International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Vaccination Certificate Supply Chain Management using Blockchain

Haydon Rex E A
Department of computer science and engineering
Karunya institute of technology and Sciences
Tamilnadu, Coimbatore, India
eahaydonrex@karunya.edu.in

***Abstract*— The efficient and secure management of the supply chain for vaccination certificates is critical in ensuring that people can safely participate in activities that require proof of vaccination. This process involves coordinating various stakeholders such as manufacturers, distributors, healthcare providers, and regulatory bodies to ensure that the necessary resources, systems, and processes are in place. Manufacturers produce the vaccines and the materials needed for creating certificates, while distributors ensure that they are distributed efficiently to healthcare providers who administer the vaccines and create the certificates. Regulatory bodies verify the authenticity of the certificates and ensure security measures are in place to prevent counterfeiting. The process also requires transparency and real-time information to ensure that stakeholders have access to up-to-date information on the production, distribution, and verification of vaccination certificates. Effective supply chain management helps to ensure that vaccines are administered safely and efficiently, providing people with the necessary proof of vaccination to participate in various activities.**

***Keywords*— Vaccination Certificate authenticity; traceability; supply chain; blockchain**

I. INTRODUCTION

The COVID-19 pandemic has caused a global health crisis, which has prompted governments worldwide to implement vaccination programs. With the increasing number of people getting vaccinated, the demand for vaccination certificates has surged. These certificates serve as proof of vaccination and are essential for travel, attending events, and accessing facilities. However, without proper vaccination certificate supply chain management, the distribution and verification of these certificates can become chaotic, leading to fraudulent activities and potential harm to public health. Not using vaccination certificate supply chain management can result in various challenges, such as fake certificates and unequal distribution. For instance, individuals can create fake certificates, misrepresenting their vaccination status, which can be used to access facilities and travel to other countries. This practice undermines public health measures that aim to contain the spread of the virus. Moreover, if individuals without vaccination access facilities or events, it could increase the risk of virus transmission, thereby putting public health at risk. In addition to fraudulent activities, the unequal distribution of vaccination certificates can become a significant problem. If certain groups receive certificates while others do not, this creates a divide that can further perpetuate inequality in society. For instance, marginalized communities that may not have equal access to vaccines may face challenges obtaining vaccination certificates. This could create a situation where only certain people can travel or attend events, while others cannot, which can lead to further social division. Furthermore, without proper vaccination certificate supply chain management, the security and integrity of these certificates can become compromised. The certificates may be vulnerable to hacking or fraud, which can lead to widespread misuse. This situation can cause panic among the public, leading to a breakdown of trust in public health measures. In contrast, vaccination certificate supply chain management can provide a solution to the challenges mentioned above. By establishing secure and transparent processes for the production, distribution, and verification of vaccination certificates, fraudulent activities can be minimized, and public trust can be

maintained. For instance, using blockchain technology can ensure that the certificates' distribution is secure and transparent, while digital wallets can provide a secure and convenient way to store the certificates. This way, the authenticity and integrity of the certificates can be guaranteed, and public health measures can be maintained. Moreover, vaccination certificate supply chain management can promote equitable access to vaccination certificates. By implementing transparent distribution processes, marginalized communities can receive the certificates they need, which can promote social equality. Also, such management ensures that everyone receives a fair chance to obtain the certificates they need to access facilities or travel. In conclusion, vaccination certificate supply chain management is necessary in the current global health crisis. The challenges associated with not implementing proper vaccination certificate supply chain management can lead to fraudulent activities, unequal distribution, and public health risks. With the increasing demand for vaccination certificates, it is imperative to establish secure and transparent processes to produce, distribute, and verify these certificates. By doing so, we can ensure the authenticity and integrity of these certificates while promoting equitable access to vaccines and vaccination certificates.

