Medicine Supply Chain Using Blockchain Technology

Kuntal chaudhari[1], Poonam Ghadage[2], Dhanashree Ghodvinde[3], Shivani kedar[4], Prof. Kanchan Doke[5]
Department of Computer Engineering
[1,2,3,4,5] Mumbai University

Abstract- *The Supply Chain (SC) has several geographical spans, modes and industries and includes several stages, where data flow in both directions, from suppliers to retail distributors, consumers, intangibles. Streaming of this data is required to support key business decisions that may affect the cost of production and market share. The modern SC system is unable to provide pseudo-tracking, confirming that it is in real time during the distribution phase. This information is available from the same source, often an airline and, along with other interested parties, are required. The system has a number of private distributor ledgers and single blockchain public ledger. A framework that allows each private individual to be detained among the export partners. Confidentiality is imperative, for example, while trading or quality products and pharmaceuticals, chemical products. The second type of ledger is a blockchain public ledger. There are signs of each specific event in addition to the event check. Subsequently, it provided a strictly independently validated immutable record of the pseudo real-time geographical status of the shipment from large number of sources using commuters sourcing.*

Keywords- blockchain; supply chain; distributed databases; peer-to-peer network.

I. INTRODUCTION

Our main goal is to provide an effective supply and customer, appearing in real time during the physical phase of the distribution supply chain (SC). This stage is associated with the goods from the supplier to the customer. There are many existing solutions that support the tracking of goods during the period of physical distribution. These solutions are often complemented by monitoring of a source, medium, and suffered from visibility identified with other stakeholders. In fact, this feature is delivered through the updates provided by the company, and when it deems necessary. These issues of trust and transparency can not affect trade between large enterprises, with full integration and international shipping links. However, model fail when either the client or supplier of small or medium-sized enterprises, and relies on the distribution of storage and multiple carriers during shipment.

This article is a structure that provides a tracking network for all stakeholders in a SC distribution phases. Flow information and exchanges supported by two types of distribution of the ledger: a private and public ledger. Each

shipment is associated with a specific private ledger that only exists in connection with a transit partner involved in the delivery. However, we believe it is necessary to maintain the level of privacy when the product is traded at high cost, risky, or double in use (e.g. pharmaceuticals and chemical products). An example of the event may involve transferring the detention from the carrier to the company or from the airline to the client.

While this article focuses on blockchain technology, specific programs to support the visibility of the supply chain during this phase of distribution, it is trying to deal with a large gap between the whole private Enable and fully open the public blockchain / architecture. Currently the innovation is basically used to check exchanges, inside advanced monetary forms however it is conceivable to digitize, code and addition for all intents and purposes any report into the blockchain. Doing as such makes a permanent record that can't be changed; moreover, the record's validness can be checked by the whole network utilizing the blockchain rather than a solitary unified expert..The main advantage of using this application is medicine supply chains merely track and store orders and deliveries, with providing features as transparency, traceability and auditability . In the medicine supply, in order to maintain trust and reliability along the whole supply chain, it is essential for the stored records to be tamper-proof, while the best case would be if each actor issuing transactions could do that without relying on any centralized third-party intermediary The Project Coding is based Several Tools are utilized to build up this versatile application (java .jdk) are so very much associated that the venture looks like to the computerization of the Web administrations activity of the firm.

II. REVIEW OF THE LITERATURE

- In existing system, each user (manufacturer, distributer, producer, retailer and end user) cannot get information about the order. In that system, data is not secured and low level of transparency. User cannot access information easily from anytime anywhere and cannot view all medical product information.
- The creation and conveyance of fake medications is a pressing and progressively basic overall issue, specially in the development countries. change proprietorship from makers to distributer, distributer and after that drug

specialist before it achieve the client. In current inventory network framework, data isn't share between systems, manufacturers do not know what happened to their products, drugs administrative specialist has zero ability to see of the framework, reviews are entangled and exorbitant, and organizations cannot follow-up patients.

- In this paper, , we disclose how to utilize blockchain innovation in medication production network to include recognizability, perceivability and security to the medications and supply framework. It likewise tracks the prescription subtleties from its assembling until its conveyance to persistent. A permissioned blockchain will be utilized for putting away exchanges and just believed gatherings will be permitted to join the system and drive information to blockchain.

