Supply Chain Management using Blockchain

Submitted by
Shaikh Sahil Ahmed (192474)
Mahesh Kankar (192599)

Abstract

Supply chain management is the management of the transfer of goods and services and includes all processes that generate raw materials into finalized products. During older days, the supply chain management doesn't have any security and there was no trust between manufacturers and other stakeholders that could provide security. So the emerging technology of blockchain helps to overcome most of the problems in the supply chain. In our work, we have provided the trust as well as security among suppliers and receivers. The transactions are well secured and are immutable. We can also trace the item from whom it was supplied to which customer.

1. Introduction

Blockchain is an emerging technology which has attracted almost all areas of the IT industry, Supply Chain management is one of them. Asset transfer from one place to another place needs to keep tracking from origin to delivery point. When a product is handovered from one person to another it is important to the identity of the receiving person as well as he should know where the given product has to be delivered and so on.

Supply Chain using blockchain not only handles the issue of managing the people involved who are responsible for product delivery but also provides many functionality such as Immutability, transparency, real time tracing of product and much more. There is a chain from raw material of product to manufacturing industry to wholesaler to retailer to end user. We need to maintain this chain of connection and blockchain solves all issues involved in this.

2. Key Features

1. **Data transparency**: Blockchain technology allows for a highly transparent network that is visible to each stakeholder at all times. This dramatically reduces the chances of illegal transactions.
2. **Immutable data**: Once a block with a set of transactions is verified by the consensus and stored in the chain, the encapsulated data can no longer be

modified.

3. **Enhanced data security**: Blockchain technology utilizes asymmetric cryptography to ensure data security and individual identity.

4. **Versatile value exchange**: Blockchain provides a secure and efficient platform for recording the transactions of intellectual property rights, the provenance of services and goods, asset ownership, cryptocurrency exchange, and more.

3. Methodology

Public-private key based chain system developed where for making the transaction supplier need its private key and it also need the public key of the receiver. All party people communicate through their keys. The public key of them is publicly available but everyone has privately maintained private keys which are used when they perform the transaction. When the manufacturer adds an item to the database it first stored in the UTXO array after collecting a few number of transactions it will be mined and will be added to the blockchain.

3.1 Architecture
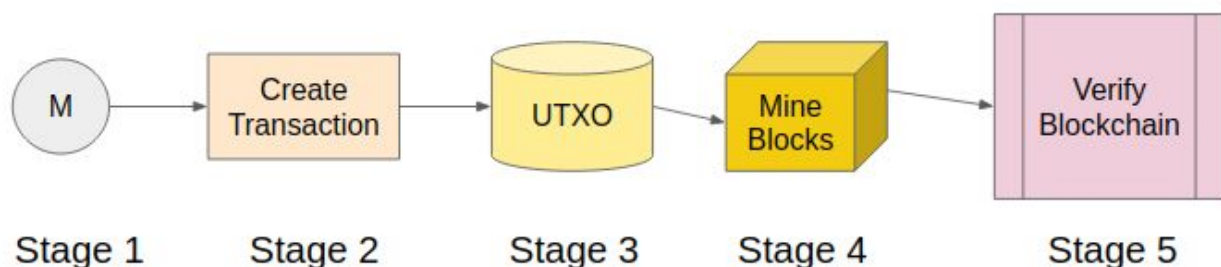
- Stage 1: There is a miner (owner of the company) and various manufacturers, stakeholders through which the product will be supplied.
- Stage 2: If a person has ordered any product or item from the company, that person will be given a product ID of that ID that he/she has bought. So, against that product the transaction will be created.
- Stage 3: Multiple people who bought items from the company their transactions will be forwarded to UTXO (Unspent Transaction Output).

- Stage 4: When the miner mines the block, some random amount of transactions are being taken and verified and added into a block after a certain amount of time.
- Stage 5: After collecting the blocks, they are added to the blockchain and verified.

