Identity in Supply Chain Using Ethereum Blockchain

Vaibhav S. Dhande ,
Student, M.E. C.S.E.
vsdhande85@gmail.com
SSBTs College of Engg. & Technology, Jalgaon

Dr. Girish K. Patnaik,
Professor
patnaik.girish@gmail.com
SSBTs College of Engg. & Technology, Jalgaon

Dr. Manoj E. Patil,
Associate Professor
mepatil@gmail.com
SSBTs College of Engg. & Technology, Jalgaon

Dinesh D. Puri
Assistant Professor
ddpuri@gmail.com
SSBTs College of Engg. & Technology, Jalgaon

***Abstract*— This paper investigates the utilization of novel identity systems in supply chain management and expounds on the role of self-sovereign identities in establishing trust between the system's issuer, entity, and verifier. The paper examines the technical issues underlying blockchain operation in supply chain systems. Recent research is surveyed to showcase the potential of blockchain applications in promoting transparency, traceability, and productivity throughout the manufacturing and distribution processes. The paper proposes the integration of self-sovereign identity into the supply chain to enhance privacy and enable greater transparency in the end-to-end tracking of goods. Using hyperledger caliper, the paper analyzes the performance of the blockchain, providing insights into the supply chain's functioning based on metrics such as transaction and read throughput, latency and resource consumption. Finally, the paper outlines the challenges that are expected to arise in supply chain management.**

Keywords: self-sovereign identities, blockchain, supply chain management, hyperledger caliper, transparency, traceability.

I. INTRODUCTION

The current use of identification platforms with centralized data storage architectures, such as cloud storage, raises significant security and privacy concerns. Issues such as control, immutability, and management of data provenance have led to various attacks and data fraud, especially when third-party access is involved. With a large volume of data stored in a central location, attackers are motivated to target the storage, making the preservation of identity information on various centralized storage platforms, including central servers and cloud storage, a significant privacy concern. To address these issues, this study proposes using blockchain as a digital identity platform based on self-sovereign identity.

1.1 The Evolution of Identity Management Systems

The landscape of identity management systems has undergone significant evolution, progressing through several stages with the introduction of newer models.

Fig. 1. Evolution of Identity Management System

1.2 SILO MODEL

The SILO model is a popular and straightforward identity management model that involves two parties, the service provider and its users. Each service provider has its own identity domain and provides its clients with an identification (such as a username) and a matching credential (such as a password) to access its services. Identity actions carried out in one domain are not valid in other domains. A user must authenticate with each service provider individually to access services from different providers, resulting in the user having numerous partial identities that are difficult to maintain. While this approach is still used by significant online service providers, trends are shifting away from it.

1.3 FEDERATED MODEL

The federated model consists of multiple service providers and a single identity provider in each identity domain. The identity provider provides users with identifiers and necessary credentials. The service provider relies on the identity provider for user authentication and to receive user attributes and their values. A user must first authenticate with the identity provider before accessing any service from the service provider. Once a foundation of trust is established between the identity provider and associated service providers, the shared identity domain or federated identity domain is established. This model is commonly used in government services and educational institutions.

1.4 USER-CENTRIC MODEL

The user-centric model is similar to the federated model, but it allows several service providers to share a single identity provider without establishing trust among the entities. When a user tries to access a service provided by a service provider, they are directed to the identity provider, where they self-identify. The service provider then makes an authorization determination based on the user's profile to approve or disapprove the user's request for service access when the identity provider releases the user's identity data using a profile. Every entity in this model trusts every other entity, making it an open-trust model. This model is commonly used in web services offered by significant social networking service providers like Facebook, Google, and others.

1.5 SELF-SOVEREIGN IDENTITY

In the self-sovereign identity (SSI) system, users retain control over their personal data and are free from having to constantly disclose it with multiple service providers to access goods and services. Public keys are used to represent identities, and possession of the private key that controls the public key establishes an identity's ownership. The SSI system uses blockchain as an identity certification authority and smart contracts to represent a user's digital identity. These smart contracts can be controlled by other smart contracts, allowing users to recover their keys.

