IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TRACEABILITY AND MONITORING OF MEDICAL DEVICES USING NFT AND BLOCKCHAIN TECHNOLOGY

[1] V.Priyadharshini, [2] V.Subasri, [3] Dr.S.Praveen Kumar

[1] Student,[2] Student,[3] Assistant Professor

[1] Department of Computer Science & Engineering, E.G.S Pillay Engineering College Nagapattinam,Tamilnadu, India

Abstract - The quality and safety of medical device products is related to human life and health, and has been widely valued by the society. Counterfeit products are often manufactured to make benefit of cheaper value of the copied product. Its high risk determines the necessity of establishing a traceability system. Most of the companies are trying to make more efforts to avoid counterfeiting. This project presents a system for QR code focused on applications, security, and privacy. Proposes a medical device traceability system based on both QR technology and blockchain technology. By integrating the traditional tracing system with the blockchain technology, based on the decentralization and non-tamper ability of the blockchain, the alliance chain and the smart contract construction system are adopted. QR codes can be used as effective and low cost solution that can help the industries and customers to check reliability of the medical devices. Generating a QR code for medical device for identification is a simple and cheap process. The proposed system uses QR code because it is easy to implement. To check the authenticity of medical devices, this paper uses a distributed blockchain technology system which ensures that customers do not rely on the third-party apps. Blockchain is a distributed ledger technology where medical device details are recorded and stored making them tamper resistant which is built around strong cryptographic technology. Finally implement DES (Data Encryption Standard) algorithm for encrypting medical device purchase details.

Index Terms - Secure Medical Device Information, QR Code Generation, Blockchain Technology, Authenticity Verification, Medical device purchase, DES Encryption.

I. INTRODUCTION

The emergence of QR has opened a vast variety of possibilities in the technology sector which made accessing, retrieving and viewing information and data from anywhere with great speed and low fault. It is a captivating way of accessing anything from a website or an application. Nowadays due to the ample use of mobile devices, using QR code technology can easily establish connections and communicate with people and share information [4]. It is also a secure way to share information because without the correct tool retrieving of data for someone else that is not intended to view is impossible. Introducing blockchain with QR code will increase this security one more level further.

1.1 BLOCKCHAIN TECHNOLOGY

Blockchain builds on the idea of P2P networks and provides a universal data set that every actor can trust, even though they might not know or trust each other. It provides a shared and trusted ledger of transactions, where immutable and encrypted copies of information are stored on every node in the network. Economic incentives in the form of native network tokens are applied to make the network fault tolerant, and attack and collusion resistant [14].

Blockchain and derived technologies provide a universal and transparent accounting and governance layer for the Internet. All network participants have equal access to the same data in real-time. Transactions running over the network are transparent to all actors and can be traced back to their origin. Blockchain can also be described as a distributed accounting machine or a supranational governance machine that is public and transparent. When the network validates a transaction by majority consensus, the transaction is permanently written to the blockchain. Otherwise, the transaction is rejected and does not go through. Only transactions that have been included in the blockchain are considered as valid and final.

Blockchain is a shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls. It is a distributed database that maintains a continuously growing list of transaction data records, cryptographically secured from tampering and revision. Blockchain has three different types, i.e. public blockchain, private blockchain, and consortium blockchain [3]. Bitcoin and Ethereum are the examples of public blockchain, anyone and from anywhere can join them and can get relieved at the time of his will. This is proofed by the complex mathematical functions. The private blockchain is the internal-public ledger of the company and the joining on that blockchain is granted by the company owning that blockchain. The block construction and mining speed is far better in the private blockchain as compared to public blockchain due to the limited nodes. The consortium blockchain however exists among the companies or group of companies and instead of the consensus the principles of memberships are designated to govern the blockchain transactions more effectively. This research uses consortium blockchain as the blockchain is to be governed by a national authority in the country. Block is the primary component of the blockchain. A block consists of the header and the body, the body of the block contains the transactions being written to the system. The header of the block contains the information about the block that includes previous hash, nonce value and difficulty, and the time stamp of the block and the transactions. The length of the block is variable and deemed to have been among1 to 8 MB of size. The header of the block uniquely identifies the block to be placed.