III. RELATED WORK

This area present a viewpoint on the development of SC management system as well as review of current state of the art in the block chain technology and its application.

In this section, we have setup a secured and trusted network, where only the trusted parties are given permission to join the network. On the backend there is a permission blockchain to store all the required transactions, and once the information entered to it – can never be changed Other than that we have an easy to use portable APP that the members will use to make exchanges to the blockchain. At the point when a plant produce another item, they will make a one of a kind hash and allocate it to the item. The item will be enlisted on the blockchain. When a factory produce a new product, they will create a unique hash and assign it to the product. The product will be registered on the blockchain using its hash (unique ID). The product will be considered as a digital asset on the blockchain network, and its hash will be used to track it any time on the network.

Any additional information of the item can be put away off-chain or on-chain relies upon maker's decision. Off-chain information will be converged with on-chain information by utilizing some sort of identifier. Traditionally, in most blockchain based applications a hash digest (e.g. SHA-256) of all the off-chain information is produced and connected it to the on-chain information. In any case, the best methodology is to store substantial records off-chain and content information on-chain. When the item is enrolled to the blockchain by the maker, its possession will be effectively exchange to another member utilizing an easy to understand versatile application. Let say the wholesaler want to purchase the medicines from the manufacturer, manufacturer will physically exchange the medications to the distributer and an

exchange will be enrolled to the blockchain simultaneously. Wholesaler will rehash a similar procedure to exchange the medicines to distributer, and distributer will do the same business with pharmacy.
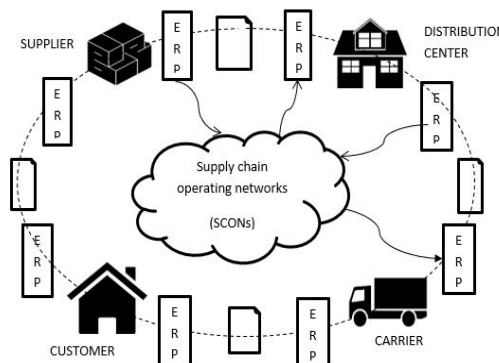

Figure 1: Current supply chain operating networks (SCON)

As originally suggested at blockchain, a blockchain is a distributed (register) public database that supports the growth of operations that are organized in blocks and secured from unauthorized access. Two types of transactions are supported: Genesis of Operations that Establish Values and Transfers Transferring Costs From One Party to Another. Each transaction was signed by the issuer and placed in the ledger. Then the group operations were collected into a block that was confirmed by a third party Each square in the chain is moving in light of the fact that it is appended to its ancestor and any adjustment in any square discredits every one of the squares downstream in the chain. In addition, more mature the block is (i.e., longer it has been in the ledger chain), the greater is its integrity. Each web host keeps a copy of the square is (i.e., longer it has been in the record chain), the more prominent is its respectability. Each web have keeps a duplicate of thee ledger, and every time you create a new block, it is published to all the participants who have added it to your local copy of the ledger.

Although designed primarily for distributed architecture, blockchain technology can be applied on central architecture. Distributed architecture often takes the role of a human touch network. Central Cloud Architecture to avoid security and privacy issues associated with distribution architecture, but also to aim for the sustainability, distribution control, scaling, and availability of a distributed architecture. IBM (International Business Machines) has provided an end to the end-of-blockchain blockbuster control. Blockfreight is a block chain public solution for tracking the container distribution telescope.

As a rule, blockchain SC technology, evidence of origin, integration and control levels of inventory and change requirements, and preservative prescriptions for

pharmaceuticals and food products. For example, some companies may not be willing to show off their production capacity to their competitors. In the health sector, sharing medical records is governed by strict laws of confidentiality. Private architecture alternative methods include the use of data storage circuits, rather than on the storage chain. For example, in it was provided blockchain ledger transfers for medical records of patients. The documents are safely stored in the clouds far away from the ledger.

