Supply Chain in Blockchain–a Review

Preyas Hanche
B.Tech Student
NMIMS MPSTME
Computer Department
Mumbai, India - 400062
hanchepreyas@gmail.com

Akash Dubey
B.Tech Student
NMIMS MPSTME
Computer Department
Mumbai, India - 400092
akash1999dubey@gmail.com

Ayush Falor
B.Tech Student
NMIMS MPSTME
Computer Department
Ahmedabad, India - 380015
ayushfalor13@gmail.com

***Abstract*—The blockchain technology acts as a foundation for distributed ledgers and an innovative platform for a new decentralized and transparent transaction mechanism in industries and businesses is offered by it. Supply chain traceability is impacted by growing consumer awareness and manufacturers internal quality requirements. When multiple parties are involved, existing centralized solutions suffer from isolated data storage and lacking trust. Decentralized blockchain-based approaches facilitate to forestall these issues by making digital representations of physical goods to facilitate tracking across multiple entities. The potential advantage of this emerging technology in manufacturing supply chain is then discussed and a vision for the future blockchain ready large scale manufacturing supply chain is proposed. Ultimately, a discussion of the requirements and challenges to adopt this technology in the future manufacturing systems is done.**

***Index Terms*—Keywords - blockchain; supply chain management; smart contracts; distributed ledger**

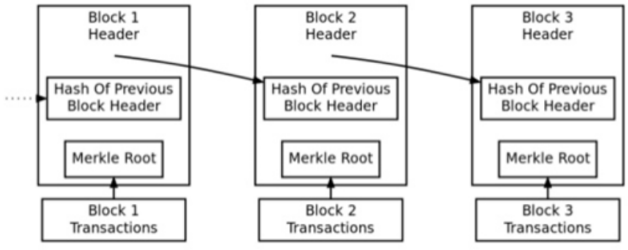
I. Introduction

Marking the dawn of a new era, Blockchain technology is a ground-breaking innovation in the industry of decentralized information technology. First invented as part of Bitcoins underlying infrastructure in 2008, its potential application reaches far beyond digital currencies and financial assets. The technology is still in its early stages and is yet to reach mainstream and enterprise adoption. As the technology gained wider recognition in recent years, there has been a flurry of advancements, new use cases, and applications. The range of potential applications of Blockchain technology is endless, from digital currencies to Blockchain enabled legal contracts with the most promising of applications yet to be developed. Providing traceability of goods from resources to retailer has become increasingly important in the past decade. Consumers have a larger interest in consuming goods that comply with certain ecological and ethical standards. Global supply chains have become complex to a greater extent, hampering quality management in manufacturers procurement. Furthermore, regulations, international standardizations an increased consumer awareness imply novel requirements towards supply chain management systems. Current blockchain-based solutions for supply chain traceability promote tracking goods over multiple tiers by utilizing markers such as RFID and QR codes. This linkage mechanism enables proving provenance for anti-counterfeit with regard to high value goods such as diamonds, medicine or generally in the post-retail supply chain. With the development of the economy worldwide, new emerging markets and constant evolution of technology, We have derived better ways for operatibility and management of the electronic data, business to business integration as well as customer satisfaction. Supply Chain is one such necessity that is implemented. It is essentially the connections of all the individuals, organizations, resources, activities and technology involved in the creation and sale of a particular product, from the delivery of raw materials from the supplier to the manufacturer, through to its eventual delivery by the retailer to the end user. Supply Chain Management is the management of such chain to ensure the availability of products/services in a timely, controlled environment. The integration of Block chain into the supply chain and furthermore, its management is seen as an advancement in both the domains. BCT (Block chain Technology) provides the infrastructure that enables secure direct exchange of value between participants without any nancial intermediary (internet of value).

II. Literature Survey

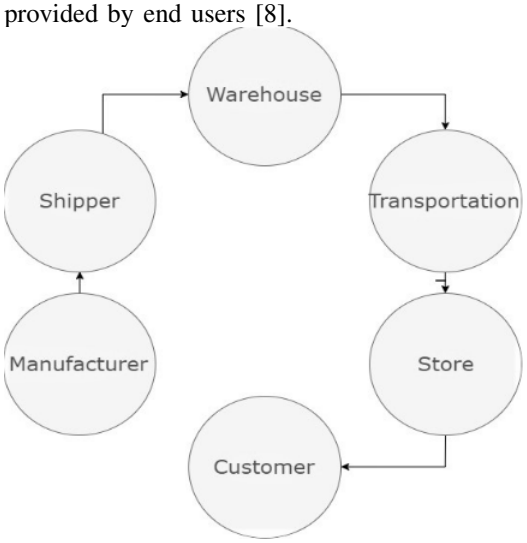
- Blockchain Technology
  In simple words, Blockchain is a ledger distributed amongst multiple peers or nodes and any transaction or interchange of data is simultaneously updated across all the nodes. A blockchain contains a single record of the data which is stored in blocks on every participants node. Each block corresponds to a timestamped record that is veried through a dened consensus protocol of the blockchain network and secured via public-key cryptography or hashing. This helps to mitigate the need for a ever-present central entity. Due to these features, it is also called the trust machine. Since blocks are chained via their hash codes, information on the blockchain is immutable and thus allows the user to obtain provenance information and to trace status changes over time. The blockchain taken as a case study is the Ethereum blockchain. Ethereum primarily uses Proof of Work concept. Ethereums proof of work mining process is used to maintain the Ethereum blockchain and to add a block to the blockchain by a distributed network of nodes. This process requires a miner to retrieve data from a block header to form an input, and then repeatedly hash