1.2 HASHING

Hashing is the process of changing the arbitrary and variable size input to a fixed size output. There are different functions that perform hashing of different level. MD5 algorithm is widely used for hashing purposes and it provides a 128 nit or 32 symbols long hash value. MD5 is the latest algorithm in the series while before that Md2, Md3, and Md4 also existed. The algorithm was designed to be used as a cryptographic hashing algorithm but it faces some problems that reduce the production of unique hash value and hence it faces some vulnerability. SHA (Secure Hashing Algorithm) is another cryptographic hash function that yields 160 bit hash value consisting of 40 hexadecimal characters. The algorithm could not resist the collusion attacks against it and its usage has declined. In this time several new algorithms have also been proposed, including SHA 3, and SHA 256. The SHA 2 set of algorithms is designed by the US's Nation Security Agency. SHA 256 and SHA 512 are new hash functions that do not have collusion problems and deemed secure otherwise, at least as yet.

In a Blockchain, each block consists of following headers.

Previous Hash:
This hash address locates the previous block.

Transaction Details:
Details of all the transactions that need to occur.

Nonce:
An arbitrary number given by cryptography to differentiate the block’s hash address.

Hash Address of the Block:
All of the above (i.e., preceding hash, transaction details, and nonce) are transmitted through a hashing algorithm. This gives an output containing a 256-bit, 64 character length value, which is called the unique ‘hash address.’ Consequently, it is referred to as the hash of the block. Numerous people around the world try to figure out the right hash value to meet a pre-determined condition using computational algorithms. The transaction completes when the predetermined condition is met. To put it more plainly, Blockchain miners attempt to solve a mathematical puzzle, which is referred to as a proof of work problem. Whoever solves it first gets a reward.

Mining
In Blockchain technology, the process of adding transactional details to the present digital/public ledger is called ‘mining.’ Though the term is associated with Bitcoin, it is used to refer to other Blockchain technologies as well. Mining involves generating the hash of a block transaction, which is tough to forge, thereby ensuring the safety of the entire Blockchain without needing a central system.

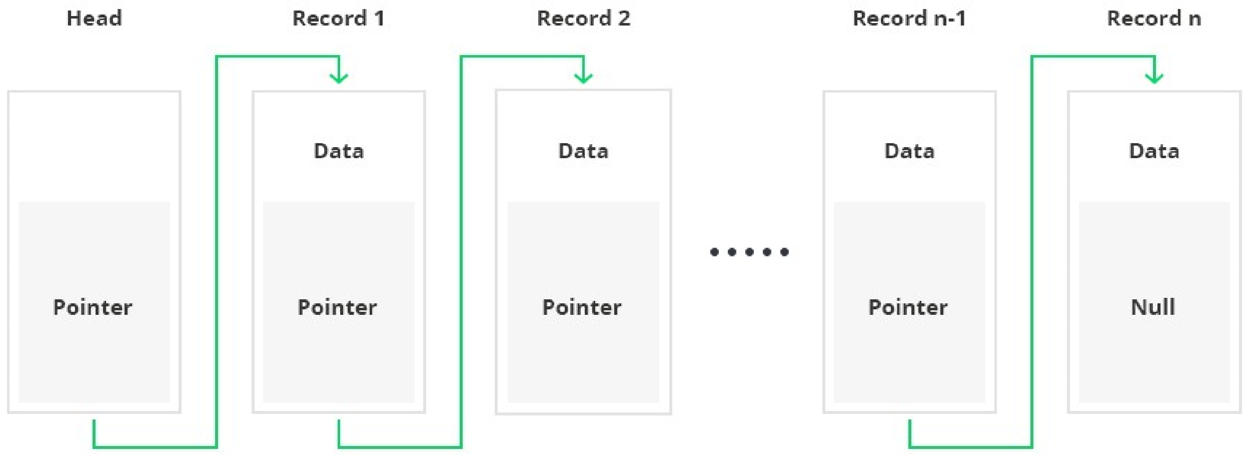

Fig 1: Block Creation

I. Related Work

A Farhad Aghili a et al,…[1] implemented a secure and energy-efficient protocol that not only provides authentication and key agreement but also satisfies access control and preserves the privacy of doctors and patients. Moreover, this is the first time that the ownership transfer of users is considered. In the ownership transfer phase of the proposed scheme, the medical server can change the ownership of patient information. In addition, the LACO protocol overcomes the security flaws of recent authentication protocols that were proposed for e-health systems, but are unfortunately vulnerable to traceability, de-synchronization, denial of service (DoS), and insider attacks. To avoid past mistakes, this present formal (i.e., conducted on ProVerif language) and informal security analysis for the LACO protocol. All this ensures that proposed scheme is secure against the most common attacks in IoT systems. This proposed new authentication and key agreement protocol that preserves anonymity and provides an access control mechanism for the user. Proposed protocol, called LACO, can also cover the transfer of user/doctor ownership. In the LACO scheme, when it is necessary to change the proprietorship of the user/doctor, the ownership transfer phase is executed with the help of the medical server. LACO is the first contribution that addresses the ownership transfer of the user/doctor in IoMT systems. Proposed approach evaluated both the security and efficiency of LACO and demonstrated that proposed scheme is secure and practical for being employed in IoMT systems.