IV. IMPLEMENTATION

To incorporate blockchain technology in medicine supply chain system, we should initially see how blockchain record functions in the engine. Blockchain has work in character component, a cryptographically secure key pair. These keys are utilized to appoint every member a particular action on the system. A member can be device person or any entity. The original identities of participants are hidden and they are known by these keys. pair contains no sign about the members, yet extra information(e.g. name, contact or expert certifications) can be related with it. Be that as it may, the best methodology is to keep these extra data off-chain and consolidation them with on-chain data(key pair) utilizing their IDs, with regards to medicine supply chain management, the participants will be the manufacturer, producer, distributer, retailer and end user etc. Each of this participants will be identified by their unique key pair on the network. Drugs will be consider as the assets, with each of them having a one of a kind key (or hash). The ID will be appended with the drug as QR code.

4.1. Architecture overview

In this section, we have setup a secured and trusted network, where only the trusted parties are given permission to join the network. In figure 2, user will first enter the username and password. Then the user is now authorized user. If the user is valid user then it will proceed to next step, otherwise the process will repeat again. If the user is logged in successfully then the user will back track the product details of company, producer, distributer and retailer. Company producer, Distributer and Retailer will follow same procedure of login as user. Company will insert the information about the product, stocks and orders such as date of manufacturing, number of products, expiry dates, etc. After this procedure it will check for order from producer and it will send product to producer and QR Code after getting order from distributer, producer first check the stock. If the number of stock is available then it will fulfill the order of distributer, otherwise request product from company. Distributer will receive the product and will scan the QR Code of product to ensure that

the quality of ordered product remains same. After that order product and send to retailer. Retailer receives the product from distributer and scan the QR Code and sell product to consumer. After all this process, user scan QR Code and buy the product.

On account of open records, a gathering of occasions are fastened to make a square, and, thusly, a binding square to shape an expansive records. The presenting of occasions on both private and open records is delineated.
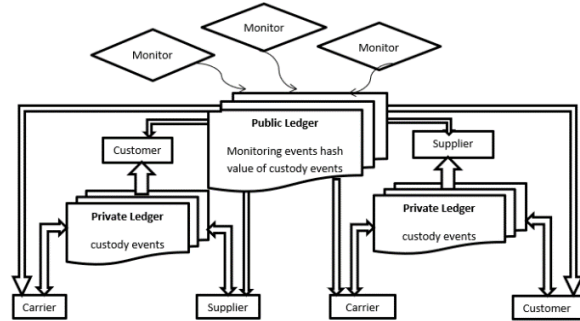

Figure 3 : Posting of events to the public and private ledgers

4.2. Algorithm used

As we have concluded previously, due to the variety of file types currently, we should only need to save the
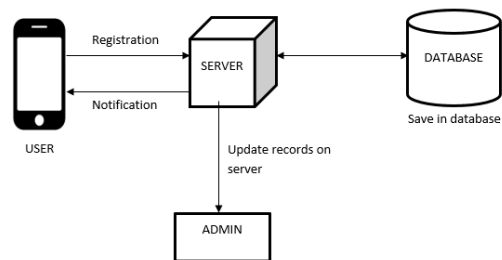

Fig 2. Architecture Diagram.

Figure 2: Architecture Diagram

It has a global network that is open to all partners as well as other observers. This global network is stable and does not stop.

necessary information like hash information of a file into our block. This Method has an arbitrary length of the output hash value which will let the user choose the level of the encryption. The reason why using this hashing method is because we are going to process files whose size may huge. If a hash method with low efficiency is used, users will get nervous while the system is calculating the hash value during the verification phase. In detail, some files with different content as pattern strings and 32-byte as the output length of the hash value because it is easy to check. Then, we use the hash function to get the abstract information of the file. After

that, we invoke the function to add the hash information into the block and create the block in the platform. At last, we use the query function to get the hash value stored in the block and check whether it is the same as the hash value we calculated from the file. If both values are the same, it means that the file is not be tampered.

We generated a series of hash values with the empty input string and pattern string previously. In addition, the length of these hash values lay in the range from 32 bytes to 512 bytes. Now, we had 16 generated hash values in total. Next, we created the test function for each hash value in a single script by invoking the smart contract we wrote to establish the block. Moreover, this test module can display the detailed time of each test function in the script so that it is convenient for us to know how much time it will take for different block length.