Blockchain technology produces a digital logbook. Information about every transaction is kept in chronological order and sent to involved parties. Participants in the system check every entry made in the book. A block is a single recorded transaction, and a chain formed by many blocks is unbreakable. A digital recording book is created using blockchain technology. Information about every transaction is kept in chronological order and sent to involved parties. Participants in the system check every entry made in the book. A block is a single recorded transaction, and a chain made up of all those transactions is known as a block. Information entered into a blockchain is irrevocable. This is because each block contains the end of the one before it, allowing for the creation of a blockchain. Satoshi Nakamoto was the person who originally disclosed blockchain technology. It is frequently referred to as "Distributed Ledger Technology (DLT)" and is the technology that underpins many cryptocurrencies like Bitcoin and Ethereum. The user is the node, and transactions are different from financial transfers or cryptocurrency transfers. A blockchain is a distributed database that operates in a group of connected nodes where information about various sorts of transactions can be kept. In fact, a digital ledger is created by blockchain technology that keeps track of individual transactions along the whole supply chain. Every stakeholder has access to the transaction's information, which is kept in chronological order. Each block has a hash and a time stamp that links it to the one before it. Participants in the system confirm each transaction before it is recorded in the ledger. A block is a single recorded transaction, and a chain formed by many blocks is unbreakable. Information entered into a blockchain becomes unalterable. This is because each block contains the last bit of the one before it, making it possible to integrate them into a blockchain. Transactions are registered and verified without the participation of the parties. Block-validating nodes are required to locate proof of work, which requires them to solve an equation whose difficulty is controlled by the algorithm. Blockchain technology makes sure that data is reliable and accurate while also ensuring the security of data transmission. Everyone with access to the system can see each transaction and the value it is paired with. The use of blockchain technology brings elements of decentralization, transparency, and trust to supply networks. Blockchain makes traceability easier by allowing users to monitor a specific product's movement throughout the entire supply chain. Every stakeholder can track the presence of a specific product, a batch, or an entire order. Every user throughout the supply chain is aware of every transaction taking place. Access to information about a specific product or an entire order is available to all users impartially. Additionally, blockchain makes it possible for users in the supply chain to build trust with one another. Most significantly, it avoids a trust gap developing between two partners in the supply chain. The usage of smart contracts is the cornerstone of every blockchain system. They make it possible for stakeholders to trade smoothly. Smart contracts have a wide range of applications, including buying a product, controlling multimodal shipping, and removing a product. Cryptocurrency tokens can be used to settle financial transactions. Tokens are more adaptable, secure, and quick when managing payment settlements than other systems like cash and credit. The information kept on the blockchain is unchangeable, meaning that once it has been created, it cannot be changed. Once it has been agreed upon by both parties, a transaction cannot be cancelled. Blockchain-enabled supply chains are auditable, in

contrast to conventional dairy supply networks, because each transaction made inside the blockchain network is recorded and kept on individual blocks in a secure manner using cryptographic hash functions. Decentralised in nature, blockchain-enabled supply networks eliminate the chance of a single point of failure. Decentralisation also reduces the possibility of data manipulation and the dissemination of false information to other stakeholders. The supply chain can operate at the highest levels of automation thanks to blockchain integration. The blockchain is used to automatically update product information, settle payments, remove products, add stakeholders, and perform all other operations. Blockchain-enabled supply chains don't need intermediaries, in contrast to conventional supply chains. Only legitimate parties engage in transactions, assuring the security of the products. No unapproved parties are allowed to carry out transactions or even add their goods to the supply chain.

II. RESEARCH METHODOLOGY

The authors' major emphasis is on preventative measures, which include getting rid of the warning indications of harmful circumstances in the chain that they initially observed. In this way, it stops negative circumstances from developing across the entire chain. The suggested method is decentralized and is centered on the sharing of information from each link's members that has been compiled in a digital ledger. Our review of the literature indicates that such a system is workable, and the authors' initial interest in the topic was the identification of false certificates.

III. SETUP

Using the Ethereum blockchain, a simulation of the proposed platform for vaccination certificate traceability is performed. The Solidity programming language is used to create smart contracts. The Ethereum test network is used to carry out every smart contract. Ether is sent from the buyer's wallet address to the seller's wallet address to represent payment settlements. The two software's utilized for creating the full blockchain-enabled supply chain platform are VS Code and Ganache.

IV. SYSTEM ARCHITECTURE

We go over the supply chain model's system architecture in this part. The User layer, Contract layer, Network layer, and Data layer are the four levels that make up the system architecture. These four layers are used throughout the supply chain for all operations.