Raja Wasim Ahmad et al, [2] proposed a decentralized blockchain-based solution to automate forward supply chain processes for the COVID-19 medical equipment and enable information exchange among all the stakeholders involved in their waste management in a manner that is fully secure, transparent, traceable, and trustworthy. Proposed approach integrate the Ethereum blockchain with decentralized storage of interplanetary file systems (IPFS) to securely fetch, store, and share the data related to the forward supply chain of COVID-19 medical equipment and their waste management. Here develop algorithms to define interaction rules regarding COVID-19 waste handling and penalties to be imposed on the stakeholders in case of violations. The proposed approach can assist authorities in assuring that the COVID-19 medical waste is disposed of properly, and COVID-19 testing centers are using genuine medical equipment to treat COVID-19 patients. Here presented a detailed cost analysis to show the affordability of the proposed approach. Here also evaluated the proposed approach against known vulnerabilities using the SmartCheck software. The proposed approach is generic and applicable to various use case scenarios with minimal modifications. Proposed implementation code is made publicly available on GitHub.

Abirami Raja Santhi et al., [3] presented an overview of the role of blockchain technology in addressing supplies chain and logistics related challenges by analyzing, organizing, and reviewing the literature. The study shows that blockchain technology can transform the supply chain and logistics into secure, agile, trusted, and transparent functions. A conceptualized application scenario demonstrates the benefits of blockchain technology in providing provenance and traceability to critical products. The major difference between a ledger or transaction stored in a conventional database such as MySQL and a blockchain network lies in the distributed, decentralized, and immutable nature of blockchain technology. For instance, as a conventional database is centralized, an administrator has the authority to control or manipulate the data. In addition, the entire database itself is vulnerable to cyberattacks. However, as a blockchain network is decentralized, all the transaction details are distributed across all the participating nodes of the chain. Hence, all the participating nodes (based on public or private blockchain) are responsible for validating the transaction and broadcasting the timestamped data to the blockchain network in the form of blocks.

Thomas K, et.al,[4] demonstrated a systematic literature review of the various technical implementation aspects of blockchain-enabled SC traceability systems. In this work apply different drivers for classifying the selected literature, such as (a) the various domains of the available blockchain-enabled SC traceability systems and relevant methodologies applied; (b) the implementation maturity of these traceability systems along with technical implementation details; and (c) the sustainability perspective (economic, environmental, social) prevalent to these implementations. This approach provides key takeaways regarding the open issues and challenges of current blockchain traceability implementations and fruitful future research areas. Despite the significant volume and plethora of blockchain-enabled SC traceability systems, academia has so far focused on unstructured experimentation of blockchain-associated SC traceability solutions, and there is a clear need for developing and testing real-life traceability solutions, especially taking into account feasibility and cost-related SC aspects.

Muhammad Azeem Akbar, et.al,…[5] implemented a roadmap to develop a maturity model for blockchain in healthcare (MMBH) based on critical barriers (CBs), critical success factors (CSFs), and the best practices for blockchain implementation in healthcare systems. As a first step to develop the MMBH, in this paper present the initial results of a SLR to identify CSFs for implementing blockchain in healthcare systems. This also applied fuzzy TOPSIS to prioritize the identified CSFs. This proposed study can be considered an initial step towards developing a MMBH, identifying the challenges reported in literature and industry and important success factors that could positively influence blockchain adoption in healthcare. This research is original and relevant as no prior studies address blockchain implementation issues by developing a roadmap. Moreover, this experiment applied fuzzy-TOPSIS analysis to prioritize the identified success factors. The proposed model can be employed in a real-world scenario utilizing a case study. Practitioners may use the results of this study in several ways.