that input using a cryptographic hashing algorithm until a fixed-length output hash value is produced. Miners hash variations of the input data by using and adding a nonce. The nonce is essentially an arbitrary number that varies the input data such that the correct output that allows the miner to add a new block to the blockchain can be found. The Ethereum algorithm called Ethash is the hashing algorithm that is used in this proof of work mining process [1]. Miners use computers for each block of transactions to repeatedly guess answers to a puzzle until one of them wins. To elaborate, the miners can run the blocks distinctive header metadata information, including timestamp and firmware version through a hash function which will return a randomised string of numbers and letters of fixed length, , only altering the nonce value, which will change the resulting hash value. If the miner searches for and finds a hash that matches the current target, the miner will be awarded ether and broadcast the block across the network for each node to check and add to their own copy of the ledger. If miner B finds the hash, miner A will stop work on the current block and repeat the process for the next block. It is virtually impossible to counterfeit this work and come away with the correct puzzle answer, which is why the puzzle-solving method is called proof-of-work. On the other hand, it takes almost no time for the nodes to verify that the hash value is correct. Around every 1215 seconds, a miner finds a block. If miners start to solve the hash puzzles more quickly or slowly than this, the algorithm automatically readjusts the difficulty of the problem so that miners start to get roughly the 12-second solution time. For example, when the blockchain trend started in December of 2017, so many servers were trying to mine Ethereum which made the difficulty skyrocket The miners arbitrarily earn these ether, and their profitability depends on luck and the amount of computing power they devote to it. The specific proof-of-work algorithmic program that ethereum uses is called ethash, designed to require more memory to make it harder to mine using expensive ASICs (Application Specific Integrated Circuits) that are now the only profitable way of mining bitcoin.



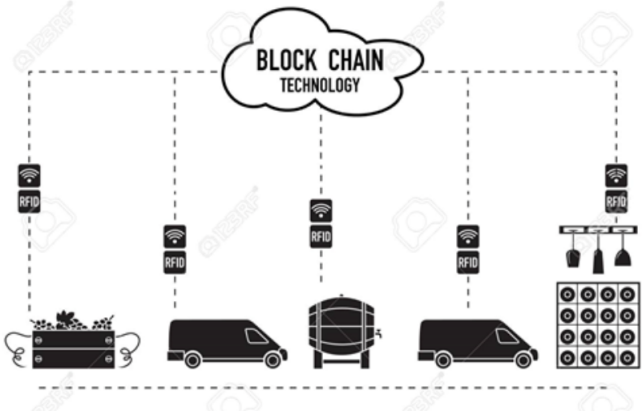
Simplified Bitcoin Block Chain

- Supply Chain Management
  In manufacturing and commerce, supply chain management (SCM), controlling the flow of goods and services, involves moving and storing raw materials, stock of work-in-process, and finished products from point of origin to point of consumption. integrated and intertwined networks, channels and node businesses combine in a supply chain with the delivery of products and services provided by end users [8].

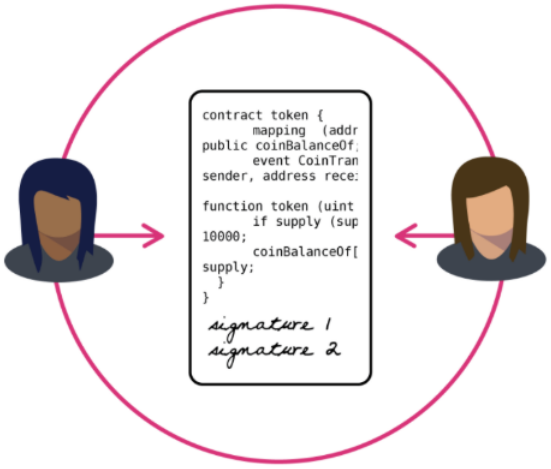


- Supply Chain Management, as defined by the Council of Supply Chain Management Professionals (CSCMP), is (i) planning, implementing, and controlling of primary activities that create and deliver value for the ultimate customer (esp. procurement, manufacturing, and logistics), and (ii) the integration and coordination of corresponding business processes within and across companies. While integration refers to the managerial and organizational challenges of forming a network of mostly independent companies, coordination is concerned with technical implementation of processes and systems to foster alignment of material, nancial, and information ows along the chain. Supply Chain works on the access of information and communication. Research going on in supply-chain management is concerned with topics related to sustainability and risk management, among others. [4].
- RFID with Blockchain
  Introduction of RFlD RFlD (Radio Frequency Identification) is a non-contact automatic identification communication technology. It can automatically identify more than one static or dynamic objects (products in high-speed transit) simultaneously even under poor environment and without manual control. It can also tag, save and manage data of objects through a radio-frequency signal. Compared to bar code, RFID tag technology has a lot of advantages, such as convenience, antipollution, mass-capacity information and recyclable. In the logistics area, RFID has been widely used in production-processing, inventory management, logistics tracing and product anti-counterfeit and so on. With the extensive applications of RFlD, the level of supply chain management has been highly improved. It contains all the information contained in a well designed barcode which is capable of being either actively or passively read electronically through

proximity sensors. The location of the product as well as other parameters are stored in the blockchain from the start of its production or delivery till the end of the production/delivery line.

