International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/120183

Design and Deployment of IoT enabled Blockchain based resilient Supply-chain Management System using Ethereum

Ayaskanta Mishra[1], Sayan Karmakar[1], Ankita Dutta[1], Ankush Bose[1] and Manaswini Mohapatro[2]

[1]*School of Electronics Engineering, Kalinga Institute of Industrial Technology, Deemed to be University, Bhubaneswar, Odisha, India, Pincode - 751024*

[2]*Infosys Technologies Ltd., Bhubaneswar, Odisha, India, Pincode - 751024*

Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 31 Oct. 2022

Abstract: With exponential growth of digital consumer purchasing behavior and the increasing implementation of IoT in retail industry, it has become imperative to provide secure, scalable, and manageable data models to the complex interconnected supply chain management systems. Blockchain technology in recent times has huge potential for deployment of secured data framework over a distributed architecture. In this paper, we have proposed a resilient Supply-Chain Management (SCM) system using Ethereum-based blockchain deployment on a distributed computing test-bed. An IoT-based Radio Frequency Identification (RFID) method is used in our use-case prototype for product information tracking at functional nodes (Manufacturers, Distributors, Retailers and Consumers) of SCM implementation. We have implemented $Ethereum^{TM}$ based blockchain using $Solidity^{TM}$ smart contracts with the help of $Remix^{TM}$ Web-based Integrated Development Environment (IDE). A python-based PyAutoGui is used for automation in blockchain deployment at multiple functional nodes distributed across the supply chain. As proof of concept, we have created a test-bed having 28 Oracle virtual machines (VMs) using Linux for successful implementation and validation of our proposed blockchain based SCM system. We have presented comprehensive results showing Ethereum-blockchain containing complete product information, transactions and tracking for secured information access with distributed digital ledger technology on our test-bed implementation.

Keywords: Supply-Chain Management (SCM), Blockchain, Ethereum, IoT, Relational database, Digital Ledger, Distributed Database, Data Security

1. Introduction and Overview

Huge surge of consumers all across the world as result of growing economy and globalization. The demand for goods has increased however the supply-chain has to keep up with the pace. The supply chain industry needs to upgrade and optimize their supply chain management using modern technologies like Internet of Things (IoT)-based sensing, tracking of logistics, digital ledger especially in the era of Industry 4.0. Various digital transformations are taking place to make these processes faster, however there are still several challenges. One of the major challenges in the technology-enabled Supply Chain Management (SCM) is to ensure transparency in digital ledger of all transactions in the supply chain. This is achievable by restricting malicious digital ledger data-modifications over a distributed relational database. Tracking of products by ensuring authentic and genuine digital transactions is the key to mitigate corruption in intermediate levels of any supply-chain. Manufacturers, distributors, logistics provider companies are struggling with this daunting task of pin-point accurate tracking of goods throughout their supply chain stages of logistic tracking, inventory management with a complete end-to-end approach from manufacturing-till-consumer. Integrating Blockchain technology with supply chain tracking database would be a game-changer in achieving a secured, resilient supply chain management system.

Blockchain technology works over a distributed database architecture with no single server but several smaller machines which make a distributed 'blocks' of data but well connected though 'chains' which is called address or hash [1]. The authenticity of each action within the Blockchain is validated not by a single device but by the various consensus algorithms - Proof of work (PoW), Proof of Stake (PoS) or Delegated Proof of Stake (DPoS). No new machines can get into the Blockchain without the validation by the consensus algorithms [2]. This is done by all the devices in the Blockchain. This makes the system very resilient against attacks; even if a device is hacked the information cannot be viewed because the

E-mail address: ayaskanta.mishra@ieee.org, mishra.ayaskanta@gmail.com, mana.mohapatro@gmail.com

information is encrypted. The device itself is not aware of the information but together as a Blockchain it conveys meaning. Figure 1 illustrates the Blockchain technology in Supply chain Management deployment scenario. Smart contracts are the essential component of the Blockchain [3]. It is what makes the system so transparent, authentic and tamper proof. Smart contracts are immutable programs which mean the code cannot be changed once it is deployed. For the proper implementation of the model there has to be support from government, industry players, raw material suppliers, regulators, distributors and consumers. This will make the supply chain industry secured and efficient by multi-fold.

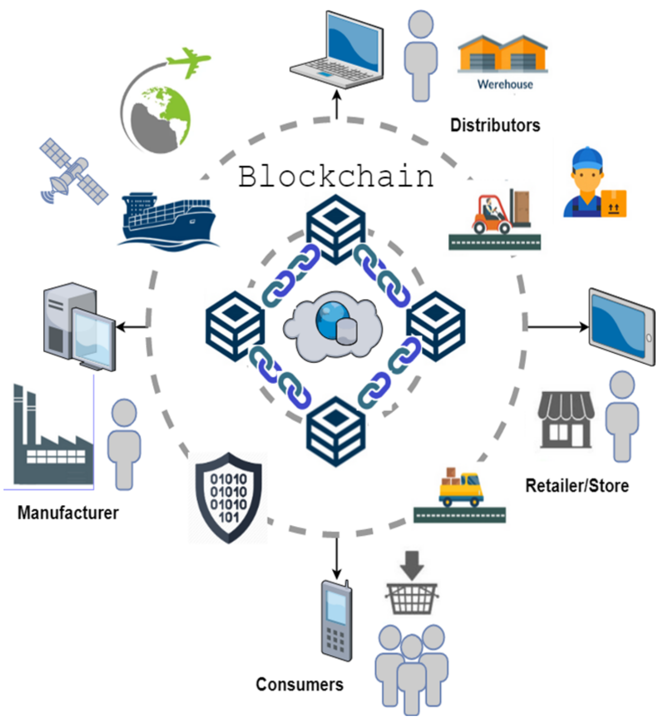

Figure 1. Blockchain technology in Supply Chain Management

The financial world is already thinking some Blockchain based transaction system by seeing the success and possibility of crypto currencies like Bit-coin, Ethereum, etc. Now time has come to induct Blockchain technology to some other industries which would greatly benefit from this technology.

An IoT-based supply chain management of goods/product would be the key to facilitate the blockchain based systems [4]. Automation in product and shipment tracking technologies like Radio Frequency Identification (RFID) and Quick Response (QR) Code sensing can generate electronic information about products and their transactions with limited to even no human intervention. This digital RFID/ QR-Code data can be stored in a secured distributed relational-database of blockchain rather than on a single-ownership cloud or server [5]. This would help in ensuring transparency in record keeping of products and their information throughout the supply chain. Identification of counterfeit products, malicious events or financial irregularity in middle points of supply chain is viable because the genuine products can be identified by regulators very easily using secured resilient blockchain as no single player can tamper the database at any instance. The data in a blockchain cannot be modified as it is distributed database and none of the system has complete information or authority/access to modify the data. Blockchain deployment is supply-chain and financial transactions would improve transparency, tax evasion can also be avoided and each transaction in the system gets noted (cannot be deleted or modified). Hence, government and tax collection and financial regulatory agencies would be benefited a lot. Organic food industry (deals with perishable foods and strict quality control policy) can prove their originality if they incorporate blockchain-based secured system. Blockchain technology is next biggest revolution for the dream of Digital India when it comes to Indian market potential of a huge consumer economy.

In this paper, we propose to implement a model which will consists of various nodes each signify a level in the supply chain like consumer, regulator, retailer, distributor, manufacturer, supplier. Each node has certain priority that is security clearance hence authorized to access certain information only and have certain functionalities which would trigger a change signifying the progress of product in the supply chain. The Blockchain is Ethereum based - Solidity, which can be hosted in JavaScript Virtual Machine (JS-VM), Injected Web3 and Web3 provider.

Globally, products are being manufactured through extreme complex supply chains which are extended to remote corners of the world. However due to such complexities the network may undergo massive breakdown due to fault at any stage of the system. An event in one corner of the globe which can be either natural or man-made can result in domino effect of problems which can lead to critical failure. A classical system doesn't ensure sustainability and reproducibility even after regular optimization in the management cycle. In order to tackle such problems technologies like Blockchain can play a significant role which ensures security, sustainability and efficiency. In countries like India agriculture sector has been the most affected sector and require reforms through use of technology.

One of massive problems in the chain is the role of middleman which promotes in authenticity among the blocks of the supply chain. In order to deal with the problems of such sensitive issues integration of blockchain technology for distributed supply chain database management can be a potential tool to ensures transparency. In a nutshell, blockchain could be defined as a chronological chain of blocks in the form of distributed ledger that content records of valid transaction activities since the last block was added to the chain. The information present in the chain are en-

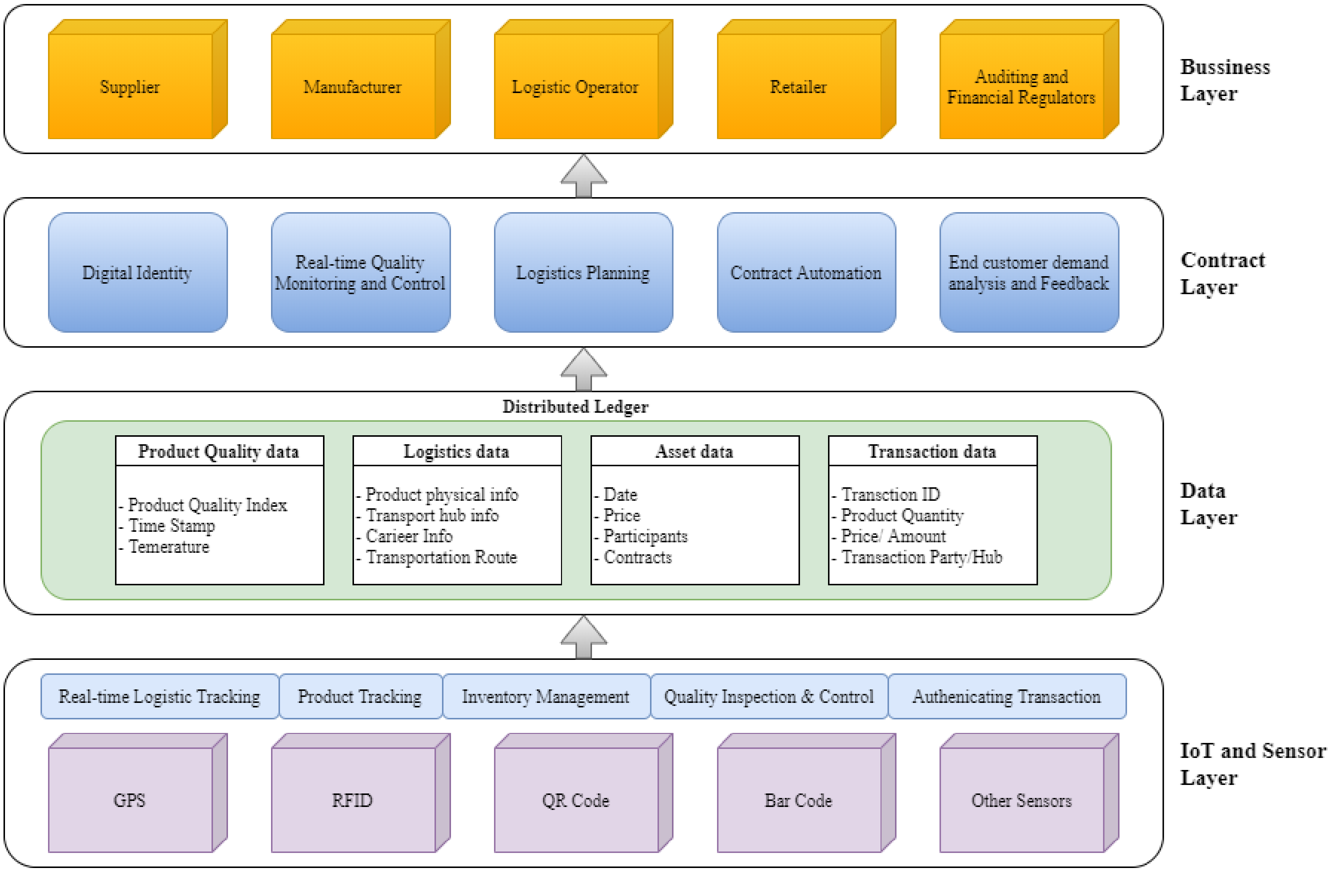

Figure 2. Layered Architecture of IoT based blockchain deployment in Supply chain Management (SCM)

crypted and that can only be accessed but cannot be changed or modified without proper digital rights. Hence if the technology is employed successfully the end users need not have to only rely on the middleman as the system guarantees authenticity of entries/transactions in the form of distributed ledger. Further the technology can be extended to GPS and IoT-based sensor systems to ensure traceability over a secured and immutable framework. Figure 2 illustrates the layered architecture of IoT based blockchain deployment in Supply chain Management scenario.

2. RELATED WORK

Müßigmann et al. [6] have presented an extensive bibliometric study of 613 articles on blockchain technology (BCT) applications in Logistics and supply Management and have provided their analysis of successful viability of BCT in digital supply chains. Guggenberger et al. in [7] has focused on blockchain technology as decentralized information hub for improving inter-organizational information sharing for vendor managed inventory. Blockchain is the key to data privacy & security which have become major concerns in every sector due to increasing number of hackers and malicious attackers. Du et al. in their research [8] have proposed a blockchain encryption technique to address data privacy and security in finance supply chains where fraudulent transactions are a major concern. Zhu et al. in [9] have contributed towards use of blockchain technology in supply chain information, and strategic product deletion management for a robust framework for data-integrity. Shakhbulatov et al. in [10] presented a survey of recent blockchain frameworks and how BCT technology would successfully address supply chain challenges such as providing data availability and transparency during information sharing between various stakeholders. A systematic review on blockchain-enabled information sharing within a supply chain is presented by Wan et al. in [11]. Chen at al. in [12] have presented a Blockchain-Based Supplier Continuous Quality Improvement (SCQI) framework that would help in improving quality management.

