Journal of Advanced Zoology

ISSN: 0253-7214

Volume ***44*** *Issue* ***Special Issue-2 Year 2023*** *Page* ***2116:2131***

Implementation of the Ethereum Blockchain for Supply Chain Management

Mr. Yogesh Dhotre[1*], Dr. B. S. Sonawane[2], Dr. Smita Kasar[3]

[1]PG Student, Department of Computer Technology, SKBP Polytechnic Kopargaon

[2]Associate Professor, Department of Computer Science and Engineering, MIT Aurangabad

[3]Professor, Department of Computer Science and Engineering, MIT Aurangabad

Mail- yogesh.kdhotre@gmail.com[1]

Article History

Received: 08July2023

Revised: 29 Aug 2023

Accepted: 12 Oct 2023

Abstract

This research looks at unique identity systems in supply chain management and how self-sovereign identities foster trust among the issuer, entity, and verifier. The article investigates blockchain technology in supply chain systems. According to recent research, blockchain applications may increase transparency, traceability, and efficiency in manufacturing and distribution. To increase privacy and transparency in end-to-end monitoring, the research advises incorporating self-sovereign identity into the supply chain. The study examines blockchain performance, including transaction and read throughput, latency, and resource utilization, using a hyperledger caliper to analyze supply chain performance. The research finishes with supply chain management issues. It is challenging to manage product and process integrity in a multi-stakeholder supply chain. Many current solutions suffer from data fragmentation, uneven provenance, and differing protocol limitations between distributions and processes. Blockchain is a pioneering technology that allows secure traceability and control, immutability, and stakeholder trust at a low cost. Blockchain use is increasing in many sectors, but supply chains confront substantial challenges in implementing it. This is the first report to look at blockchain-enabled supply chain concerns and prospects. We look at supply chain digitalization as well as GS1 standards and technologies. Compile a list of blockchain-enabled supply chain use cases and businesses. The technical and non-technical impediments to blockchain adoption for supply chain applications are investigated, as well as the applicability of consensus algorithms. Diagrams and assessments of blockchain ecosystem technology and tools Some critical future research areas are also suggested in order to achieve widespread blockchain-based supply chain traceability adoption. Finally, we introduce MOHBS Chain, a novel supply chain architecture powered by blockchain.

Keywords: Blockchain, Supply Chain Management, Hyperledger Caliper, Transparency, Traceability, Self-Sovereign Identities.

1. Introduction

The supply chain is made up of the businesses, procedures, resources, people, and information involved in the transportation of raw materials and components from the manufacturing stage to the retail shelf. Hypersegmentation, localization of product sources and manufacturing, Manufacturing 2.0, heightened consumer expectations, and end-to-end visibility for businesses, suppliers, and consumers are key drivers of conventional supply chain change [1]. As a consequence of these reasons, leading technology companies have begun joint efforts to improve supply chain automation by using a hybrid configuration [2]. To increase the supply chain's reliability, agility, and efficiency, a holistic approach that consolidated the previously different ordering, buying, manufacturing, and transportation processes was implemented. A variety of sensing, communication, storage, and processing technologies, including data science, the Internet of Things (IoT), 5G, cloud computing, and edge/fog computing, have improved the digital capabilities of supply chain organizational levels. This digital project has the potential to improve supply chain system integration and homogeneity. Uber, Careem, Alibaba, Netfix, and Airbnb, among others, profit from the present disruptive trend toward digital supply chains. The following technologies make it easier to oversee and supervise product handling at various locations throughout a supply chain: [3] robotic goods handling; [4] pick and drop autonomous vehicles; [6] a certification system; [7] an electronic healthcare records system; and [8] vision picking. End-to-end track and trace is based on the technological integration of supply chain divisions, which integrate previously separate pieces into a single system. While the words "tracing" and "tracking" are sometimes used interchangeably in academic circles, "tracing" suggests a more thorough investigation and reproduction of an object's or process's sequential movements, while "tracking" denotes a less rigorous observation of the working path.

2. How Blockchain works?

The source of money is the node's wallet (the one initiating the transaction). All transactions are first put in the unconfirmed transaction pool. The miners pick up a transaction when it occurs in the pool. Following the confirmation of a transaction, the data involved in the transaction is put into the SHA256 hashing algorithm (which needs six parameters) to generate a hash. In a similar vein, the Merkle tree is built by hashing all verified transactions and eventually agreeing on a single hash value known as the Merkle root. Each confirmed transaction is put into a pool that the miners themselves oversee. After the Merkle root has been formed, the nodes tackle the difficulty of creating the nonce value. The blockchain containing the newly formed block is broadcast to the network's other miners by the first successful miner. To generate this new block, the SHA256 hashing algorithm was used with the generated nonce and five additional parameters. All other miners instantly stop producing nonces and start confirming the winner's copy of the blockchain. Once more than 51% of miners have validated the authenticity of the shared chain, it is replicated for all miners via DLT. Figure 4 depicts the insight acquired from this method. Figure 5 depicts the blockchain protocol stack as well. For a more in-depth discussion of blockchain and its numerous features (functioning, applications, issues, and so on), the reader is advised to read [11].