3.2 Consensus

An agreement between nodes in a blockchain network that submits transactional information, and is one of the most critical components of blockchain technology. A blockchain network is updated via the deployed consensus protocol to ensure that transactions and blocks are ordered correctly, to guarantee the integrity and consistency of the distributed ledger, and, ultimately, to enhance trust between stakeholders (nodes). In our project as based on our interest we have implemented a Proof of Work Consensus algorithm.
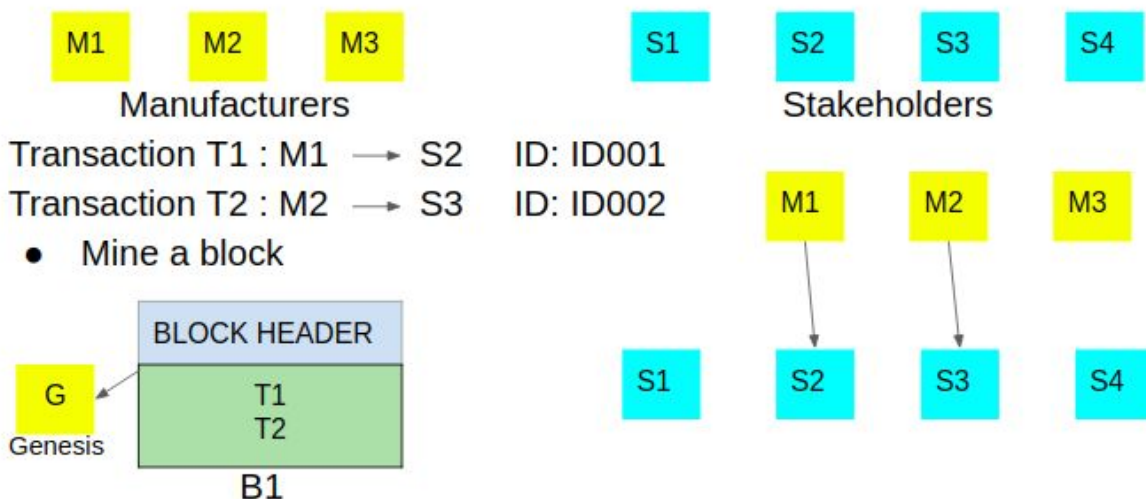
3.2.1 Proof of Work

The implementation of proof of work uses SHA 256 hash function. The miner collects the transaction and starts mining the Proof of Work.

3.3 Example

Considering the architecture and all the points, let us understand with the example given below.

For number of manufacturers as 3 and Stakeholder as 4.

Suppose there are 3 manufacturers and 4 stakeholders. Manufacture M1 created a

transaction T1 with transaction id ID001 to stakeholder S2 and manufacture M2 created a transaction T2 with transaction id ID002 to stakeholder S3. The transactions are now available in UTXO. Further they are mined and added in the block and after that the block is added to the blockchain.
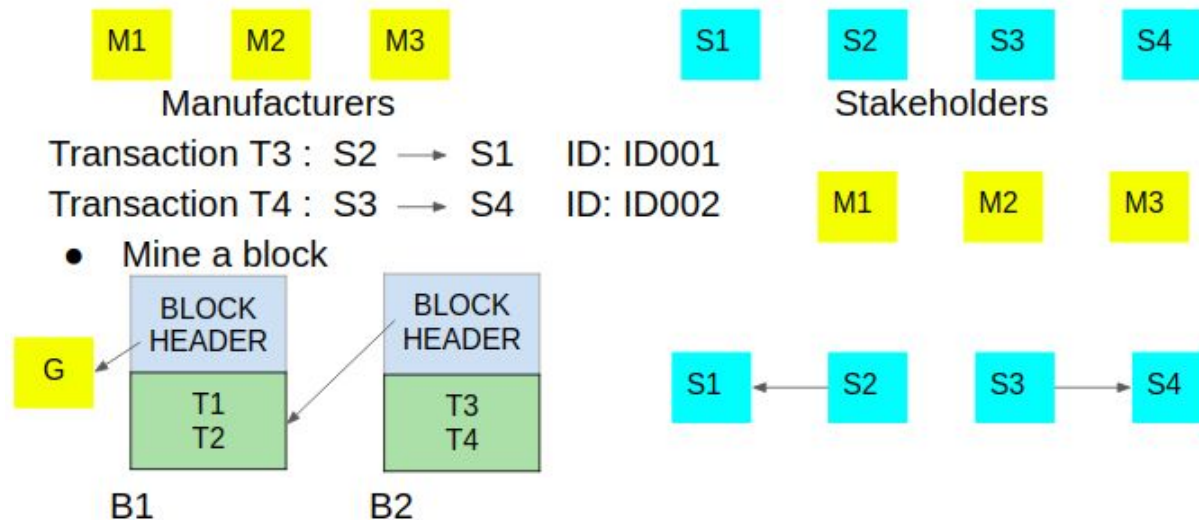
After that there is a transaction where stakeholder S1 created a transaction T3 with transaction id ID001 to stakeholder S1 and stakeholder S3 created a transaction T4 with transaction id ID002 to stakeholder S4. Similarly as of earlier, the transactions are now available in UTXO. Further they are mined and added in the block and after that the block is added to the blockchain.