Various research articles have recommended Blockchain technology for efficiently managing SCM operation in various industries. Research article by Nasih et al. in [13] have proposed Blockchain technology in the supply chain of maritime industry for providing decentralization and disintermediation of operations. Ahamed et al. [14] have conducted a detailed review on Blockchain Technology for Food Supply Chain Management where the authors have suggested BCT for effectively tracking, tracing, and maintaining transparency of the food products. Yousuf et al.

in [15] have given a conceptual overview of areas in SCM where blockchain can be integrated to resolve issues such as product lifecycle management, logistics history etc. Wu et al. in [16] have provided a study of blockchain-based SCM systems through a case study by designing blockchain-based food traceability system that addresses various technical challenges. A platform-independent, generic-purpose, and blockchain-based supply chain tracking is proposed by Niya et al. in their research paper [17]. Asyrofi et al. have proposed "CLOUDITY"- a JUGO and blockchain based cloud supply chain framework in [18]. Su and Wang in [19] have presented the use of blockchain technology for building digital bulk commodities service platform. In [20] the authors have reviewed electronic warehouse receipt systems and how blockchain technology can improve operations in supply chain financial services.

Various application-specific Blockchain based supply-chain management research papers have discussed incorporating BCT in Supply chain operations in various industrial sectors. Hedge et al. in [21] have reviewed agricultural supply chain management systems. Research paper [22] has highlighted the use of BCT for tackling issues related to counterfeit drugs. Yue et al. in [23] have presented BCT applicability for lifecycle management and traceability of medical equipment. [24] Lei et al. have conducted a comparative study before and after implementation of BCT for digital assets. There are many research works on blockchain for IoT based supply-chain management systems. Few of prominent research contributions have been studied as part of this research work by citing their contribution in their field of research. Xu et al in [25] have presented a Cyber-Physical System approach for blockchain based cargo supply chain security enhancement. Aich et al. in [26] have presented the benefits of IoT integrated blockchain based supply chain management implemented across diverse sectors. Malik et al. in [27] have proposed "TrustChain" a system for trust management in blockchain and IoT supported supply chains. Tsang et al. in their research [28] have proposed a novel blockchain-IoT-based food traceability system (BIFTS) for life management system of perishable food. Ali et al. in [29] have conducted a review on the adoption and challenges of integrating blockchain with IoT. Research on use of IoT and allied technologies like Machine Learning (ML) in supply chain management is the key to have secure and resilient Blockchain technology seamlessly integrated with IoT & ML technologies in future supply chains for improved data-integrity. In this direction Mishra et al. have proposed a real-time RFID-based item tracking using IoT & efficient inventory management using machine learning in their research [30]. Shahin et al. in [31] have presented implementation of ML algorithms for detecting compromised IoT devices so as to ensure reliable data storage in blockchain. The authors have carried out extensive research by training IoTID20 dataset for detecting anomalous activity detection in IoT network.

3. PROPOSED SYSTEM

In this paper, we are proposing an IoT-Ethereum based secured framework for resilient SCM system. The proposed system is comprising of a RFID based data acquisition system for product information tracking using IoT and Ethereum based blockchain implementation on the acquired digital SCM data to provide data immutability and optimum security which is imperative for a digital SCM system with the vision of Industry 4.0.

A. *Blockchain-based secured framework for Supply-chain Management informatics*

In this paper, we are proposing an Ethereum-based blockchain implementation for Supply Chain Management (SCM) functional nodes. The SCM product tracking data is obtained through an IoT-based RFID data acquisition system.

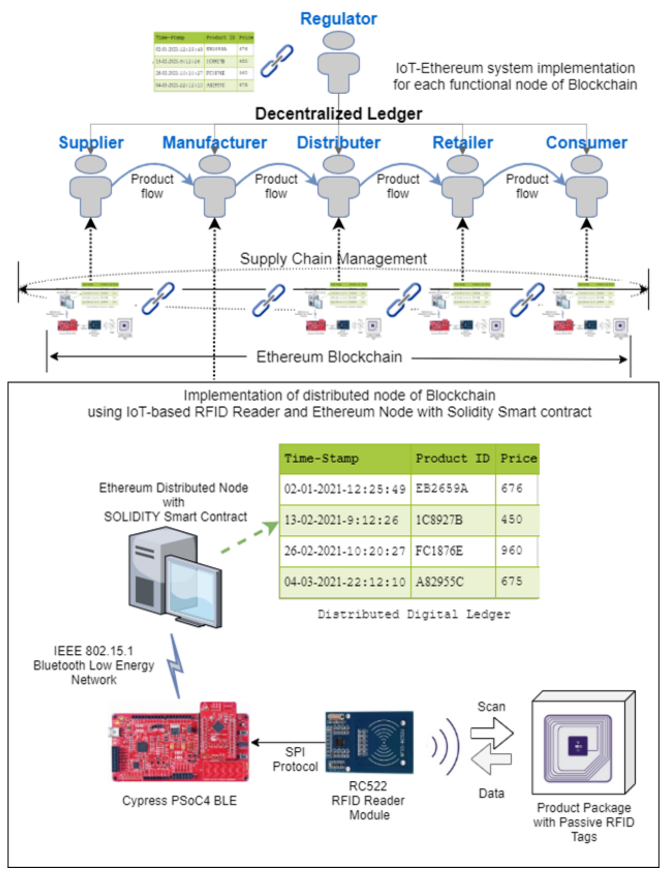

Figure 3. Proposed IoT-Ethereum based secured architecture for Blockchain in Supply Chain Management System

In our deployment scenario we have considered different functional nodes (supplier, manufacturer, distributor, retailer, consumer and regulator) for multiple product types and their supply-chain. At each node we have implemented proposed IoT-based RFID scanner system for automation of product tracking and record keeping that fetch information of products at each functional node. All the products (Units) are equipped with passive RFID tags hence can be automatically scanned and tracked using the RFID readers deployed on entry and exit of each functional node throughout the supply-chain.This data obtained from RFID are pushed to the Ethereum-based secured framework of blockchain's distributed relational database architecture with solidity smart contracts for resilient supply-chain management informatics. Figure 3 shows our proposed IoT-Ethereum based Supply Chain Management system architecture.

B. *IoT-based RFID data acquisition System for Ethereum Blockchain in SCM*

Real-time tracking of products and their information during their end-to-end movement in the supply-chain from manufacturer-to-consumer is first step in any digital SCM system. To achieve automation in this objective we are proposing an IoT-based real-time product tracking mechanism using RFID technology, the same has been used by Ahamed et al. in [32]. However, there are some other technique like QR-Code based image scanning is technologically feasible for this purpose but we have selected RFID technology since it requires almost no human intervention and does not require and exact alignment between product package with reader/scanner. RFID can operate with close proximity between product package and reader using Radio-waves and hence do not require any line-of-Sight (LOS) or proper optical alignment like QR-Code method. RFID method is better suitable for large product packages and consignments over the supply-chain. For this research work and proof of concept and prototyping we have used a RC522 chip by NXP Semi-conductors as RFID reader. We have used Cypress Semiconductor's PSoC4-BLE kit as the embedded development platform for implementation of IoT-based passive RFID-tag scanning system. Figure 4 shows the flowchart of algorithm running on PSoC4 embedded system for RFID data acquisition.

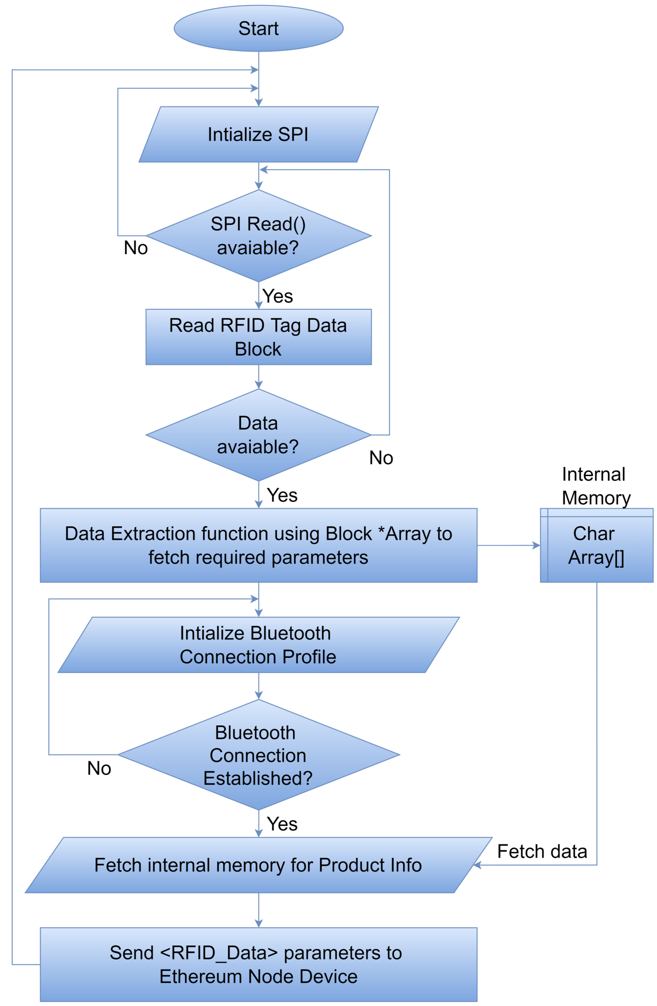

Figure 4. Flow-chart of algorithm running on PSoC4 embedded system for RFID data acquisition

The data acquired from passive-RFID tags are fetched using RC522 module through the PSoC4-BLE Embedded development platform and the RFID-tag data is sent to the local Ethereum machine over IEEE 802.15.1 Bluetooth Low-Energy Personal Area Network (PAN). The real-time data from RFID-tags contains product information like Product ID, Time-stamp, transaction price at the node (manufacture, distributor, retailer and consumer have different transaction price), Product Quality Index (based on current status of product), distance cover and route information. These are some of the parameters we have considered for our study the data-set may be customized as per the requirements of any specific supply-chain or SCM operator specific requirements. We have used NXP RC522 module to interface with our CY8CKIT-042-BLE-A PIONEER KIT Embedded development platform for prototyping of RFID based data acquisition system. Serial Peripheral Interface (SPI) protocol is used to interface the RC522 module with PSoC4. Here PSoC4 is SPI master and RC522 is slave device. Serial Clock (SCK), Master-Out-Slave-In (MOSI), Master-In-Slave-Out (MISO), Slave Select (SS) are the interfacing pins used for a 4-wire interfacing between PSoC4 and RC522. Apart from these SPI interface 4-pins RC522 would require power pins +Vcc (+3.3V.) and GND. A Reset (RST) digital input is given to the RC522 module from General Purpose Input-Output (GPIO) pin of PSoC4.

Figure 5 shows the prototype of IoT-based RFID data acquisition system implementation. Figure 5 shows the prototype of IoT-based RFID data acquisition system implementation. The prototype photograph shows all the functional modules of the implemented system. RFID reader NXP RC522 module is reading passive RFID tag attached with a package displayed in the photograph. The RC522 RFID reader module is interfaced with the CY8CKIT-042-BLE-A PIONEER KIT through SPI protocol as shown in the prototype. The IEEE 802.15.1 Bluetooth Low Energy communication between Ethereum platform connected PC with the Embedded system can seen in the photograph. This shows the complete prototyping and system implementation of our proposed IoT-based RFID data acquisition system.

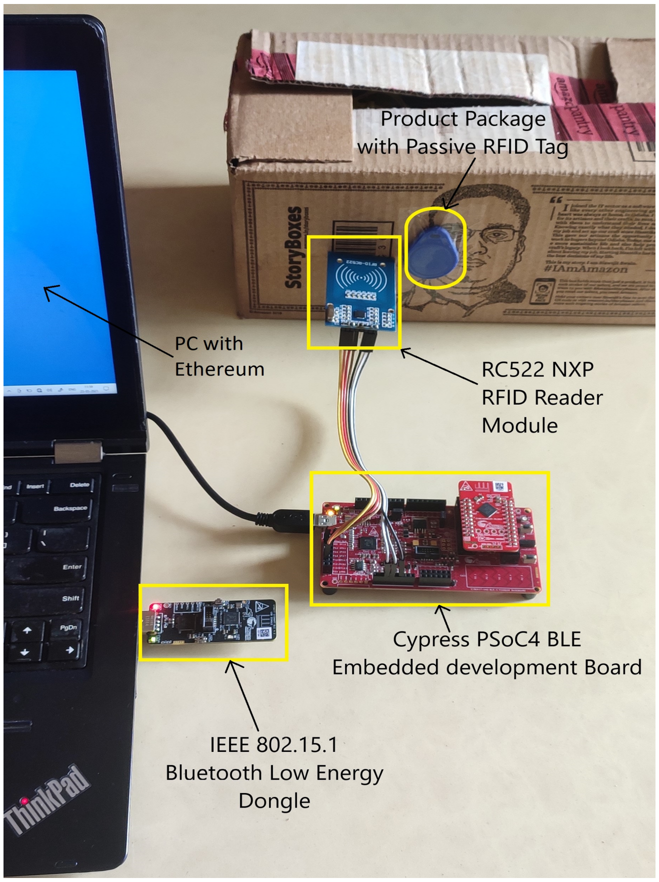

Figure 5. Prototype of IoT and RFID based product tracking for implementation of Ethereum-Blockchain

C. Ethereum based blockchain using Solidity secured smart contracts for resilient SCM

The proposed system consists of an Ethereum based blockchain [33], [34] which is made of smart contracts using solidity framework. The system allows several levels of information access - supplier, manufacturer, distributor, retailer, consumer and regulator. Each level has access to different information and functionalities which can be set during deployment of the Blockchain. Each node identifies itself in the level of security clearance by the Blockchain hash address. These addresses cannot be created by any organization but by the Blockchain itself which is a distributed hence no unauthorized tampering or manipulation for transaction or ledger is possible. The figure 6 depicts the data management of functional nodes proposed Blockchain based Supply Chain Management (SCM) system.

