2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)
Manipal University, Jaipur. Jan 19-20, 2023

2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT) | 978-1-6654-5357-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCT56969.2023.10076043

Counterfeit Drug Prevention in Pharma Supply Chain using Blockchain Technology

Ram Krishna Jha, Parvez Alam, Nitin Priyadarshi, Mohammad Asad Ghazi, M S Bhargavi*
Department of Computer Science and Engineering, Bangalore Institute of Technology,
Bengaluru, Karnataka, India
* corresponding author: ms.bhargavi@gmail.com

***Abstract*— Fake drugs are a growing serious issue related to the healthcare industry which causes extraordinary dangers to the society and the environment. Tracing the drugs at every step of the pharma supply chain is a difficult task. The goal of the research is to create a blockchain-based model that can forestall drug forging in drug store networks. The scope of the research lies where irregularities in the pharmaceutical supply chain affect public health and economy. The advanced elements of Blockchain makes it fit for complete recognizability of medications from producer to end patients, and the capacity to prevent fake prescriptions or medications. Drugs change proprietorship from producers to distributors and afterward retailers before it arrives at the client. Through the proposed model, the producer would have the option to transfer the subtleties relating to a medication, after which it will be sent for endorsement to the Government. From there on, distributors and retailers, in view of their prerequisites, can demand the endorsed drugs. Later on, in the event that a patient needs some drug, the person should demand it on the blockchain network. The solicitation will be shipped off the closest retailer/drug store and from that point, the patient can gather their medicine. Hyperledger fabric is utilized because they are permissioned and have an open source blockchain framework, meaning all the organization and pears are well known and confirmed. Our execution of the proposed blockchain based model features that the model can effectively forestall any medication being fake. This will be advantageous for the clients getting impacted with fake medications.**

Keywords*— *Blockchain, Hyperledger fabric, Smart Contract, Pharma Supply Chain

I. INTRODUCTION

In this period, the universe of robbery and falsifying has contacted each item including drugs and medications. The test of fake medications in the drug business has been expanding across the globe over the course of the last numerous years. As per WHO around 10.5% of the prescribed drugs in the business sectors of low or center pay nations are phony [1]. Fake medications are a growing grave issue related to the medical services industry which makes outrageous threats to the general public. Supply chain network of drug endeavor is obsolete, and doesn't offer perceivability and control for makers and administrative power over the dispersion and it can't avoid the 21st century digital protection dangers. As indicated by the International Anti-Counterfeiting Coalition (IACC), forging has become one among world's biggest and quick creating law breaker organizations, with an anticipated expense of more than US dollar 600 billion yearly [2]. Subsequently, there is a need to foster areas of strength in order to beat the issue of falsifying drugs.

Blockchain is a decentralized record that is shared by all organization members [3]. In view of its temperament, it isn't numerically imaginable to change a current record. This is accomplished utilizing cryptographic algorithms. Blockchain information structure is a rundown of information hinders that are timestamped, unchanging, and in severe request. Immutability is carried out utilizing a hash, a computerized unique finger impression of information. Each block has a reference to a past block's hash and in this manner provides a server request to the blockchain. Following hashes from the ongoing block closes with block 0 — called the genesis block. It is the primary made block on a particular blockchain. Blocks contain a rundown of exchanges. This kind of information structure empowers provenance, or at least, a solitary spot of beginning for any exchange. Since all blockchain exchanges are timestamped and unchanging, false medication dealers can be effortlessly distinguished.

A. Smart Contract

A smart contract is a self-executing contract with the provisions of the understanding among two organizations being straightforwardly composed into lines of code [4]. The code and the agreements present in it exist across a distributed and decentralized blockchain network. Smart contracts confided in exchanges and arrangements to be completed among dissimilar, anonymous organizations without the requirement for a central authority or external enforcement mechanism.

A smart contract is a kind of program that encodes business logic and works on a dedicated virtual machine embedded in a blockchain or other distributed ledger. An organization of PCs which are connected together executes the program when predefined conditions have been met and affirmed. They can be utilized for straightforward monetary exchanges, for example, moving cash from point A to point B. It also provides smart access to the executives in the sharing economy. The blockchain is refreshed after the exchange has been completed. Banking, energy, insurance, music business, telecommunications, mobility, education, art and numerous different ventures have use cases.