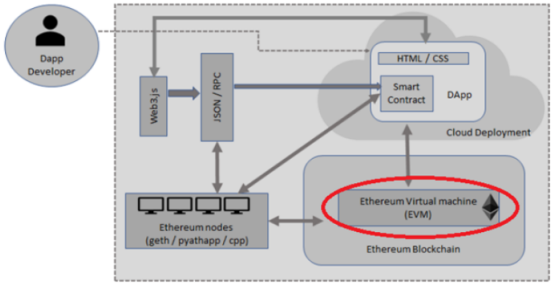


- Blockchain Smart Contracts
  A smart contract is a computer program that controls the transfer of digital currencies (cryptocurrencies or government-issued cash) or assets between parties under specific conditions. A smart contract can define the rules and penalties related to an agreement in the same way that a traditional contract does, on top of that it can also automatically enforce those obligations. It does this by taking in information as input, assigning a value to that input through the rules set out in the contract and executing the actions just like computer code, required by those contractual clauses – for example, determining whether an asset should go to one person or should be returned to the other person from whom the asset originated. A blockchain may execute computational logic in the form of smart contracts (often referred to as chaincode).



A smart contract is a trusted application that is installed on the nodes of the blockchain. With respect to access rights, permissionless and permissioned blockchains can be distinguished. Both of these types can be either private or public depending on the ownership over data and infrastructure. There are two dominant types of blockchains: permissionless-public blockchains are freely accessible via the internet (e.g. Bitcoin blockchain). In permissioned-private blockchains (e.g. Hyperledger Fabric), however, users need to register and are granted access by a network administrator based on a pre-dened approval process.

- Ethereum Virtual Machine
  An Ethereum Virtual Machine (EVM) can be thought of as a Turing-complete machine that processes and executes smart contracts. It is considered as the translator from the smart contract language to the Ethereum nodes. EVM is an abstraction layer above the underlying hardware, which connects the requests (transactions) to the network. Multiple devices and technological concepts have sprouted since the advent of the blockchain technology. The Ethereum Virtual Machine popularly known as EVM is one of such elements that has its root in the blockchain. Its functionality is built around Ethereum blockchain. Ethereums blockchain is programmable, allowing users to create their own operations of different complexity. The Ethereum network allows developers to create decentralized applications, which includes cryptocurrencies but is not limited to this function.



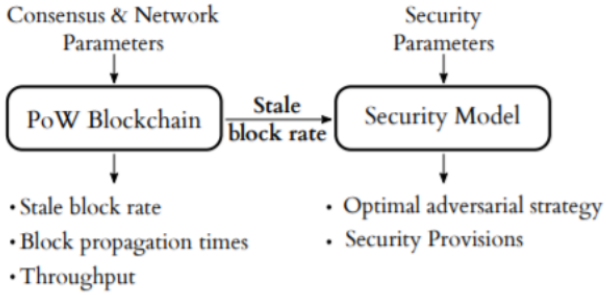
- Connection between SCM and BCT Blockchain provides for many important functionalities which, if included into supply chain eases the its management. It helps to enhance the coordination and integration amongst members of supply chain. Immutability of records and consensus-based verication enable validation of information. Automation refers to the opportunity to execute smart contracts based on veried information on the blockchain. BCT allows creation of tokens that represent a specic claim on any valuable asset and their exchange between blockchain members (tokenization). These features are:

  1) Transparency : One of the biggest drawbacks is the poor end-to-end communication between actors of the supply chain which leads to the Bullwhip effect. The bullwhip effect is an error where the supply chain malfunctions and its inefficiency is displayed.It occurs when a change in collection of products in response to a change in the customer demands as one of the old orders further moves up the

supply chain. Information is shared as the product moves with all vital data such as location, status and other details shared between all stakeholders involved This improves data accuracy enhancing collaborative planning and execution as well as the implementation of preventive and reactive risk management measures.

2) Immutability: Although the shared ledger is transparent, the records contained are immutable. This provides a sense of security where different assets can be traced back to their origin. As information is readily available with each change recorded which helps to prevent counterfeit products and other fraudulent actions. Applications involve asset ownership after sale for warranty purposes. Furthermore, this eases the amount of paperwork involved and fast tracks the process.
3) Orchestration: Combining transparency and validation with automation via smart contracts, one could envision SCs that operate highly automated based on pre-specied rules. This increases speed and eases coordination since information and corresponding decisions.or measures are propagated throughout the supply chain. More specically in the case of a machine failure, the machine could order spare parts from the supplier, request maintenance service, and inform downstream parties about expected delays. Another benefit of automation is the remote requirement of human interaction which is beneficial for both speed of the entire process and also removes any human error involved.
4) Virtualization: Virtualization is a well-known approach in IT infrastructure management to increase utilization and exibility of IT assets by creating a logical representation of physical hardware in software. Tokenization of physical SC assets such as technical equipment and inventories follows a similar idea since there is another opportunity besides shifting acquisition/sale of SC assets to the blockchain. Claims on capacities or ordering options could be issued as tokens and circulated outside normal (bilateral) contractual relationships. This allows for efficient use of assets and assets in tokenized formats can be shared which allows for contractual flexibility.

