward the concept of using permissioned blockchain by using an authorized login system for adding and updating data. This eliminates the components of trust that need to be programmed in the public blockchain systems. They have also introduced the concept of Proof of Elapsed Time (PoET) to add the blocks. This means that new blocks can be added to the blockchain only after a certain time interval has elapsed. This helps to save the processing power required to mine the blocks as in this case, the participating nodes do not have to do the complex mathematical calculations required

each time. This also helps in preventing the tampering of the blockchain as adding new blocks will not be easy and fast even if the chain is compromised. They have used the Sawtooth framework which is a modular blockchain framework for business use cases based on the Hyperledger (which is an open-source blockchain project by Linux Foundation).

Advantages: The permissioned blockchain helps to save time and also helps in reducing the computing power required to implement the blockchain. A permissioned blockchain system such as the one introduced in the paper also enables greater customization in the data fields that are added to the block as the fields can be specified according to the user needs.

Limitations: The main limitations of the system compared to a private blockchain that we are aiming to build is that the system runs on defined hash algorithms while with a complete private implementation of the blockchain like the one proposed in this project will enable customization for even the hashing algorithms.

3. Requirement Analysis

- **Introduction**

3.1. Description: The project aims to implement a distributed database system using the concept of private blockchain implemented through an authorized user login system.

3.2. Environmental Characteristics

3.1.2.1. Hardware: The system will be able to run and access the records on normal PCs and servers. The suggested PC hardware requirements of such a system are as follows:

1. RAM: 4GB or higher
2. Secondary memory: 512 GB or higher
3. Processor: Any processor of Intel 3rd generation or higher with 4 or more cores.

3.1.2.3. Software Requirements: The system will require a Windows Operating System with a version of 7 or higher. The system will run on C++ compiler and Python.

3.1.2.2. Actors: The stakeholders involved in using and maintaining the system are nodal officers adding the records, the farmers providing the information, the government and other stakeholders like the insurance companies, the auditing companies, etc.

- **Functional Requirements**

3.2.1 Maintain farm records.

3.2.2 Provides easy traceability of the data by searching for hash values within a chain.

3.2.3 Valid users are provided with a username and password for login.

- **Non-Functional Requirements**

- 3.3.1** A time stamp should be maintained which contains date and time at which the block was created.
- 3.3.2** Maintain hash of the latest block so that a new block can be added to the chain using the hash value of the previous block.
- 3.3.3** Implement the above project using private blockchain.
- 3.3.4** Allow only authenticated users to update or add record.
- 3.3.5** Data or a block can only be added in the chain if and only if it is verified by the majority of the existing blocks.

- **Use Case Diagram**

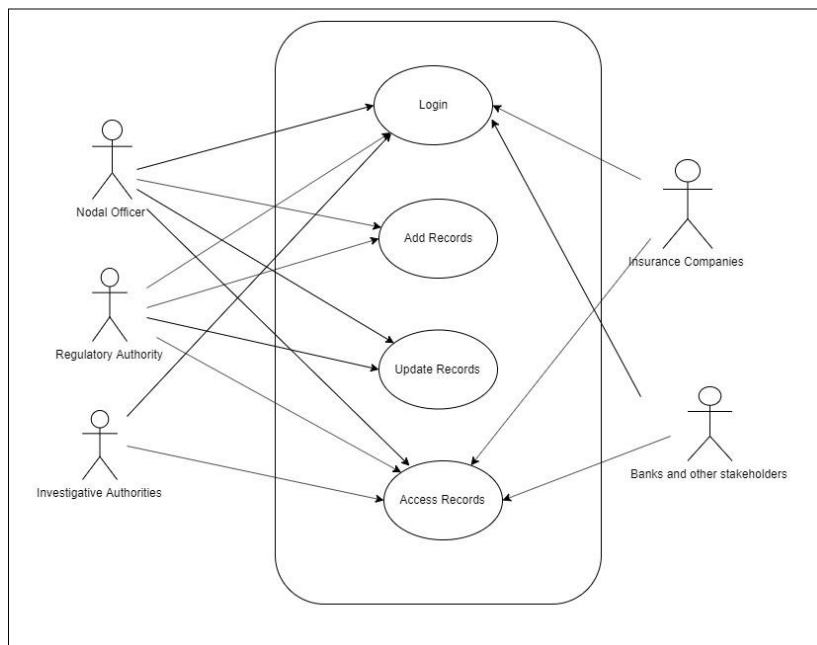


Figure 3: Use Case Diagram

4. Detailed Design

In the given blockchain-based distributed system, we can structure the system in the following manner.