M. M. Kamruzzaman, et.al,…[6] proposed a model attempted to conduct a systematic review of the documents pertaining to the impact of the IoT, blockchain, and fog on the healthcare systems and practices in the context of smart cities. Due to the very little availability of relevant data, 10 studies were selected for the review and their findings have been analyzed. It was found from the systematic review that IoT has been the most applied technology among the three by the healthcare sector in smart cities. The smart city has been understood as a geographical area characterized by emerging information and communication technologies facilitating the flow and exchange of information. Thus, with the incorporation of information and communication technologies, the efficiency of the information exchange increases in terms of both cost and speed. In order to support healthcare in the context of smart cities and incorporating smart initiatives, IoT, blockchain technology, and fog computing appear to be quite relevant. /e application of these technologies can automate the processes and support healthcare in smart cities. To conceptualize, IoT can be understood as the combination of devices that can interact with each other for sharing and exchanging information. The blockchain has been understood as a distributed database comprising a chain of blocks whereby each block represents a different transaction that acts as a public ledger. Lastly, fog computing is understood as a virtual platform between the computing device and the cloud center.

Kazi Tamzid Akhter Md Hasib, et.al,…[7] Implemented the system for monitoring health data sharing through internet using blockchain technology. It focuses on limiting third-party engagement in medical health data and improving data security. Rough out the process, this will improve accessibility and time efficiency. People will feel safer during the payment procedure, which is the most significant benefit. A smart contract and a peer-to-peer encrypted technology were used. The hacker will not be able to gain access to this system since this document uses an immutable ledger. They will not be able to change any of the data if they gain access to the system. If the items are found to be defective, the transaction will be halted. Transaction security will be a viable option for recasting these problems using cryptographic methodologies. Here developed a website where patients and doctors will both benefit because of the use of blockchain technology to ensure the security of medical data. This have different profiles for doctors and patients. In the patient profile, they can create their own account by using a unique address, name, and age. This unique address will be created from the genesis block. The unique address is completely private to the owner, who will remain fully secure in proposed network. After creating an account, the patient can view the doctors' list and they can upload their medical reports such as prescriptions and X-rays. All the records uploaded by the patient will be stored on local server.

Suyel Namasudra,, et.al,…[8] Proposed a blockchain-based technique based on Mobile Application (MA) for IoT-enabled healthcare systems to provide a privacy-preserving environment. The proposed system supports the prevention of improper access to medical certificates and their preservation. Furthermore, it also speeds up verifying a physical certificate and prevents unauthorized access to records of birth, death, and sick leave. This work proposes a blockchain-based application to generate, and maintain medical certificates on IoT devices. The proposed system utilizes the Ethereum public blockchain network with the Proof of Stack consortium algorithm. The proposed blockchain structure stores and maintains the generated certificates on Inter Planetary File System (IPFS). After storage, the IPFS returns a unique hash of the certificate with a unique transaction ID. The users can use or show their unique ID received from MA, whenever they want to access the corresponding certificate.

Kebira Azbeg, et.al,…[9] Presented a Blockchain-based system to secure the IoT healthcare devices and the interaction between them at different levels. Proposed solution aims to collect, store, and share patient health data with healthcare teams in a secure manner while preserving patients' privacy. The distributed nature of Blockchain technology can make the system more robust to a single point of failure. In addition, the use of smart contracts can allow secure authentication for devices and handle access control to data. The system architecture is based on a set of technologies, namely, IoT healthcare devices, Blockchain technology, Smart contracts, Interplanetary file system (IPFS), and proxy re-encryption. Health data are encrypted before being stored in an off-chain database that relies on a private IPFS. Using a scenario-based diabetes management system, this empirically validates a secure approach that provides remote monitoring for diabetic patients. The proposed system offers a high security level compared to the state-of-the-art methods. Currently, here developing a web version of proposed solution. In future work, a plan to add a fog layer between medical devices and the hospital in order to filter data before sending them to the hospital. It can also process data and provide the patient with real-time analysis.

Ammar Odeh, et.al,…[10] presented a detailed review of the issues and applications of utilizing blockchain in the healthcare and medical fields emphasizing the particular challenges and aspects. This includes specific applications such as drug traceability, observation of patients, and Electronic Health Records (ERH). Confidentiality (also called secretiveness) is one of the core principles of ethics. The relationship between the patient and the healthcare professional expert is only based on trust. Every medical record, therefore, needs to be made under the main premise that all health information of any given patient will at all times be made confidential not only by the doctor but also by any other members of the healthcare team who have the legal and professional right to access such records. There is always a great need for such information to be protected from access by any unauthorized persons or disclosure to any family member except in the circumstances that it is required by law or in the situation where the patient has given out consent in writing. As for protecting the data from any project, the data from any of the above findings show securely, blockchain technology has failed to securely protect the data from unauthorized dealers. This is contrary to the academic expectations that always medical records must be stored in a safe place without fail to address.