B. Permissioned vs Permissionless Blockchain

Permissionless blockchains, otherwise called trust less or public blockchains, are open organizations accessible to everybody to take part in the agreement cycle that blockchains use to approve exchanges and information [5]. They are

completely decentralized across obscure members. The vital qualities of permissionless blockchains are full straightforwardness of exchanges, open source improvement, secrecy for certain exemptions, absence of central authority and weighty utilization of tokens and other computerized resources as motivators to take part.

The cons are: unfortunate energy productivity because of the asset seriousness of organization wide check of exchanges, lower execution and scalability from the strain this confirmation process puts on registering assets, less protection and client command over data.

Conversely, permissioned blockchains also known as private blockchains or permissioned sandboxes are shut organizations in which recently assigned parties, in some cases, individuals from a consortium, communicate and partake in agreement and information approval [5]. They are to some extent decentralized in the feeling of being circulated across known members as opposed to obscure members, as in permissionless blockchains. Tokens and advanced resources are conceivable, however more uncommon than in permissionless. The vital qualities of permissioned blockchains are: controlled straightforwardness in view of the objectives of partaking associations, improvement by confidential substances, absence of namelessness and absence of a focal power, yet a confidential gathering approves choices.

Their advantages are strong protection since consent is expected to get to exchange data; adaptability for explicit purposes, since it permits assorted designs, secluded parts and hybrid incorporations; Execution and scalability in light of the fact that less hubs oversee transactions check and agreement.

C. *Hyperledger Fabric*

Hyperledger Fabric is an open-source undertaking grade permissioned disseminated record innovation (DLT) stage hosted by The Linux Foundation, which is intended for use in big business settings, that conveys some key separating abilities over other well-known distributed ledger and blockchain platforms [6].

Hyperledger was laid out under the Linux Foundation, which itself has a long and surprisingly effective history of supporting open-source projects under open administration that develop further supporting networks and flourishing environments. Hyperledger is represented by a different specialized controlling panel, and the Hyperledger Fabric project by an assorted arrangement of maintainers from numerous associations.

Fabric has a profoundly designed modular and configurable design, empowering development, flexibility and enhancement for a wide scope of industry use cases including banking, finance, insurance, medical care, HR, production network and surprisingly, computerized music conveyance. It is the first distributed ledger platform to help smart contracts composed in universally useful programming languages like Java, Go and Node.js, instead of constrained domain-specific languages (DSL). This implies that most ventures as of now have the range of abilities expected to develop smart contracts, and no extra preparation to gain proficiency with another language or DSL is required.

The Fabric stage is permissioned, intending that, unlike with a public permissionless organization, the members are known to one another, instead of mysterious and malicious users. This intends that while the members may not completely trust each other (they may, for instance, be rivals in a similar industry), an organization can be worked under an administration model that is worked off of what trust exists between members, like a lawful understanding or structure for taking care of disagreement or arguments.

In the proposed model Hyperledger fabric is used because it has a highly modular and permissioned architecture. It has support for developing smart contracts in JavaScript and has a flexible endorser model to achieve connectivity among different organizations. Smart contracts are used to execute backend transactions between different peers. It plays a vital role in transferring assets from one peer to another.

II. Related work

Alexander Dolgui and Jean-Marie Proth [7] proposed an RFID, which comprises a reader and a tag which is a silicon chip associated with a radio antenna. At the point when a tag goes through the field covered by a reader the data present inside the tag is sent to the reader. RFID systems can be considered as the replacements of bar codes. RFID readers can be connected to different tags. As an outcome, it is feasible to collect all the data concerning a whole shipment. Sometimes it is not as accurate or reliable as barcode scanners and they are expensive.

In the centralized method proposed by Samantha Crossfield [8], the electronic health record is stored in the centralized database, which stores all the information regarding stakeholders involved in the supply chain and transactions happening between them. Information storage for all the stakeholders involved in the pharma supply chain is done in RDBMS and NOSQL databases and their performance is compared. Storing electronic health records in a centralized database raises a security concern as anyone who can access the main database can tamper with the information. There is another problem of single point of failure as any damage happening to the database can result in failure of the entire supply chain.

Berk Kucukatlan et al. [9] introduce the whole supply chain model which is applicable in the Medical, Food, Electronics Industry and is secured with only QR codes. The peers verify data sent by each other through scanning of QR codes. The codes contain data of the stakeholder along with the product information. Furthermore, the usage of this technology together with social media tools is proposed. QR codes have a security concern: they can easily be replicated and thus introduce risk of tampering of data in blockchain.