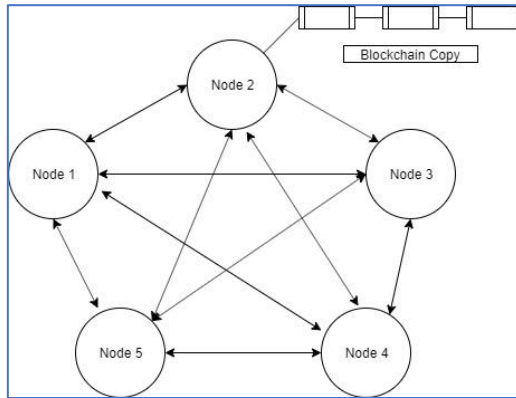


Figure 4: Representation of the nodes in the network

Each node represented by the circle shows a different entity and contains a blockchain copy as shown with the node 2.

Like node 2, each node contains its own blockchain copy.

Each node represents a participating entity in the network. For example, Node 1 can represent the nodal officer entering the data, Node 2 represents the government authority, Node 3 represents the insurance company and so on. Also, each node contains its own copy of the blockchain and each node can interact with all the other nodes in the network.

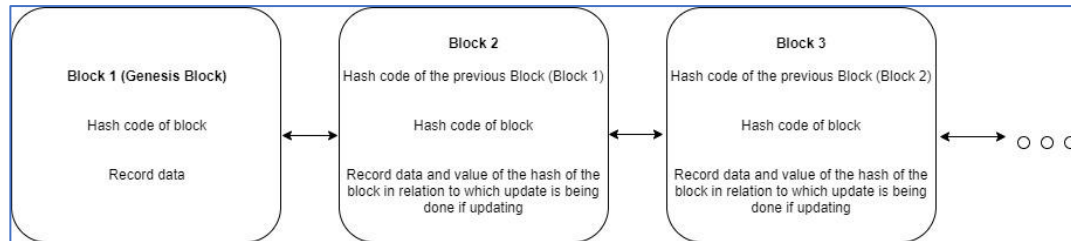


Figure 5: Diagram representing the blockchain structure in the form of blocks

The first block (as shown in figure 4) is called the genesis block and it contains only its own hash and data and it will not have any update data as it is the first block in the chain. After that, the second block contains its own hash, the hash of its previous block, i.e., the genesis block and data. In the data field, we plan to store the following things:

1. Update data and the hash of the block in relation to which the update is being done if any.
2. The land records. This will contain the following fields:
 - 2.1. The name, permanent address and contact info of the owner.
 - 2.2. The area of the land piece under cultivation.
 - 2.3. The serial number assigned by the government to the land piece.
 - 2.4. The complete location details and neighboring land pieces.
3. The crop records. These will contain the following fields:
 - 3.1. The type and name of the crop grown along with the time period of the harvest.

3.2. The quality of the soil of the land piece, the number of resources it requires and the suitable crops that can be cultivated on it.

- **Features of the system and the problems that will be solved**

The main features of the project and the major problems that this project will be able to solve are as follows:

4..1. Traceability

The centralized systems make it very difficult to trace the data stored on the servers. For example, if we want to trace the entries related to a particular farm on the system, then we will have to search the entire directory on the server. This method leads to the complete data of that farm being exposed every time an update is made. So, in this approach we compromise security to get better traceability. In the blockchain based database, we can approach this problem in the following manner:

- Each update made to the database regarding a particular farm will be treated as a separate block addition to the blockchain.
- This block will contain all the data fields that were updated.
- In such a system, the search will be easy as the search will begin from the end of the blockchain. This means that the latest updates will be available right from the beginning.
- After the first data match of the farm ID is found, it becomes easy to trace all the changes as the search algorithm will only have to search for the block hash rather than the complete data field. Unlike the traditional centralized server system that relies on matching complete field values, the system will provide speed in the search.

4..2. Security

The key advantages of a blockchain-based record-keeping system are as follows:

- The blockchain itself provides a very strong layer of security for the entire database. Every new node being entered has to be verified and updated in all the copies of the blockchain. Also, only certain users authorized by a login system can add new nodes to the database. This ensures that no outsider can access the information.
- To change any particular block of information in the entire blockchain, you need to have control of more than 50% of the entire chain. Only then can you prove verification of the entire chain with the changed block. A single change of hash at any particular block will make the entire blockchain invalid.
- Compared to a traditional record system, the blockchain-based system will be less prone to hacking attacks. Since there is no centralized server storing all the data and you will have to gain control of more than 50% of the network to change the data, this system will be virtually very difficult to attack.