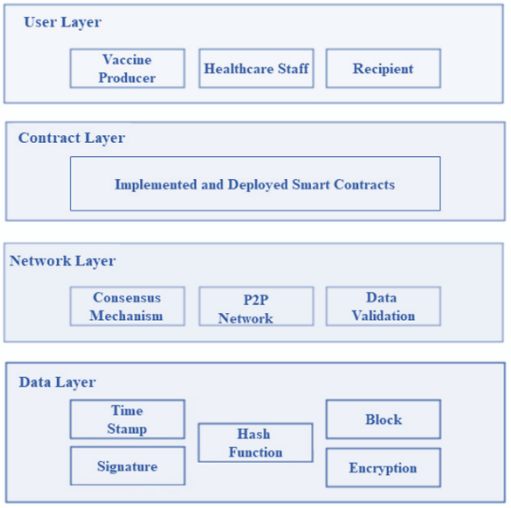

Fig. 2 Information exchange within the platform.

A. Data Layer

In this layer, several cryptographic mechanisms are employed to ensure the security and integrity of the data. These mechanisms include time stamps, digital signatures, hash functions, blocks, and encryption.

1. Time-stamps: Time-stamping is used to record the exact time when a particular event or data is entered into the blockchain. This ensures that the data is chronologically ordered, and provides an auditable trail of events. Time-stamping is typically achieved through the use of network time protocol (NTP) servers, which synchronize the time across all nodes in the network.
2. Digital signatures: Digital signatures are used to ensure the authenticity and integrity of the data. A digital signature is created by applying a mathematical function to the data, which generates a unique identifier known as a hash. This hash is then encrypted using the sender's private key, which can only be decrypted by the receiver's public key. This ensures that the data can be verified as coming from a particular sender and that it has not been tampered with.

3. Hash functions: Hash functions are used to generate unique identifiers for data stored on the blockchain. Hash functions take a message of any length and produce a fixed-length output, known as a hash. Even a small change in the message will result in a completely different hash value, making it impossible to modify the data without being detected.
4. Blocks: Blocks are used to store data on the blockchain in a tamper-evident and immutable manner. Each block contains a set of transactions or data, along with a unique identifier known as a hash. The hash of each block is based on the data in the block, as well as the hash of the previous block in the chain. This creates a chain of blocks, where each block is cryptographically linked to the previous block, making it impossible to modify any data without breaking the entire chain.
5. Encryption: Encryption is used to protect the confidentiality of the data. Encryption involves converting the data into a form that can only be read by those with the proper decryption key. This ensures that even if the data is intercepted or stolen, it cannot be read without the proper key.

Overall, these cryptographic mechanisms provide high security and integrity for the data stored in the data layer of a vaccination certificate supply chain using blockchain. By combining these mechanisms, the data can be stored, secured, and transmitted in a tamper-evident and confidential manner, ensuring that the data can be trusted and relied upon by all parties involved in the supply chain.

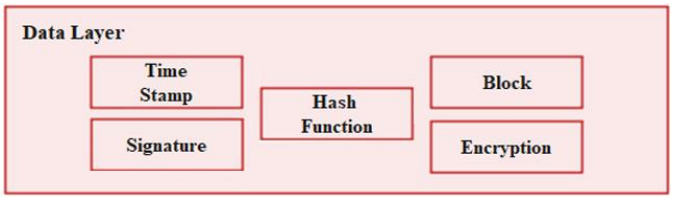

Fig. 3 Data Layer

B. Network Layer

In this layer several mechanisms are employed to ensure the security, integrity, and accuracy of the data. These mechanisms include consensus mechanisms, peer-to-peer (P2P) networks, and data validation.

1. Consensus Mechanisms: Consensus mechanisms are used to ensure that all nodes in the network agree on the current state of the blockchain. Consensus is achieved by having all nodes in the network validate transactions or data before they are added to the blockchain. There are various consensus mechanisms, such as Proof of Work (PoW), and Proof of Stake (PoS), that can be used to achieve consensus.
2. Peer-to-Peer (P2P) Networks: In a P2P network, all nodes in the network are connected directly to each other, without the need for a central server. This allows for more efficient and decentralized communication between nodes. P2P networks also provide a high level of fault tolerance, as there is no single point of failure in the network.
3. Data Validation: Data validation is used to ensure that the data being added to the blockchain is accurate and valid. This is typically achieved by having multiple nodes in the network validate each transaction or data point before it is added to the blockchain. If a transaction is found to be invalid or fraudulent, it will not be added to the blockchain. This ensures that the blockchain contains only valid and accurate data.