Kavitha Kumari et al. [10] proposed a model in which every peer first enters their information and encrypts it using the DES algorithm and then inserts it in the blockchain. The information is distributed in the form of blocks thus reducing the disadvantage of centralized databases. The DES cryptographic algorithm is slow compared to other algorithms. The 56-bit key size of the algorithm is the biggest defect due to

which it can be easily decrypted by current developed code cracking systems.

In [2], a decentralized Blockchain network where similar stakeholders involved in a Pharma Supply Chain are made as peers. While transferring data from peer-to-peer Symmetric Cryptographic Algorithm AES is used in order to encrypt the data and insert in the blockchain network. Manufacturer will enter the drug's information and apply an encryption algorithm to create the cipher text. The block contains cipher text of the current peer appended with cipher text of previous peer and then these blocks are added in the blockchain. The most concerning issue with symmetric key encryption is that you really want to have a method for the key to get to the party prior to sending the genuine information.

In [11] an instance was created on the Ethereum blockchain platform, which is at present one of the largest public blockchain networks and open-source framework, flaunting a functioning local area and a sizable public storehouse of Decentralized Apps. The platform as of now utilizes a Proof-of-Work (PoW) consensus algorithm called Ethash. The scalability limitation of proof-of-work slows down the transaction speed in a particular PoW-based blockchain. Also, it increases the associated cost with developing a blockchain application

The Decentralized Peer to Peer network proposed by Vishwesh Lingayat et al. [12] is designed with proof of work as Consensus Algorithm. Here QR codes are used to encrypt the blocks and inserted in the blockchain. One by one each peer scans the QR code and verifies the block and creates their own blocks through QR code and enters in the blockchain. QR codes have a security concern: they can easily be replicated and thus introduce risk of tampering of data in blockchain.

We have [13], in which the Blockchain network is designed using the Ethereum blockchain platform, which is currently one of the largest public blockchain networks and it also has an open source framework, along with this Smart Contracts are used to build applications for implementing transactions in the Blockchain. Ethereum is a permissionless blockchain. In a permissionless blockchain, anybody can interact with the network by creating their own address thus reducing security provided by blockchain.

II. Proposed Methodology

A. Objective of the Proposed method

The aim of the research work is to create a blockchain model that can forestall fake drugs in drug store networks. The drug development is monitored from the business to the patients by applying blockchain.

Blockchain innovation is profoundly fit for monitoring the medication history all through the drug production network. Two significant perspectives that make blockchain data secure and safe are that, the blocks are timestamped and unchanging making altering of data unimaginable.

Associations can have either a public blockchain or a confidential one. The associations will divide a distributed record among the gatherings engaged with the production and dispersion of the medication on these blockchains. Also, in these blockchains just restricted access is given which relies upon the information dividing contract between the two peers. Our peer to peer blockchain network is developed using Hyperledger fabric which is a private blockchain where whenever any user tries to enter the blockchain their enrollment is done by properly taking their credentials and based on it the certificates are given to them, thus providing a better Identity management system. Hyperledger is not a permissionless blockchain like Ethereum which is commonly used in Bitcoin.

Smart Contracts are used in the blockchain to construct and control transactions happening between stakeholders. Smart Contracts is a couple of lines of code which is consequently executed at whatever point a few agreements are met. They are used for designing transaction functionality.

The proposed model can be divided into 3 modules:

First module is *ledger* which consists of:

- *Channel-artifacts:* It contains information about channel configuration like types of organization and peers in the blockchain.
- *Crypto-config:* It contains information about the configuration of the organization and their peers like their domain name, count of peers etc.
- *Docker configuration files:* This file consists of peer network information i.e., information about which peer belongs to which organization along with fabric server name on which the network will be running, on which port a container will be running
- *Fabric Scripts:* This is a shell script which consists of all necessary commands and functions to start the fabric network through docker engine-like commands for installing chain code.

The second module is smart contracts which consists of:

- *RegistrationContract:* This file contains smart contract code for registration of entities in the network. For implementing a contract, it imports fabric-contract-api and takes details about the entity from the user for registration.
- *Node modules:* This folder consists of all the node modules necessary for using the functions in the api and contract files designed for their respective uses.
- *TransferDrug:* This file contains smart contract code for updating shipment information by taking purchase order and shipment order transaction information and changing ownership of the drug from one entity to the other thus transferring drug.
- *Fabric-Contract Api:* This programming interface gives the contract interface a significant level API for application engineers to carry out Smart Contracts.

The third module is User interface which consist of:

- *Api to expose backend:* Api indicates code for writing all necessary transactions to be done by each

individual entity like code for creating purchase order or shipment order, buying drugs, sending shipment etc. These api require contract code to function properly.