- Also, the system and the records as a whole will be very much difficult to delete because you will have to delete the blockchain copies on all the systems to delete the entire record.

4.3. Credibility

One of the main issues with the traditional database systems is that of credibility. Since these records are more prone to hacking attacks and are not considered safe, the various entities involved in the agricultural system do not trust them. For example, if a company is providing crop insurance, then it is very possible that the company might not trust the database stored on the central servers as the data on them can be modified by various other players. So, the company decides to collect its own information. This leads to additional costs which are ultimately paid by the end customer. However, a distributed database system such as the one provided by the blockchain will not be easy to modify. There will be multiple copies of the chain stored on many participating nodes. These all will act as points of verification for the entire record. Any entity that needs to verify the data can use any of them or all for verification. Hence, the system reduces the costs for everyone involved in the supply chain.

This feature also helps to control the middlemen in the supply chain. All the farms and the output will have easily traceable and verifiable records. The regulatory authorities will be able to know precisely the amount of the food grains that have been produced in a particular time period. If the amount that is being sold in the market is less than the expected amount of food from the data retrieved by the blockchain system, then it might point to a problem in the supply chain or the problem of hoarding of stocks. This implies that the system will play an instrumental role in detecting problems in the supply chain and will provide timely warnings about any coming problem.

4.4. Transaction Processing

The transaction processing, i.e., updating and adding new records to the database will be far more efficient. We are including a new block to the chain with each update and this means that we don't have to overwrite any existing data values to change the previous values. This results in less time being wasted to search and then add another node. For example, if a sale of a farm is being done, we don't have to delete the entire record of the farm being sold, we only have to add another block that shows that this farm record is being updated. Thus, the blockchain-based system provides greater efficiency in transaction processing by reducing the time and overhead.

5. Implementation

Each block in the blockchain contains the hash of the previous block, its own hash value and the data regarding the crops and the land ownership.