By taking the advantage of this kind of hash pointer, we can prevent hackers from tampering the content of the original file. Meanwhile, adopting users' signature can make sure that the creator of the block is the real user himself effectively so that hackers could not be able to masquerade as the original user to establish a block with malicious content unless hackers get the private key of the user in the real world. Nevertheless, it is only feasible when hackers know the user very much.

4.3. Blockchain

The primary segment of the framework, containing all the business rationale, actualized through savvy contracts on the square chain, as a portal to the square chain itself. Contingent upon the chose square chain, this module will change in unpredictability. Square chain records can be viewed as a circulation database, with a developing rundown of events .According to the program capabilities of selected block chain, as well as the capabilities of the client interfaces for that block chain. We used block chain to store the medicine records so that it is infeasible for hackers to tampered the record. Although it is very effective to keep the validity of the medicine records, the size of full medical records will be enormous as the time passed by. As a result the storage of system will be a performance bottleneck because each node in the block chain system holds the full records of the whole data. So the idea raised from this project has some limitations.

Due to the property that the block contains a pointer to previous one, it is infeasible for a hacker to change the content of specific block. In the blockchain, each block holds the hash value points to the previous block and hash value of the next block is calculated by hash value of previous block and the content of this block together. If hacker want to tamper the content of specific block, the hash value calculated now will be different from the one save in the next block. As a result, the hacker need to change the hash value of the next block again and this will make the hash value of the second next block mismatch too. To tamper a specific block, hacker should change the hash value of the block time after time until the latest one has been tampered while the latest hash value is supervised and kept by every node in the blockchain. It seems impossible for hackers to persuade more than half of the nodes admitting the modification.

V. CONCLUSION

The medicine supply is useful for the company, producers, distributer, retailer and user that help the user to provide information regarding the medicine supply chain. Using this android application information about the medicine supply chain, every user of the medicine supply saves details about the medicine details into server. By using this application transparency and trust between all users should be maintained. So that, there is no chance for corruption or fraud. Blockchain technologies, creating transparent, fault-tolerance, immutable and auditable records which can be used for a medicine supply traceability system. We may hereby conclude that with the use of this application the organization would be able to save significant costs on paper, printing, labor, etc. through hiding a lot of vital content and information to be communicated with the use of QR code. This application/tool would help the company bring advancement in its processes by the use of latest technology which is considered as superior that its closest substitute. As the QR codes could be customized or formatted as per the company's wish by applying color, embedding logo image or label, it shall help the organization to communicate the information in a more emphasized and differentiating manner than others. The secured QR codes will help the company to securely communicate the information thereby serving the double purpose of secure and obscure data exchange.

REFERENCES

[1] Harrison, A.; van Hoek, R.I. Logistics Management and Strategy; Pearson Education: London, UK, 2008.

[2] Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P. A Taxonomy of Blockchain-Based Systems for Architecture Design. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3– 7 April 2017; pp. 243–252.

[3] Lundbaek, L.N.; Huth, M. Oligarchic Control of Business-to-Business Blockchains. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017;pp. 68–71.

[4] Schollmeier, R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In Proceedings of the IEEE First International Conference on Peer-To-Peer Computing, Linkoping, Sweden, 27– 29 August 2001; pp. 101– 102.

[5] Ripeanu, M. Shared design contextual investigation: Gnutella organize. In Proceedings of the IEEE First International Conference on Peer-To-Peer Computing, Linkoping, Sweden, 27– 29 August 2001; pp. 99– 100.

[6] Iacovou, C.L Benbasat , I .; Dexter, A.S. Electronic data interchange and small organizations: Adoption and impact of technology. Manag. Inf. Syst. Q. 1995, 19, 465–485.

[7] Pezoa, F.; Reutter, J.L.; Suarez, F.; Ugarte, M.; Vrgoˇc, D. Foundations of JSON schema. In Proceedings of the 25th International Conference on World Wide Web, Montréal, Xcv+QC, Canada, 11–15 April 2016; pp. 263– 273.