



Covid-19 Verification and Supply Chain Management.

Abhijith L Kotian

Assistant Professor,
Computer Science and
Engineering,
Alva's Institute of Science and
Technology.
Mijar, India.

Prinson D'Souza

Computer Science and
Engineering,
Alva's Institute of Science and
Technology.
Mijar, India.

Swasthik Suvarna

Computer Science and
Engineering,
Alva's Institute of Science and
Technology.
Mijar, India.

Upasana Shenoy R

U
Computer Science and
Engineering,
Alva's Institute of Science and
Technology.
Mijar, India.

Vaibhav S Soorinje

Computer Science and
Engineering,
Alva's Institute of Science and
Technology.
Mijar, India.

Date of Submission: 18-04-2023

Date of Acceptance: 03-05-2023

Abstract—The worldwide economy was highly affected by the Covid-19 pandemic. Through the rigorous research and the scientific developments, an effective vaccine for Covid-19 was discovered. The government made it compulsory to produce the vaccination certificates for the individuals to access various facilities including transport, restaurants, cinema theaters or business in order to prevent the spreading of virus. This led to the forging of the certificates by the people. The paper introduces a blockchain solution that focuses on the registration of vaccinating authorities and issuance of vaccine certificates that can be quickly verified by anyone. The solution is application-based and aims to streamline the process of verifying vaccine certificates. Furthermore, the paper highlights the importance of analyzing the data retrieved from the blockchain, as this data will be accessed by numerous authorities.

Keywords—*Block Chain, Digital Signature, Verification.*

I. INTRODUCTION

The lifestyle of individuals has been transformed due to advancements in information technology, widespread availability of the internet, and the widespread use of mobile devices. People are starting to take notice of blockchain, the underlying technology. Blockchain boasts a decentralized and

tamper-proof database that has the potential for various applications.

The application of blockchain technology extends beyond storing information, conducting transactions, and building trust in a unique way. Blockchain is viewed as a ground-breaking technology for cryptography and cybersecurity, and it has diverse applications, such as healthcare, cryptocurrency, smart contracts, Internet of Things, smart grids, governance, and supply chain management. The present research work seeks to provide a comprehensive analysis of blockchain security, privacy, and trust. It also examines the challenges associated with implementing blockchain technology in the field of Healthcare mainly focusing on valid Covid-19 certificate generation. Finally, the research proposes a blockchain-based framework for secure and dependable management of valid Covid-19 vaccine records.

The Covid-19 vaccine certificate is a guaranteed proof issued by the Government that a person has received COVID-19 vaccine. Currently, there are different types of certificates being issued, i.e., for the First Dose, Second Dose and a consolidated certificate for all doses, whether you've received "Covishield" or "Covaxin".

It's no surprise that there is been a lot of discussion about Covid-19 certificates being able to prove that one has actually received the vaccination. Here, we deal with 3 scenarios:



- Many people's vaccine certificates were rejected due to fraudulent claims.
- The WHO suspended the approval process for a specific vaccine due to inspection issues at the manufacturing plants.
- A large people with valid and original COVID-19 certificates were denied entry in many countries because the country at ports of entry did not receive any database from the original country to access and verify if the people are actually vaccinated or not.

The process of distinguishing between forged and authentic certificates is time-consuming and requires significant concentration. However, the introduction of blockchain technology has solved this problem. Blockchain technology is reliable because data cannot be changed under realistic conditions, and tampering is quickly detected. Multiple parties validate data or nodes in a blockchain system, resulting in a reliable and authenticated system at all times. The proposed system not only validates certificates but also generates them, saving time and making the process more efficient. As everything is automated, the validation process takes only a few seconds. Storing certificates digitally ensures that the authorities do not have to worry about losing or damaging them during the validation process. The proposed system is a practical and effective solution that eliminates the drawbacks of the current system.

II. EXISTING SYSTEM

The certificates are currently stored in a centralized manner and verified manually, which is a time-consuming process. Unfortunately, there is no guarantee for the safety of the certificates issued. Additionally, the data stored on these certificates may be vulnerable to unauthorized modification, deletion, or alteration. This presents a serious risk of certificate forgery and duplication. It is common for people to produce their certificates to the authorities, but there is no secure method of verifying their authenticity.

The main disadvantages of the existing system are:

- The existing system uses web 2.0 which leads to various security threats.
- Information overload - Too much information is daily posted by many people with different thoughts. This creates confusion for the readers and the quality of the content is not reliable.
- Freedom to post views and comments provides good opportunities for competitors and rivals to post negative comments about other companies.
- Too many fake ids and spammers. Forgeries and hackers commit crimes.