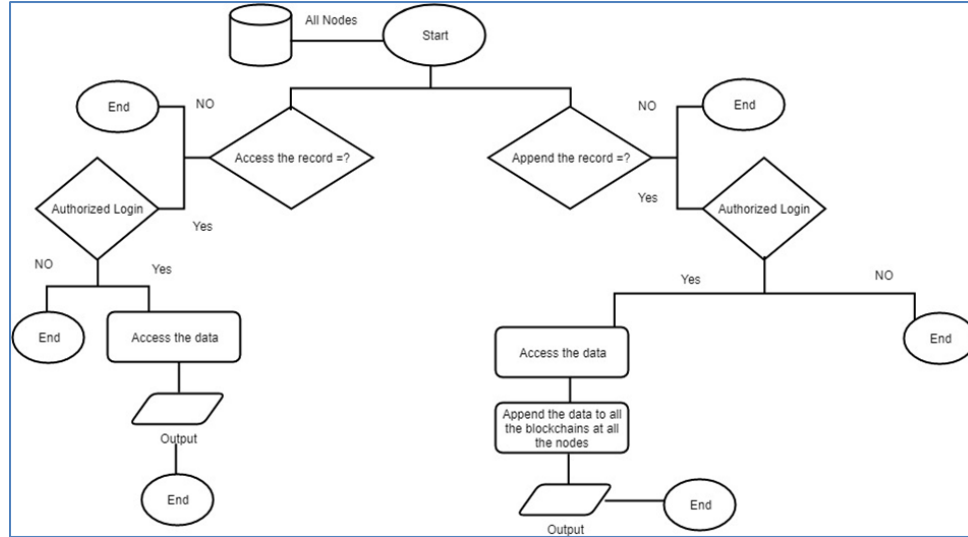


Figure 6: Flowchart for access control

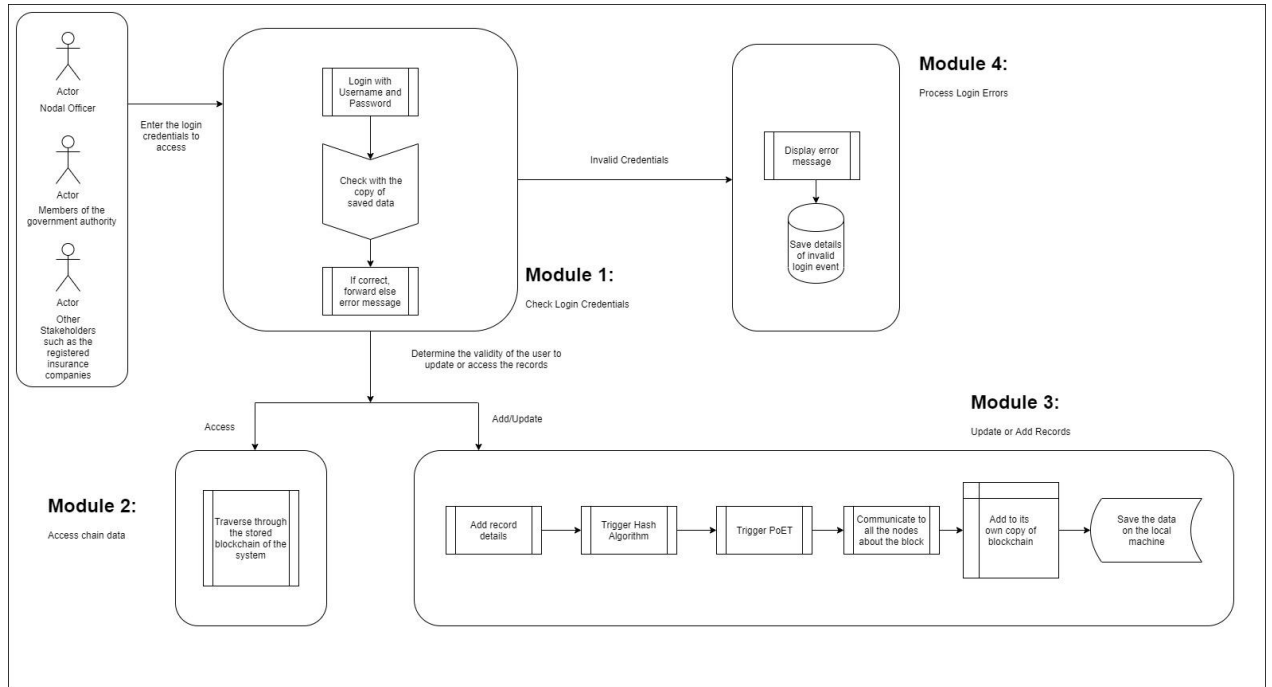


Figure 7: Control and Data flow in the System

There are four modules of the system. Figure 7 shows the flow of interaction between the modules. The Module 1 checks the login credentials of any type of request and checks its validity. If it is invalid, it goes to error processing module (Module 4). Module 4 shows error message if incorrect credentials are given. If the request is of Access type (such as the one given by Insurance Companies),

then the Module 2 traverses the locally stored chain for the data. If the request is of add/update type, it goes to Module 3. This module first takes the input of the record details. Then, it triggers the Hash algorithm and the PoET (Proof of Elapsed Time) function. After this, the added record is communicated to the other node. In the last step, the record is added to the local copy of the blockchain also.