- Digital Supply Chains and integration with Blockchain
As digital supply chains are becoming dynamic with their customer demand increasing, integration with block chain can be considered as an effective method to keep in the check content, user profiles and sharing of information. Blockchain technology can be regarded as a potential means to improve security and cost effectiveness of transactions. Our aim with this integration is to achieve regularity between all transfers and all collaboration processes in the supply chain keeping all those involved in loop. We wish to deliver goods via this method to consumer without any Time lags and any errors and provide service to a huge network of supply chains. While two organizations may exchange supply chain documents directly via a document exchange platform, specialized intermediate companies are often used to conduct supply chain transactions with a related exchange of documents. There are many limitations while implementing the digital supply chain. To address these limitations, we consider the use of blockchain technology. The following features can be used as potential solutions: a copy of transfers in which we maintain a record of all nodes used , the use of public key infrastructure (PKI) to deploy an encryption which alerts all involved about the aspect of a transfer taking place [9].
- Consensus Layer for governance of Blockchain system
We looked at the most commonly used consensus algorithm used in blockchain system: the proof of work (PoW) consensus mechanism. PoW was introduced by Satoshi Nakamoto with his Bitcoin whitepaper [1] and assumes that each peer votes with his computing power to enforce governance by solving proof of work instances and constructing the appropriate blocks. Bitcoin, for example, employs a hash-based PoW which entails finding a nonce value, such that when hashed with additional block parameters (e.g., a Merkle hash, the previous block hash), the value of the hash has to be smaller than the current target value.



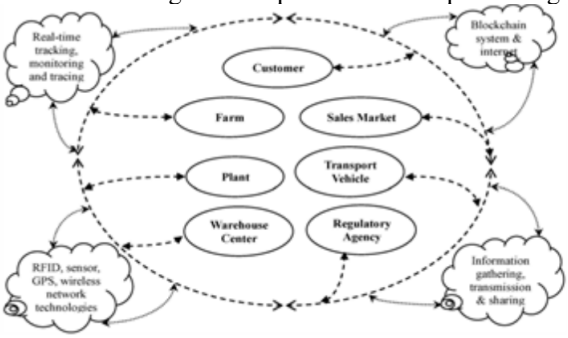
When such a nonce is found, the miner creates the block and forwards it on the network layer. to its peers. Other peers in the network can verify the PoW by computing the hash of the block and check whether it satisfies the condition to be smaller than the current target value. The block interval defines the latency at which content is recorded on the blockchain. The smaller the block interval is, the faster a transaction is confirmed and the higher is the probability of stale blocks. The adjustment of block interval directly relates to the change in difficulty of the PoW mechanism. A lower difficulty results in a larger number of blocks in the network, while a higher difficulty results in less blocks within the same timeframe. It is of utmost importance to analyse whether changing the difficulty affects the adversarial capabilities in attacking the longest chain which is the main pillar of security of most PoW-based blockchains.

This also implies the adjustment of the required number of confirmations that a merchant should wait in order to safely accept transactions (and avoid double-spending attacks).

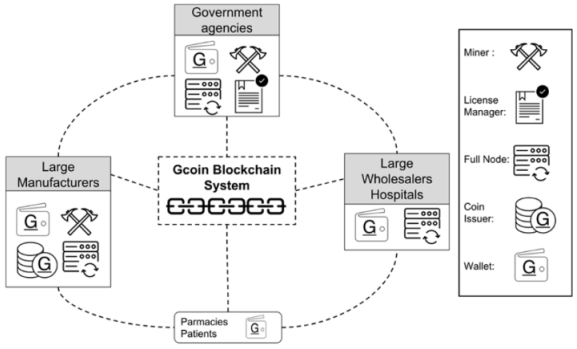
III. Use Cases

We looked at some real life applications involving blockchain that are being used in sophisticated supply chains. As this is a relatively new technology, use cases keep expanding in number as well as form.

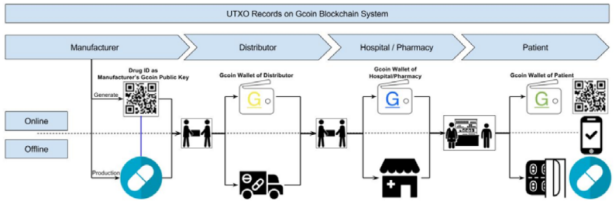
- Application of RFlD technology with blockchain in agri-food supply chain
  Agri-food supply chains including production (planting/feeding), picking/slaughter, processing, warehousing, distribution and sales. In these series of links, the value of the agri-food could be extremely improved by strictly guaranteeing the quality and safety of the agri-food. The agri-food we mentioned in this paper contains two types: fresh fruits vegetables, and meats which include pork, mutton, chicken and beef. The supply chain system being used in field of farming constructed in this review, depends heavily on RFID to implement different aspects of information gathering, distribution and dividing it between different steps involved in farming such as production and processing [7].



- Gcoin Blockchain to govern drug supply chain
  Gcoin blockchain tracks every pill for identification similar to how blockchain performs in Bitcoin. Every giver (seller) and receiver (buyer) in the drug supply chain has its own address (similar to the address in Bitcoin networks). For use in the drug supply chain, we observed the usage of batch or serial number, quantities, and all required drug information to generate a hash number as the public key. This public key could generate a Quick Response code (QR code) as the identification of the medicines (Drug ID).