2.1 Blockchain in smart supply chain

Attaining verifiable provenance and combating fraudulent and counterfeiting operations are two issues inherent in modern supply chain traceability systems that are impractical or impossible to overcome with current technology. The current version of provenance systems [12] uses both centralized and decentralized methodologies. Centralized architectures are vulnerable to three possible problems: (i) a single node assault, (ii) data manipulation, and (iii) information leakage. The capacity to generate and disseminate visibility event data on digital and physical things inside and across organizations is what characterizes a distributed architecture, including an EPCIS-based system. EPCIS-based systems are still vulnerable to data tampering and data loss [13]. Despite this, the bulk of existing Internet of Things (IoT) solutions continue to depend on centralized cloud infrastructure, presenting security flaws such as restricted visibility, auditability, data lock-in, and secrecy [14–16]. Due to its offering of three basic benefits in cost-effective IT solutions, blockchain offers itself as a viable technical solution to meet these challenges: (i) safe control and traceability; (ii) data immutability; and (iii) trust establishment. This innovative technology has the potential to drastically alter the worldwide functioning of all technologies. Supply chain management [17], asset management [19, 20], land-record registry traceability [21], vehicular network [22], e-contracts [23], retail [24], decentralized exchanges [25], business modeling [26], energy trading and sharing [27], transaction process automation [28], and mission-critical scenarios [29] have all used it. Within the technical, professional, and other stakeholder groups, blockchain has both supporters and adversaries.

2.2 Benefits of using blockchain in supply chains

The potential advantages of using blockchain technology in supply chains are many. Increased openness is a key benefit. Because of its immutability and storage on the blockchain, the information on the distributed ledger can be relied on by all parties in the supply chain. This openness encourages more cooperation and information sharing by making it easier to identify and prevent supply chain fraud.

An additional significant advantage is increased safety. Because of the installation of cryptographic methods inside the blockchain, changing or altering data within a supply chain is very difficult. Through its decentralized and distributed design and extensive security layer, it protects sensitive data such as transaction histories and product origins from compromise by lowering the likelihood of system-wide intrusions.

Furthermore, blockchain technology improves supply chain transparency. It gives total visibility across the supply chain, alerting all stakeholders to the position of their items on a constant basis. This is particularly beneficial in industries such as medicine and food, where customers place a high value on reliability and safety. When product recalls or quality issues emerge, blockchain technology may help firms mitigate the effect on customers while also lowering financial losses. The features listed above make blockchain a potentially important tool for supply chain management in the twenty-first century, as they allow firms to simplify processes, cut costs, and inspire confidence among business partners and consumers.

2.3 Applications of using blockchain in supply chains

Each of the several possible blockchain supply chain applications has the potential to have a significant impact on the manufacturing, distribution, and retail sectors. In the realm of provenance monitoring, blockchain technology may be used to maintain an auditable and

immutable record of a product's path from maker to customer. This is especially useful in areas like agriculture and luxury goods, where buyers appreciate authenticity and want to know where their food comes from. The unchangeable record that blockchain technology may employ to verify product authenticity reduces the danger of counterfeit products. Another key use is supply chain optimization. Through the simplification and automation of transactions via smart contracts, blockchain technology improves the efficiency of supply chain operations. When certain circumstances are satisfied, such as the item being successfully delivered, a smart contract may autonomously follow out pre-established actions, such as beginning payments. Reduced time spent on administrative tasks, faster order-to-cash cycles, and fewer mistakes all contribute to improved supply chain efficiency and cost reduction.

Blockchain technology has the potential to improve trade finance, especially for multinational transactions. Blockchain technology has the ability to speed transaction settlement and minimize the time and expense associated with international commerce by digitizing trade-related documentation and automating operations. It improves openness and honesty among trade partners, lowering the risk of conflicts and deception, making it a desirable option for international firms. The use cases shown above demonstrate the adaptability of blockchain technology in terms of increasing supply chain efficiency, fostering more transparency, and bolstering the security and integrity of financial transactions.