The whole process is configured according to the digital profile of the actors of the network which consists of the following attributes given in Table I.

Figure 7 illustrates the secured transaction sequence of digital ledger and data flow over the proposed blockchain based SCM system. Data modes are part of transactions which takes place in a SCM system. A product getting manufactured till reaching the consumer is part of a connected supply chain. However, managing the supply chain is a very complex and resource consuming affair. The data modes proposed in our work is to ensure a secure and resilient digital SCM system. Firstly, at each functional node the data-set generated based on the product health and information parameters with product ID, time-stamp of data-entry, quality, temperature, supply chain route, manufactured batch no. Secondly, the data-set contenting status parameters of product with completed, active, halted, cancelled, waiting, shipped etc. 3rd step is identity of functional node before doing any transaction for write data-access to the blockchain relational database. 4th step is the transaction followed by the 5th step where reverification of functional nodes to ensure a more double-layer security approach. Step 6 data-set contents logistics parameters like dimension of product package, quantity, quality and service. Finally, 7th step has meta-data containing time-stamp with date, address of nodes.

TABLE I. DIGITAL PROFILE AND ATTRIBUTES OF FUNCTIONAL NODES OF SUPPLY-CHAIN SYSTEM

Functional Nodes	**Digital Profile and Attributes**
Supplier	The supplier will have access to the data which is essential for transparency. Further it can access the data of the demanded products and can act accordingly.
Distributor	The distributor will have access to the data of distribution of the product will have information about the demand of the product accordingly it can deploy the process.
Regulator	The body provides unique id to the individuals according to their digital profile of the network and will act as a hawk eye for the whole automated supply chain.
Retailer	The Retailer will sell the product to the customer and can accordingly share necessary info or requests to the up hand of supply chain.
Manufacturer	The manufacturer can similarly track the product and will have knowledge about the supply and demand of the product accordingly it can communicate with the other actors of the supply chain.
Consumers	The consumer will have access to customized user interface which will display data of the product starting from the supply to the end, which will ensure traceability and transparency.

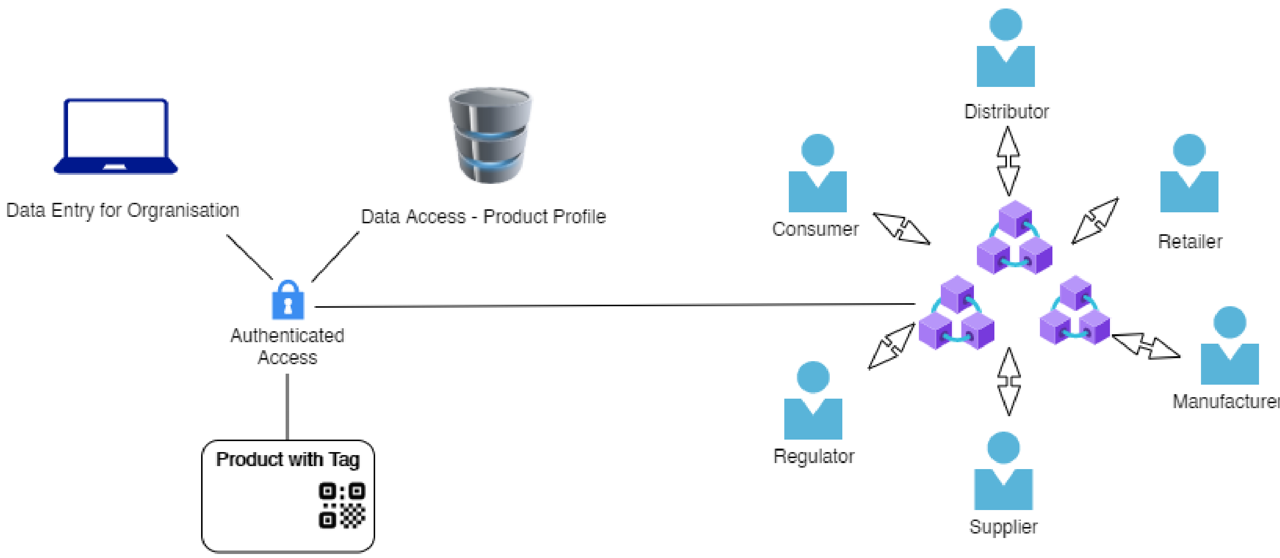

Figure 6. Data management of functional nodes proposed Blockchain based Supply Chain Management (SCM) system

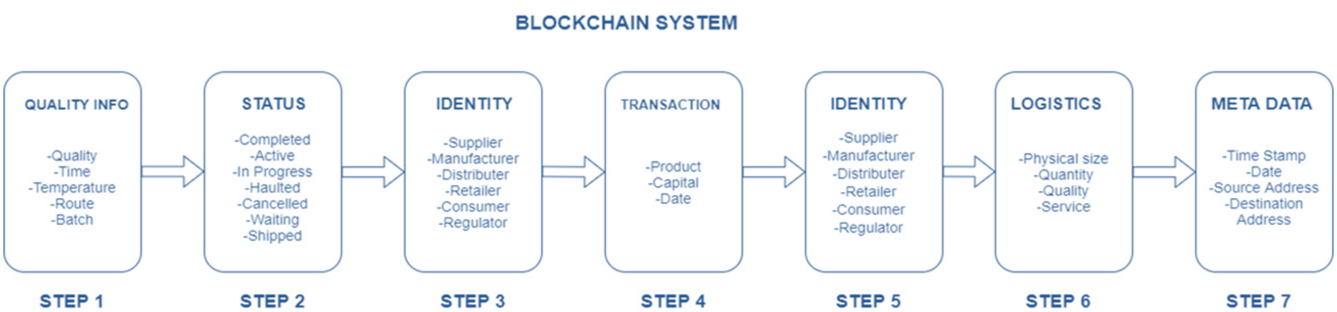

Figure 7. Transaction sequence of digital ledger for blockchain in digital Supply Chain Management (SCM) system

4. MODELING THE BLOCKCHAIN

Blockchain is distributed security mechanism use many cryptographic models to ensure security over a peer-to-peer framework. Here we are highlighting the security model used in blockchain [35].

A. *Hash function*

Blockchain use fixed size data blocks interconnected with the links (chains). A hash function converts the arbitrary huge data into fixed sized data blocks. Hash functions are non-invertible. A SHA256 hash is shown in figure 8 with hash function basic mathematical properties.

B. *Merkle Tree*

Merkle tree is used to check the data integrity over a blockchain to ensure that none of the data is changed or modified. This function is critical for blockchain to ensure that past transactions cannot be modified. Let's consider the set of data 'D' of 'n' number of blocks given in (1).

$$D = \{d_1, d_2, d_3, ..., d_n\} \quad (1)$$

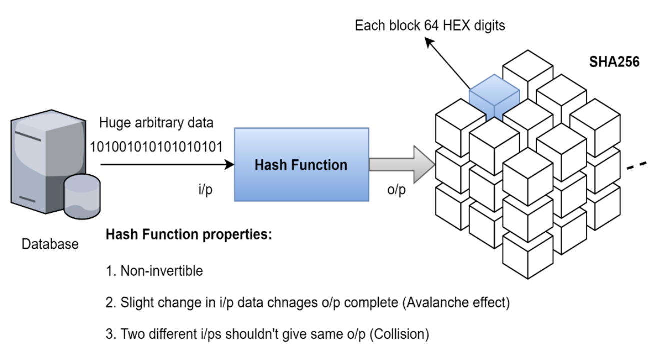

Figure 8. Hash function used in blockchain

Merkle tree is made up off hash values of elements within $D : H(d_1), H(d_2)$ etc. A four-layer recursive Merkle Tree of $D = \{L_1, L_2, L_3, L_4\}$ is given in figure 9.

The Merkle root of (1) is denoted as$R^H(D)$ as it is the top hash of the corresponding Merkle tree. A small change

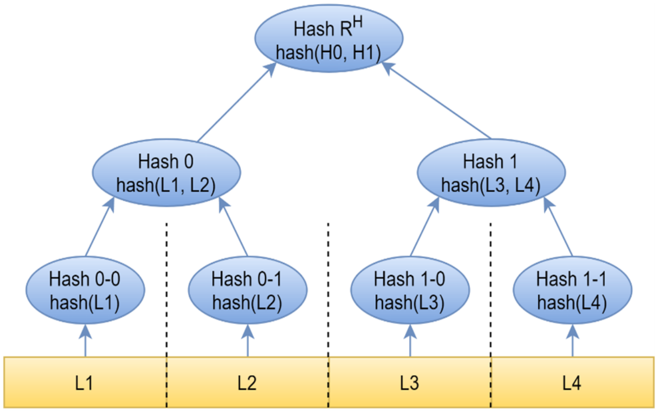

Figure 9. Multi-layer recursive Merkle Tree

in data would change its hash function o/p drastically. In general, for $D = \{d_1, d_2, d_3, ..., d_n\}$ the hash root is a function of all the different hash from recursive Merkle tree given in (2).

$$R^H(D) = H^{MT}\{d1, d2, d3, ..., dn\} \quad (2)$$

Markle tree with hash function together create an immutable distributive data-structure. For an instance, if there is a slight change in any data its hash would change hence trigger a chain-reaction in Merkle tree. This makes blockchain robust and digital ledger or transaction cannot be modified as it will change the hash and hash would not match for block headers.

C. Asymmetric Cryptography

The notations for Asymmetric key encipherment is given in Table. II.

TABLE II. ASYMMETRIC CRYPTOGRAPHY NOTATIONS

Notation	Description
K^A_{Pr}	Private Key of Node 'A'
K^A_{Pu}	Public Key of Node 'A'
K^B_{Pr}	Private Key of Node 'B'
K^B_{Pu}	Public Key of Node 'B'
Ec	Encryption function
Dc	Decryption function
M	Message: Plain text (Numeric data)
C	Cipher text (Encrypted data)
S	Digital Signature
m	Decrypted Digitally Signed message

Apart from immutable distributed data-structure of blockchain another key aspect of security is encryption.

The data in blockchain are end to end encrypted using Asymmetric key encipherment most popular one RSA algorithm. The data integrity is not only validated using encryption rather the sender identity is also validated using digital signature.

1) Encryption process:

$$C = En(K^B_{Pu}, M) \quad (3)$$

2) Decryption process:

$$M = De(K^B_{Pr}, C) \quad (4)$$

3) Digital Signature and Signing process:

$$S = En(K^A_{Pr}, M) \quad (5)$$

4) Message retrieval from Signature:

$$m = De(K^B_{Pu}, S) \quad (6)$$

5) Signature validation process: From (4) and (6) we can find the following condition. If it is true then data and the identity is successfully verified and validated hence the blockchain would accept the new digital ledger.

$$m = M \quad (7)$$

Figure 10 shows the encryption-decryption process for data validation and digital signature exchange for identity validation for nodes in blockchain. Asymmetric key encipherment is a very important aspect of blockchain. All the transaction and communication take place using Asymmetric cryptography (e.g. RSA Algorithm).

D. Entry in Blockchain (Tr)

Entry in blockchain is a staple piece of information which is stored securely in blockchain. In Blockchain's terminologies these are called transaction (Tr) and the very purpose of blockchain is to store these Tr securely. In our Supply Chain Management (SCM) scenario all our information about product tracking, logistics tracking, Product financial transaction and Product Quality Monitoring can be considered as Entries. In a typical SCM scenario there would be let's say 'N' number of Tr.

E. Block

A Block is a vector of Entries (Tr). Let's consider in our SCM blockchain at any instance there are 'NB' numbers of Entries to create a single Block represented in (8).

$$B = \{Tr_1, Tr_2, Tr_3, ..., Tr_{N_B}\} \quad (8)$$

F. Proof-Of-Work (PoW)

PoW creates link between two consecutive blocks. B^{Prev} be the notation of 1st and B for 2nd block. The PoW gets materialized in the header of the 2nd block (B). The hash of 1st block is $H(B^{Prev})$ is in typical implementation case 64-digit HEX-code (SHA256). Solving PoW to find the 'Nonce' mathematically is a computationally regressive operation called 'mining' in blockchain terminology. H(B) i.e. hash of 2nd block at time instant t^0 is given in (9).

$$H(B) = H(H(B^{Prev})\theta R^H(B)\theta timestamp(t^0)\theta b\theta nonce^0 \quad (9)$$

Here, denotes concatenation operation and time stamp denotes the current time in seconds. The condition to