By using consensus mechanisms to ensure agreement on the current state of the blockchain, P2P networks to facilitate efficient and decentralized communication between nodes, and data validation to ensure the accuracy and validity of the data, the network layer ensures that the blockchain can be trusted and relied upon by all parties involved in the supply chain.

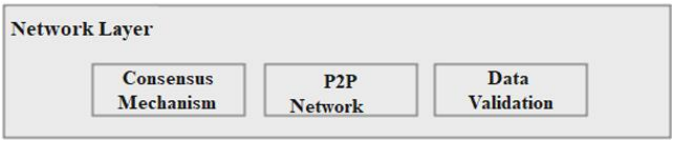

Fig. 3 Network Layer

C. Contract Layer

The contract layer is a critical component that enables the creation and execution of smart contracts. Smart contracts are self-executing programs that are stored on the blockchain and automatically execute when certain conditions are met. In a vaccination certificate supply chain, smart contracts can be used to automate the verification and validation of vaccination records, thereby streamlining the supply chain process and reducing the potential for errors or fraud. The contract layer

provides a platform for creating and deploying smart contracts on the blockchain. Smart contracts are typically written in programming languages such as Solidity and are deployed on the blockchain as autonomous software agents. Once deployed, smart contracts can be triggered by external events or by other smart contracts and can execute pre-determined actions based on the conditions that have been programmed into them.

Smart contracts in a vaccination certificate supply chain can be used to automate a variety of tasks, such as verifying the authenticity of vaccination records, tracking the distribution and administration of vaccines, and ensuring that all parties in the supply chain comply with relevant regulations and guidelines.

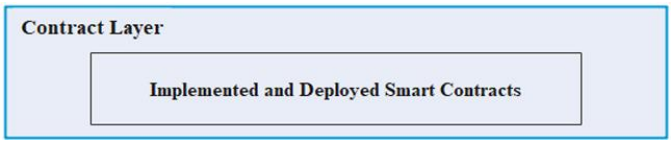

Fig. 4 Blockchain Layer

D. User layer

This layer refers to the interface that users interact with to access and manage their vaccination records and other relevant information. This layer provides a user-friendly interface that enables users to view, verify, and share their vaccination records securely and efficiently.

1. Authentication: Users can authenticate themselves using secure login credentials, such as a username and password, or biometric authentication, such as facial recognition or fingerprint scanning.
2. Viewing vaccination records: Users can view their vaccination records, which are stored on the blockchain, and verify that the records are accurate and up-to-date.
3. Sharing vaccination records: Users can share their vaccination records with third parties, such as employers, healthcare providers, or travel authorities, by providing them with access to their records via a secure link or QR code.
4. Tracking vaccination history: Users can track their vaccination history and receive notifications when they are due for a new vaccination.
5. Managing consent: Users can manage their consent settings, specifying which parties are allowed to access their vaccination records and for what purposes.

The user layer plays a critical role in ensuring the widespread adoption and success of a blockchain-based vaccination certificate supply chain. By providing users with a user-friendly interface that enables them to securely access and manage their vaccination records, the user layer can help to build trust and confidence in the system, while also facilitating the efficient and effective management of the supply chain.

Fig. 5 User Layer

V. USE CASE

With many businesses and organizations returning to in-person operations, ensuring the health and safety of employees and customers is a top priority. A blockchain-based vaccination certificate supply chain can help organizations manage the vaccination status of their employees and visitors, and ensure compliance with safety regulations.

1. Employees and visitors receive a vaccine, and their vaccination data is recorded in a blockchain-based system. The system could include information such as the type of vaccine received, the date of vaccination, and the location of the vaccination center.
2. The individual's vaccination data is encrypted and stored on the blockchain, ensuring that it cannot be tampered with or accessed by unauthorized parties.
3. When employees and visitors enter the workplace, they present their vaccination certificate to a designated safety officer or manager. The safety officer can use a blockchain-based system to verify the authenticity of the certificate and confirm that the individual has received a valid vaccine.
4. The blockchain-based system can also provide real-time updates on the vaccination status of employees and visitors, allowing organizations to quickly respond to any potential outbreaks or safety concerns.

Overall, a blockchain-based vaccination certificate supply chain can help organizations ensure workplace safety and compliance with safety regulations by providing a secure and efficient system for managing and verifying vaccination certificates.