1.6 BACKGROUND OF IDENTITY SYSTEM

An approach to digital identity called self-sovereign identity (SSI) provides people ownership over their online personas

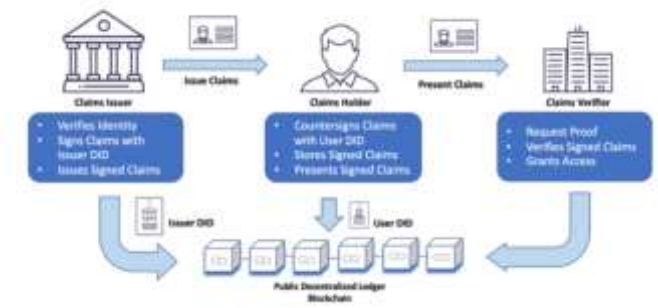

Fig. 2. Trust Triangle of Self Sovereign Identity

The challenge of establishing trust during an interaction is addressed by Self-Sovereign Identity (SSI). To establish trust, one party must present credentials to other parties who must confirm that the credentials are from an issuer they trust. In this way, the holder of the credentials gains access to the verifier's trust in the issuer. The "trust triangle" refers to the three-part structure of SSI. It is widely acknowledged that users manage their verifiable credentials and their consent is required for an identity system to be self-sovereign. This results in a decrease in unintentional sharing of user data. This is in contrast to the centralized identity paradigm, where an external entity grants identity. In an SSI system, holders create and manage decentralized IDs that are unique identifiers. In most SSI systems, public-key cryptography is used to verify credentials, which are stored on a distributed ledger using digital wallets. The credentials may include data from an issuer's database, a social network account, a history of online purchases, or verification from colleagues or friends.

2. LITERATURE SURVEY

In the last few years, several studies have been conducted to investigate the potential benefits, challenges, and opportunities associated with integrating blockchain technology into supply chain management. The following is a summary of some of the most relevant literature in this area:

Khan and Zhang Yu [1] conducted a systematic literature survey to explore the drivers and benefits associated with supply chain management. They analyzed and synthesized 48 articles published between 2013 and 2019 in international journals. The study focused on reviewing the integration of blockchain technology in the domain.

Chang and Chen [2] conducted a literature and analytical review of blockchain-based supply chain research. They analyzed 106 articles and provided an overview of blockchain and smart contracts. The study sheds light on the benefits, issues, and challenges in this blockchain paradigm.

Sani et al. [3] proposed an approach for identifying and authenticating a component based on Idenx smart contracts that facilitate supply chain security agreements without trusted third parties. The study presented the security analysis of Idenx and their results showed resilience to supply chain attacks.

Scully and Habig [4] explored the application of blockchain technology in supply chain management. They examined the recent literature to identify inefficiencies in the existing supply chain and ways to improve it.

Wu et al. [5] provided a comprehensive analysis of potential opportunities, requirements, and principles of design for blockchain-based supply chain management. They discussed four crucial technical challenges in terms of scalability, throughput, access control, data retrieval, and review. Finally, they provided a case study of a design based on a food traceability system and its deep insight to tackle challenges.

Surjandy et al. [6] focused on the automotive market-based supply chain using blockchain. They addressed the open issues based on operational aspects, such as supplier, logistics, manufacturer, distribution, and customer.

Muessigmann et al. [7] provided insights based on business, management studies, and research-based logistics in supply chain management. They analyzed data from over 613 articles from academic research papers. This review is based on bibliometric analysis methodology, which adopts citation network analysis and cocitation analysis.

Sangeetha et al. [8] conducted research on the supply chain based on the vaccine of SARS-CoV3. They found blockchain to be a solution to fraudulent activities like bribery, money laundering, forged checks, sanction violations, misrepresentation of goods and services that have disrupted the supply to the world. They integrated blockchain with supply chain management to increase productivity and accountability, from warehousing to distribution to payment.

Aich et al. [9] conducted a detailed literature survey and highlighted the differences between the conventional and blockchain-based supply chain in various sectors such as automotive, pharmaceutical, food industry, and retail. They also addressed the current challenges faced by all the mentioned industries and how blockchain helps improve the efficiency in these systems.

Naik and Jenkins [10] contributed towards achieving an architecture based on self-sovereign identity, i.e. "uPort Identity Management System." They developed a decentralized app to demonstrate and evaluate its operational services and efficiency. The study did the experimental analysis and explained the advantages and limitations of the system.

Overall, the literature survey gave insights into the challenges, technical issues, and benefits required for supply chain management and blockchain.