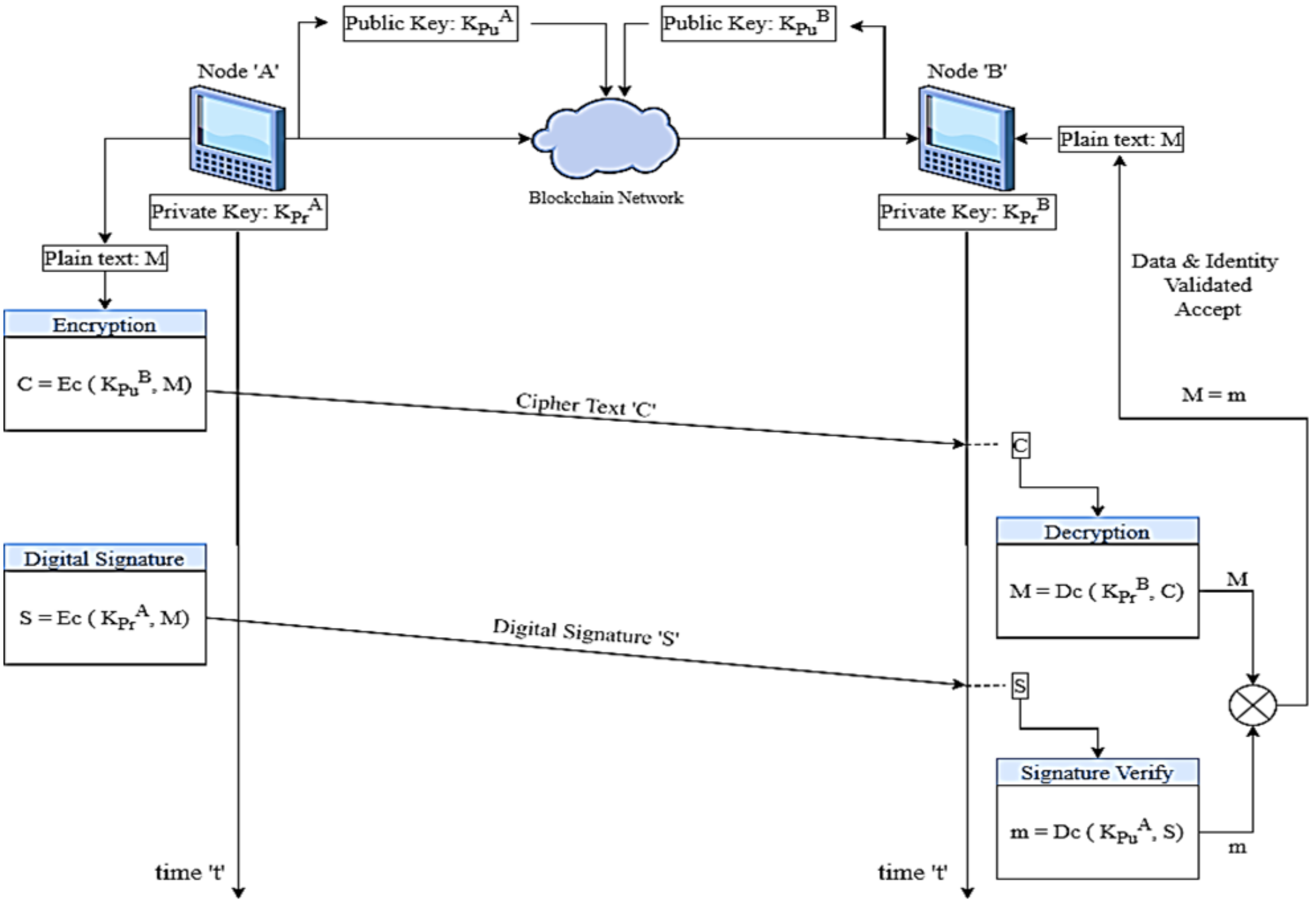

Figure 10. Asymmetric Cryptography: Data and Signature validation

calculate hash brutally is given in (10).

$$H(B) <= target \tag{10}$$

G. Block Header

A Block header is the data-structure of parameters given in Table. III. The header of Block 'B' called Head(B) can be structured after the Proof-of-Work has be successfully calculated to link between two consecutive blocks (B^{Prev}, B).

TABLE III. HEAD(B): BLOCK HEADER

Notation	Description
id_m	Identity of Mining entity
$H(B^{Prev})$	Hash of previous Block (B^{Prev})
$R^H(B)$	Merkle root of Block B
$timestamp(t^0)$	Time-stamp of instance t^0 (in sec.)
b	Proof-of-work from b to target
$nonce^0$	Calculated Nonce at instance t^0
$H(B)$	Hash of current Block (B)

H. Distributed Architecture: Nodes

Blockchain works on a distributed and decentralized nodes architecture. Figure 11 shows the Blockchain nodes deployment over a distributed network.

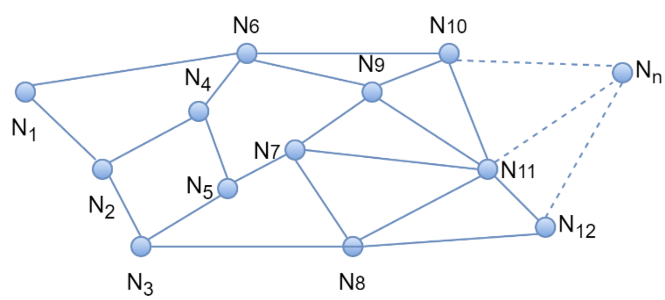

Figure 11. Distributed Nodes Architecture of Blockchain

There are two types of Nodes: 1) Simple Node- Only to transmit information, 2) Complete Node- Mine new blocks and has a local copy of the whole blockchain.

I. Revolution of trust

Blockchain has distributed network architecture for data security. In conventional data security approach, the control lies with the decisive central nodes (Security Servers which are virtually impenetrable or hard to hack), but in blockchain the control does not lie with any node (not even complete node) rather it's a collaborative effort by all nodes. Even the safest nodes can be considered hackable in modern era, hence in blockchain there is no room for confidence.

J. New Entry Validation Protocol

In blockchain, no node trusts the information/ transaction without proper validation. Let's say for an instance Tr_X received from node n_{enter}. The receiving node does not trust Tr_X without validating it. The node validates via the validation protocol which can be seen as a function as given in (11):

$$PrV : NXE -> \{True, False\}; (n, Tr) -> PrV(n, Tr) \quad (11)$$

Here 'N' is the set of all nodes in blockchain and 'E' is the set of all transactions. If $PrV(n_{enter}, TrX)$ is true then n_{enter} considers it as a valid entry and TrX is transmitted, if it is false then n_{enter} rejects the entry.

There are two types of invalid transactions: 1) Fake identity; 2) Unauthorized actions/without rights to do certain type of transaction. However, the prior one can be dealt at any node but the later one can only be validated by a complete node (which has a local copy of complete blockchain) to verify the authority based on prior transaction history.

K. Entry processing at Complete Node

When a transaction Tr_Xeventually received at a complete node called n_c, firstly it validates the identity by performing validation protocol $PrV(n, Tr_X)$. Secondly, it checks for transaction authority/rights based on prior transaction history record from its local database. If, Tr_X is valid then n_c appends it to local valid transaction list i.e.$L_{Loc}^{n_c}$ given in (12) and then transmit it to nearby nodes.

$$L_{Loc}^{n_c}.append(Tr_x) \quad (12)$$

Complete node 'n_c' creates a new block by adding into previously validated transaction. New block creation is given in (13).

$$B_{n_c} = (Tr_1, Tr_2, Tr_3, .., Tr_N) \quad (13)$$

Where, $Tr_i \epsilon L_{Loc}^{n_c}$ for 1<=i<=N and n_c calculates PoW for $(B_{n_c}^{Prev}, B_{n_c})$

L. New Block Emission

After the n_c creates and transmit new block B_{nc}^{new} it will be received by subsequent nearby nodes. Upon reception of B_{nc}^{new} at the receiving node, the node would do the validation as there is no trust in blockchain even if receiving from a complete node or miner who has claimed the PoW. After verifying if it is found to be valid it will be accepted or rejected.

M. Conflict of Versions

Due to distributiveness of blockchain there might be a case where a node n_1 has a different version than node n_2. This possible as there is no central control and no trust for each other. Upon reception of a different transaction record which does not match with local record they are placed in an intermediary block (*). This phenomenon is called conflict of version in blockchain. This conflict can be mitigated by the longest chain rule. The longest branch is retained and every node in the network adheres to the rule of consensus on the valid structure. Wang et al. [36] have discussed various consensus mechanisms to mitigate such conflicts.

N. Mitigation of Conflict of Version: Longest chain rule

As blockchain is a decentralized network all the nodes are independent entities and they are autonomous in mining the future blocks and link them with chains with the help of computation of current block hash by taking into consideration the previous block hash. When multiple versions of PoW are available in a blockchain it might arise conflict by creating a branch for each version of PoW. To mitigate conflict of multiple versions, we take into consideration only the longest chain that has been mined the most. As shown in figure 12, there are three versions A, B and C.

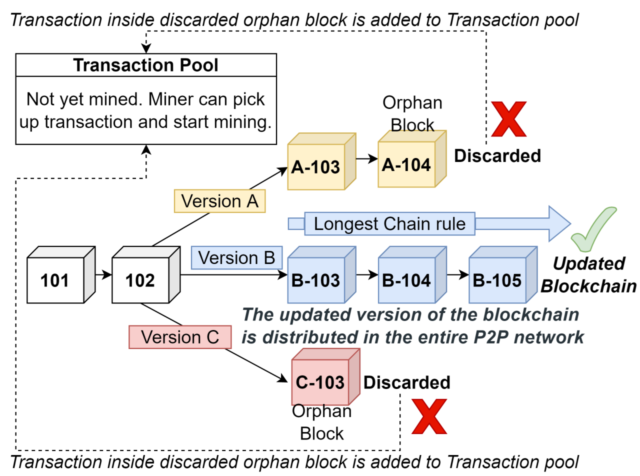

Figure 12. Mitigating Conflict of Version: longest chain rule

Version A has been mined twice with A-103 and A-104 blocks. Version B has been mined thrice with B-103, B-104 and B-105. Version C has been mined once as C-103. As per longest chain rule version B wins the competition here and is selected and updated as the correct version in blockchain P2P network. Here one important aspect must be highlighted about the computing resources available with a mining node. If mining node has faster GPU then it will be able to mine PoW faster hence would have higher probability to win the competition for conflict of version. Version A and C has been discarded as orphan blocks and transactions inside orphan blocks are put into the transaction pool, which may be picked up by future miners for PoW.

Conflict of Version is mitigated by consensus rules and protocols. One of the popular approaches is Nakamoto protocols for consensus [36].

O. Rules of Consensus

As there exists a conflict of version in blockchain, it is definitely requiring a solution to mitigate the conflict. To facilitate this, we have rules of consensus in blockchain. The most common approach is the complete node will retain the 'longest version' among all the local copies (*) it has. The meaning of 'longest version' is the one which requires maximum PoW.

5. SYSTEM IMPLEMENTATION

In this research, for the implementation of the Blockchain we used the Ethereum Blockchain platform. Ethereum is a Blockchain based distributed computing platform that is open source in nature. Here we built the smart contracts on a custom build Blockchain and executed those in the run time environment in Ethereum. The IDE used here is Remix IDE, a strong open source tool that helps in writing the Smart Contracts directly from the web browser. The testing and the debugging were performed using the Remix IDE. For proof-of-concept of successful Ethereum based blockchain deployment for SCM application we have created a Virtual machine test-bed comprising of 28 nodes (7 use-case of supply chain with 4 nodes for each supply-chain: Manufacture, distributor, retailer and consumer). The four functional nodes of a supply-chain have been deployed as 4 independent Oracle virtual machines (VMs) running on Ubuntu 14.04 as native OS. We have deployed Remix IDE over each of these VMs to simulate the seven different Supply-chain scenarios. Figure 13 shows the graphical representation of our Virtual Machine (VMs) test-bed for Ethereum based blockchain implementation.

The supply chain management is considered to have multiple nodes accessing the Blockchain, even possible at concurrent times. First the nodes were set, predefined with certain conditions to determine the type and the concurrency of the nodes. The run time environment used in the project is the JavaScript VM. The smart contracts were then developed accordingly. Being browser based, remix has the flexibility to use multiple accounts and addresses for deployment. The deployment system here can be accessed from both the computers and smartphones. A python-based automation tool, PyAutoGui is used for the auto-deployment of the Blockchain from a computer by controlling the mouse pointer's location programmatically for the auto-deployment of the Blockchain depending on the node user. A particular address in the remix account was set for the compilation and deployment.

Smart contracts were developed using Solidity, being contract oriented. Different methods were defined depending on the use cases and the types of the nodes, applying proper conditions maintaining the privacy and the security of each node. Numeric values are assigned to identify each node and to access them while deploying the Blockchain. Attributes are defined within the methods of the specific nodes displaying proper messages for user-friendly easy understanding. The common method, SHOWINFO allows any user to check the position or any attribute in the supply change, provides the node is specific. The status of the Blockchain is updated after each deployment.

A node needs to know the address of the account specified for the deployment. After compilation, the address has to be entered by the node user, followed by the numeric value of the node for deployment in a smartphone. In computers, the mouse pointer's location for the deploy button in remix is pre-fetched using PyAutoGui and on executing the python code, the deployment button gets activated and the blockchain gets auto deployed with the specified address. In this case, the node numeric value and the address is preset and need not to be changed manually. Conditions are set, such as to maintain the security and the confidentiality of one node from others. A particular user of a particular node type will be able to trace and access the details of a particular item only from same authorized access node only. Appropriate warnings and messages are displayed in case of a privacy breach, i.e. if any other user of a different node type tries to access a method of different node type then the system would show warning message to notify the same. A user of a particular node type is able to access the method of the same type only after deployment.

After deployment, proper messages are displayed to the node user. Certain qualities of the nodes are set and can be fetched for verification. There can be multiple manufactures, consumers and even distributor i.e. multiple node users of a particular node type. The same Blockchain can be deployed on a different or same address with the same or different node type simultaneously when it's already deployed on an address. For deployment $< accountaddress >$ has to be the input to the MINER and $< nodenumericvalue >$ to the THISIDENTITY . On deployment, the methods of the deployed contracts are visible and are ready for interactions. Figure 14 shows the deployment flow-chart of the algorithm used for the blockchain in Supply-chain management using Ethereum Platform.