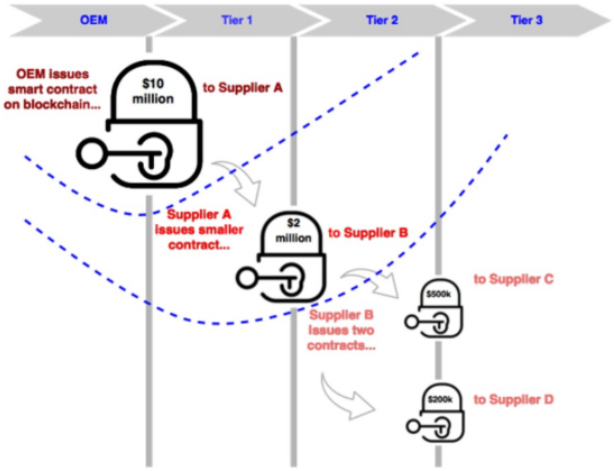
As for a top to bottom drug supply chain (from drug manufacturers to consumers), manufacturers give their transaction data to drug receivers directly, and this data is recorded in the Gcoin blockchain. The transaction data of the digital signatures of the drug seller and buyer, the drug information (including the time stamp, location, item name, etc.), and the amount of drugs are verified on the chain. Then, all of this data is hashed as a digest to be recorded on the Gcoin blockchain. Whenever an illegal distributor wishes to sell counterfeit drugs (with fake Drug ID mentioned above) to buyers, the transaction will be judged invalid because of the presence of fraudulent information about unspent transaction output (UTXO) stored in the Gcoin blockchain. On the other hand, unauthorized personnel would not able to carry out drug transactions in this system without a valid private key. Hence, the buyer as well as seller would be immediately aware of any anomalies within the transactions. Participants of drug supply chains include medicine and drug manufacturers, wholesalers, retailers, pharmacies, hospitals and consumers. As for the hierarchy in the system, the government should monitor transactions and drug information and should take the role of an alliance member in the Gcoin blockchain system [3].



An alliance member has the authority to issue a minter and miner license. Since the drug manufacturers are the source of drugs identified by the Gcoin blockchain system, they should take the role of coin issuer, also known as the minter. Miners who are in charge of verifying transactions and generating blocks would be the large manufacturers and government agencies. The large wholesalers, hospitals, medical centres or third parties could be full nodes who are responsible for storing a backup of historical transactions. Also, the remaining pharmacies and consumers should be the normal node (Wallet), which has the authority to

implement transactions.

- Supply chain in Finance
  Blockchain technology and its applications in finance supply chains are a great fit due to the close ties of cryptocurrencies and its importance to the financial intermediaries in global trade. Primary use of Blockchain technology eases and helps in subsequent settlements of multi-party and multi-tier nancial transactions in supply chains that result from collaborative value creation of blockchain members. Also, transparent and validated records as well as automated transactions and tokenized nancial claims simplify nancing of working capital (including inventories and accounts receivable net of accounts payable from blockchain members which also lowers nancing costs. For this purpose, supply chain assets could be collateralized by issuing corresponding nancial claims using tokens [6].



- RFID Tags for cattle with Blockchain
  In agri-food supply chain, RFID technology has been widely used for many years. Early in 1998, ”Cattle tracking systems plan” had been implemented in Britain. In this plan, RFlD electronic ear tag is used for tracking and identifying livestock like cattle, sheep, horse and pig during their raising stage. And in January 2008, European Union passed legislation to pressure livestock farm to use electronic identification for sheep. In the USA and Japan, RFlD system had been used for tracking agri-food in the entire supply chain from planting to the distributor and retailer. In these supply chain processes, RFID systems provide management information and safety data of agri-food for producer, wholesaler, retailer and consumer. During the 2008 Beijing Olympic Games, RFTD technology had been used for tracking and monitoring the Olympic food. Athletes and staff could get the information about the food they eat, including what kinds of food they have eaten; where are these foods come from; and what processes these foods have gone through, by their personal RFlD lD card. Another example would be the current beef industry which uses BeefChain, which places cattle into specific block chains. This allows consumers to track the steak on their plate all the way back to the ranch that it was raised on. This gives ranchers greater control over the value of their sales by proving, via blockchain technology, that the beef they are selling is of desired quality or not. Through the use of RFID tags, each beef case carries a unique digital identifier that can trace the individual case from farm to table. These identifiers will be hashed into Beefchains ethereum based blockchain network to provide the details of the entire global transaction. This helps to provide a sense of security, quality, safety and trust, all of which are huge factors in the beef industry [5].

Synthesis of Concepts

- Building Process

The structure of blockchain technology is depicted by a listing of blocks with transactions in a very explicit order. These lists can be stored as a flat file (txt. format) or in the form of a simple database. Two vital data structures used in blockchain include:

1) Pointers - variables that keep information about the location of another variable. Specifically, this is pointing to the position of another variable.
2) Linked lists - a sequence of blocks where each block has specific data and links to the following block with the help of a pointer.

All blockchain structures fall into three categories:

1) Public blockchain architecture
   A public blockchain architecture implies that the information and access to the system is accessible to anyone who is willing to participate (e.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public).
2) Private blockchain architecture
   As opposed to public blockchain architecture, the private system is controlled only by users from a specific organization or authorized users who have an invitation for participation.
3) Consortium blockchain architecture

This blockchain structure can incorporate a few organizations. In a consortium, procedures are set up and controlled by the preliminary assigned users. Essentially, blockchain is a distributed journal where all parties hold a local copy. However, based on

the type of blockchain structure and its context, the system can be more centralized or decentralized. This merely refers to the blockchain architecture design style and who controls the ledger. A private blockchain is considered more centralized since it is controlled by a particular group with increased privacy. On the contrary, a public blockchain is open-ended and thus decentralized.