- *User Interface:* All front end is designed with the help of HTML, CSS and JavaScript framework.
- *addToWalletForAllOrg:* Before writing any api functionality with the help of smart contracts, identity of the entity needs to be added to the wallet. Identity is added by importing crypto materials from crypto-config file and key from keystore.
- *ContractHelper:* This file contains smart contract code for creating a contract instance in general for all backend api to use for their functionality. This file contains code for importing entity identity from the wallet and crypto materials from the crypto-config file.

B. *Architecture:*

The overall system architecture and system design is depicted in Fig. 1. and Fig. 2. respectively. Smart Contract is a couple of lines of code which is naturally executed at whatever point a few agreements are fulfilled in a blockchain network. It can incorporate the exchange of resources starting with one level then onto the next or an update in the network of some sort. Fundamentally, a piece of code upholds the understanding done between two peers without bothering any third person. They likewise empower the clients to deal with their access privileges and their resources among various peers. They are stored on ledgers and are secured from any kind of counterfeiting.

Whenever a user enters some information in the front end of the application it triggers the smart contract related to the user's transaction. There is a smart contract for every possible transaction in the application. The solicitation for transactions is shipped off to all the peer hubs. Endorsers execute the transaction on the off chance that it is legitimate. Committers approve the outcome by executing those solicitations before it is updated in the ledger. These endorsers execute the contract of mentioned transactions in their simulated environment prior to updating the ledger. Then endorsers return the executed transactions to the user application alongside RW sets. The client again presents the marked transaction with all RW sets to

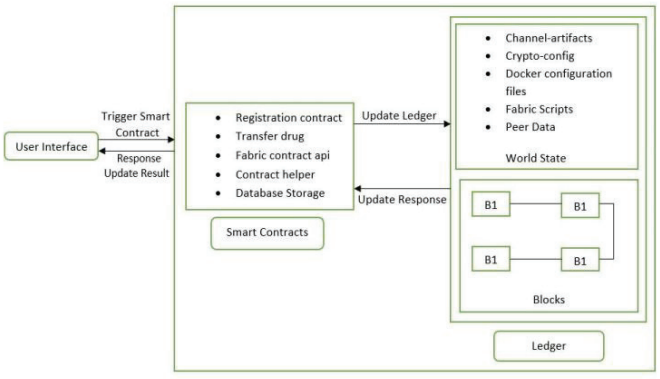

Fig. 1. System Architecture

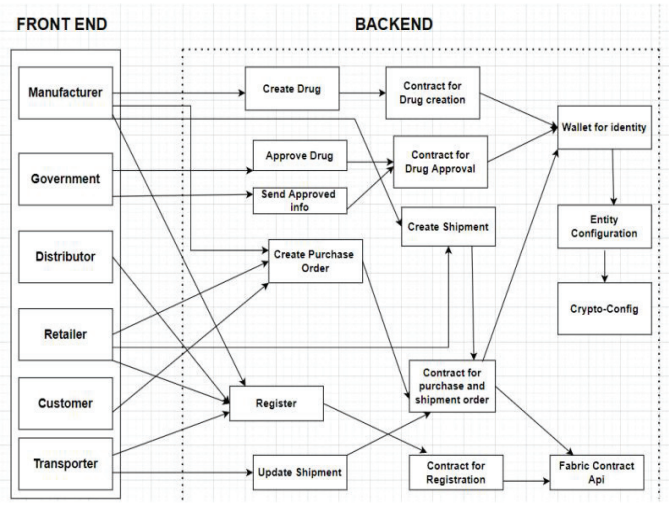

Fig. 2. System Design

the consensus node. The consensus node sends the updates to the committers. The committers approve by matching the ongoing world state and in the event that is coordinated, it is updated into the ledger.

Algorithm for Registration
Input: Details of the entity
Output: Entity Object
Steps involved are:
Step 1: Import fabric-contract-api.
Step 2: Create a composite key for the company.
Step 3: Get the state from the ledger to check if the company already exists with the given CRN.
Step 4: Create entity objects with details such as companyID, name, location and organization.
Step 5: Create a buffer and store the entity object by stringifying the object.
Step 6: Add the object to the world state.
Step 7: Return entity object.

Algorithm for creating contract instances
Input: Object from registration
Output: Contract instance
Steps involved are:
Step 1: Import file system, yaml and fabric-contract module.
Step 2: Create gateway.
Step 3: Get organization identity from wallet and load the organization configuration.
Step 4: Set connection options.
Step 5: Connect to gateway using specified parameters.
Step 6: Access certification channel.
Step 7: Return instance of the contract.