The Ethereum based blockchain deployment process as discussed before has six functional nodes as Consumer Function, Distributor Function, Manufacturer Function, Regulator Function, Retailer Function and Supplier Function considered in practical system implementation for the scope of this work. As discussed before Remix IDE is used for JavaScript VM deployment of functional nodes and their data attributes. Figure 15 shows the screenshot of the Remix IDE window showing various functional node deployment over Ethereum using Solidity smart contracts. Each node has it set of attributes are functions and are explicitly authenticated to work on their assigned attributes. The figure shows the JavaScript functions for two sample cases *DistributorFunction()* and *RetailerFunction()*. However similar functionality programming is done using

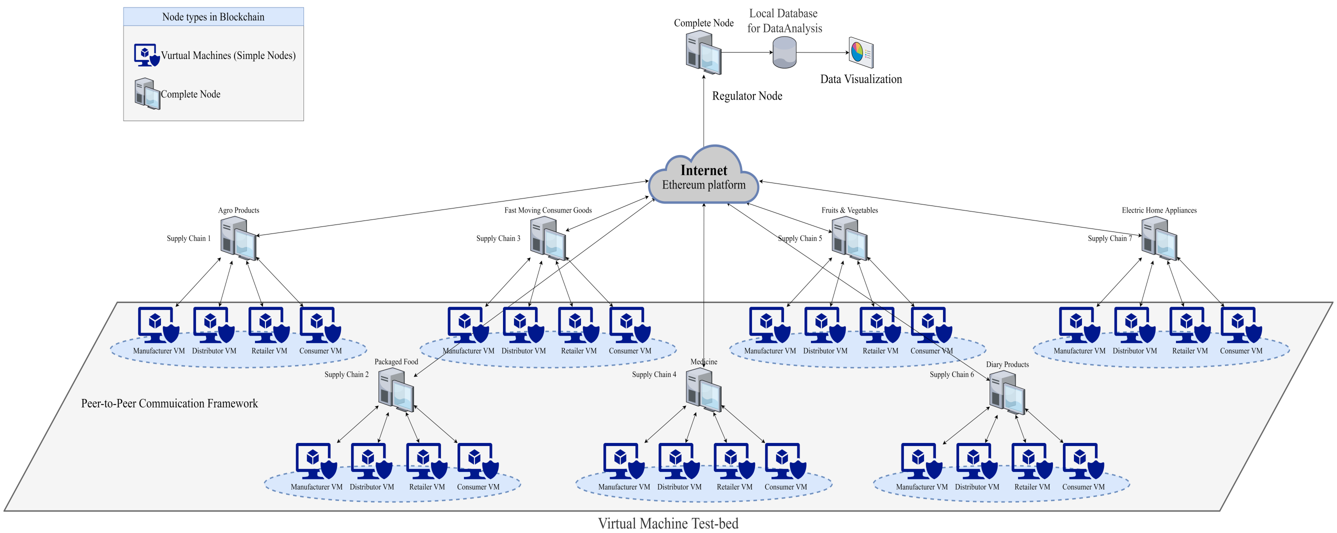

Figure 13. Virtual Machine Test-bed for proposed system implementation

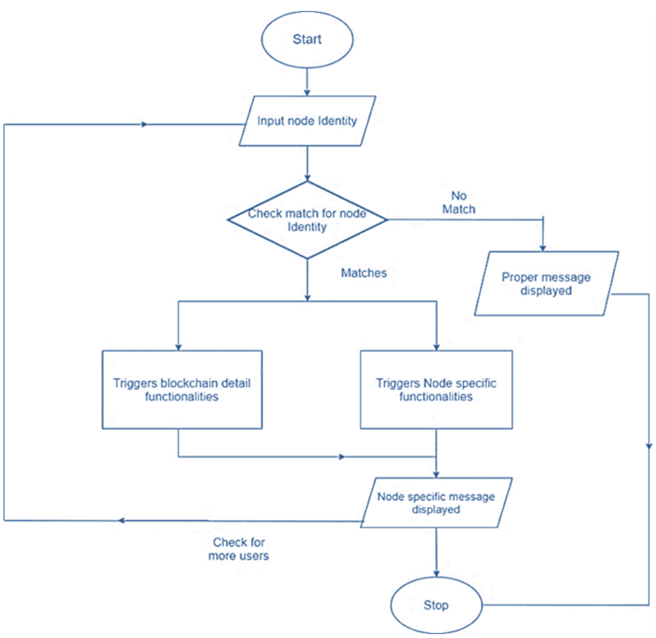

Figure 14. Flow-chart of the algorithm used for the Blockchain deployment in Supply-chain management using Ethereum Platform

JavaScript VM over web-based Remix IDE for other four functional nodes as discussed. Figure 16 shows the Remix IDE screenshot of output after successful deployment and triggering as a sample node with *ConsumerFuntion()*. Similar deployment cases are implemented for other functional nodes as part of the Ethereum blockchain.

Figure 17 shows the screenshot of Remix IDE with implementation of PyAutoGui which is a python-based Graphical User Interface (GUI) automation tool. PyAutoGui does the mouse click automation required for the web-based GUI of Remix IDE environment. This integration of PyAutoGui with web-based Remix IDE GUI would provide the much-needed feature to automate the all the six functional nodes which are part of the Ethereum-based blockchain using python script-based environment for deployment in our Supply chain management scenario.

6. RESULTS AND DISCUSSION

After successfully deploying the Blockchain, the methods can be triggered based on the type of node, displaying the required information in the Blockchain. All the data acquired from the regulator function which has access to all data and transactions over the blockchain deployment in our supply chain management system. For purpose of this study, we are monitoring four functional nodes Manufacture Function, Distributor Function, Retailer Function and Consumer Function nodes for multiple supply chains deployed over Ethereum blockchain. All the data collected are from a simulated deployment environment of seven products supply chain. For analysis and study, we have seven different use-case of supply chains scenarios considered in Indian context are: 1) Agro/Agricultural Products, 2) Packaged Food, 3) Fast Moving Consumer Goods, 4) Medicine, 5) Fruits and Vegetables, 6) Diary Products and 7) Home appliances. All the data are fed to the blockchain from simulated functional nodes over these seven supply chains. We have used 28 numbers of Oracle Virtual Machines (VMs) to simulate (4 functional nodes x 7 supply chains) 28 Remix IDE with PyAutoGui instances running for our simulation test-bed. All the simulated supply chain data is fetched by a single regulator functional node deployed over a dedicated Linux machine (Ubuntu 14.04 LTE) with MySQL database installed. All the structured data retrieved from the blockchain relational database is stored on the regulator local machine using MySQL database and PHP scripts for database handler. Table. IV shows the data acquired from Blockchain relational database. The retrieved

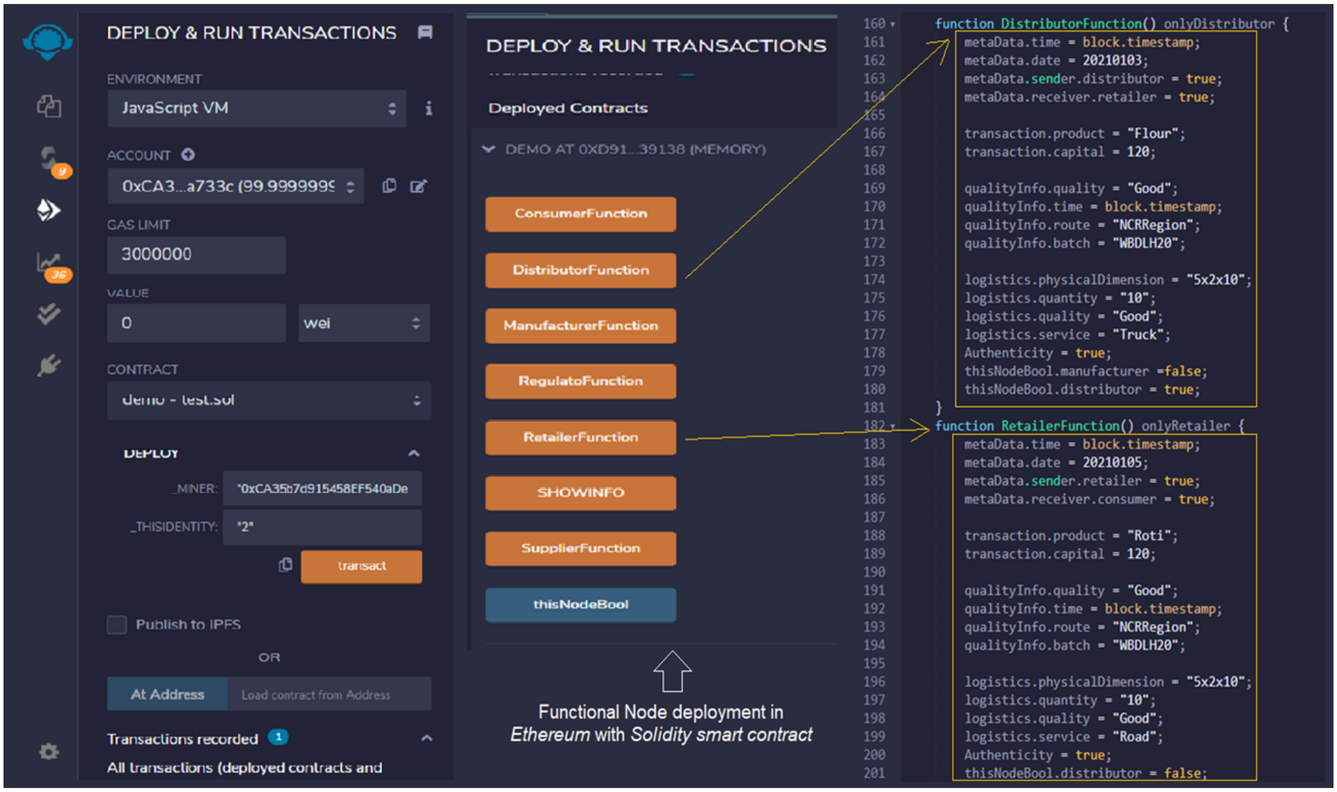

Figure 15. Digital SCM functional node deployment process using Remix IDE for Ethereum based blockchain

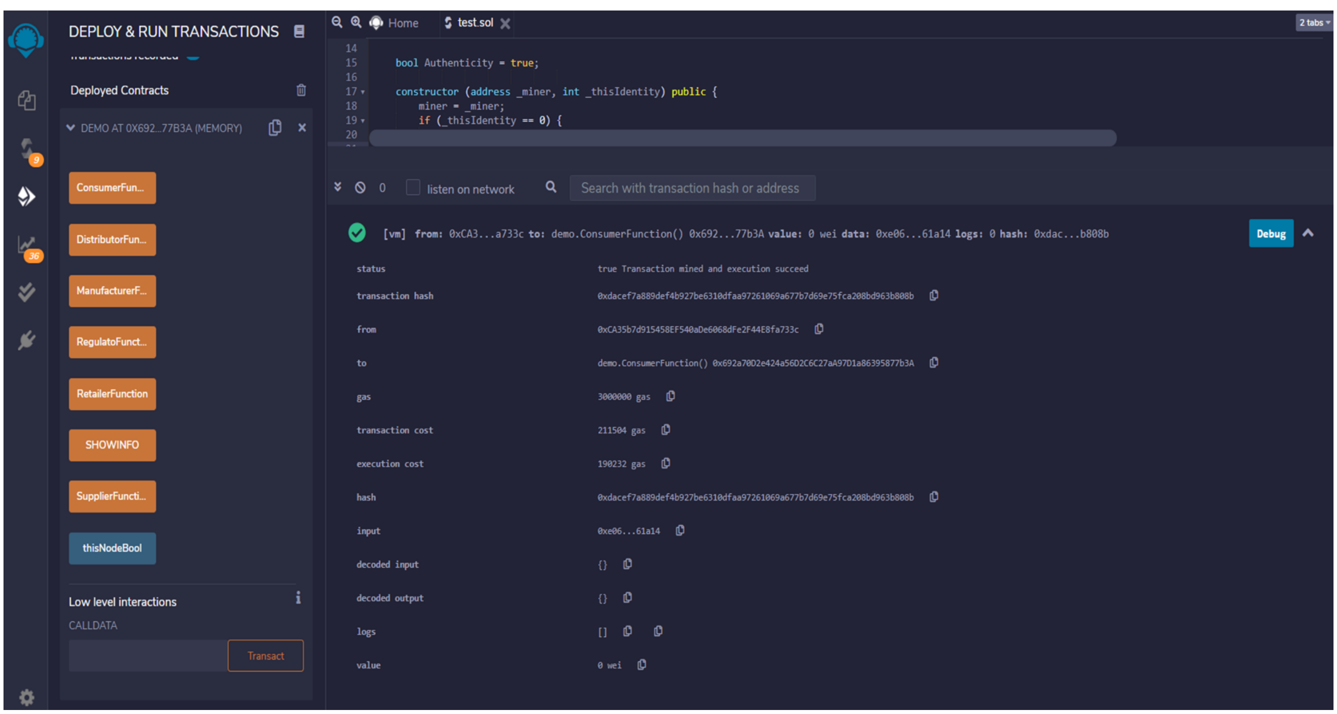

Figure 16. Output after successful deployment and triggering as a Consumer fucntional node of Digital SCM

