Block Chain in Food Supply Chain

Shubham Tiwari[1] Vidyanshu Kumar Mishra[2] Akshay Kumar Mishra[3] Abhishek Jaideep[4]
[1,2,3,4]Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract— With the increase in the complexity of the industrial food supply chain, the traceability is becoming scarce. It has becoming a tedious and costly task to trace the processing of a packed product , as the data is stored in the relational databases it is quite easy to tamper the data stored in the database through an unauthorized access. To tackle all these issues and address the problem of traceability Blockchain is a suitable technique to store the data in the database. By making the use of blockchain we can generate a ledger where each processing unit will make the transactions in the system and all the data related to the processing of product made at that unit is appended easily to the blockchain. By doing this, we are creating a tamper free ledger which is used to trace the processing details of the product in a really fast and cost effective manner. We are here, creating a peer to peer network of different systems which will keep on making the transactions and the data will be stored in the ledger. A server will be there to monitor the transactions and to trace the product details if requested by the system administrator or by the end user. There will be a backup server also which will take the command of the requests once the main server becomes down and it also maintains a copy of the whole data. In this way it is feasible to trace the processing details of a product, once unique identity of the product is provided to the server.

Keywords: Block Chain, Food Supply Chain

I. INTRODUCTION

Let's take an example of Google spreadsheet or MS Excel (Windows). This spreadsheet is shared among different networks of computer, where everyone has copy of it. The spreadsheet contains information of the transactions committed by real people. Anyone can access that spreadsheet but no one can edit it. This is Blockchain. It works with Blocks, whereas spreadsheet works with "rows" and "columns".

A block in a blockchain is a collection of data. The data is added to the block in blockchain, by connecting it with other blocks in chronological others creating a chain of blocks linked together. The first block in the Blockchain is called Genesis Block. Blockchain is a *distributed ledger*, which simply means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

Some key attributes of Blockchain are which proves that blockchain is better than traditional systems of ledger information keeping:

1) Peer-To-Peer: No central authority to control or manipulate it. All participant talks to each other directly. This allows for data exchange to be made directly with third-parties involvement.
2) Distributed: The ledger is spread across the whole network which makes tampering not so easy.
3) Cryptographically Secured: Cryptography is used for the security services to make the ledger tamper-proof.
4) Add-Only: Data can only be added in the blockchain with time-sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable. We can say it has: "*The right to be forgotten* or *right to erasure"* defined.
5) Consensus: This is the most critical attribute of all. This gives blockchain the ability to update the ledger via consensus. This is what gives it the power of decentralization. No central authority is in control of updating the ledger. Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.

A. How Does It Work?

1) A node starts a transaction by first creating and then digitally signing it with its private key (created via cryptography). A transaction can represent various actions in a blockchain. Most commonly this is a data structure that represents transfer of value between users on the blockchain network. Transaction data structure usually consists of some logic of transfer of value, relevant rules, source and destination addresses, and other validation information.
2) A transaction is propagated (flooded) by using a flooding protocol, called Gossip protocol, to peers that validate the transaction based on preset criteria. Usually, more than one node is required to verify the transaction.
3) Once the transaction is validated, it is included in a block, which is then propagated onto the network. At this point, the transaction is considered confirmed.
4) The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.
5) Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in a network are required to consider the transaction final.