If the track item has ID "ID001", the tracker shows that the M1 supplied the item to S2 and then S2 supplied the item to S1.

If the track item has ID "ID002", the tracker shows that the M2 supplied the item to S3 and then S3 supplied the item to S4.

3.4 Functionalities

The functionalities present in the project that are available to the user are as follows:

1. View the blockchain.
2. Enter a transaction.
3. View the UTXO array.
4. Mine a block.
5. Verify the blockchain.
6. Generate RSA keys.
7. Track an item.

1. View the blockchain: This functionality shows the information about the blockchain such as inde, timestamp, supply data, proof of work, hash and previous hash.

2. Enter a transaction: For each of the transactions being added to UTXO, an product id to the related item bought by a person will be recorded. The transaction may be from "one manufacturer to other manufacturer" or "one manufacturer to other stakeholder" or "one stakeholder to other manufacturer" or "one stakeholder to other stakeholder". For transactions the supplier public key will be encrypted by SHA 256 hash algorithm and the new transaction will be created supplier_puk, receiver_puk, item_id, timestamp, and signature. An example for transactions is shown below.

> Select type of key (M/O) for supplier: M
> There are a total of 3 users. Enter your selection: 1
>
> Select type of key (M/O) for receiver: O
> There are a total of 4 users. Enter your selection: 1
> Enter the ID of the tracked item: ID1

The above transaction shows the supply of item from Manufacturer (M) to stakeholder (O) with the item ID "ID1".

3. View the UTXO array: All the pending transactions are added to UTXO and further they will be mined such that the transaction will be added to the blockchain.

4. Mine a block: In this functionality, some random transactions from the UTXO are taken and mined and added to a block.

5. Verify the blockchain: The item id and hash values of the current as well as the previous hash are verified.

6. Generate RSA keys: RSA keys are generated for the manufacturers and stakeholders. The keys generated can be used for further transaction between the manufactures and the stakeholders.

7. Track an item: By this option an item can be easily tracked while giving an input of item id. The whole history of the item is fetched from which to which person the item is going through.

4. Conclusion and Future Work

Blockchain based supply chain is created which provide the some outstanding functionalities such as non updation of transaction once it has happened, which is an advantage in sense of temper proof data,it also enables the users to let them track their item that what is the status means which person holds the item now and what is the approximate time to reach the item to the destination.it also reduces the paperwork and maintain the history data that is publicly available.

5. References

[1] Blockchains and Smart Contracts for the Internet of Things

[2] https://www.edureka.co/blog/interview-questions/blockchain-interview-questions/
[3]https://consensys.net/blockchain-use-cases/supply-chain-management/#:~:text=Supply%20chain%20traceability%20is%20one,physical%20product%20throughout%20its%20lifecycle.

[4]https://www.capgemini.com/wp-content/uploads/2018/10/Digital-Blockchain-in-Supply-Chain-Report.pdf

[5]https://www.goodworklabs.com/blockchain-in-supply-chain-industry/