2.4 Challenges of in supply chains using blockchain

Several hurdles must be overcome before blockchain technology can be fully implemented. The demand for consensus among supply chain actors is a key impediment. Standardized protocols, data formats, and standards are required for the proper deployment of blockchain technology. Consensus-building may be very difficult in a global, complicated supply chain with various players. Conflicting interests, the need to build trust among participants, and resistance to change are all reasons that might stymie agreement and acceptance. The problem of scalability in blockchain networks is another obstacle. Due to the frequency of information and transactions within a supply chain, blockchain networks may be necessary to calculate massive amounts of data. Current blockchain systems may have transaction throughput and scalability difficulties, especially in the case of public blockchains like Bitcoin and Ethereum. Confronting the significant obstacles offered by a global supply chain's efficiency and security needs is a complicated technical conundrum.

The use of blockchain technology in supply chains raises worries about data anonymity and security. Although blockchain technology is inherently safe, adding data to the ledger must be done with the utmost care. Financial information, product information, and shipment details are all examples of sensitive supply chain data that should be protected. Robust encryption and access restrictions are essential to guaranteeing the secrecy of individual data while respecting the public nature of a blockchain.

Although blockchain technology has great potential in the field of supply chains, it is not without obstacles and does not serve as a panacea. To successfully incorporate blockchain into supply chain processes, firms must efficiently manage the challenges of consensus, scalability, and data protection and security. To overcome these obstacles and fully use the

possibilities of blockchain technology in the field of supply chain management, thorough stakeholder collaboration and preparation are required.

3. Emergence of Blockchain-enabled supply chain

Blockchain technology is being used in supply chain applications to increase process optimization and efficiency, notably in the financial and industrial sectors. Blockchain is one of the most interesting new technologies due to its potential to disrupt established systems and its easy interaction with the Internet of Things. This technological convergence is assisting firms in improving communication and cooperation with important constituencies, such as present and future customers. Businesses in the food and pharmaceutical industries, for example, are allegedly suffering significant financial losses as a result of a variety of supply chain issues. Selling counterfeit products, product theft, the gray market, fraud, and product recalls are a few examples. These factors have resulted in a trend among supply chain players toward more transparency and traceability. Because of its immutability, transparency, security, and fault tolerance, blockchain holds promise as a solution, at least for trust and traceability problems. There are currently firms employing this technology to help with the process, and some of them have had positive results. Walmart and IBM launched a trial project to monitor mangoes from farm to table [30]. Walmart, IBM, and Beijing Tsinghua University collaborated to create a model for monitoring and tracking in the Chinese pig industry using blockchain technology. IBM has teamed with Walmart as part of the IBM Food Trust initiative to integrate blockchain technology into their respective food supply chains. Walmart's leafy green vegetable suppliers have already been warned that their data must be transferred to the blockchain by September 2019. The latest current details on Walmart's initiatives to give unparalleled transparency to the food supply chain.

3.1 The Evolution of Identity Management Systems

Due to the increasing digitization of our lives, identity management systems (IDM) have developed in a dynamic way. Identity management was primitive in the early days of the internet, with basic username-password combinations acting as the main form of authentication. These systems were susceptible to breaches, which might have resulted in identity theft and illegal access. Single Sign-On (SSO) solutions arose in response, enabling users to access numerous services with a single set of credentials. They did, however, have security and control restrictions.

The introduction of multi-factor authentication (MFA) and biometric authentication was the next key stage in IDM. MFA increased security by asking users to supply more than a password, such as a one-time code texted to a mobile device. Biometric identification, such as fingerprint and face recognition, added ease and security to IDM. These innovations improved the user experience while making account compromise more difficult for unauthorized actors. Aside from these developments, there was an increasing focus on user-centric identity management, which gave users greater control over their digital identities and personal data.Blockchain technology and self-sovereign identification (SSI) are the most current developments in identity management systems. Blockchain technology offers a secure and immutable record for identification data, minimizing the need for centralized identity providers. Individuals with SSI have complete control over their digital identities, selecting what information to disclose and with whom. These improvements are intended to provide users with better privacy, security, and control over their digital identities, therefore lowering

the danger of identity theft and data breaches. Furthermore, they have the potential to alter a variety of sectors, ranging from banking to healthcare, by allowing safe and fast identification verification and sharing while preserving individual privacy rights. Identity management solutions will most certainly continue to adapt and develop as the digital environment evolves to suit the ever-increasing needs for security and convenience in the digital era.

Evolution of Identity Management System

3.2 Silo Model

In the context of blockchain, the Silo Model refers to a scenario in which distinct blockchain networks or platforms operate autonomously with no interoperability or communication between them. Each blockchain in this scenario functions as a distinct "silo," with its own set of rules, consensus methods, and data structures. While this paradigm may give some autonomy and security, it also presents significant issues, especially when data exchange and cooperation across multiple blockchain ecosystems are required.