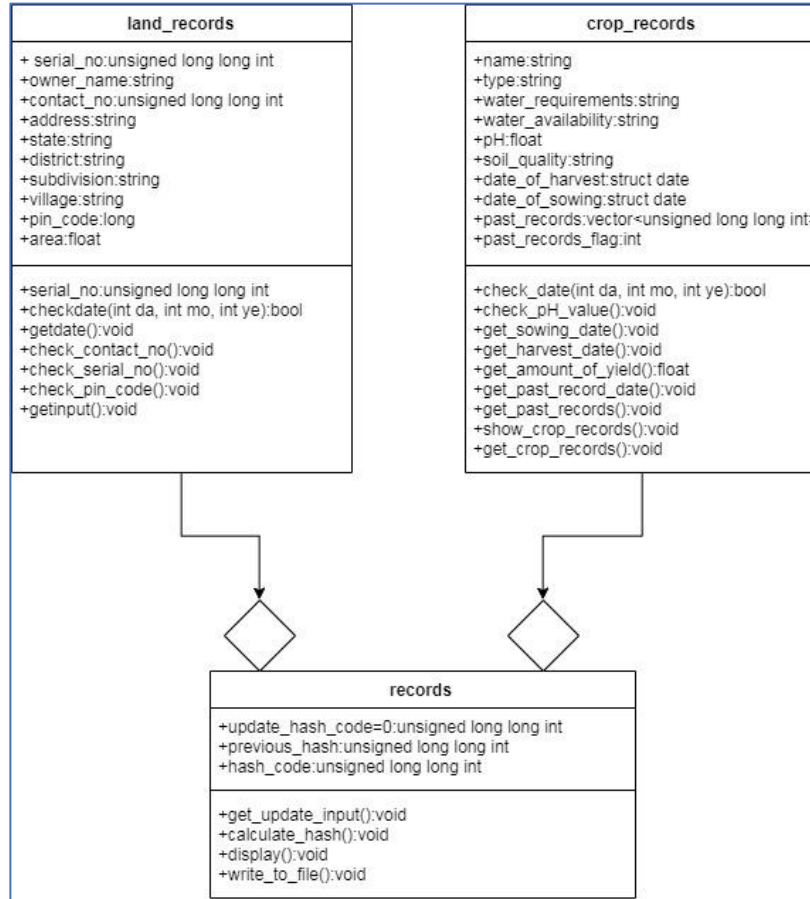


Figure 8: UML Diagram

The hash function calculates the hash by using the values of all the variables. It first takes all the integer and float values and adds them to get a final value. An array of random variables is generated taking the system time as an argument. Then, it takes each character of the string variables and converts them into ASCII value and multiplies it with a random number from the array of random numbers previously generated. These values are finally added to the hash code value of the block to get the final hash value of the block. With the help of the random variables, it is ensured that the values of the hash functions of the block are unique.

The login authorization module ensures that the proper access is provided to appropriate entities. The username and the passwords are stored in a file for implementing this.

The system then transfers the files generated for the blockchain using virtual implementation of client and server machines using Python program.

6. Results and Analysis

The C++ program is able to get the inputs and write them on the text file as specified in the project.

```

he genesis block has been created.
Do you want to add this record as an update to a previous block?
Enter the Name of the owner whose record you want to enter:
Abhishek
Enter the Contact number of the owner:
8368741777
Enter the Government assigned serial number of the land piece:
123456789147
Enter the State in which the land piece falls:
UP
Enter the District in which the land piece falls:
Meerut
Enter the Sub Division in which the land piece falls:
Hastinapur
Enter the Name of the village area:
Rampur
Enter the PIN Code of the region:
203001
Enter the area of the region:
2.3
Enter the date in which the record was added:
5
Enter the day: 6
Enter the month: 2019
Enter the serial nos. of the neighboring fields:
123456951

The serial number of the field according to the government records:123456789147
The name of the owner of the field:
Abhishek
The contact number of the owner is as follows:
8368741777
The complete address of the field:
The State is: UP
The District is: Meerut
The Sub Division is: Hastinapur
The Village is: Rampur
The PIN Code of the area is: 203001
The area of the field is:
2.3
The date on which the record was taken is: 5-6-2019
The serial numbers of all the neighboring fields are as follows:
123456951
Enter the type of the crop in details:
Grain
Enter the name of the crop with biological name:
Wheat
Enter the water requirements of the crop with explanation:
Medium
Enter the availability of the water resources with all the details:
High
Enter the details of the soil quality of the field:
GOOD
Enter the pH value of the soil:
6.5
Enter the Date on which the crop was shown:
5
Enter the day:
5

The name of the crop: Wheat
The type of the crop: Grain
The water requirements for the crop:
Medium
The water availability for the crop:
High
The pH value of the soil: 6.5
The description of the soil quality:
GOOD
The date of sowing: 5-4-2019
The expected date of harvest for the current crop: 5-12-2019
The contents of the file are as follows:
Hash Code 0
This is the genesis block. 02570Hash Code 18133991912973480
Previous Hash Code 12884901888
Owner Name Abhishek
Contact No 8368741777
Serial No 123456789147
State UP
District Meerut
Subdivision Hastinapur
Village Rampur
PIN Code 203001
Area 2.3
5 6 2019
Crop Name Wheat
Crop Type Grain
Crop Water Requirements Medium
Crop Water Availability High
pH Value 6.5
Crop Date of Sowing 5 4 2019
Crop Date of Harvest 5 12 2019

```

Figure 9: Output from the C++ program.