3. PROPOSED METHODOLOGY

Following section provides the details of the proposed work.

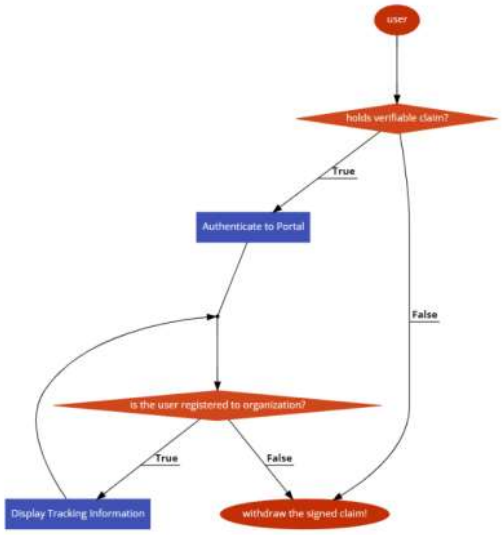

Fig. 3. Algoritham for proposed system

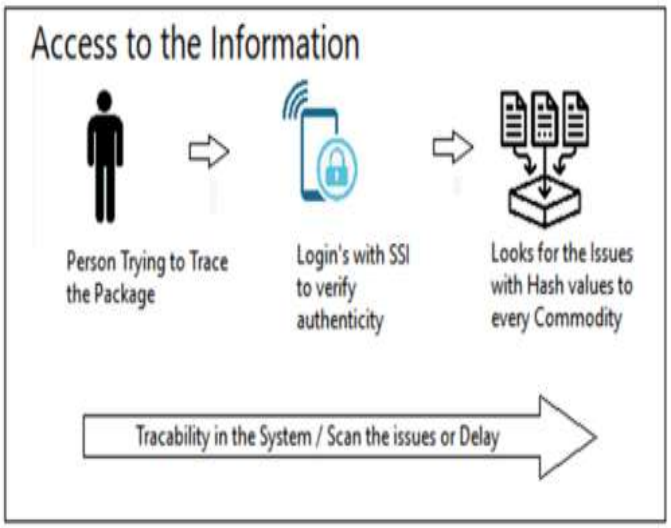

Fig. 4. Acess to information in supply chain within distributed leadger

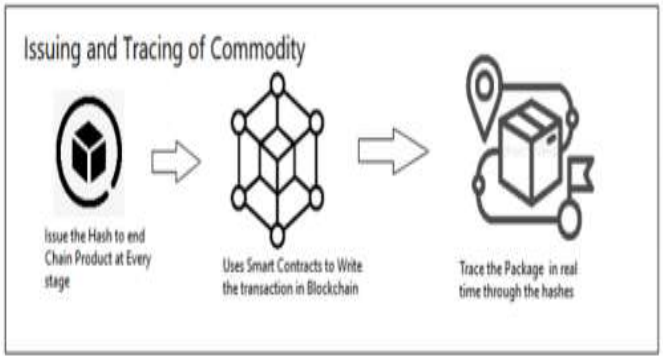

Fig. 5. Issuing and trcaking commodity in SC

We use the notation $assertion^{user}_{supplyChain}$ to denote an assertion consisting of a $claim^{user_{authorised}}$ regarding a $user \in U$ in $supplyChain \in Domain$. The assertion is formally defined as a signed claim in the following way, where key^{-1}_{issuer} represents the public key of the provider-$issuer$, so the private key can be represented as :

$$assertion^{User}_{supplyChain} = \{claim^{user_{authorised}}\}_{key^{-1}_{issuer}}$$

Based on this, we mathematically define a profile in the following way :

$$profile^{user}_{SCM} = \{\bigcup assertion^{user}_{supplyChain} | supplyChain \in domain\}$$

Let $REG_{supplychain} : (\{ID_{supplychain} \times \{av^{ID}\}x) \times (\{c_{scm}\} \times \{av^c\}) \longrightarrow \{parIdent^u_{d^{dec}}\}$ be the function that upon providing values for the identifier and the corresponding credential creates a new partial identity of a user u in the decentralized domain d^{dec}.