The lack of interoperability is a key concern with the Silo Model in blockchain. Different blockchains often employ incompatible protocols and standards, making communication and data sharing problematic. This lack of interoperability might impede the smooth interchange of assets, information, and value across various blockchain networks, limiting blockchain technology's potential advantages.

Furthermore, the Silo Model may lead to duplication and inefficiency. Organizations or sectors that employ many segregated blockchains may duplicate efforts in terms of infrastructure maintenance, security measures, and development initiatives. This may result in higher operating expenses and complexity. To solve these issues, there is a rising focus on establishing blockchain interoperability solutions and standards that enable various blockchains to interact more fluidly together, simplifying data and asset transfers while ensuring security and privacy. These activities attempt to break down walls across blockchain networks, resulting in a more linked and efficient environment for blockchain technology adoption.

3.3 Federated Model

The federated model, also known as the federated blockchain model, is a blockchain architectural method that incorporates characteristics of both public and private blockchains. Multiple companies or entities collaborate to form a consortium or network of blockchain nodes under a federated model, where each member maintains a node and shares governance. This method is often used in situations where businesses need to securely interact and exchange data while maintaining some level of control and privacy.

The capacity of the federated architecture to achieve a compromise between the openness of public blockchains and the control of private blockchains is one of its primary features.

Participants in a federated network have a vote in the blockchain's governance and regulations, allowing for collective decision-making while maintaining a degree of confidence among known organizations. This makes it appropriate for scenarios in which several businesses must collaborate on a shared blockchain without entirely losing control. Furthermore, the federated paradigm may improve scalability and performance. The network can manage a larger number of transactions and data more effectively than a centralized system since the tasks of managing blockchain nodes are distributed among multiple participants. This is especially useful in sectors that demand rapid and dependable transaction processing.

The federated concept, however, is not without its difficulties. It may be difficult to establish governance, define rules, and ensure that people interact properly. Furthermore, if the governance structure is not well-balanced, worries about centralization may develop, possibly weakening some of the main concepts of blockchain technology. Nonetheless, the federated model offers a flexible way for enterprises looking to reap the advantages of blockchain while maintaining some level of control and privacy inside their network.

3.4 User-Centric Model

In the context of digital identity and data management, the user-centric approach reflects a paradigm shift in which people acquire greater control over their personal information and how it is shared across multiple digital platforms and services. In older models, companies and service providers often controlled user data, raising issues about privacy, security, and the exploitation of personal information. However, the user-centric paradigm allows people to choose what data they share, with whom, and for what objectives. Improved privacy and data management are two of the key benefits of the user-centric strategy. Users may opt to share only the information required with service providers, decreasing the risk of overexposure and data breaches. This strategy is consistent with emerging data protection rules, such as Europe's General Data Protection Regulation (GDPR), which emphasizes user permission and data minimization. Individuals may utilize tools and platforms under the user-centric paradigm to manage their digital identities and regulate the data they share. To maintain the confidentiality and immutability of identity-related information, these technologies often make use of blockchain technology and decentralized identifiers (DIDs). This paradigm fosters confidence between users and service providers by increasing user autonomy and transparency. It does, however, pose certain obstacles, such as the need for broad adoption and data management education, as well as the creation of strong and user-friendly identity management systems. Overall, the user-centric paradigm marks a substantial change in the approach to digital identity and data management, with an emphasis on enabling people to take control of their personal information in the digital environment.

3.5 Self-Sovereign Identity

Self-sovereign identification (SSI) is a ground-breaking approach to digital identity management that gives people complete control over their personal data and how it is shared. Individuals often give control of their data to centralized authorities or service providers in conventional identification systems, posing privacy and security issues. The goal of SSI is to provide people the opportunity to establish, own, and manage their digital identities in a safe and decentralized way.

The use of decentralized identifiers (DIDs) and verified credentials is one of the main ideas of SSI. DIDs are individual-specific, self-generated identities, while verified credentials are assertions provided by trustworthy organizations (such as governments or institutions) that people may submit to confirm their identity without exposing the underlying data. This design improves privacy by allowing only required information to be disclosed, lowering the risk of identity theft and data breaches.

SSI also facilitates digital identity interoperability across platforms and services, encouraging a unified user experience. Users may take their digital identities with them across several online services, avoiding the need to register or establish new accounts on a regular basis. Individuals benefit from this since it increases trust and security in online interactions. However, broad implementation of SSI is fraught with difficulties, including the requirement for established procedures, user education, and legal and regulatory adjustments to accommodate this novel approach to identity management. Nonetheless, in an increasingly linked world, self-sovereign identification has the ability to empower people, safeguard their privacy, and improve the security of digital interactions.