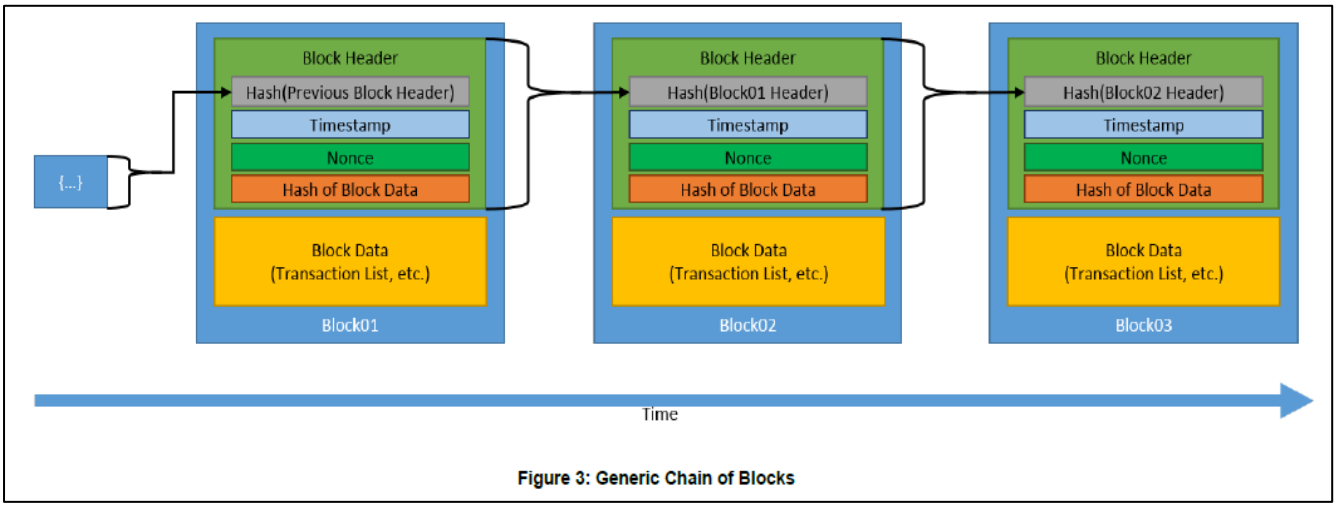


Figure 3: Generic Chain of Blocks

II. P2P(PEER TO PEER) FILE SHARING

A. INTRODUCTION

In Computer Networking, P2P is a file sharing technology, allowing the users to access mainly the multimedia files like videos, music, e-books, games etc. The individual users in this network are referred to as peers. The peers request for the files from other peers by establishing TCP or UDP connections.

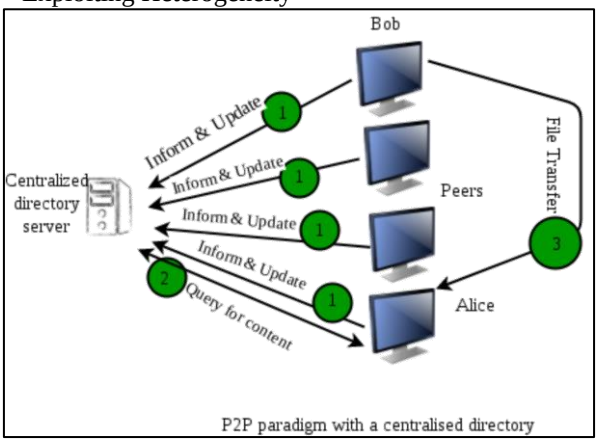
B. HOW P2P WORKS?

A peer-to-peer network allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture, there is no central server for processing requests in a P2P architecture. The peers directly interact with one another without the requirement of a central server.

Now, when one peer makes a request, it is possible that multiple peers have the copy of that requested object. Now the problem is how to get the IP addresses of all those peers. This is decided by the underlying architecture supported by the P2P systems. By means of one of these methods, the client peer can get to know about all the peers which have the requested object/file and the file transfer takes place directly between these two peers.

C. THREE SUCH ARCHITECTURES EXIST:

1) Centralized Directory
2) Query Flooding
3) Exploiting Heterogeneity



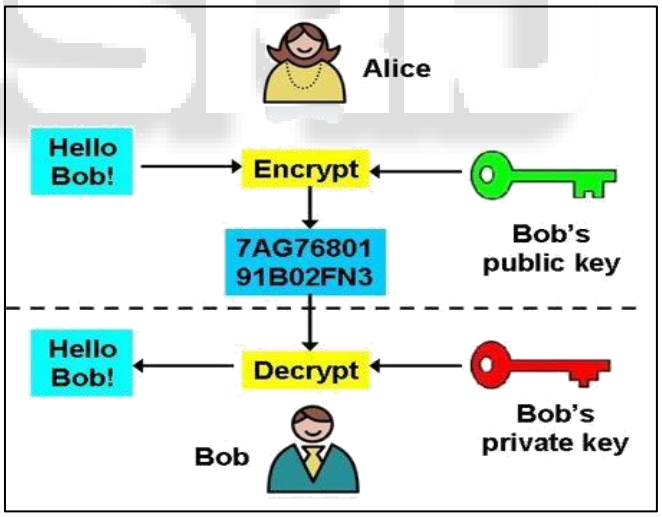
P2P paradigm with a centralised directory

III. CRYPTOGRAPHY

Cryptography is the practice of developing protocols that prevent third parties from viewing private data. Modern cryptography combines the disciplines of math, computer science, physics, engineering, and more.

Some important terms are defined below:

- Encryption: Encoding text into an unreadable format.
- Decryption: Reserving encryption – converting a jumbled message into its original form.
- Cipher: An algorithm for performing encryption or decryption, usually a well-defined set of steps that can be followed.