1. $ID_{supplychain}$ denotes the identifier of Stakeholder in Supplychain
2. av^{ID} denotes the created/provided value for $ID_{supplychain}$ such that $av^{ID} \in AV_{d^{dec}}$
3. c_{scm} denotes the corresponding credential and av^c represents the provided/created value of the credential where $av^c \in AV_{d^{dec}}$
4. $parIdent^u_{d^{dec}}$ represents the set of partial identities in supply chain. Registering a new set of users and attribute values in the given domain

in the following way :

$$U'_{d^{dec}} = U_{d^{dec}} \bigcup \{u\}$$

$$AV'_{d^{dec}} = AV_{d^{dec}} \bigcup \{av^i\} \bigcup \{av^c\}$$

3.1 USE OF SELF SOVEREIGN IDENTITY

The foundation of self-sovereign identification is a decentralised network of trust. Blockchain is the only technology that can do this. Additionally, according to a survey of the literature in the field of supply chains, it improves accountability and inherits security qualities like immutability, resilience, and hash proof. As a result, the system can become more transparent and fraudulent behaviours can be prevented. Since the distributed ledger keeps account of all system actions, there is no single point of failure. By writing scripts that execute on the specified supply chain scenario, one can automate the system using smart contracts, which are lines of code that run when certain criteria are met.

To manage the supply chain more efficiently, parties can keep track of price, date, location, quality, certification, and other pertinent information using a blockchain supply chain. The availability of this data within blockchain can improve visibility and compliance over outsourced contract manufacturing, increase traceability of the material supply chain, reduce losses from grey market and counterfeit products, and possibly strengthen an organization's position as a pioneer in ethical manufacturing.

A distributed immutable record of all transactions and the digitization of physical assets by companies can make it

possible to track assets from manufacture to shipment or end-user use, improving transparency and accuracy throughout the supply chain. Businesses and consumers can see more information because to the improved supply chain transparency. In order to prevent fraud for expensive items like gold and medicines, blockchain can enable enhanced supply chain transparency. Blockchain technology might help businesses better understand how ingredients and finished goods are transferred through each subcontractor, reduce financial losses from grey market and counterfeit trading, and boost consumer confidence by eliminating or reducing the negative effects of fake goods.

Additionally, companies have more control over contract production that is outsourced. Blockchain possibly reduces communication or data transfer errors by giving all participants in a given supply chain access to the same information. It is possible to spend less time verifying data and more time delivering goods and services—either raising quality, lowering costs, or doing both. Finally, by enabling a successful audit of supply chain data, blockchain can improve administrative processes and lower expenses. A distributed ledger of all pertinent information can speed up processes that currently involve manual checks for compliance or credit that could take weeks.

3.2 DESIGNED SUPPLY CHAIN SYSTEM

A supply chain is a sequence of steps used to convey a good or service to the consumer. The operations entail transferring and converting raw resources into finished goods, transporting those goods, and giving them to the final consumer. Producers, vendors, warehouses, transportation companies, distribution centres, and retailers are among the organisations participating in the supply chain. Supply chain management aims to increase efficiency by coordinating the actions of the different supply chain participants. By doing this a business may be able to outperform its competitors and improve the quality of the products it produces, both of which may result in higher sales and revenue.