3.6 Use of Self Sovereign Identity

As it overcomes many of the issues associated with conventional identification systems, self-sovereign identity (SSI) offers a broad variety of possible use cases across multiple industries. Here are a few examples of where SSI may be used:

Digital Identity Verification: SSI has the potential to transform digital identity verification. Individuals may securely keep verified credentials in a digital wallet, such as passports, driver's licenses, and educational diplomas. They may submit certain credentials when asked to establish their identity without providing any additional personal information. This use case is especially significant in online banking, e-commerce, and remote service access, where safe and user-controlled identity verification is critical.

Healthcare: SSI has the potential to alter the healthcare business by allowing people to securely control their health information and share it as required with healthcare providers. Patients may have control over their medical history, medications, and test results, ensuring data accuracy and privacy. This use case is notably useful in telemedicine, medical research, and emergency situations where immediate access to a patient's medical history is critical.

Access to Government Services: SSI may make it easier to get government services and benefits. Citizens may use their digital IDs to verify their identity while paying taxes, voting, or applying for social services. The self-sovereign identification concept has the potential to minimize fraud, streamline bureaucratic procedures, and give individuals greater control over their contacts with government institutions. Several governments throughout the globe are investigating or deploying SSI-based citizen service solutions.

These examples show how SSI may improve security, privacy, and user control in a variety of applications. However, the effective implementation of self-sovereign identification is dependent on the creation of interoperable standards, the widespread use of digital wallets, and ongoing efforts to educate people and organizations about the advantages of this novel approach to identity management.

4. Designed Supply Chain System

A supply chain is a series of actions used to provide a product or service to a customer. Transferring and processing raw materials into completed commodities, transporting those goods, and delivering them to the end customer are all part of the activities. The supply chain includes organizations such as producers, suppliers, warehouses, transportation firms, distribution centers, and retailers. The goal of supply chain management is to improve efficiency by coordinating the operations of the many supply chain actors. By doing so, a company may be able to outperform its rivals and enhance the quality of its goods, both of which may lead to increased sales and revenue.

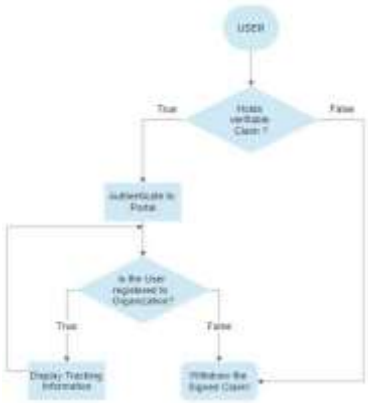
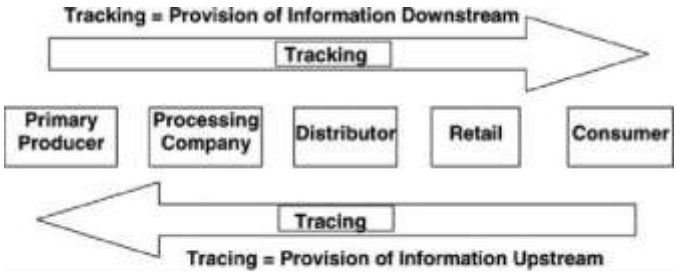


Fig. 6. Algorithm of Proposed System

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract SupplyChain {
    address public owner;
    uint public productCount = 0;

    struct Product {
        uint id;
        string name;
        uint price;
        address owner;
        address payable buyer;
    }
    mapping(uint => Product) public products;
    event ProductCreated(uint id, string name, uint price, address owner);
    event ProductPurchased(uint id, string name, uint price, address owner, address buyer);
    constructor() {
        owner = msg.sender;
    }
```

```
    modifier onlyOwner() {
        require(msg.sender == owner, "Only the contract owner can execute this.");
        _;
    }

    function createProduct(string memory _name, uint _price) public onlyOwner {
        productCount++;
        products[productCount] = Product(productCount, _name, _price, msg.sender,
payable(address(0)));
        emit ProductCreated(productCount, _name, _price, msg.sender);
    }