In a public blockchain, all records are visible to the public and anyone could take part in the agreement process. On the other hand, this is less efficient since it takes a considerable amount of time to accept each new record into the blockchain architecture. In terms of potency, we observed that the time for each transaction in a public blockchain is less eco-friendly since it requires a huge amount of computation power compared to private blockchain architecture.
These are the core blockchain architecture components:

1) Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
2) Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
3) Block - a data structure used for keeping a set of transactions which is distributed to all nodes in the network
4) Chain - a sequence of blocks in a specific order
5) Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure
6) Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system. Each blockchain block consists of certain data, the hash of the block, the hash from the previous block. The data stored inside each block depends on the type of blockchain. For instance, in the Bitcoin blockchain structure, the block maintains data about the receiver, sender, and the amount of coins. A hash is basically a long record consisting of some digits and letters. Each block hash is generated with the help of a cryptographic hash algorithm (SHA 256 or MD5). Consequently, this helps to identify each block in a blockchain structure easily. The moment a block is created, it automatically attaches a hash, while any changes made in a block affect the change of a hash too. Simply stated, hashes help to detect any changes in blocks [1]. The final element within the block is the hash from a previous block. This creates a chain of blocks and is the main element behind blockchain architectures security. For example, block 45 points to block 46. The very first block in a chain is a bit special - all confirmed and validated blocks are derived from the genesis block. Any corrupt attempts provoke the blocks to change. All the following blocks then carry incorrect information and render the whole blockchain system invalid. It could be possible to adjust all the blocks with the help of strong computer processors. However, there is a solution that eliminates this possibility called proof-of-work. This allows a user to slow down the process of creation of new blocks. In Bitcoin blockchain architecture, it takes around 10 minutes to determine the necessary proof-of-work and add a new block to the chain. This work is done by miners - special nodes within the Bitcoin blockchain structure. Miners get to keep the transaction fees from the block that they verified as a reward. Each new user (node) joining the peer-to-peer network of blockchain receives a full copy of the system. When a new block is formed, it is sent to each node within the blockchain system. Then, each node verifies the block and checks whether the information stated there is correct. If everything is alright, the block is added to the local blockchain in each node. All the nodes inside a blockchain architecture create a consensus protocol. A consensus system is a set of network rules, and if everyone abides by them, they become self-enforced inside the blockchain.

- Speculative Analysis:

1) Integration of Block chain with e-commerce websites for individual user
   Block chain is great tool in the cases if information hiding and data abstraction. This can prove to be a valuable asset in the creation of new user accounts or profiles in many online websites. Taking the example of an Ecommerce website, if we could assign a block or node to each user which could hold all information. This information will be protected as everyone but the user as only they will have the appropriate access requirements to add/change information stored in that node. This concept can be also be considered if the use of smart-contracts is applied (with the added help of IoT) where certain products that are used regularly can be ordered and stocked up long before they are needed. Although great in theory, the main problems arises in access times and concurrent access available to eac node. Also, it is heavily expensive to assign an individual node followed by a chain to a single user. For the implementation of this method, proof-of-work procedures have to be greatly sped up along with individual mining speeds of new nodes.
2) Using Blockchain as a government aided tool
   The existing identity management system is neither secure nor reliable. At every point, you are being asked to identify yourself through multiple government- authorized IDs like Voter ID, Passport, Pan Card and so on. Sharing multiple IDs leads

to privacy concerns and data breaches. Therefore, the blockchain can pave the path to self-sovereign identity through decentralized networks. Everyone uses identity document on a regular basis, which gets shared with third-parties without their explicit consent and stored at an unknown location. Whether a person needs to apply for a loan, open a bank account, buy a sim card, or book a ticket, use of identity documents can be experienced in our day-to-day lives. Companies such as government institutes, banks, credit agencies are considered to be the weakest point in the current identity management system as they are vulnerable to theft and hacking of data. Thus, the blockchain comes with the possibility to eliminate the intermediaries while allowing citizens to manage identity on their own. Challenges faced by existing traditional identity management systems include Identity Theft, KYC Onboarding, Lack of Control etc. Blockchain offers a potential solution to the above challenges by allowing users a sense of security that no third party can share their PII without their consent. With the help of Block chain, each individual citizen can be uniquely identified where their information is safely stored in a decentralized structure, If a ser is verified, ie., the documents uploaded by them matches with the documents stored in the government registry, they are assigned a trust score using the help of smart contacts. This can not only help to provide a UID for each citizen which is linked to their Voter ID, PAN card, Bank Accounts, Drivers License etc, it also provides for an ato-updating trust score that can help in verifying the citizen along with their criminal records, loan applications, past records, properties, assets and something as trivial as ecommerce check-outs.

3) Usage of Block chain tokenization in DSC to mitigate sharing of digital content
   Digital Content is one of the most shared products online. Thousands upon thousands of illegal sites, torrents and streaming sites exist which share copyrighted digital content for profit. This can be controlled in such a manner where access of content is not only controlled but also verified at every step. In the supply chain of products, a manifest system is used that has to be signed every time the product changes hands, This help to track the origin, required documents, handler and companies involved in the process.This can also be done for digital content whereby content is only applicable to users that have paid for it and are using it legally. Digital content in this case can be anything from software, videos, photos etc, where each time it is accessed, it verifies with the source node. If due to some reason, access is not granted or the usage lacks the appropriate access permissions, then the content gets digitally locked. This will help to protect un-restricted usage of material and also limit the number of users that can share the digital content.