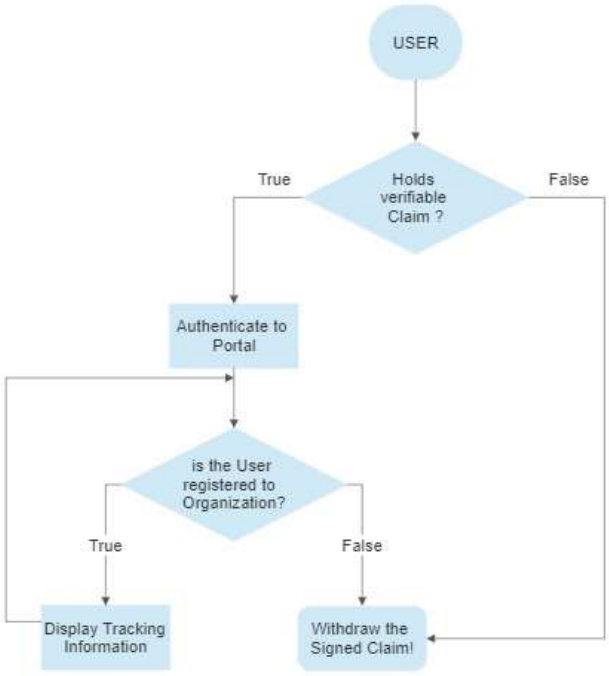

Fig. 6. Algorithm of Proposed System

Our proposed model works on ethereum blockchain, where we run the authentication of the people at every step and record their activities in the distributed ledger, The authenticity is checked with the help of the self soverign identity paradigm, The blockchain runs smart contract to validate any user thereby providing the access to the information for tracking (refer figure 3.2). but in smart contract process the user is led to provide his verifiable credentials for the contract to initiate, then their activities are recorded. Lets take an example to demonstrate this. Nike decides to create a limited edition shoes for its customer, it starts procuring the raw materials in bulk,like polyester,wool etc. whose sources are not known, as the organization and its activities are spread across the globe, it becomes hard for them to check the authenticity of every source.Since the company is committed to the quality of the product it becomes more important for people to known that its product is genuine. After the product is manufactured it assigns a SKU to every product line, but in the step of transportation to reaching the retailer, the product can end up in hands of people who can make second copy of the same product. Making it hard to realize even if we have SKU in place

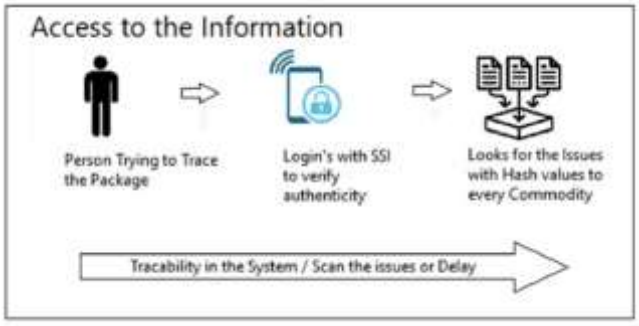

Fig. 7. Access to the information in supply chain within distributed ledger

Since, all of these processes are not transparent right from start of supply to demand, their accountability is questionable. Blockchain can solve this issue by keeping ledger of all the activities and with self soverign identity.

.

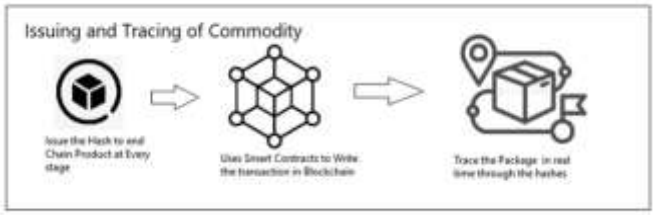

Fig. 8. Issuing and tracing of Commodity in Supply chain

In the SSI , there are three components which help create the trust in the system - issuer, verifier, identity holder. The identity holder is any person who is directly involved or indirectly involved with company. The verifier is the company that creates the products for the customers, the issuer is any organization which issues verifiable credential like passport or ID card which company trusts. whenever any identity holder tries to access any service for tracking his/her package needs to provide verifiable credential to service provider.i.e. company. In the above mentioned scenario, the user is issued verifiable credential which is stored in users digital wallet. it is in encrypted format hence whenever, it accesses the service it needs to provide consent as user has private key to his wallet. The company verifies the authenticity by looking into distributed ledger i.e. blockchain for issuers signature in it.In all of this process the intermediaries are eliminated, the user has full control over where it provides its identity and other sensitive information. the privacy of all the stake holders is not compromised at any cost. the blockchain can also keep the track of other information through the distributed ledger.

We simulated the basic network of supply chain by keeping in mind the stakeholders, the issuer, and verifier. We used solidity language to create smart contracts and truffle framework-"Ganache" for creating blockchain on local host. we create the entities for supply chain, with each requiring different sets of attributes to be provided to Verifier. for every smart contract run, it creates hash which can help track the activity.

1. 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'
2. 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).
3. The distributed ledger uses DID to hold account of activity also keeping in mind the privacy of the user.

However, the acceptance of this distributed ledger technology is still in the initial stage. Traditional supply chain systems still face many technical inefficiencies like scalability and diversified systems, which can be addressed with the implementation of blockchain technology. With continued research and development, the potential for blockchain to revolutionize supply chain management is immense..