    function purchaseProduct(uint _id) public payable {
        Product memory _product = products[_id];
        require(_product.id > 0 && msg.value >= _product.price, "Product does not exist or
insufficient payment.");
        _product.owner = msg.sender;
        _product.buyer = payable(msg.sender);
        products[_id] = _product;
        emit ProductPurchased(_id, _product.name, _product.price, _product.owner,
_product.buyer);
    }
}
```

Our suggested concept is based on the Ethereum blockchain, where we authenticate users at each stage and record their activity in the distributed ledger. The authenticity is verified using the self-soverign identity paradigm. The blockchain uses smart contracts to authenticate any user, granting access to information for tracking (see Figure 3.2). However, in the smart contract procedure, the user is directed to supply verified credentials in order for the contract to be initiated, and their actions are then logged. Let me provide an example to illustrate this. When Nike chooses to develop a limited-edition sneaker for its customers, it begins collecting raw materials in bulk, such as polyester, wool, and so on, from unknown sources. Because the organization and its operations are dispersed around the world, it is difficult for them to confirm the legitimacy of every source. Because the firm is devoted to product quality, it is more crucial for customers to know that its product is authentic. After the product is made, an SKU is assigned to each product line, but throughout the transportation process to the merchant, the product may wind up in the hands of people who can make duplicates of the same product. Even with SKUs in place, it is difficult to comprehend. Because all of these processes are opaque from the beginning of supply to the end of demand, their accountability is called into doubt. Blockchain may alleviate this problem by maintaining a record of all actions and providing self-soverign identification.



Source: Schw gele (2005)

Fig. 8. Issuing and tracing of Commodity in Supply chain

The SSI has three components that contribute to system trust: issuer, verifier, and identity holder. Any individual who is directly or indirectly engaged with the firm is considered the identity holder. The verifier is the firm that provides the goods for the clients, and the issuer is any entity that gives verifiable credentials, such as a passport or ID card, in which the company has faith. When an identity holder attempts to use a service for monitoring his or her package, the service provider must be provided with verified credentials. i.e. business. In the situation described above, the user is given a verified credential, which is kept in the user's digital wallet. Because it is in encrypted format, anytime it uses the service, the user must express approval because he possesses the private key to his wallet. The firm validates the validity by searching the distributed ledger, or blockchain, for the issuer's signature. All middlemen are removed in this process, and the user has complete control over where it transmits its identity and other sensitive information. The privacy of all stakeholders is protected at all costs. Through the distributed ledger, the blockchain may also keep track of other information.

We simulated the fundamental supply chain network while keeping the stakeholders, issuer, and verifier in mind. We utilized the Solidity programming language to develop smart contracts and the truffle framework,Ganache," to build a blockchain on a local host. We establish supply chain entities, each with its own set of properties that must be submitted to Verifier. Every time a smart contract is executed, it generates a hash that may be used to trace the action.

- The user 'CT ' registers himself with DID (decentralized identity) issued by the 'Claim Issuer' to the vendor. The vendor verifies the person and keeps ledger of all the activity done by 'LT'
- When the user wants to track his package, it does so by providing a verifiable claim', which can be signed by entity itself with its private key (using DID).
- The distributed ledger uses DID to hold account of activity also keeping in mind the privacy of the user.

However, this distributed ledger technology is still in its early stages of adoption. Traditional supply chain systems continue to suffer from several technological

inefficiencies, such as scalability and diverse systems, which may be solved by using blockchain technology. With further study and development, blockchain has the potential to transform supply chain management.

4.1 Performance Analysis

We perform the testing and analysis using benchmarkingtool of the simulated blockchain. The model represents the supply chain of automobile industry.

4.2 Experimental Analysis

Assessed the performance of the Ethereum blockchain by modeling a supply chain system model. It implements smart contracts at every stage of the process, from procurement to distribution, and validates stakeholders using the self-sovereign identity paradigm.

Table 1. Analysis of Test Network

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
open	100	0	31.83	3.98	1.86	3.14	24.13
query	100	0	L00.3	2.11	1.28	1.76	77.13
transfer	42.23	60.23	26.83	5.19	2.56	3.88	9.03