IV. Advantages and Disadvantages

Advantages

1) Greater Transparency
   Transaction histories are becoming more transparent because of blockchain technology. Because blockchain is essentially a distributed ledger, all network participants share the same documentation as opposed to individual copies. The shared version will only be updated if everyone agrees upon it. To change a single transaction record would require the heavy-duty alterations of all subsequent records and the collusion of the entire network. Thus, data on a blockchain is more accurate, consistent and transparent compared to when it is pushed through paper-heavy processes. It is also available to all participants who have permissioned access.
2) Enhanced Security
   There are several ways a blockchain network is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded in the blockchain. After a transaction is approved, it is hashed, encrypted and linked to the previous transaction in the network. This, along with the fact that information is stored across a network of computers instead of on a single server, makes it very difficult for hackers to compromise the transaction data. In the supply chain industry where protecting sensitive data is crucial, blockchain has an opportunity to really change how critical information is shared by helping to prevent fraud and unauthorized activity.
3) Increased Efficiency
   When supply chains use traditional, paper-heavy processes, trading anything is a time-consuming process that is prone to human error and often requires third-party mediation. By streamlining and automating these processes with blockchain, transactions can be completed faster and more efficiently compared to older methods. Since record-keeping is performed using a single digital ledger that is shared among participants, industries do not have to reconcile multiple ledgers and they end up with less clutter. And when everyone has access to the same information, it becomes easier to trust each other without the need for numerous middlemen. Thus, clearing and settlement can occur much quicker.
4) Reduced Costs
   For most businesses, reducing costs is a priority. With blockchain, they do not need as many third parties or middlemen to make guarantees because it doesnt matter if you can trust your trading partner.

Instead, they just have to trust the data on the blockchain. They also would not have to review so much documentation to complete a trade because everyone will have permissioned access to a single, immutable version.

Disadvantages

1) Network Size
   Blockchains (like all distributed systems) are not so much resistant to bad actors as they are antifragile that is, they respond to attacks and grow stronger. This requires a large network of users, however. If a blockchain is not a strong network with a widely distributed grid of nodes, it becomes more difficult to reap the full benefit. There is some discussion and debate about whether this a fatal flaw for some permissioned blockchain projects, due to the number of nodes compared to public blockchains.
2) Complexity
   Blockchain technology involves an entirely new vocabulary and skill-set. It has made cryptography more mainstream, but the highly specialized industry is filled with jargon. Thankfully, there are many efforts at providing glossaries and indexes that are thorough and easy to understand for the common individual. Old supply chain companies might be hesitant to move to the new technology on account of this complexity.
3) Storage
   Blockchain ledgers can grow very large over time. The Bitcoin blockchain currently requires more than 200 GB of storage. The current growth in blockchain size appears to be overtaking the growth in hard drives and the network may lose nodes if the ledger becomes too large for individuals to download and store.
4) Unavoidable Liability
   The Proof of Work consensus algorithm that protects the Bitcoin blockchain has proven to be very effective over the years. However, among the few potential attacks that can be performed against blockchain networks and 51% attacks are among the most discussed. Such an attack may happen if one entity manages to control more than 50% of the network hashing power, which would eventually allow them to disrupt the network by intentionally excluding or modifying the ordering of transactions. To counter this, Proof of Work algorithms are being replaced by more sophisticated algorithms such as Proof of Stake which is planned to be used in the Ethereum Blockchain.
5) Consensus Model Issues
   We have found that while mining offers real world solutions it also uses a large amount of real world resources. Mining requires ongoing purchasing of hardware and an immense amount of electricity.. It takes a lot of power to run the ASICs (application-specific Integrated Circuits) that calculate different potential solutions. And the constant turnover of equipment creates a massive stockyard of obsolete parts. From an ecological standpoint, this isnt ideal. Additionally, the fact that we need a serious amount of computing power, more than the average person can afford, means the mining community is getting smaller and more exclusive. This goes against the idea of decentralization and can create the risk of a take-over by someone who controls more than 51% of the networks computational power which we have discussed.

V. Inferences

We reviewed an established blockchain system and compared it to a traditional database system and observed various differences and solutions as follows:

1) Durability Decentralized networks eliminate single points of failure as opposed to centralized systems. This distribution of risk among its nodes makes blockchains much more durable than centralized systems and are better suited to deter malicious accesses.
2) Transparency An identical copy of a blockchain is maintained by each node on the network, allowing auditing and inspecting of the data sets in real time. This level of transparency makes network activities and operations highly visible, thereby reducing the need for trust.
3) Immutability Data that is stored on a distributed public blockchain is practically immutable due to the need for validation by other nodes and traceability of changes. This allows users to operate with the highest degree of confidence that the chain of data is unaltered and accurate.
4) Process Integrity Distributed open source protocols are by nature executed exactly as written in the code. Users can be certain that actions described on the protocol are executed correctly and timely without the need for human intervention [2].