The output of the server and the client program running on Python are also as follows:

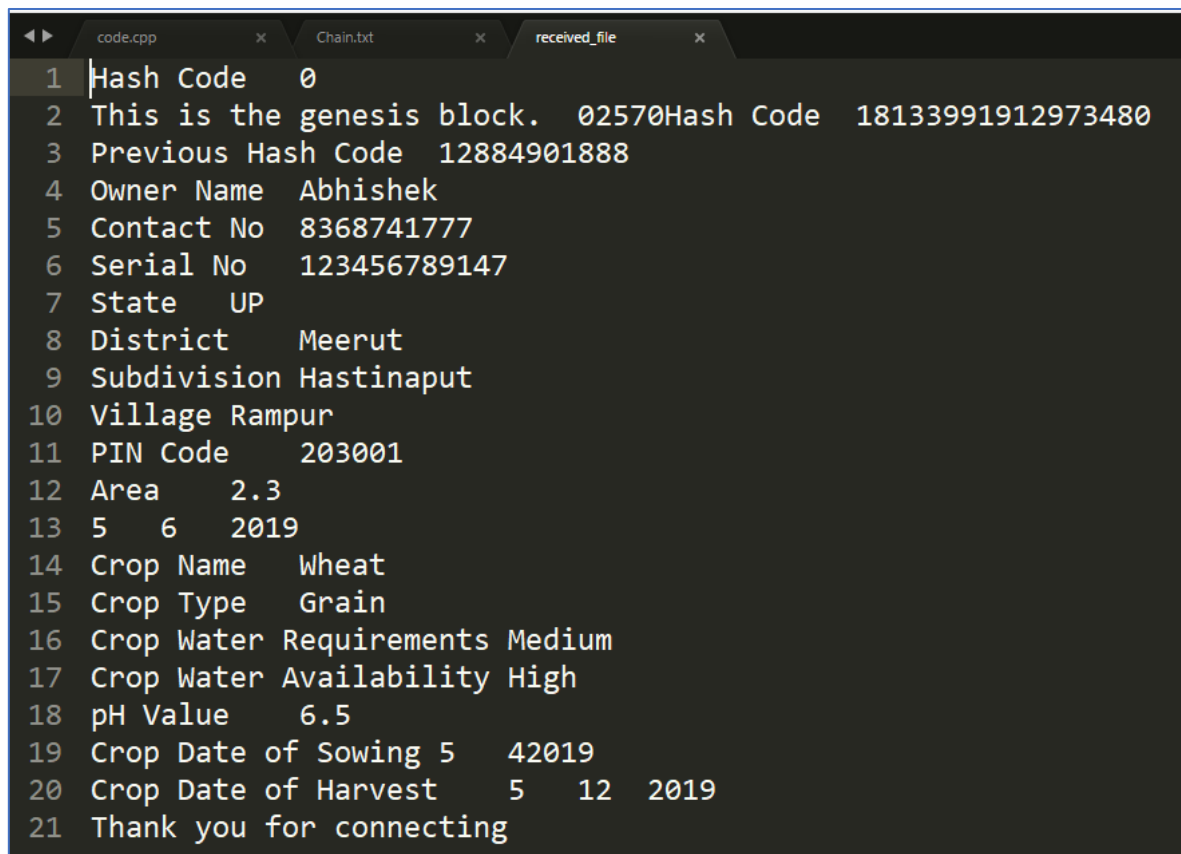
```

Python 2.7.13 Shell
File Edit Shell Debug Options Window Help
Python 2.7.13 (v2.7.13:a06454b1afai, Dec 17 2016, 20:42:59) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\Abhishek\Desktop\Serv.py =====
Server listening...
Got connection from ('192.168.1.6', 53133)
('Server received', 'Hello server!')
('Sent ', 'Hash Code\t0\t\nThis is the genesis block.\t02570Hash Code\t18133991912973480\t\nPrevious Hash Code\t12884901888\t\nOwner Name\tAbhishek\t\nContact No\t8368741777\t\nSerial No\t123456789147\t\nState\tUP\t\nDistrict\tMeerut\t\nSubdivision\tHastinapur\t\nVillage\tRampur\t\nPIN Code\t203001\t\nArea\t2.3\t\n5\t6\t2019\t\nCrop Name\tWheat\t\nCrop Type\tGrain\t\nCrop Water Requirements\tMedium\t\nCrop Water Availability\tHigh\t\npH Value\t6.5\t\nCrop Date of Sowing\t5\t4\t2019\t\nCrop Date of Harvest\t5\t12\t2019\t\n')
Done sending
|

Python 2.7.13 Shell
File Edit Shell Debug Options Window Help
Python 2.7.13 (v2.7.13:a06454b1afai, Dec 17 2016, 20:42:59) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\Abhishek\Desktop\Clie.py =====
file opened
receiving data...
('data=%s', 'Hash Code\t0\t\nThis is the genesis block.\t02570Hash Code\t18133991912973480\t\nPrevious Hash Code\t12884901888\t\nOwner Name\tAbhishek\t\nContact No\t8368741777\t\nSerial No\t123456789147\t\nState\tUP\t\nDistrict\tMeerut\t\nSubdivision\tHastinapur\t\nVillage\tRampur\t\nPIN Code\t203001\t\nArea\t2.3\t\n5\t6\t2019\t\nCrop Name\tWheat\t\nCrop Type\tGrain\t\nCrop Water Requirements\tMedium\t\nCrop Water Availability\tHigh\t\npH Value\t6.5\t\nCrop Date of Sowing\t5\t4\t2019\t\nCrop Date of Harvest\t5\t12\t2019\t\n')
receiving data...
('data=%s', 'Thank you for connecting')
receiving data...
('data=%s', '')
Successfully get the file
connection closed
>>>