II. EXISTING METHODOLOGIES

In existing system a non-fungible token (NFT) based solution was proposed that exploits blockchain smart contracts, integrates tokenization protocols, and utilizes a decentralized storage system for a reliable and efficient medical devices traceability system and ownership management solution. In proposed system, NFTs are used to represent the digital twin of the medical device. This digital twin captures the medical device attributes and its relevant metadata during its life cycle from production, manufacturing, distribution and movement, to current use and ownership. As a first step, all system participants and stakeholders must register and authenticate their identity through the proposed application. This is an important step because NFTs only reveal the wallet address of its owner and not the real identity associated with the wallet and it is crucial to identify participants in the proposed system as it involves selling and delivering physically existing medical devices. In a private blockchain, this is solved easily as stakeholders need to receive an invitation and then complete a registration process before joining the network. In a public blockchain, on the other hand, digital certificates can be used to authenticate the identity of individuals or entities.

Digital certificates can also be used as part of the authentication and registration process. If the proposed system is implemented in a public blockchain, users can submit their digital certificates to authenticate and verify the identities of stakeholders. An authenticated user who wishes to sell a medical device submits, as part of the NFT metadata, a hashed content of the device's digital twin, which includes a certificate of authenticity, all stored on IPFS. The certificate of authenticity (COA) is any kind of official document that is used to prove the originality or genuineness of the medical device. This document is drawn up by the manufacturer or a trusted and reputable third party certificate provider. To add an extra layer of trust for buyers, the COA is digitally signed, through the DApp, using the manufacturer's private key, which is a cryptographic value used to encrypt data. The template for the COA should contain technical details, including the device name, its unique identifier, manufacture data, as well as information about the manufacturer. Through the NFT contract, stakeholders including the manufacturer of the device, and regulatory authorities such as the FDA and other certification service providers, have the ability to verify all submitted details, approvals, and certifications. Once that is complete, a token certificate representing the physical medical device is minted and stored in the blockchain. The NFT metadata generated by the smart contract is also shared with all the stakeholders and stored in IPFS storage. A registered buyer submits a purchase request for the medical device NFT through the DApp. Once the purchase is approved, ownership of the NFT is transferred to the buyer. The transaction is recorded on the blockchain and it is announced to all the stakeholders.

III. MEDICAL DEVICE TRACKING USING QR CODE WITH BLOCKCHAIN STORAGE AND DES ENCRYPTION

The quality and safety of medical device products is related to human life and health, and has been widely valued by the society. In this proposed work focus on implementing authentic medical device purchase system that uses both Quick Response (QR) code technology and Blockchain technology. Its high risk determines the necessity of establishing a traceability system. Tracking medical devices not only reduces medical accidents, but also prevents the spread of counterfeit or unqualified medical devices. It also helps companies find the source of the problem and determine the flow of the same batch of products, and ensure the rights of consumers. This project proposes a medical device traceability system based on blockchain technology. It uses a blockchain consensus mechanism, distributed storage, encryption and other technical features to establish a decentralized traceability system, which can solve the problems of malicious tampering of intermediate link data and unknown data sources in the traceability system for medical devices**.** Manufacturers, distributors, hospitals and consumers in the system can access product information and trace the entire circulation process of the product through QR code. Consumer only scans the QR code and gets the details regarding it. In addition, consumers use QR code for getting products related information, such as the shelf life, production enterprises, production time, product price, etc.

Here ensure the process of tracking medical device information, approving, and selling medical devices is safe and certified by authorized members. At first, medical device information are stored by manufacturers. This information is stored as a “blocks” in blockchain that is monitored by the block chain manager. It provides an immutable history for the medical device information from dispatching the original lot by the manufacturer until a seller collects it using blockchain technology. All nodes jointly make decisions and verify the legitimacy of the medical device information system. Even if some nodes in the system are attacked and destroyed, it will not damage the entire block chain system. With manufacturer and customers being able to track medical devices throughout the supply chain, they will trust each other. Manufacturers will be able to see that the products they want to deliver are safely received by the intended client. On the other hand, client will be able to see that the product he wants to buy is developed by a legitimate manufacturer, and he got it in its original form. A conventional medical device purchase process can track product information throughout its journey, i.e., from the manufacturer to the buyer. However, employing blockchain extends this functionality to expand the chain of custody to include the consumers of this medical device information system, where it can record the purchase of any medical device along with the customer.