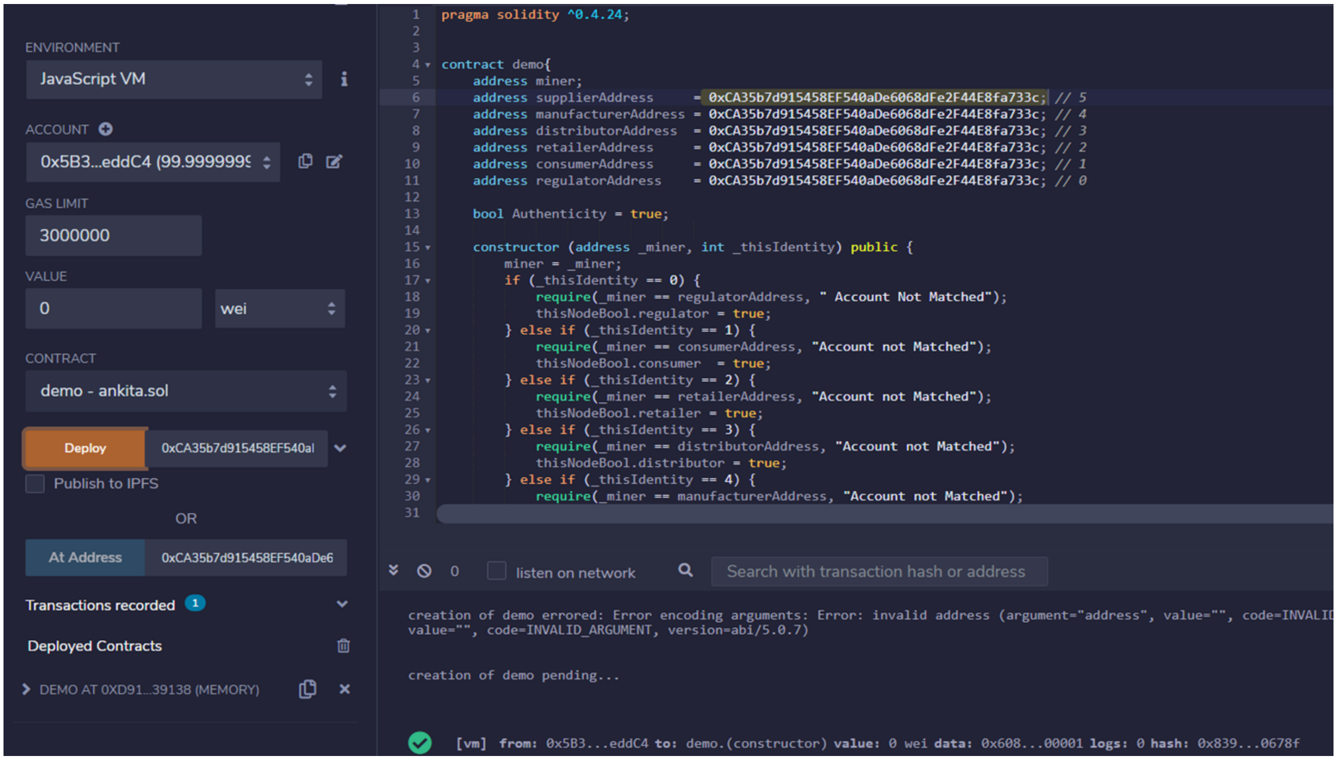

Figure 17. Digital SCM fucntional node deployment automation using PyAutoGui

database contents product IDs Info, Quantity, date and time of transactions, temperature (in °F) of the product at the time of entry, transaction unit price (in), Quality Index score (in a scale of [5 -1], where 5 being the Best to 1 being the worst), physical dimensions, batch number, Route and Distance (in k.m) and Logistics and Transport Mode of products in supply chain using Blockchain database.

In this paper, we have considered four types of tracking parameters to provide an analysis in the perspective of SCM application. The key information regarding any SCM would be the date and time of arrival/departure of package at differnet functional nodes (time-stamp tracking), distance travelled by packages between functional nodes (logistic tracking), finacial transaction/cost/price at different functional nodes (financial transaction tracking) and quality of product at different functional node (quality index tracking).

These four types of tracking are selected for practical use-case scenario of any supply chain implementation. These four type of tracking are extracted from the eleven parameters from relational database of blockchain implemented using Ethereum. However, this may be further extended as per specific requirements of any supply chain.

A. Time stamp tracking

Figure 18 shows the graph generated from the regulator node MySQL database for date and time Tracking of products at four functional nodes (Manufacturer, Distributor, Retailer and Consumer).

B. Logistic tracking

Figure 19 shows the graph generated from the regulator node MySQL database for logistic tracking transit distance of products between different functional nodes (Manufacturer-to-Distributor, Distributor-to-Retailer and Retailer-to-Consumer).

C. Finacial transaction tracking

Figure 20 shows the graph generated from the regulator node MySQL database for Tracking of Transaction amount per unit (in) of products at four functional nodes (Manufacturer, Distributor, Retailer and Consumer).

D. Product Quality Index tracking

Figure 21 shows the graph generated from the regulator node MySQL database for Product Quality Tracking (Quality Index Scale [5 – 1] at four functional nodes (Manufacturer, Distributor, Retailer and Consumer).

The system is scalable and not generic to any node of an organization. When a different method is triggered other than that of the particular node type, deployment fails with proper message displaying the cause. To make the deployment procedure easier and more convenient, the system was automated using PyAutoGui based on python scripting. First, the location details of the "Deploy" button was fetched programmatically and that data was used as a parameter to auto-click on that particular location using the PyAutoGui. A user has to execute the python code and the

TABLE IV. BLOCKCHAIN BASED RELATIONAL DATABASE IN SUPPLY CHAIN MANAGEMENT

Functional Nodes of Supply Chain	Product ID Info	Quantity (Units)	Date	Time	Temperature (in °F)	Transaction on Unit price (in INR)	Quality Index Scale(5-1)	Physical Dimensions in cm	batch (No.)	Route Distance Mode	Logistics & Transport
					Product: Agro Products						
Manufacturer	EB2659A	725	02-01-2021	12:25:49	96	676	5	11 x 9.7 x 4.1	g304b7	0	-
Distributer	EB2659A	725	10-01-2021	17:28:12	96.3	937	4	11 x 9.7 x 4.1	g304b7	1234	Railway
Retailer	EB2659A	725	22-01-2021	18:00:17	95.8	1043	4	11 x 9.7 x 4.1	g304b7	173	Roadway
Consumer	EB2659A	725	05-02-2021	11:26:37	97.5	1283	3	11 x 9.7 x 4.1	g304b7	34	Roadway
					Product: Packaged Foods						
Manufacturer	1C8927B	110	13-02-2021	9:12:26	66.2	450	5	30 x 25 x 15	ac08d4	0	-
Distributer	1C8927B	110	17-02-2021	17:12:44	78.3	587	5	30 x 25 x 15	ac08d4	783	Railway
Retailer	1C8927B	110	20-02-2021	14:27:18	82.1	620	4	30 x 25 x 15	ac08d4	271	Roadway
Consumer	1C8927B	110	25-02-2021	10:10:02	95.6	742	3	30 x 25 x 15	ac08d4	28	Roadway
					Product: Fast Moving Consumer Goods						
Manufacturer	FC1876E	512	26-02-2021	10:20:27	78.2	960	5	27 x 22 x 20	c045v2	0	-
Distributer	FC1876E	512	28-02-2021	12:18:11	87.4	1100	5	27 x 22 x 20	c045v2	1067	Railway
Retailer	FC1876E	512	01-03-2021	10:10:01	96.8	1250	4	27 x 22 x 20	c045v2	311	Roadway
Consumer	FC1876E	512	03-03-2021	20:06:20	98.1	1360	3	27 x 22 x 20	c045v2	76	Roadway
					Product: Medicine						
Manufacturer	A82955C	746	04-03-2021	22:12:10	59.7	675	5	15 x 7 x 7	d308b5	0	-
Distributer	A82955C	746	05-03-2021	21:09:17	61.8	933	5	15 x 7 x 7	d308b5	1389	Airway
Retailer	A82955C	746	06-03-2021	8:10:27	73.2	1143	5	15 x 7 x 7	d308b5	254	Railway
Consumer	A82955C	746	07-03-2021	14:20:19	76.6	1478	5	15 x 7 x 7	d308b5	17	Roadway
					Product: Fruits & Vegetables						
Manufacturer	DE1543E	88	08-03-2021	18:23:09	77.8	520	5	31 x 27 x 17	h789j0	0	-
Distributer	DE1543E	88	10-03-2021	23:11:37	83.5	756	4	31 x 27 x 17	h789j0	753	Airways
Retailer	DE1543E	88	11-03-2021	14:05:15	91.6	855	3	31 x 27 x 17	h789j0	117	Railway
Consumer	DE1543E	88	12-03-2021	16:22:18	100.1	932	2	31 x 27 x 17	h789j0	26	Roadway
					Product: Diary Products						
Manufacturer	2B8721F	480	13-03-2021	12:07:17	33.8	1028	5	20 x 30 x 40	j609k6	0	-
Distributer	2B8721F	480	14-03-2021	10:08:15	33.8	1250	4	20 x 30 x 40	j609k6	591	Airways
Retailer	2B8721F	480	14-03-2021	20:11:23	34.6	1340	3	20 x 30 x 40	j609k6	76	Roadway
Consumer	2B8721F	480	15-03-2021	08:19:11	41.9	1676	2	20 x 30 x 40	j609k6	7	Roadway
					Product: Electric Home Appliances						
Manufacturer	3E2958A	1000	16-03-2021	6:54:10	86.7	1500	5	7.7 x 35 x 35	f5r9t2	0	-
Distributer	3E2958A	1000	20-03-2021	7:30:34	88.9	1785	5	7.7 x 35 x 35	f5r9t2	1756	Railway
Retailer	3E2958A	1000	25-03-2021	12:44:00	90.7	1944	5	7.7 x 35 x 35	f5r9t2	436	Roadway
Consumer	3E2958A	1000	31-03-2021	11:38:32	100.5	2567	4	7.7 x 35 x 35	f5r9t2	57	Roadway

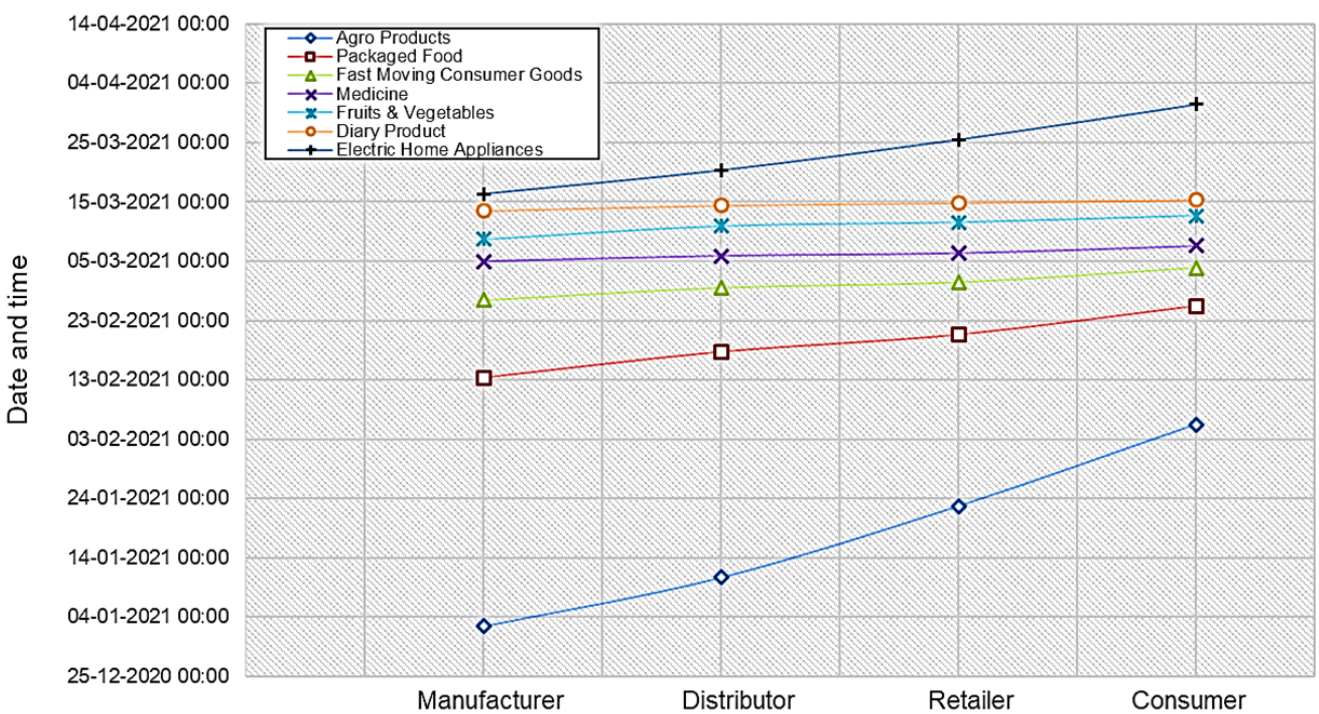

Figure 18. Date and Time Tracking of goods at functional nodes (Manufacturer, Distributor, Retailer and Consumer)

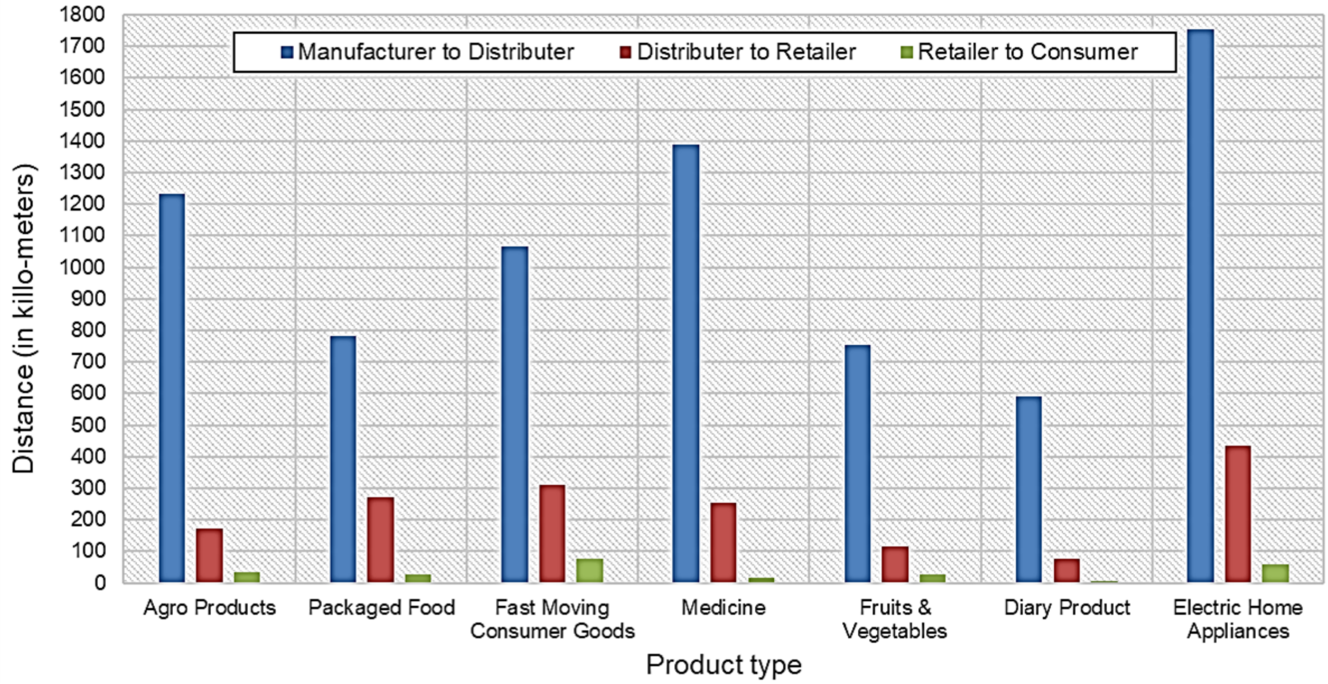

Figure 19. Logistic tracking with transit distance between different functional nodes