```

Figure 10: Output of the Python program for the Server and Client



```
1 Hash Code 0
2 This is the genesis block. 02570Hash Code 18133991912973480
3 Previous Hash Code 12884901888
4 Owner Name Abhishek
5 Contact No 8368741777
6 Serial No 123456789147
7 State UP
8 District Meerut
9 Subdivision Hastinaput
10 Village Rampur
11 PIN Code 203001
12 Area 2.3
13 5 6 2019
14 Crop Name Wheat
15 Crop Type Grain
16 Crop Water Requirements Medium
17 Crop Water Availability High
18 pH Value 6.5
19 Crop Date of Sowing 5 42019
20 Crop Date of Harvest 5 12 2019
21 Thank you for connecting
```

Figure 11: The contents of the file received at the other virtual node.

The project also generated a file “hash_codes.dat” to store the hash values of all the blocks in order. It also uses a “login.dat” file to keep a track of the username and the password details of the authorized users as well as the type of access available to them according to the specified constraints.

The project has been able to implement the private blockchain modules as specified. The task of distributing networking can be done in the future. In this project, we have tried to demonstrate that functioning of the distributed networking by creating two virtual nodes. With the help of socket programming, the file is sent to the other node and is received in the same format with the file name “received_file”.

7. Conclusion of the Report and Future Scope

The system uses the idea of the private blockchain along with complete user authorization at every participating node to implement traceability, credibility, security and efficient transaction processing for the farm records. The system will be scalable for future data collection although this will mean a change in the hardware requirements too.

This project can also be improved in the future through following steps:

- The distributed networking system can be implemented with the help of customized hardware to create a complete peer-to-peer system in which every node can talk to every other node.
- Encryption algorithms can further be implemented to ensure more security of the files on which the data is being stored.
- Complete linking of the client-server script of Python and the main C++ code can be done using third party libraries and development environments to create a more efficient project.
- For further improvements in the future, the data too can be distributed among different chains divided into the zones with each zone having a localized chain. This can be completed in future work on this project.

8. References

- [1] Food Safety Traceability System based Blockchain and EPCIS: Qijun Lin, Huaizhen Wang, Xiaofu, Junyu Wang <https://ieeexplore.ieee.org/abstract/document/8640818#full-text-header> (2018)
- [2] Yu-Pin Lin, Joy R. Petway, Johnnathen Anthony, Hussnain Mukhtar, Shih-Wei Liao, Cheng-Fu Chou and Yi-Fong Ho: Blockchain: The Evolutionary Next Step for ICT E-Agriculture <https://www.mdpi.com/2076-3298/4/3/50/htm> (2017)
- [3] Use of Blockchain Technology in Agribusiness: Gavina Baralla, Andrea Pinna, Giacomo Corrias https://www.researchgate.net/profile/Andrea_Pinna4/publication/331564321_Ensure_Traceability_in_European_Food_Supply_Chain_by_using_a_blockchain_System/links/5c80ee22299bf1268d4080c6/Ensure-Traceability-in-European-Food-Supply-Chain-by-using-a-blockchain-System.pdf (2018)