A. Public-key cryptography

It is a cryptographic system that uses a pair of keys – a public key and a private key.

The public key may be widely distributed, but the private key is meant to be known only by its owner. Keys are always created in a pair every public key must have a corresponding private key.

Let's say Alice wants to send message to Bob:

- Alice uses Bob's public key to encrypt the message.
- Alice sends the encrypted message to Bob – if a third party intercepted it, all they would see is random numbers and letters.

– Bob uses his private key to decrypt and read the message.

The algorithms which we are going to use in the proposed model is RSA algorithm. It is really helpful for the low scale system cryptography and is very efficient in terms of the memory and the processing resources. SHA algorithm was also an option but it comes with so many demerits and disadvantages which can affect the efficiency of the running system. Since we are dealing with the real time production industry even the minutes of delay can cause a great loss to the company so to be on a safer side we opted to use the RSA algorithm. In return we observed in the proposed system.

B. RSA algorithm (Rivest-Shamir-Adleman)

Public key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys -- one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm Encryption strength is directly tied to key size, and doubling key length can deliver an exponential increase in strength, although it does impair performance. RSA keys are typically 1024- or 2048-bits long, but experts believe that 1024-bit keys are no longer fully secure against all attacks. This is why the government and some industries are moving to a minimum key length of 2048-bits.

C. Problem of Traceability

The main issue of supply chain is lack of Traceability, or the ability to track the food product through all stages of the supply chain. Many consumers now want to know from where all products and their ingredients come from. Traceability problem is also faced within an organization. If an organization wants to get the complete processing detail of a product which was developed long ago then they have to invest huge amount of money to get the detail. This causes loss to the organization. And even then also, it is not guaranteed that we could pin point the exact details of a product which was processed some time ago. The main reason behind this problem is the conventional data storage mechanisms in the production industry which uses human dependent registers and Relational Databases, sometimes it is observed that many industries are using flat files to maintain the product processing data. The data in the flat files becomes vulnerable and can be easily corrupted with human intervention.

D. Solution

The problem of traceability in supply chain can be solved using Blockchain. We propose to develop an application through which the user can get all the details of the product that is the whole cycle of the product from farm to his/her hand. The application can also be used by the organization in its operations like getting the history of a product which was manufactured long ago in very less time.

When we are using blockchain we can fully ensure that the data stored within our model is tamper proof, which means the data stored in such a manner that it cannot be altered with the efforts of someone who is not authorized to alter the data manually. The hashing techniques are used which are one way hash functions and are efficient from shielding the sensitive data from any malicious access. Document store model of NoSql is preferred over flat files which gives us ease of access in handling the data and making the transactions in order to log the data in the form of block in our blockchain network. This approach is also used to append new blocks.

E. Mathematical model

1) Dependent Variables:

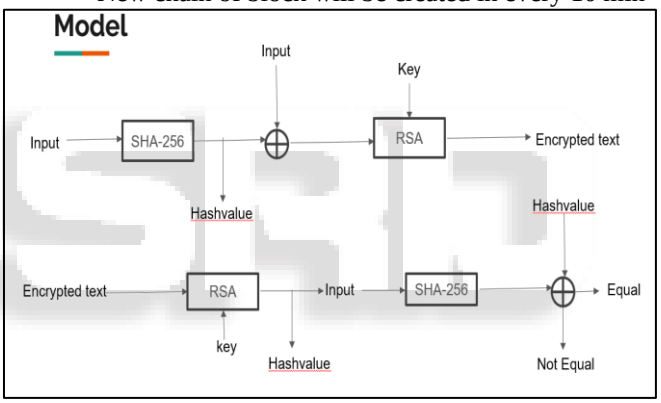
– Hash value generated
– Encrypted text generated
– Final status

2) Independent Variables:

– Block id
– Block creation time
– Block creation date

3) Assumptions

– New chain of block will be created in every 10 min



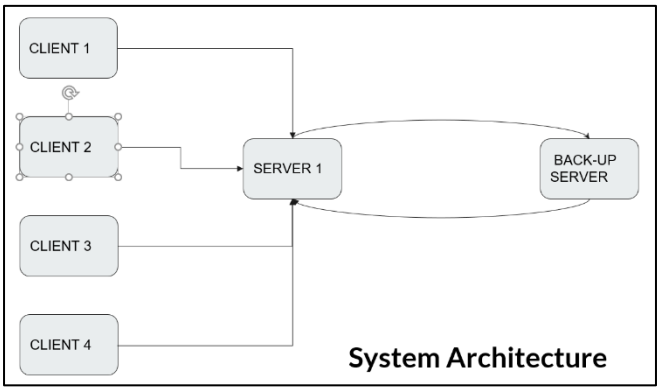
IV. SHA-256

SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.A sha256 is 256 bits long -- as its name indicates. The larger the key the stronger hash value will be generated. The key can be any length. However, the recommended size is 64 bytes. If the key is more than 64 bytes long, it is hashed to derive a 64-byte key. If it is less than 64 bytes long, it is padded to 64 bytes.