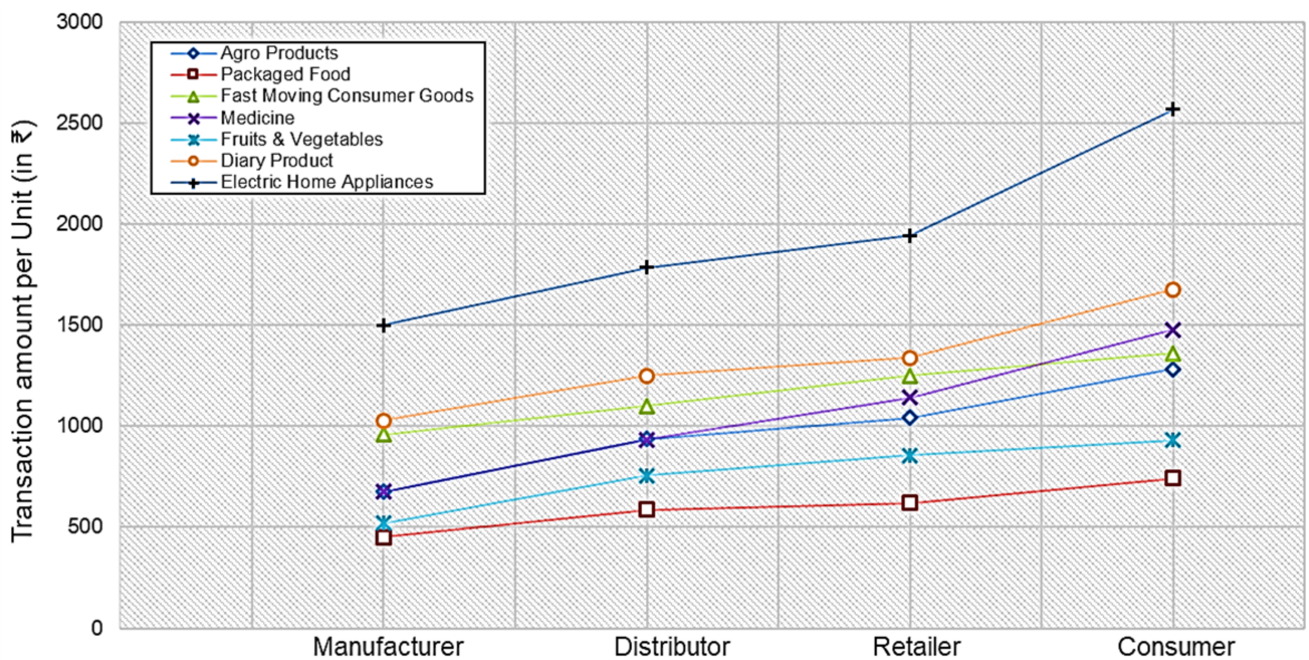

Figure 20. Tracking of financial transaction amount per unit (in Indian Rupee) at different functional nodes (Manufacturer, Distributor, Retailer and Consumer)

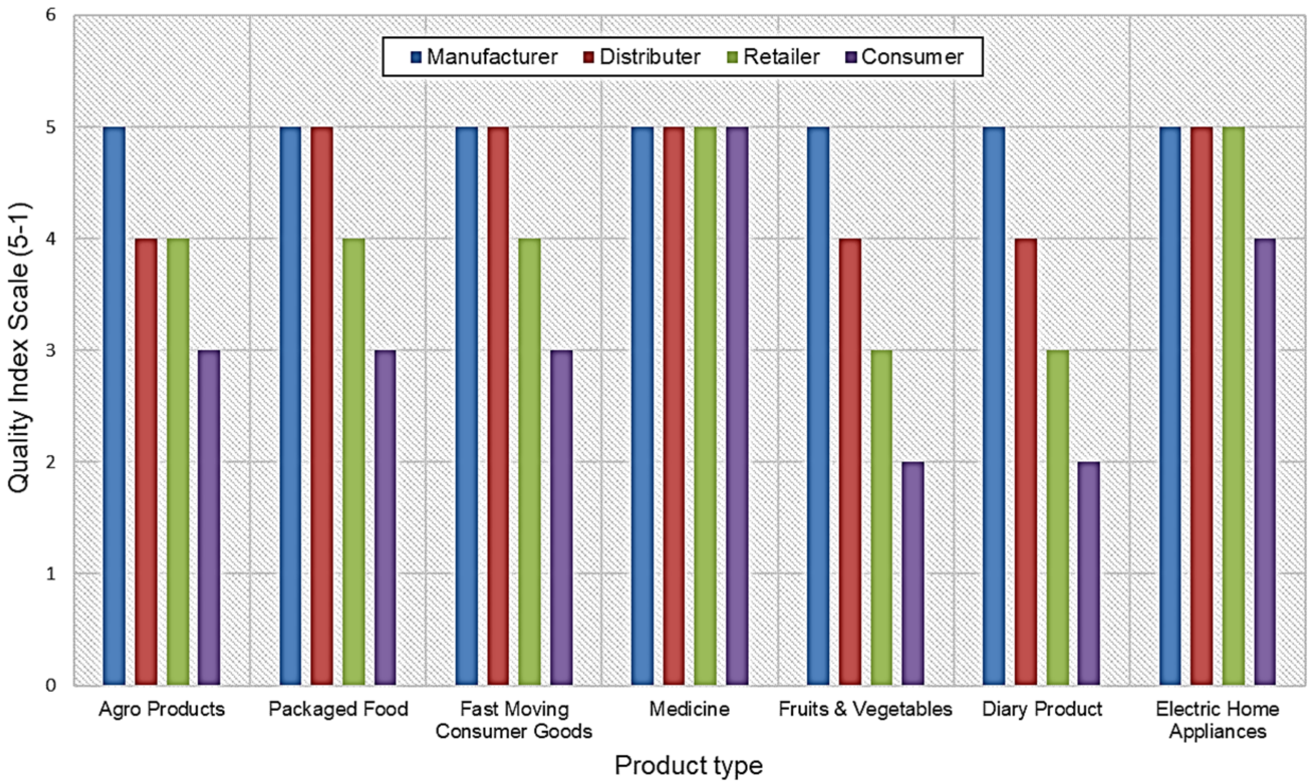

Figure 21. Product Quality Tracking Quality Index Scale [5 – 1] at different functional nodes

blockchain gets deployed automatically, provided the node numeric and the address are predefined or preset. However, the address validation can also be automated by fetching the location value of the address bar and using PyAutoGui. Considerably, having multiple systems for accessing each different node, automating deployment is a better approach.

In this work, we made a contract on remix.ethereum.org where a simple supply chain management is shown and how blockchain is used to know the status, condition and provenance of products. Nowadays provenance has become one of the most important issue for the consumers. Transparency in supply chain is also an important aspect. Hence keeping in mind of all these factors, a smart contract is created which involves supplier, manufacturer, distributor, regulator and miner.

Here it is observed that when respective addresses of each of the distributer, consumer, retailer, manufacturer and consumer is given in the address panel, complied and deployed then their respective information is shown in the console panel. The whole system is automated using 'PyAutoGui', which makes the process a lot easier.

In the result, it is observed that in the address bar consumer's address is given and with the help of PyAutoGui, the deployed button is pressed. With this the results are shown in the console panel. The addresses are unique in nature therefore only that particular person or organization can see the information in the console hence this feature of blockchain maintains privacy, which is necessary in supply chain management. This is done so that third party intermediaries are not able to misuse and obtain any data. The owners of such data (in this project suppliers, distributors, retailer, manufacturers etc.) are the sole controller and manager of the data.

There is a growing need for automation in supply chain and removal of middlemen, as well as huge data management. Hence blockchain in supply chain is the perfect solution.

E. Comparison of proposed IoT enabled blockchain in SCM state-of-the-art with some other recent work

This proposed state-of-the-art contribution in IoT-enabled blockchain based SCM is compared with some recent research work is shown in figure 22 (last 5 years: 2018 - 22) [5], [27], [34], [37], [38], [39]. The comparison is done with respect to technical aspects with development trend of blockchain (BC) aided SCM chronologically. Most of the recent research contribution proposed qualitative analysis on used of BC in SCM rather than practical deployment unlike this paper hence a quantitative comparison is far from realizable as of now.

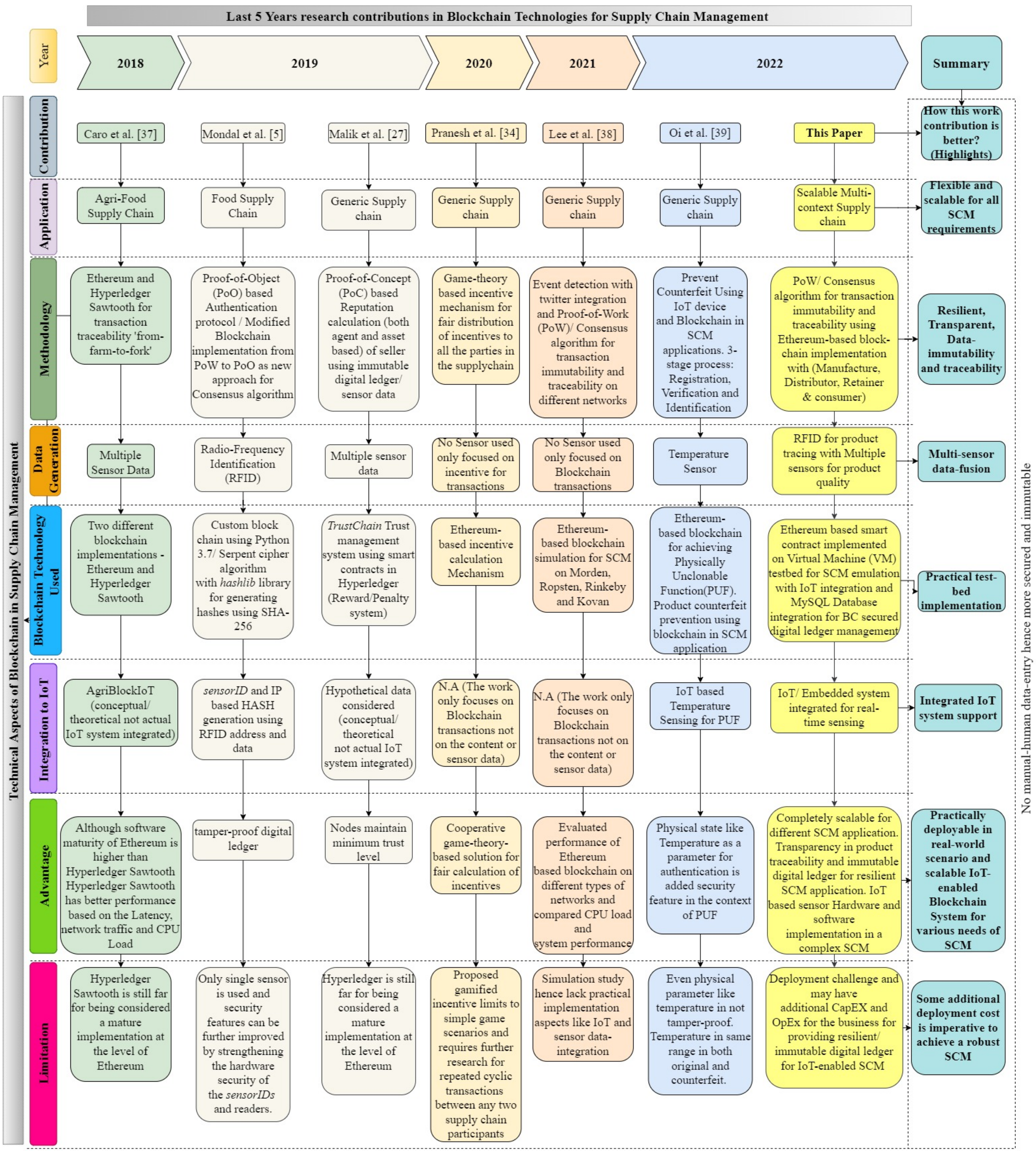

Figure 22. Comparison of proposed IoT enabled blockchain in SCM state-of-the-art with some other recent work (last 5 years: 2018 - 22)

F. Accuracy, Reliability of proposed IoT-Blockchain based SCM System Model

Implementation of Blockchain technology in supply-chain is to make the data immutable for restricting data manipulation at any of the stake holders and functional nodes. Decentralized / distributive nature of blockchain does not allow any particular node to manipulate the digital ledger, hence making the supply chain database secured and resilient. Due to the implementation of Ethereum based smart contracts the data entry at each functional node is highly accurate and immutable towards data-tampering. The IoT enabled RFID technology proposed in the paper is making the data-entry to the blockchain accurate and reliable with the help of digital technologies and automation and not depending on human manual entries. This makes the system more secured and tamper proof hence resilient. Use of IoT/ RFID and sensor-based system makes the overall working of the supply chain management (SCM) system more reliable. This paper presents a "Design and deployment of IoT enabled blockchain for SCM application using Ethereum". All the results presented in section 6 (figure 18 -21) is produced with blockchain deployment on a test-bed using system implementation presented in section 5. This process may be suggested as emulation of SCM system on a test-bed of 28 Virtual Machines (VMs) running four functional nodes (Manufacture, distributor, retailer and consumer) for 7 use-case scenarios. All the data presented in the result section is produced by the 28 VMs with 7 use-case supply-chain goods. All the parameters like Date, time, distance, transaction unit price, product quality is based on the emulation environment of blockchain deployment on the testbed SCM system. All the results are validated with original VM generated local data with the blockchain digital ledger and there is no change (immutability of blockchain database). When it comes to comparison of blockchain deployment on test-bed results with calculated or measurement results there is no difference at all. Because, blockchain database is tamper-proof hence no difference in measurement data and the blockchain data.