VI. CHALLENGES

One of the major challenges we face is the authenticity and ethical behavior of the system participants. In the case where storage unit malfunction is not addressed, or electricity disruption is not fixed, might lead to ineffective vials of the Vaccine. In cases where IoT devices cannot be used, we need to be at the mercy of the actor's ethical behavior.

One more major challenge is keeping the Smart Contracts immutable and their presence in a device might lead to any party altering it and making it a private blockchain instead of a Public blockchain. All the smart contracts must follow permission login and all transactions must be declared to all participants making it a truly peer-to-peer network with highly immutable smart contracts. Another challenge is our need for participants in the supply chain to set up the environment and their commercial agreements.

The final concern is from energy conservationists about the Carbon emissions of Blockchain Mining. Cambridge's Center for Alternative Finances estimates that bitcoin's annualized electricity consumption hovers just above 115 terawatt-hours (TWh) while Digiconomist's closely tracked index puts it closer to 80 Twh. A single Ethereum transaction absorbs more energy than an average U.S. transaction. uses in a day. There are various ways in which this matter can be solved for example using Proof of Stake(PoS) instead of the Proof of Work(PoW) consensus algorithm. This reduces energy consumption and hence the lowered amount of carbon footprint. We have to make sure we keep a balance of energy consumption as well as data in the blockchain safe and secure.

VII. CONCLUSION

Blockchain-based vaccination certificate supply chain has the potential to transform the way we manage and verify vaccination certificates, making it more secure, transparent, and efficient. By leveraging the immutable and decentralized nature of blockchain technology, a vaccination certificate supply chain can provide a secure and reliable system for managing vaccination data and ensuring compliance with safety regulations. However, there are also several challenges that need to be addressed, including privacy concerns, interoperability issues, and adoption and compliance. Addressing these challenges will be crucial to ensuring the effectiveness and success of blockchain-based vaccination certificate supply chains. Despite the challenges, the potential benefits of a blockchain-based vaccination certificate supply chain are significant, and it represents an exciting opportunity to leverage technology to improve public health and safety.

REFERENCES

[1] Sohrabi, C., Alsafi, Z., O'Neill, N., Khan, M., Kerwan, A., Al-Jabir, A., ... & Agha, R. (2020).World Health Organization declares global emergency: A review of the 2019 novel coronavirus(COVID-19). International journal of surgery, 76, 71-76.

[2] Kartoglu, U.H.; Moore, K.L.; Lloyd, J.S. Logistical challenges for potential SARS-CoV-2 vaccine and a call to research institutions, developers and manufacturers. Vaccine 2020, 38, 5393.

[3] Rahi, M.; Sharma, A. Mass vaccination against COVID-19 may require replays of the polio vaccination drives. EClinicalMedicine 2020, 25, 100501.

[4] Chen, S.I.; Norman, B.A.; Rajgopal, J.; Assi, T.M.; Lee, B.Y.; Brown, S.T. A planning model for the WHO-EPI vaccine distribution network in developing countries. IIE Trans. 2014, 46, 853–865.

[5] Holm, M.R.; Poland, G.A. Critical aspects of packaging, storage, preparation, and administration of mRNA and adenovirus vectored COVID-19 vaccines for optimal efficacy. Vaccine 2021, 39, 457.

[6] Yang, Y.; Bidkhori, H.; Rajgopal, J. Optimizing vaccine distribution networks in low and middle-income countries. Omega 2021, 99, 102197.

[7] Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J.Am. Med. Inform. Assoc. 2017, 24, 1211–1220.

[8] Fusco, A.; Dicuonzo, G.; Dell'Atti, V.; Tatullo, M. Blockchain in healthcare: Insights on COVID-19. Int. J. Environ. Res. Public Health 2020, 17, 7167.

[9] Manoj, M.; Srivastava, G.; Somayaji, S.R.K.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. An Incentive-Based Approach for COVID-19 planning using Blockchain Technology. In 2020 IEEE Globecom Workshops (GC Wkshps); IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.

[10] Yong, B.; Shen, J.; Liu, X.; Li, F.; Chen, H.; Zhou, Q. An intelligent blockchain-based system for safe vaccine supply and supervision. Int. J. Inf. Manag. 2020, 52, 102024.