

Blockchain for Sustainable Supply Chains

INTRODUCTION

Blockchain is a distributed digital database containing a chronological chain of records stored in encrypted form (using encryption algorithms) to ensure security. It is a shared, immutable digital code that can be used to track transactions and assets across a business network. A distributed ledger is shared transparently among blockchain participants, and a consensus algorithm is used to ensure that transactions are completed once confirmed by all network partners. Once a new transaction is recorded on the blockchain, it cannot be changed, ensuring security and preventing unauthorized access.

Supply chain can be defined as the production process of a product or service that begins with the collection of raw materials from suppliers and the delivery of finished products from the manufacturer to consumers. Sustainable supply chains integrate ethical and the environment friendly practices at every level of to create a competitive and successful model. Effective product quality control is essential to ensure that product quality meets required standards at all levels without causing any environmental degradation. As demand for products increases and production increases, a focus on speed, reliability, and operating costs, as well as the need to manage the environment and material ethics, has led to the creation of sustainable and ethical supply chains. This includes addressing global challenges such as climate change, water security, deforestation, human rights, fair labour treatment and corruption.

The decentralized, secure, transparent, immutable, and consensus-based characteristics of blockchain technology make it suitable for sustainable supply chain management. All activity on the chain can be tracked by recording transactions on the blockchain.

KEY FEATURES

Blockchain features make it suitable to be applied to the supply chain for monitoring the proceedings in real time efficiently:

- **Immutable:** Every transaction recorded in the blockchain being immutable helps to maintain permanent unalterable transaction records in the supply chain which can be referred in future for analysis to modify production practices optimize revenue generated.
- **Distributed ledger:** All nodes in the peer network have the same copy of the distributed ledger, hence same version of transaction information is available to every network participant. Complete transparency thus achieved in the blockchain prevents any invalid transaction or unethical activity in the supply chain.
- **Decentralised:** In a blockchain, every node has equal authority in the distributed network. A new transaction before being appended to the blockchain is verified by each node and added only after validation from all nodes. Any change in the blockchain is quickly reflected in the ledger after validation from the nodes, without involving intermediaries thus ensuring real time monitoring of supply chain.
- **Secure:** Every transaction in the blockchain is stores in encrypted form preventing unauthorised access to supply chain details. All blocks are uniquely identified by a hash value. Every block stores the hash value of the previous block, thus linking the blocks cryptographically.
- **Consensus:** Consensus algorithm is used to ensure all nodes agree to a common version of the transaction information. New transaction after verification and validation gets added to the blockchain by a single node as decided mutually by all nodes and this node called miner gets a reward signifying proof of work. Supply chain transactions are thus performed and added to the blockchain without duplication.
- **Transparency:** Distributed ledger makes the transaction details accessible by all network nodes creating highly trusted system.

A standard supply chain involves the following key stages:

- **Planning:** This stage integrates strategy development for elaborate analysis of statistics to understand customer demand, followed by production planning and material requirement planning.
- **Sourcing or Procurement:** The production of goods or services planned requires raw materials from reliable suppliers who provide good quality raw materials at reasonable prices, ensuring product quality without violation of ethical standards or environmental degradation.
- **Production:** The procedure appropriate for manufacturing the target product with the procured raw materials is decided and followed.
- **Inventory management:** The final products are transported from the manufacturers to the warehouses for storage followed by delivery to the retailers.
- **Logistics:** Logistics involves transportation management and warehousing. Planning, optimising, and executing the use of suitable transport for the movement of goods between warehouses, retailers, customers is important to prevent any damage due to mishandling. Warehouse management involves handling the warehouse infrastructure to keep track of the movement of stored goods, monitor the storage conditions, examine the quality of products and so on.

Every stage of supply chain requires ensuring that product quality standards are maintained. In addition, sustainable supply chains also ensure the environment is not degraded such as release of toxic gases, use of adulterated raw materials due to any of the supply chain processes and ethical standards are not violated such as practise of child labour, inappropriate working conditions etc.

Blockchain technology can be applied to each stage of the supply chain to monitor transactions and maintain immutable records free from any duplication and unauthorised access thereby achieving economic, environmental, and societal sustainability.