G. Limitations of the Proposed IoT-Blockchain based SCM System Model

- High Energy consumption and costly: More Computational resource required hence more energy consumption. Blockchain Mining require high-end GPUs to do computation hash mining. Latency or delay may be encountered to computation of digital ledger which may be considered as a tradeoff for the security and resilient Supply Chain Management (SCM) application deployment. The implementation cost and process in resource consuming hence expensive.

- Slow processing: As number of Nodes increases in blockchain the digital ledger calculation or computing process may slow down. This can be a major challenge as the SCM application involves large number of operational nodes like suppliers, manufactures, distributors, retailers etc.

- Hard to Scale: Unlike centralized systems Blockchain based systems are difficult to achieve scalability due to consensus methods.

- Lack of interoperability and Integration with legacy systems: Many SCM companies use legacy system hence it is sometime not feasible to replace all their existing infrastructure with blockchain based system. Blockchain suffers from interoperability issue as different blockchain based networks operates differently. All the SCM nodes must have sensors and communication systems for IoT based logistic tracking infrastructure to automation and tracking. Capital Expenditure (CapEx) required and maintenance of digital infrastructure require Operational Expenditure (OpEx). However, proposed system can substantially reduce the Man-power required for tracking and record keeping securely.

- Security flaws still exists and Blockchain technology is not yet matured: Blockchain as a technology is only few years old and not fully matured as a technology has many known security challenges and exploitable loopholes. For an example, 51 % attack. If anyone has more than 50 % of node in network he can manipulate ledger by compromising the complete blockchain. Double-spending may be another challenge. Blockchain system use decentralized network architecture hence nodes use private-keys which may be compromised.

- Lack of Expert Human resource: To deploy and management complex blockchain based SCM systems needs well-trained technical human resource which is hard to get and expensive at current time.

7. CONCLUSION

Blockchain is one of the revolutionizing technologies which has huge potential in securing the digital supply chain market. Supply chain is growing and has become more complex in nature. It involves lot of stakeholders and also relies on a number of intermediaries externally. Blockchain has been emerging and evolving day by day as a strong technology enabler which organizes and de-tangles all the data, documents and communication happening in the system. In this paper, we tried to implement a proof of concept prototype of deployment scenario of blockchain in supply chain management in Indian scenario. With the proposed system we succeeded in creating a smart contract which can be accessed by different people in different levels of management in the supply chain. The prototype is completely scalable and can be changed according to the type of supply chain. This prototype can further evolve on diverse technological and managerial aspects. Blockchain has eased up the process of managing and organizing a huge amount of data with the right features which are associated with it. Although, Blockchain makes all aspects of supply chain interconnected and secured, the energy intensiveness of Ethereum poses a major drawback in actual implementation. The PoW has multiple disadvantages such as high latency, low transaction rate and more energy expenditure [40]. Proof of Stake (PoS) is an alternative approach to consensus in blockchain that can overcome the drawbacks of PoW. Nevertheless, the future work should address many more aspects such as cryptographic ledgers, proof of origin, shared databases which will ultimately establish trust in the contract.

Blockchain has also diversified and is used in different fields such as medical, logistics, insurance, public sector and many more. Blockchain can further be implemented with other technologies such as Internet of Things, Networking and work on many promising areas. Blockchain can be a potential technology enabler as an emerging technology for secured and resilient Next-generation Cyber Physical System (NG-CPS) [41]. The blockchain may come in the application-layer of NG-CPS [42]. With this work we have tried to unveil practical design aspects of secured Ethereum-based blockchain deployment environment using solidity smart contract which can be scalable and flexible to specific needs of any supply chain.

Acknowledgment

We would like to thank Cypress Semiconductor University Alliance for providing CY8CKIT-042-BLE-A PIONEER KIT for prototyping of our IoT-base RFID sensing model and School of Electronics Engineering, Kalinga Institute of Industrial Technology, Deemed to be University, Bhubaneswar, INDIA for providing all the computational and laboratory resources for implementation of this work.

References

[1] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[3] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *The Review of Financial Studies*, vol. 32, no. 5, pp. 1754–1797, 2019.

[4] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE technology & engineering management conference (TEMSCON)*. IEEE, 2017, pp. 137–141.

[5] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired rfid-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019.

[6] B. Muessigmann, H. von der Gracht, and E. Hartmann, "Blockchain technology in logistics and supply chain management—a bibliometric literature review from 2016 to january 2020," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 988–1007, 2020.

[7] T. Guggenberger, A. Schweizer, and N. Urbach, "Improving interorganizational information sharing for vendor managed inventory: Toward a decentralized information hub using blockchain technology," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1074–1085, 2020.

[8] M. Du, Q. Chen, J. Xiao, H. Yang, and X. Ma, "Supply chain finance innovation using blockchain," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1045–1058, 2020.

[9] Q. Zhu and M. Kouhizadeh, "Blockchain technology, supply chain information, and strategic product deletion management," *IEEE Engineering Management Review*, vol. 47, no. 1, pp. 36–44, 2019.

[10] D. Shakhbulatov, J. Medina, Z. Dong, and R. Rojas-Cessa, "How blockchain enhances supply chain management: A survey," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 230–249, 2020.

[11] P. K. Wan, L. Huang, and H. Holtskog, "Blockchain-enabled information sharing within a supply chain: A systematic literature review," *IEEE access*, vol. 8, pp. 49 645–49 656, 2020.

[12] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A blockchain-based supply chain quality management framework," in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*. IEEE, 2017, pp. 172–176.

[13] S. NASIH, S. AREZKI, and G. Taoufiq, "Enhancement of supply chain management by integrating blockchain technology," in *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*. IEEE, 2019, pp. 1–2.

[14] N. N. Ahamed and R. Vignesh, "A literature review on blockchain technology for food supply chain management," *International Journal Of Computing and Digital System*, 2021.

[15] S. Yousuf and D. Svetinovic, "Blockchain technology in supply chain management: Preliminary study," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 2019, pp. 537–538.

[16] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang, and Y. Deng, "Data management in supply chain using blockchain: Challenges and a case study," in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2019, pp. 1–8.

[17] S. R. Niya, D. Dordevic, A. G. Nabi, T. Mann, and B. Stiller, "A platform-independent, generic-purpose, and blockchain-based supply chain tracking," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 11–12.

[18] R. Asyrofi and N. Zulfa, "Cloudity: cloud supply chain framework design based on jugo and blockchain," in *2020 6th Information Technology International Seminar (ITIS)*. IEEE, 2020, pp. 19–23.

[19] L. Su and H. Wang, "Supply chain finance research in digital bulk commodities service platform based on blockchain," in *2020 International Conference on E-Commerce and Internet Technology (ECIT)*. IEEE, 2020, pp. 341–344.

[20] ——, "Analysis on electronic warehouse receipt of bulk commodity in supply chain finance practice," in *2020 International Conference on Computer Information and Big Data Applications (CIBDA)*. IEEE, 2020, pp. 33–36.

[21] B. Hegde, B. Ravishankar, and M. Appaiah, "Agricultural supply

chain management using blockchain technology," in *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*. IEEE, 2020, pp. 1–4.

[22] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, and P. Lund, "Blockchain: A solution for improved traceability with reduced counterfeits in supply chain of drugs," in *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*. IEEE, 2020, pp. 1–5.

[23] Y. Yue and X. Fu, "Research on medical equipment supply chain management method based on blockchain technology," in *2020 International Conference on Service Science (ICSS)*. IEEE, 2020, pp. 143–148.

[24] S. Lei and W. Haiying, "Case study of how to help manufacturing enterprises obtain loan through supply chain documents on blockchain platform," in *2020 international conference on computer engineering and application (ICCEA)*. IEEE, 2020, pp. 192–195.

[25] L. Xu, L. Chen, Z. Gao, Y. Chang, E. Iakovou, and W. Shi, "Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 2018, pp. 1–5.

[26] S. Aich, S. Chakraborty, M. Sain, H.-i. Lee, and H.-C. Kim, "A review on benefits of iot integrated blockchain based supply chain management implementations across different sectors with case study," in *2019 21st international conference on advanced communication technology (ICACT)*. IEEE, 2019, pp. 138–141.

[27] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: Trust management in blockchain and iot supported supply chains," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 184–193.

[28] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven iot for food traceability with an integrated consensus mechanism," *IEEE access*, vol. 7, pp. 129 000–129 017, 2019.

[29] J. Ali and S. Sofi, "Ensuring security and transparency in distributed communication in iot ecosystems using blockchain technology: Protocols, applications and challenges," *International Journal of Computing and Digital System*, 2021.

[30] A. Mishra and M. Mohapatro, "Real-time rfid-based item tracking using iot & efficient inventory management using machine learning," in *2020 IEEE 4th Conference on Information & Communication Technology (CICT)*. IEEE, 2020, pp. 1–6.

[31] R. Shahin and K. E. Sabri, "A secure iot framework based on blockchain and machine learning," *International Journal of Computing and Digital System*, 2021.

[32] N. N. Ahamed, P. Karthikeyan, S. Anandaraj, and R. Vignesh, "Sea food supply chain management using blockchain," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. IEEE, 2020, pp. 473–476.

[33] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food safety traceability system based on blockchain and epcis," *IEEE access*, vol. 7, pp. 20 698–20 707, 2019.

[34] S. Pranesh, N. Viswanathan, M. Vijayalakshmi *et al.*, "Design and analysis of incentive mechanism for ethereum-based supply chain management systems," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2020, pp. 1–6.

[35] "How to represent a blockchain through a mathematical model," https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf, accessed: 2021-05-28.

[36] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *Ieee Access*, vol. 7, pp. 22 328–22 370, 2019.

[37] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*. IEEE, 2018, pp. 1–4.

[38] C.-H. Lee, H.-C. Yang, Y.-C. Wei, and W.-K. Hsu, "Enabling blockchain based scm systems with a real time event monitoring function for preemptive risk management," *Applied Sciences*, vol. 11, no. 11, p. 4811, 2021.

[39] S. Oi, K. Kaneda, and K. Iwamura, "Implementation of supply chain management system to prevent counterfeit using iot device and blockchain," in *2022 2nd International Conference on Image Processing and Robotics (ICIPRob)*. IEEE, 2022, pp. 1–6.

[40] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[41] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective," *International Journal of System Assurance Engineering and Management*, pp. 1–23, 2022.

[42] A. Mishra and A. K. Ray, "A novel layered architecture and modular design framework for next-gen cyber physical system," in *2022 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2022, pp. 1–8.

Ayaskanta Mishra Ayaskanta Mishra is currently Assistant Professor in School of Electronics Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar, India and pursuing Ph.D. He has received his master degree from IIIT, Pune, India (2011) and B.E. degree (Distinction) from Sathyabama Institute of Science and Technology, Chennai, India (2007). He has 11+ years of experience in academics/research and also worked in industry with SIEMENS India Ltd. He has many reputed WoS/SCOPUS indexed journals and conference proceedings to his credit. He has been appointed as reviewer (Publons recognised Peer-reviews) by many reputed journals and also technical committee member in International Conferences. He is professional society member of IEEE (ComSoc.), IET (U.K) and Life member of Indian Science Congress Association (ISCA). E-mail: ayaskanta.mishra@ieee.org

Sayan Karmakar Sayan Karmakar received his B.Tech degree in Electronics and Telecommunication Engineering at School of Electronics Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar, India (2021). A Tech enthusiast, trained in IoT, Cloud Computing, Computer Networking, Advanced Electronics along with experience in Data Science and Augmented Reality (AR). He was an intern at HighRadius Corporation (India). Email: sayankarmakar35@gmail.com

Ankita Dutta Ankita Dutta received her B.Tech degree in Electronics and Telecommunication Engineering at School of Electronics Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar, India (2021).She was an intern at HighRadius Corporation (India). E-mail: adutta0110@gmail.com

Ankush Bose Ankush Bose is currently working in Deloitte (India). He received his B.Tech degree in Electronics and Telecommunication Engineering at School of Electronics Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar, India (2021). A Tech enthusiast, trained in IoT, Cloud Computing, Computer Networking, Advanced Electronics along with experience in Data Science and Augmented Reality (AR). E-mail: ankush.bose.02@gmail.com

Manaswini Mohapatro Manaswini Mohapatro is currently working as Technology Lead at Infosys Technologies Ltd, India. She has received her B.Tech degree from BPUT, Odisha (2010). She has more than 11 years of experience in IT industry with domain expertise in broad spectrum of technologies. Her research interest includes IoT, Machine Learning, Artificial Intelligence and Blockchain technologies. She has reputed indexed journals and conference proceedings to her credit. E-mail: mana.mohapatro@gmail.com