3.3 PERFORMANCE ANALYSIS

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

4. EXPERIMENTAL ANALYSIS

We did performance evaluation of the ethereum blockchain simulating the model of supply chain system. It runs smart contract for every step of the process right from procurement to distribution and verifies the stakeholder with help of 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	30.6	2.75	0.63	1.91	22.9
query	100	0	L00.3	0.88	0.05	0.53	75.9
transfer	41	59	25.6	3.96	1.33	2.65	7.8

We ran 3 rounds of testing (check figure 4.2-4.4 for reference) for the blockchain with 12 nodes as shown in figure below , the framework that we used was truffle ganache which creates the blocks on localhost. The "Open"function helps open a user account for the transactions to occur it is the measure of how many users are up and ready state to use the network. The "Query" is the estimate of the commands given to the nodes for calculating the hashes. And in return the miners get award for calculating the hashes in the form of currency of distributed ledger i.e. in this case (ETH).
The "Transfer" is where the gas fees is transferred to entities who run the smart contract.

Send Rate - It is the measure of transactions done per second.
Latency — It is the time between submitting a transaction to a network and the first confirmation of acceptance by the network.
Throughput -Throughput is the rate at which valid transactions are committed by the blockchain SUT in a defined time period. The "Open" function helps open a user account for the transactions to occur it is the measure of how many users are up and ready state to use the network. The "Transfer" is where the gas fees is transferred to entities who run the smart contract.

5. CONCLUSION

Blockchain technology has already been implemented in many financial systems, and our objective was to explore its potential for supply chain management. Through the use of self-sovereign identity, we were able to provide enhanced privacy and security for the system. By eliminating intermediaries or third parties that store sensitive data, trust in the system can be enhanced using blockchain technology, thereby improving productivity and transparency to meet the supply and demand of a company while also protecting the privacy of employees and stakeholders. The use of private blockchain within a close organization can help eliminate competition and keep information confidential to stakeholders.

6. FUTURE WORK

Blockchain technology has been successfully implemented in various financial systems, but its potential use in supply chain management is also gaining attention. Our objective was to explore the implementation of blockchain technology in supply chain systems and simulate the process to analyse its performance.

One of the key features of our system was the implementation of self-sovereign identity, which provides better privacy and security. By eliminating intermediaries or third parties that keep sensitive data from the system, trust is enhanced and productivity and transparency are improved. This can help companies meet supply and demand more seamlessly while also ensuring the privacy of their employees and stakeholders.

Private blockchain networks within a close organization can also help eliminate competition and keep information confidential to stakeholders.

REFERENCES

[1] Khan, A., & Zhang Yu. (2019). Blockchain-based supply chain management: a systematic literature review. Journal of Enterprise Information Management, 32(4), 761-797.

[2] Chang, K., & Chen, T. (2019). Blockchain-based supply chain research: a literature review. Future Generation Computer Systems, 101, 207-215.

[3] Sani, M. A., Mohd, M., & Alias, R. A. (2020). An approach to supply chain security agreements via index smart contracts. Journal of Ambient Intelligence and Humanized Computing, 11(2), 819-832.

[4] Scully, P., & Habig, M. (2019). Blockchain technology in supply chain management: a review. International Journal of Production Research, 57(7), 2119-2135.

[5] Wu, H., Xu, B., Liang, Q., & Liang, Y. (2019). Blockchain-based supply chain management: a comprehensive analysis. Journal of Applied Research and Technology, 17(3), 252-263.

[6] Surjandy, A. I., Rahman, T. A., & Sulaiman, R. (2020). Blockchain for the automotive supply chain: a review of current status, drivers, and barriers. IEEE Access, 8, 29007-29025.

[7] Muessigmann, V., Schumacher, T., & Kuhn, H. (2020). Blockchain in supply chain management: a bibliometric review. Sustainability, 12(3), 849.

[8] Sangeetha, A. S., Nagashree, B. G., Ramesh, S., & Krishna, V. (2020). Blockchain-based vaccine supply chain management for COVID-19 pandemic. Journal of Ambient Intelligence and Humanized Computing, 11(10), 4293-4306.

[9] Aich, S., Biswas, G., & Ray, P. (2019). Blockchain in supply chain management: a review, current trends, and future potential. In Proceedings of the 2019 11th

International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 1-5). IEEE.

[10] Naik, N., & Jenkins, P. (2020). Decentralized self-sovereign identity management for supply chain applications using uPort. In Proceedings of the 2020 IEEE 12th International Conference on Communication Software and Networks (ICCSN) (pp.442-446). IEEE