BLOCKCHAIN WORKING

The basic workflow of blockchain involves:

- **Facilitating a new transaction:** When a new transaction occurs, it needs to be appended to the existing blockchain. All the associated information is doubly encrypted with public and private keys to be transmitted to the blockchain network.
- **Verification of new transaction:** The new transaction information thus transmitted to the distributed network of nodes is verified for validity such as predefined standards are followed, sufficient balance is available to carry out the transaction etc. This enhances transparency and security of the network.
- **Creation of new block:** Multiple transactions can be verified and validated as legitimate simultaneously. All verified transactions at a blockchain node form a mempool and multiple mempools constitute a new block, which is immutable and highly secure.
- **Consensus Algorithm:** Every node attempting to append the new block can disrupt the of the blockchain. A consensus algorithm is used to ensure only a single version of the valid block is connected to the blockchain unanimously agreed by all the network nodes. The consensus algorithm adds a unique identifier to the block called hash. The node selected to add the new block gets a reward as proof of work and is called miner.
- **Addition of new node:** After receiving the hash value, the newly authenticated block is added to the existing blockchain. The new block also contains hash value of the previous block, thereby cryptographically linking blocks in the blockchain together.
- **Transaction completed:** The addition of new block marks the transaction completion and details of transaction are permanently stored in the blockchain to be used for reference in future by the network nodes.

METHODOLOGY

A public-private key based blockchain is created to monitor transactions in a supply chain. In order to make a new transaction, supplier will need its private key and the public key of the receiver. The communication among different supply chain participants occurs via keys. The participants' public keys are publicly available while their private keys are utilized to make transactions. When the manufacturer adds a new item, it is initially added to the UTXO array.

A Proof of Work based consensus algorithm is applied to ensure consistency in the blockchain records. After adding and verifying a few transactions, the block is mined and the transactions are added to the block. Finally, after verification the newly created block is appended to the blockchain.

Basic workflow:

- The supply chain participants include the product developer, manufacturers, retailers, and suppliers.
- Whenever an order is placed, a product ID for the product is used to create transaction against the product.
- Transactions for multiple orders placed for the product are added to the UTXO (Unspent Transaction Output).
- When a block is mined by the miner, some transactions are taken for verification and then added to the block.
- Some blocks are thus collected and then added to the blockchain after verification.

Proof of Work based Consensus Algorithm:

- Consensus algorithm used in a blockchain ensure that all peers in the blockchain network unanimously agree on the current state of the distributed ledger.
- Every new block added to the blockchain is the only version of the transaction recorded, eliminating duplication, and enhancing the trust and integrity of the blockchain network.
- In this project, proof of work-based consensus algorithm is applied.
- Mining: This involves solving a computationally complex mathematical challenge to add new blocks to the existing valid blockchain, called mining and the participating nodes are known

as miners. When a miner finds correct solution and broadcasts to the entire network, it receives a reward as incentive.

- Energy and time consumption: The time and energy consumed in verification of the new block transactions, arrangement in chronological order and announcement to the network is less than that during mining.
- The implementation of proof of work has used the SHA256 hash function.

Project Functionalities:

- View blockchain: Information about current state of the blockchain such as timestamp, supply data, hash values of present and previous blocks can be viewed.
- Enter transaction: For each new transaction, either between two suppliers or supplier and manufacturer or two manufacturers etc, product ID of the related item is recorded in the UTXO array. The transactions are encrypted using SHA 256 hash algorithm. The new transaction is recorded with supply_puk, receiver_puk, timestamp, item-id and signature.
- View UTXO array: The pending transactions get recorded here and can be viewed. These transactions are then mined and new block appended to the blockchain.
- Mine a block: A random number of transactions from the UTXO array are mined and added to a block.
- Verification of blockchain: The item id and hash values of current and previous block are verified.
- Generate RSA keys: RSA encryption keys generated for manufacturers and stakeholders for future transactions.
- Track item: This feature enables monitoring any item using its item id, which provides entire information about the item.

Sustainable and ethical supply chains can thus be achieved by allowing the stakeholders to keep track of all transactions performed throughout the supply chain. The use of blockchain technology creates a highly secure, trusted network.

CONCLUSION

Sustainable and ethical supply chains can thus be designed using blockchain technology. The use of blockchain technology to store information about the transactions performed throughout the supply chain network enable the product developers to closely monitor the proceedings at every stage in real time as every newly added recorded is available to the distributed network nodes instantaneously. Any new transaction when performed, its details are appended to blockchain only after collective approval from every network node. This prevents activity that violate sustainability or ethical standards.