METHODOLOGY

QR CODE GENERATION

A QR code is a scannable barcode encoded with data. Encoded means converted into a particular form. In the case of QR codes, numeric and alphanumeric characters, bytes, and kanji convert into a unique two-dimensional arrangement of squares. When an optical scanner passes over those squares, it translates their arrangement back into that data’s original form.

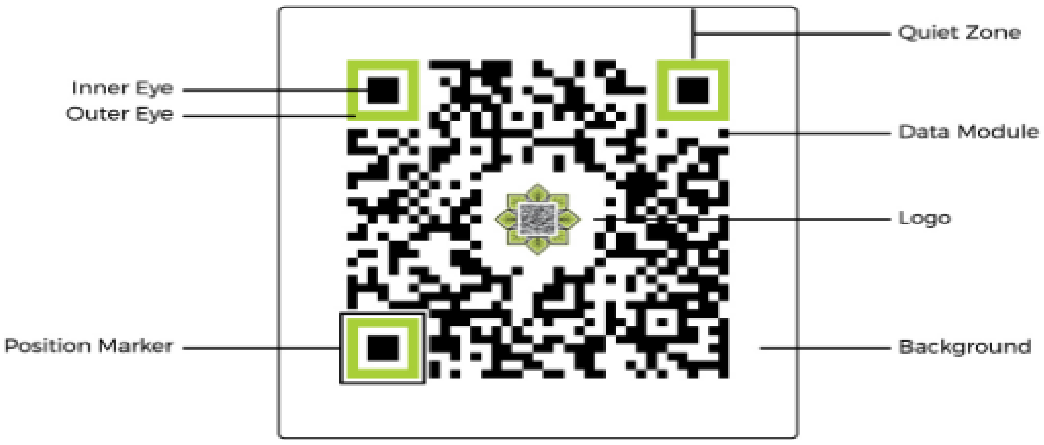

Fig 2: QR Code Structure

The most important parts of a QR code are:

- **Data module**. This is the standard unit of the QR code. It’s typically a black square set against a white background. Though the colors and contrast can be different, black-on-white is the most optimal when creating a custom QR code. The arrangement of these black squares, or data modules, is what makes up the majority of a QR code.

- **Position marker**. There are three position markers on every QR code. Consisting of an inner and outer eye, they allow scanners and cameras to quickly and accurately locate the data modules and the scanning direction.

- **Quiet zone**. This is the blank area on all sides of the data module matrix that contains all the data modules and position markers. It allows scanners and readers to optically place where the QR code begins and ends.

BLOCKCHAIN TECHNOLOGY

A blockchain is a digital concept to store data. These blocks are chained together, and this makes their data immutable. When a block of data is chained to the other blocks, its data can never be changed again. It will be publicly available to anyone who wants to see it ever again, in exactly the way it was once added to the blockchain.
The most adopted secure algorithms associated with the blockchain technology are (SHA-1, SHA2, and SHA-256) encryption because of their unique quality of hash function that creates unique outputs when given different inputs. The hash function here is a unique key created to identify a transaction that at the same time identifies an individual in the petroleum supply chain [19].

Blockchain technology functions are reliable for use in a hashing crypto method, which helps create an adequate and strong hashing code and convert it from a bit of fixed size data to strings of character. Each transaction proposed in a blockchain are hashed together before shoving in a block, and the hash pointers connect each block to the next block for holding of previous hash data as it is undisputable. Therefore, any changes in the blockchain transaction of hashing function will result in different hash string of character and affect all the involved blocks [27].

Block and Hash Generation

1. A Block containing information about current transactions.
2. Each data generates a hash.
3. A hash is a string of numbers and letters.
4. Transactions are entered in the order in which they occurred.
5. The hash depends not only on the transaction but the previous transaction's hash.
6. Even a small change in a transaction creates a completely new hash.
7. The nodes check to make sure a transaction has not been changed by inspecting the hash.
8. If a transaction is approved by a majority of the nodes then it is written into a block.
9. Each block refers to the previous block and together make the Blockchain.
10. A Blockchain is effective as it is spread over many computers, each of which has a copy of the Blockchain.