By combining these two algorithms with our proposed model we developed a Web based application which is used to maintain the transactional data of different industrial processes running in an production industry and also the data related to the raw material and till the final product is processed is appended in the block chain and it can be accessed with proper authority just by few clicks which makes it highly traceable.

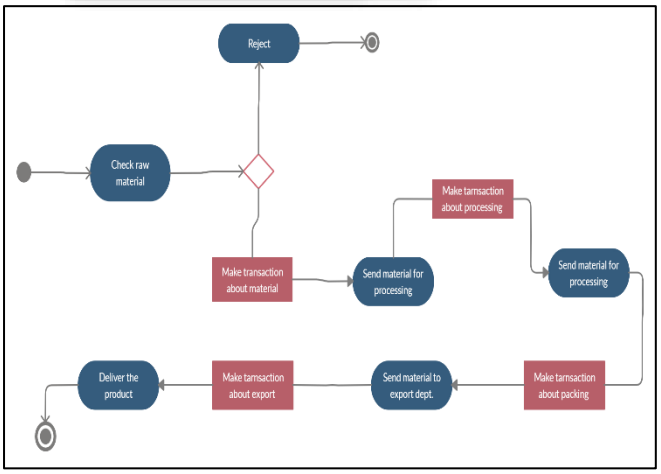
V. SHIP CHAIN: THE WEB APPLICATION

Our combined efforts on the research which we have presented above yielded a efficient and optimized web application to manage the transactional data of a product. The whole journey of the product from it being a raw material to a fully processed product and the data related to it is appended in the datastore which is based on block chain.



For achieving this functionality we need to setup the client stations at every processing unit and we will append the data related to the current batch of the product to the server which will be centrally hosted in the organization. Server will have all the authority to publish the blocks in the blockchain. The client nodes will request for the ID of the current lot and when they get associated with the ID then they send all the product related data to the server, upon verifying the cryptography keys the server publishes the data received from the client nodes to the blockchain. Each block published to the ledger will have its unique id and data is stored in an encrypted format such that it cannot be tempered once it is published.

VI. ACTIVITY DIAGRAM



VII. FUTURE SCOPE

This system can be employed by the production industries in order to trace the processing details of a product which is already processed and packaged. Transparency can be achieved and hence increase in the profits of the firm.

In order to trace the details, a unique number is attached with every product and when that unique number is entered in the system then the system looks for the values associated with that key and fetches the information to the user.

Statistical analysis can also be done with the help of the proposed model and the efficiency of the different processing units can also be determined

Sources can be identified on the basis of quality, the sources from where good quality products are packaged can be marked as genuine class of sources.

VIII. CONCLUSION

On the concluding notes, we proposed a web based cryptographic solution to solve the problem of traceability in the food supply chain. The proposed web application can be used to log the transactional data from a food processing industry and it is stored over a blockchain ledger in a tamperproof manner. The algorithms used to solve the problem are RSA and SHA256, there were no significant changes made to the original approach of the problems. The web application can be setup by different client and a single server node, the server node has all the authority to publish blocks on verifying the authenticity of the data received from the client nodes.

REFERENCES

[1] Blockchain Security and Relevant Attacks, Joanna Moubarak, Eric Filiol, 2018
[2] A Concept Framework for Agri-Food Supply Chain Integration in China, Juan Xu, DeBin Zhang
[3] Blockchain Application in Food Supply Information Security, Daniel Tse, Haoran Mu, 2018
[4] Challenges in the Management of Food Products Supply chain, Aleksandra PABIAN
[5] Blockchain-based Traceability in Agri-Food Supply Chain Management, Muhammad Salek Ali, 2017
[6] Blockchain In supply chain (https://hackernoon.com/how-is-blockchain-disrupting-the-supply-chain-industry-f3a1c599daef)
[7] (https://blockgeeks.com/guides/blockchain-and-supply-chain/)
[8] Supply chain problems(https://www.dataversity.net/blockchain-solution-underlying-issues-supply-chain-management/)