We completed three rounds of testing for the blockchain with 12 nodes using the truffle ganache framework, which produces blocks on localhost. The "Openfunction aids in the creation of a user account in order for transactions to take place; it is a measure of how many people are online and ready to utilize the network. The "Query" is an approximation of the instructions delivered to the nodes for hash calculation. In exchange, miners are compensated for computing hashes in the form of distributed ledger money, in this example, ETH. "Transfer" is the process by which the gas fees are transferred to the organizations that manage the smart contract. Send Rate: This is the number of transactions completed per second. Latency is defined as the time elapsed between submitting a transaction to a network and receiving the first confirmation of acceptance from the network. Flow rate—throughput—is the pace at which the blockchain SUT commits valid transactions in a given time period. The "Open" feature aids in the creation of a user account in order for transactions to take place; it is a measure of how many people are online and ready to utilize the network. "Transfer" is the process by which the gas fees are transferred to the organizations that manage the smart contract.

5. Conclusion

The supply chain is a complicated structure made up of several companies and individuals that collaborate. A formerly distinct process for ordering, purchasing, production, and shipping has been combined owing to a common digital method. GS1 has made a significant contribution to the openness, safety, and effectiveness of both physical and digital supply

chain networks. Traceability enables the tracking, integration, and documentation of commodity flows by recording the history of both the product and the manufacturing process. Current supply chain traceability systems include flaws such as faulty data, a lack of storage redundancy, unreliable monitoring data, concerns regarding the authority's data, and no record of where the data originated from. Although EPCIS-based systems have made significant progress in addressing these challenges, more work needs to be done. There are currently several supply chain applications that employ blockchain technology. Its promises of honesty and safety, particularly in terms of trust and monitoring, make it an appealing option.

According to The Innovator's Map, around 800 blockchain-related enterprises are now operational. Furthermore, much effort is required to prepare blockchain for broad application in a number of industries, with a concentration on the supply chain. The current status of technology and non-technological cooperation is rather difficult. Scalability and interoperability are only two of the numerous technical and non-technical barriers that blockchain must overcome before it can attain widespread adoption. Blockchain's operation and applications rely significantly on consensus. Several books and articles have been published on agreement algorithms (CAs). There is no ideal CA since they all have various strengths and applications. It is not unusual for PoW, PoS, and BFT to collaborate, just as it does in SCP. Storage, application logic, and smart contract-based apps need the appropriate DLT type, level of accessibility, blockchain platform, consensus process, integrated development environment, testing tools, libraries, programming language, and more resources. Because there are many combinations of these development layers, determining the best one for a single application requires trial and error. A number of prominent firms have had initial success using blockchain technology for supply chain management. Our objective was to look into the potential applications of blockchain technology, which is currently being employed by a number of enterprises, in the context of logistics management. The system was made more private and secure by using sovereign registration. Blockchain technology protects the privacy of a company's partners and employees by eliminating the need for intermediaries or agents to store sensitive information while simultaneously making it simpler to match supply and demand. An approved organization may manage who has access to sensitive information and prevent it from becoming public by utilizing a private blockchain.

6. FUTURE WORK

In the future, the application of blockchain in supply chains will evolve to address challenges like interoperability, scalability, privacy, and regulatory compliance. Advancements in integrating blockchain with emerging technologies like IoT and AI will enable more sophisticated data analytics, enhance supply chain optimization, and improve real-time monitoring. Additionally, there will be a growing emphasis on establishing standardized protocols and educating industry professionals to foster wider adoption and unlock the full potential of blockchain technology in creating transparent, efficient, and resilient supply chain ecosystems.

References

1. Tseng, M.-L., Islam, M.S., Karia, N., Fauzi, F.A., Afrin, S.: A literature review on green supply chain management: trends and future challenges. Resources Conserv. Recycl.

141, 145–162 (2019)
2. Kelechi, G., Akujuobi, C. M., Sadiku, M. N., Chouikha, M., Alam, S.: Internet of things and blockchain integration: Use cases and implementation challenges, in: Business Information Systems Workshops: BIS 2019 International Workshops, Seville, Spain, June 26–28, 2019, Revised Papers, volume 373, Springer Nature, p. 287(2020)
3. Bonazzoli, S., Borgianni, M., Falcone, C., Fioravanti, A., Longobardi, G., Lutri, S., Presti, L., Salerno, P., Tomasi, A., Ziantoni, F. et al.: Package delivery and reception with drones, (2020).US Patent 10,526,088