Algorithm for loading a user's Identity to his wallet.
Input: Crypto Materials and key store.
Output: Organization entity added to the wallet.
Steps involved are:
Step 1: Import file system and fabric-contract module.
Step 2: Get the crypto Materials from crypto-config.

Step 3: Fetch the credentials from Crypto Materials such as certificate and private key.
Step 4: Load credentials into wallet.

III. RESULT AND DISCUSSION

We have used Hyperledger fabric version 1.0 as our blockchain model for constructing our distributed network. Ubuntu version 14.04 LTS is used as the operating system for developing the application along with Docker Engine version 17.03 and docker compose version 1.8 along with node version 12. Execution Time and Latency are calculated with the help of the console module of JavaScript.

The graphs mentioned below express the importance of creating different organization structures for monitoring transactions of numerous peers in order to improve performance of applications and how newer versions of Hyperledger are better than previous ones.

Fig. 3. Execution Time Graph varying organization

In Fig. 3, the graph compares Hyperledger fabric's performance when there is a single organization and two organizations. The execution time is calculated for transaction execution as the number of peers in the organization increases. As we can see for the same number of peers multiple organization networks perform better than single organization networks.

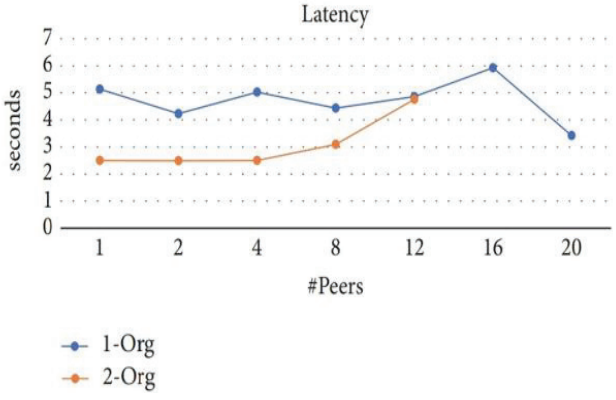

Fig. 4. Latency Graph varying organization

In Fig. 4, the graph compares Hyperledger fabric's performance when there is a single organization and two organizations. The latency is calculated for transaction execution as the number of peers in the organization increases. As we can see for the same number of peers multiple organization networks perform better than single organization networks.

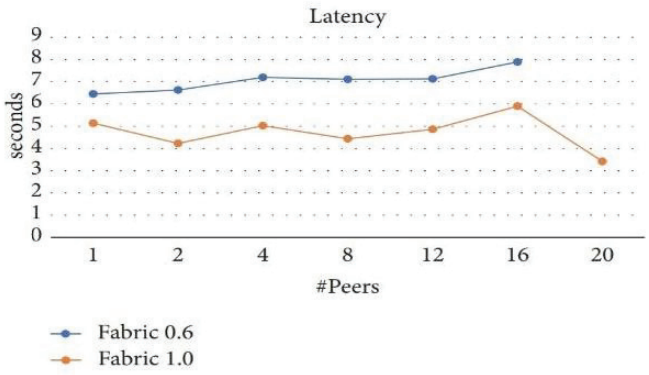

Fig. 5. Latency Graph for different fabric version

In Fig. 5, the graph compares Hyperledger fabric's performance for version 1.0 and 0.6. The latency is calculated for transaction execution as the number of peers in the network increases. As we can see for the same number of peers version 1.0 performs better than 0.6.

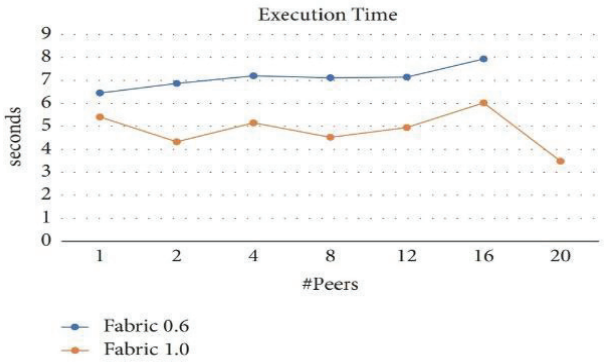

Fig. 6. Execution Time Graph for different fabric version

In Fig. 6, the graph compares Hyperledger fabric's performance for version 1.0 and 0.6. The execution time is calculated for transaction execution as the number of peers in the network increases. As we can see for the same number of peers version 1.0 performs better than 0.6.