DES CERYPTOGRAPHY

The Data Encryption Standard (DES) algorithm is a symmetric encryption algorithm that takes a fixed-length plaintext as input and produces a fixed-length ciphertext as output. Here are the steps involved in the DES algorithm:

Key Generation: A 64-bit encryption key is generated from a user-supplied passphrase using a key derivation function. This key is used to encrypt and decrypt the plaintext.
Initial Permutation: The 64-bit plaintext block is permuted using a fixed permutation table.
Splitting: The permuted plaintext is split into two 32-bit blocks, referred to as the left half and right half.
Round Function: A series of 16 rounds is performed, where each round consists of the following steps:
Expansion: The right half of the plaintext is expanded from 32 bits to 48 bits using a fixed expansion table.
Key Mixing: The expanded right half is XORed with a 48-bit subkey derived from the encryption key for the current round.
Substitution: The 48-bit result is split into 8 6-bit blocks, each of which is substituted using a fixed S-box table to produce 8 4-bit blocks.
Permutation: The 32-bit result of the substitution step is permuted using a fixed permutation table.
Mixing: The permuted result is XORed with the left half of the plaintext.
Final Permutation: After the 16 rounds are completed, the left and right halves of the plaintext are swapped and permuted using a fixed permutation table to produce the final ciphertext.

The above steps summarize the basic DES algorithm. In practice, there are variations of DES that include key strengthening, multiple encryptions, and other modifications to improve security. Additionally, DES has been largely superseded by more advanced encryption algorithms like AES.

PROCEDURE

Admin Credentials

Blockchain provides a secure channel for medical device supply chain stakeholders such as manufacturers, patients, Distributors, etc. The movement of medical device at every step in supply chain is stored on the blockchain. In this module, admin can verify manufacturer using company certificate information. Admin has unique authentication factors for login process; he can initialize the process with the help of login process.

Medical Device Details with QR

In this module, manufacturer can add medical device details to the application server. The QR code can be placed at each set of medical device information during information registration process. During medical device register process the unique QR code was generated for each medical device. This can be used to identify the object throughout the supply chain. Along with this, the information about that medical device will be stored in block chain.

Blockchain Creation

The manufacturer manufactures medical device and binds it with a unique QR code. The manufacturing details of the medical device along with the QR code are stored on the blockchain. The information added by the manufacturer gets stored on the blockchain, providing transparency to the supply chain to other stakeholders. Once information is added to the blockchain, a hash ID is produced that can be used for tracking the transactions. At first, medical device information are stored by manufacturers. This information is stored as a "blocks" in blockchain that is monitored by the block chain manager. It provides an immutable history for the medical device information from dispatching the original lot by the manufacturer until a seller collects it using blockchain technology. All nodes jointly make decisions and verify the legitimacy of the medical device information system.

Information Tracking

QR code based medical device information tracking and purchase with blockchain technology can provide a secure and efficient system for tracking and purchasing medical devices. Each medical device can be assigned a unique QR code that contains all relevant information, including the device's manufacturing and expiration dates, batch numbers, and maintenance history. Healthcare providers can scan the QR code using a mobile device to access the device information and verify its authenticity.

Medical Device Purchase

Healthcare providers can purchase medical devices directly from the manufacturer using a blockchain-based payment system. This system can be designed to facilitate secure and transparent transactions and eliminate the need for intermediaries. The blockchain-based system can also enable healthcare providers to track the device's usage and maintenance history, ensuring that the devices are functioning correctly and minimizing the risk of device failure. In this proposed work, purchase details are encrypted using DES algorithm. This ensures the confidentiality of medical device purchase information.