Relying on one single organization to broker such sensitive and valuable insformation requires a great deal of trust to be invested by every actor in a supply chain. Such organization (as an entity of the manufacturing system) will also gain significant power through the possession of this valuable data, which could be misused to extort or damage organizations if biased. Even if this entity can be trusted to be a good actor, it must possess the technical capabilities to store and handle this information effectively. A major issue of having this type of centralized system, is that it becomes a single point of failure which leaves the whole system vulnerable to failure (e.g. hacking, or corruption). Various incidents in the past decades have shown that even a tight and costly

security mechanism cannot guarantee complete data security, leaving organizations in a network at potential risk. We also reviewed some consensus models for governance on the blockchain system, including unique features of each as well as advantages and disadvantages. Proof-Of-Work is found to be resistant to various DDoS attacks, even if one node goes down due to some external conditions, other nodes will keep working, hence the network will keep working. Proof-of-work imposes certain restrictions on the actions of the participants, because the task requires considerable effort. Effective attack also requires a high computing capacity and a long calculation, so it is possible, but disadvantageous against the background of high costs.

VI. Suggestions and Future Scope

We have found out more efficient consensus algorithms compared to Proof-of-Work which are less energy consuming while providing the distributed and decentralised governing solution: Practical Byzantine fault tolerant Mechanism. Distributed networks could use Practical Byzantine fault-tolerant (PBFT) mechanism. Every node distributes a public key. Messages getting through the node is designated by the node to confirm its organization. When enough indistinguishable reactions are achieved, at that point a consensus is met that the message is a legitimate transaction. PBFT is a network formed for the low-latency storage framework. This is pertinent to digital resource-based platforms that don't need a lot of through puts yet ask numerous transactions. Not at all like PoW and PoS, a PBFT consensus mechanism does not require any hashing energy to approve exchanges in a blockchain, which implies there is no requirement for high energy utilization and the danger of centralization is lower than in both of those blockchain mechanisms. PBFT is presently being utilized by the Hyperledger venture, which enables developers to fabricate their own particular digital resources on a disseminated ledger. We find that in an improved model, this mechanism can be used to improve the supply chain network. We have found that if block times are high it can cause a large delay due to increased traffic. Our proposed model has shorter block times, which makes the platform more efficient. Hence it allows for blocks, or the records of cryptocurrency transactions, to be created more quickly than currently established blockchain systems. This efficiency leads to quicker transactions, and allows our model to process the large number of transactions that take place across its network. Since smart contracts can be written and deployed on a blockchain network, we propose a dApp (decentralised Application) that will help suppliers connect to retailers without dealing with any technical jargon related to the inner workings of the blockchain network. Decentralized applications are a piece of software that communicates with the blockchain, which manages the state of all network actors. The interface of the decentralized applications does not look any different than any website or mobile app today. The smart contract represents the core logic of a decentralized application. Smart contracts are integral building blocks of blockchains, that process information from external sensors or events and help the blockchain manage the state of all network actors. We propose a dApp that will connect a smartphone of a retailer/supplier that shows them the data of any product in the supply chain through an IoT device, like an RFID chip whose data will be stored in the network and can be seen by anyone with data access to the network in real time.

VII. Conclusion

In this paper, we discuss the working of Blockchain, its use cases and applications in the field of supply chain and its management. This technology has varied applications in many fields such as food product tracking and management, sharing and privacy involved with digital chains, tokenization of assets and its management, with precise tracking of each part and its different management according to the use cases. Although this technology is not ready for application on the current market scenario but this issue can be easily overcome. With the current strides taken in the betterment of the technology, it will not be long before blockchain can be applied in all fields of technology and become economical to use/produce and interact with. Keeping the future in mind, the implementation of blockchain for supply chain, at least must start from today, albeit in small controlled cases. This will give enough time to integrate SCM based blockchain into the economic standards and also provide new insights about the operation and working of the technology.

VIII. Acknowledgement

The authors of this review paper would like to thank Prof. Sanjay Deshmukh and Dr. Dhirendra Mishra for helping with research methodology and paper writing techniques. Their constant guidance has been very valuable.

References

[1] Token Recipes model Manufacturing Processes- Martin Westerkamp, Friedhelm Victor, Axel Kpper, Service-centric Networking, Telekom Innovation Laboratories, Technische Universitat Berlin, Berlin, Germany

[2] Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger- Saveen A. Abeyratne, Radmehr P. Monfared, Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, UK

[3] Governance on the Drug Supply Chain via Gcoin Blockchain-Jen-Hung Tseng, Division of Risk Management, Taiwan Food and Drug Administration, No.161-2, Kunyang St, Nangang District, Taipei City 11561, Taiwan, Yen-Chih Liao, Shih-wei Liao, Department of Computer Science and Information Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan, Bin Chong, College of Chemistry and Molecular Engineering, Peking University, Beijing 100871, China

[4] Blockchain Technology in Supply Chain Management: An Application Perspective - Gregor Blossey, Jannick Eisenardt, German Graduate School of Management and Law, Heilbronn

[5] An Agri-food Supply Chain Traceability System for China Based on RFID Blockchain Technology - Feng Tian, Department of Information Systems and Operations Vienna University of Economics and Business Vienna, Austria
[6] Digital Supply Chain Transformation toward Blockchain Integration- Kari Korpela, Jukka Hallikas Lappeenranta University of Technology, Finland and Tomi Dahlberg, University of Turku, Finland
[7] A supply chain traceability system for food safety based on HACCP, blockchain Internet of things - Feng Tian, Department of Information Systems and Operations Vienna University of Economics and Business Vienna, Austria
[8] Blockchain technology and its relationships to sustainable supply chain management - Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis Robert A. Foisie School of Business, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA
[9] Blockchains roles in meeting key supply chain management objectives - Nir Kshetri, Business and Economics/The University of North Carolina at Greensboro, Bryan Building, Room: 368, P. O. Box 26165 Greensboro, NC 274026165, USA