4. Angelini, F., Petrocelli, C., Catalano, M., Garabini, M., Grioli, G., Bicchi, A.: Softhandler: An integrated soft robotic system for the handling of heterogeneous objects. IEEE Robotics & Automation Magazine (2020)
5. Hammoudeh, M., Ghafir, I., Bounceur, A., Rawlinson, T.: Continuous monitoring in mission-critical applications using the internet of things and blockchain, in: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, ICFNDS âĂŹ19,Association for Computing Machinery,New York, NY, USA, 2019. 10.1145/3341325.3342018
6. Rychtyckyj, N., Yang, H. H.: Handling rider service at autonomous vehicles, (2020) .US Patent App. 16/023,874
7. Xie, R., Wang, Y., Tan, M., Zhu, W., Yang, Z., Wu, J., Jeon, G.: Ethereum-blockchain-based technology of decentralized smart contract certifcate system. IEEE Internet Things Mag. 3, 44–50 (2020)
8. Wang, J., Han, K., Alexandridis, A., Chen, Z., Zilic, Z., Pang, Y., Jeon, G., Piccialli, F.: A blockchain-based ehealthcare system interoperating with wbans. Future Generation Comput. Syst. 110, 675–685 (2020)
9. Vidovič, E., Gajšek, B.: Analysing picking errors in vision picking systems. Logistics Sustain. Trans. 11, 90–100 (2020)
10. UK, G.: Welcome to gs1 uk, the global language of business - all you need to know about gs1 standards, Last accessed 06 January 2020.https://www.gs1uk.org/support-and-training/ourstandards
11. Singhal, B., Dhameja, G., Panda, P. S.: How blockchain works, in: Beginning Blockchain, Springer, pp. 31–148 (2018)
12. Kamble, S.S., Gunasekaran, A., Sharma, R.: Modeling the blockchain enabled traceability in agriculture supply chain. Int. J. Inform. Manag. 52, 101967 (2020)
13. Lin, Q., Wang, H., Pei, X., Wang, J.: Food safety traceability system based on blockchain and epcis. IEEE Access 7, 20698–20707 (2019)
14. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., Imran, M.: Securing iots in distributed blockchain: Analysis, requirements and open issues. Future Gener. Comput. Syst. 100, 325–343 (2019)
15. Mudassir, M., Bennbaia, S., Unal, D., Hammoudeh, M.: Timeseries forecasting of bitcoin prices using high-dimensional features: a machine learning approach. Neural Computing and Applications 1–15 (2020)
16. Unal, D., Hammoudeh, M., Kiraz, M. S.: Policy specifcation and verifcation for blockchain and smart contracts in 5g networks, ICT Express 6 (2020) 43 – 47. http://www.sciencedir ect.com/science/article/pii/S240595951930181X. https://doi.

org/10.1016/j.icte.2019.07.002
17. Jangirala, S., Das, A.K., Vasilakos, A.V.: Designing secure lightweight blockchain-enabled rfd-based authentication protocol for supply chains in 5g mobile edge computing environment. IEEE Transactions on Industrial Informatics (2019)
18. Kravitz, D. W.: Transaction immutability and reputation traceability: Blockchain as a platform for access controlled iot and human interactivity, in: 2017 15th Annual Conference on Privacy, Security and Trust (PST), IEEE, pp. 3–309 (2017)
19. Koirala, R. C., Dahal, K., Matalonga, S.: Supply chain using smart contract: a blockchain enabled model with traceability and ownership management, in: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confuence), IEEE, pp. 538–544 (2019)
20. Imeri, A., Khadraoui, D.: The security and traceability of shared information in the process of transportation of dangerous goods, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, pp. 1–5 , (2018)
21. Yapa, I., Heanthenna, S., Bandara, N., Prasad, I., Mallawarachchi, Y., Decentralized ledger for land and property transactions in sri lanka acresense, in, : IEEE region 10 humanitarian technology conference (R10-HTC). IEEE 2018, 1–6 (2018)
22. Shahid, M. R., Mahmood, S., Hafeez, S., Zahid, B., Jabbar, S., Ashraf, R.: Blockchain based share economy trust point: Case study based validation, in: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, ACM , p. 41 , (2019)
23. Wang, S., Li, D., Zhang, Y., Chen, J.: Smart contract-based product traceability system in the supply chain scenario. IEEE Access 7, 115122–115133 (2019)
24. Liu, D., Alahmadi, A., Ni, J., Lin, X., Shen, X.: Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain. IEEE Trans. Ind. Inform. 15, 3527–3537 (2019)
25. Ferrag, M.A., Maglaras, L.: Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Transactions on Engineering Management (2019)
26. Gul, M. j. j., Paul, A., Ahmad, A., Khan, M., Jeon, G.: Smart contract's interface for user centric business model in blockchain, in: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 709–714 (2019),
27. Jogunola, O., Hammoudeh, M., Adebisi, B., Anoh, K., Demonstrating blockchain-enabled peer-to-peer energy trading and sharing, in, : IEEE Canadian conference of electrical and computer engineering (CCECE). IEEE 2019, 1–4 (2019)
28. Habib, M. A., Sardar, M. B., Jabbar, S., Faisal, C. N., Mahmood, N., Ahmad, M.: Blockchain-based supply chain for the automation of transaction process: Case study based validation, in: 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp. 1–7 (2020)
29. Hammoudeh, M., Ghafr, I., Bounceur, A., Rawlinson, T.: Continuous monitoring in mission-critical applications using the internet of things and blockchain, in: Proceedings of the 3rd International Conference on Future Networks and Distributed Systems , pp. 1–5 (2019)
30. Shanaev, S., Shuraeva, A., Vasenin, M., Kuznetsov, M.: Cryptocurrency value and 51%

attacks: evidence from event studies. J. Altern. Invest. 22, 65–77 (2019) 31. Boireau, O.: Securing the blockchain against hackers. Netw. Secur. 2018, 8–11 (2018)