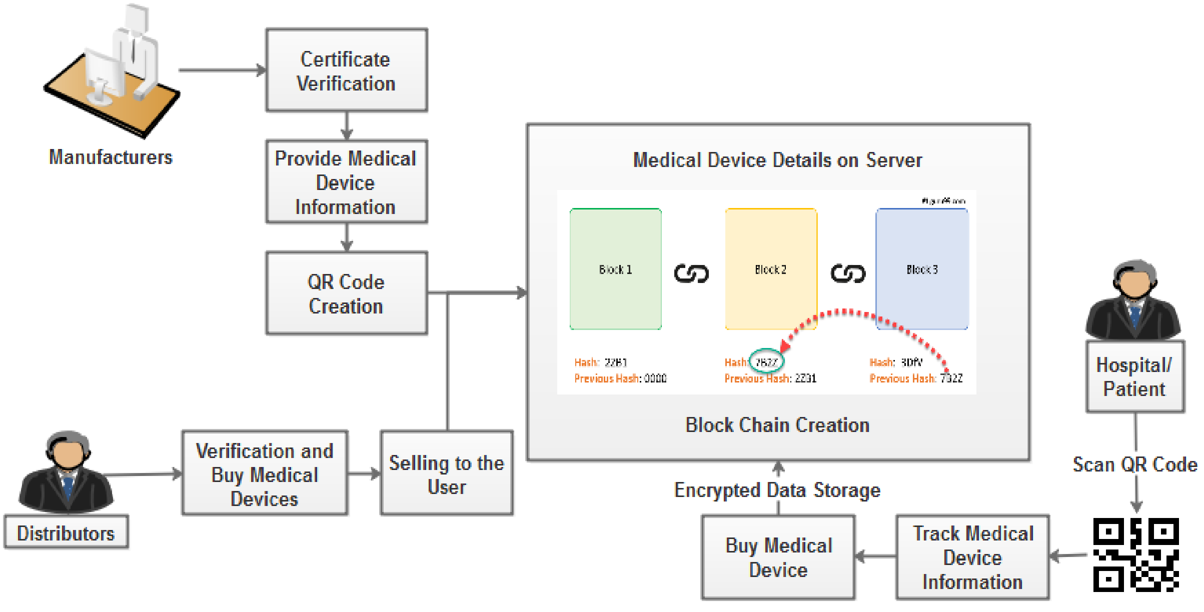

Fig 3: Architecture for Proposed Work

V Conclusion

Proposed system gives the customers an easy and effective method to verify the manufacturer and authenticity of the manufacturer, so that any duplicates or fake products can be avoided. Origin information is stored in blockchain and they can't be changed or modified, hence once the product is verified by using QR code. In addition to detecting alteration, cloning, and tag replication attacks, this Blockchain Ledger can track products without the use of a centralized managing server. They can't be reusable. It is important to note that reducing counterfeits cannot be achieved by only using technological means. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging must also take into account.

REFERENCES

[1] Aghili, Seyed Farhad, Hamid Mala, Mohammad Shojafar, and Pedro Peris-Lopez. "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT." future generation computer systems 96 (2019): 410-424.

[2] Ahmad, Raja Wasim, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Mohammed Omar, and Samer Ellahham. "Blockchain-based forward supply chain and waste management for COVID-19 medical equipment and supplies." Ieee Access 9 (2021): 44905-44927.

[3] Raja Santhi, Abirami, and Padmakumar Muthuswamy. "Influence of blockchain technology in manufacturing supply chain and logistics." Logistics 6, no. 1 (2022): 15.

[4] Dasaklis, Thomas K., Theodore G. Voutsinas, Giannis T. Tsoulfas, and Fran Casino. "A systematic literature review of blockchain-enabled supply chain traceability implementations." Sustainability 14, no. 4 (2022): 2439.

[5] Akbar, Muhammad Azeem, Víctor Leiva, Saima Rafi, Syed Furqan Qadri, Sajjad Mahmood, and Ahmed Alsanad. "Towards roadmap to implement blockchain in healthcare systems based on a maturity model." Journal of Software: Evolution and Process (2022): e2500.

[6] Kamruzzaman, M. M., Bingxin Yan, Md Nazirul Islam Sarker, Omar Alruwaili, Min Wu, and Ibrahim Alrashdi. "Blockchain and fog computing in IoT-driven healthcare services for smart cities." Journal of Healthcare Engineering 2022 (2022).

[7] Akhter Md Hasib, Kazi Tamzid, Ixion Chowdhury, Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. "Electronic health record monitoring system and data security using blockchain technology." Security and Communication Networks 2022 (2022): 1-15.

[8] Namasudra, Suyel, Pratima Sharma, Ruben Gonzalez Crespo, and Vimal Shanmuganathan. "Blockchain-based medical certificate generation and verification for IoT-based healthcare systems." IEEE Consumer Electronics Magazine (2022).

[9] Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management." IEEE Transactions on Computational Social Systems (2022).

[10] Odeh, Ammar, Ismail Keshta, and Qasem Abu Al-Haija. "Analysis of Blockchain in the Healthcare Sector: Application and Issues." Symmetry 14, no. 9 (2022): 1760.

[11] D. Bentley. The Insidious Problem of Counterfeiting in Healthcare. Accessed: Feb. 26, 2022. [Online].

[12] S. Webster. Tackling the Challenge of Counterfeit Medical Devices Across Global Healthcare Settings. Accessed: Mar. 9, 2022.

[13] Medical Device & Equipment Fraud. Accessed: Mar. 2, 2022. [Online].

[14] A. Hern. Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears. Accessed: Mar. 9, 2022.

[15] U. S. Food and Drug Administration. Classify Your Medical Device. Accessed: Sep. 12, 2022.