IV. CONCLUSION

Serious medical problems, including demise, may happen assuming that the clients consume fake medications. The proposed structure can give both producer's legitimacy as well as medication security. The ongoing philosophies for fighting fake medications deals with outsider trust and consequently needs terms of safety for the medication security. In contrast with these ongoing techniques, the proposed system depends on Blockchain and is consequently exceptionally secure and equipped for managing the phony medications danger. In this undertaking, we have proposed a blockchain based model to

recognize such phony medications. The proposed model additionally intends to follow the development of medications from the business to the customer. We have utilized the Hyperledger fabric to carry out the whole model.

The study design has the following limitations:

1) The proposed framework might have the option to recognize drug developments that follow official circulation links known to the administrative organization. It can't follow adulterated drugs that are circulated through courses beyond official dissemination chains.

2) The proposed framework is created and tested in a controlled, mimicked network, consequently, results obtained from this study may not be intelligent of actual execution when sent in a real-world setting.

In future we can implement this concept in different marketing, social apps and websites.

REFERENCES

[1] The impact of counterfeit drugs in south and south east Asia, Available at: https://www.europeanpharmaceuticalreview.com/article/92194/the-impact-of-counterfeit-drugs-in-south-and-south-east-asia/

[2] Kajal Bharat Adsul and S.P. Kosbatwar, "A Novel Approach for Traceability & Detection of Counterfeit Medicines Through Blockchain", International Journal of Current Engineering and Technology, 2020

[3] Monrat, Ahmed Afif, Olov Schelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities" IEEE Access, vol. 7, pp. 117134-117151, 2019. doi:10.1109/ACCESS.2019.2936094.

[4] Tharaka Mawanane Hewa, Yining Hu, Madhusanka Liyanage, Salil S. Kanhare, Mika Ylianttila, "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research", IEEE Access, vol. 9, pp. 87643-87662, 2021 DOI: 10.1109/ access. 2021. 3068178.

[5] Siamak Solat and P. Calvez December, "Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice", J. Softw., vol. 16, issue. 3, pp. 95-106. , 2021, DOI:10.17706/jsw.16.3.95-1016.

[6] Christian Gorenflo, Stephen Lee, Lukasz Golab, Srinivasan Keshav "FastFabric: Scaling hyperledger fabric to 20000 transactions per second", International Journal of Network Management, vol. 30, issue 5, pp. e2099, 2020, DOI:10.1002/nem.2099.

[7] Alexander Dolgui, Jean-Marie Proth; (July 6-11, 2008) "RFID Technology in Supply Chain Management state of the art and perspectives", IFAC Proceedings Volumes, Volume 41, Issue 2, pp. 4464-4475, 2008, DOI:10.3182/20080706-5-KR-1001.00753

[8] Samantha Crossfield and Susan E. Clamp, "Centralised Electronic Health Records Research Across Health Organisation Types" International Joint Conference on Biomedical Engineering Systems and Technologies, pp. 394-406, 2013, DOI:10.1007/978-3-662-44485-6_27

[9] Berk Kucukatlan and Deniz Herand; (2014): "QR code usage for Marketing Activities of Logistic Companies", Management, vol. 4, Issue 3A, pp. 27-33, 2014, DOI:10.5923/s.mm.201401.04.

[10] Kavita Kumari and Kavita Saini, "CFDD (Counter Feit Drug Detection) using Blockchain in the Pharmaceutical Industry", IJERT, vol. 8, Issue 12, 2019, DOI:10.17577/IJERTV8IS120292.

[11] Patrick Sylim, Fang Liu, Alvin Marcelo, Paul Fontelo, "Blockchain Technology for Detecting Falsified and Substandard Drugs in the Pharmaceuticals Distribution System", JMIR research protocols, vol. 7, issue 9, pp. e10163, 2018

[12] Vishwesh Lingayat, Isha Pardikar, Shubham Yewalekar, Shyamal Khachane and Sachin Pande, "Securing Pharmaceutical Supply Chain using Blockchain Technology", ITM Web of Conferences, vol. 37, pp. 01013, 2021, DOI:10.1051/itmconf/20213701013

[13] P. Zhu, J. Hu, Y. Zhang and X. Li, "A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability," in IEEE Access, vol. 8, pp. 184256-184272, 2020, DOI: 10.1109/ACCESS.2020.3029196.