III. LITERATURE REVIEW

A. *Block Chain based proposals for Covid-19 certification*

In their proposal, the various authors suggest using verifiable credentials to provide proof of vaccination or immunity test results. The process involves the issuer, who is a representative of the National Health Service in this case, verifying the identity of the holder and then issuing a digitally signed Verifiable Credential. This credential is stored on a Consortium blockchain that operates on a Proof of Authority consensus mechanism. With this credential, the holder can present a valid certificate to the verifier, such as an airport or school authority. The system utilizes the open-Ethereum platform and employs zero-knowledge proofs to minimize the amount of information shared with verifiers.

Several researchers have proposed blockchain-based solutions to improve the underlying technologies of digital certificates, including public key infrastructure (PKI) and certificate authority (CA) systems. These proposals typically focus on technical improvements, with the goal of enhancing performance from various angles. For example, Madala et al have suggested a blockchain-based system [1] to address security issues with current CA systems, preventing a CA from issuing certificates for a domain without the domain owner's consent. Wang et al, have developed an append-only public blockchain-based storage scheme [2] to enable recording of certificates and revocation status for better transparency. Other researchers have focused on improving the certificate revocation process with blockchain technology, with a focus on efficiency and security.

B. *Ethereum*

Ethereum is a decentralized platform that supports various derivative applications and features Turing completeness. Most smart contracts and decentralized autonomous organizations are created using Ethereum. Ethereum can be considered a global computing system, similar to how Bitcoin blockchains are a global payment network. Like Android (developed by Google), Ethereum is an open-source platform that provides an infrastructure for developers to create applications. Both Ethereum and developers maintain the infrastructure, and its major characteristics include being incorruptible, secure, and permanent (even if an individual computer or server crashes).



The Ethereum Virtual Machine (EVM) is a programmable blockchain that allows developers to run any programs they wish, unlike Bitcoin, which provides a fixed set of commands. Developers use a high-level language called Solidity to instruct the EVM to execute applications. Solidity is like JavaScript and is used for implementing smart contracts. Once a Solidity-programmed smart contract is completed, it needs to be compiled using a compiler called "solc" to transform the Solidity code into contract bytecode, which is then interpreted by the EVM. The compiled instructions are then deployed in an Ethereum blockchain, completing the entire process.

IV. PROBLEM AREA

The strict enforcement of vaccine certificate requirements for accessing facilities has compelled reluctant vaccine recipients to resort to buying counterfeit certificates, bypassing entry restrictions. This has created an opportunity for unscrupulous individuals, including those from the medical profession, to produce fraudulent documents. Despite the vaccine information being stored in a centralized database, some insiders can manipulate the database to create and sell fake certificates, which may appear to be genuine.

Recent reports suggest that the problem of counterfeit certificates is on the rise. For instance, Kazakhstan has reported 65 cases of criminal activities involving fake vaccination certificates and PCR tests. A private tourism firm was also implicated in providing fraudulent travel vaccine certificates. Typically, fake Covid-19 vaccination certificates are peddled to people who are not fully vaccinated but are eager to travel. The investigations have revealed that medical personnel have been involved in producing fake certificates. Additionally, counterfeit certificates have been circulated globally, including in countries such as India, Russia, Ukraine, and the USA. In yet another report, Italian law enforcement agencies busted several online scams that offered fake EU COVID travel certificates and even vaccines.

The demand for counterfeit vaccine certificates is increasing not only for travel but also to gain entry to public places such as restaurants and cinemas. Russia has reported the circulation of phony vaccine certificates in various regions after the government mandated vaccinations for service sectors and access to public areas. In an effort to combat the proliferation of physical certificates, the Moscow government has introduced digital certificates issued by hospitals through government

portals. Nevertheless, there have been instances where individuals can purchase QR certificates that grant them the same benefits as fully vaccinated individuals, despite such initiatives.

V. PROPOSED METHODOLOGY

A. Modules

1) *Blockchain*: The concept of Blockchain can be comprehended as an unchangeable database that serves as the groundwork for the entire project. It creates a reliable space where all the executed actions are visible and impossible to alter.

2) *Ethereum*: It is a decentralized open-source Blockchain platform that supports smart contract functionality. It serves as an exemplary model of the potential of Blockchain technology. In addition, Ethereum has its own cryptocurrency system, which is widely utilized and considered the second most valuable cryptocurrency after Bitcoin.

3) *Solidity*: Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various Blockchain platforms, most notably, Ethereum. It is closely similar to Typescript but with more specific data types.

4) *Metamask*: Metamask is a browser extension that enables access to distributed applications or "Dapps" on the Ethereum network. By injecting the Ethereum web3 API into the javascript context of every website, the extension allows Dapps to retrieve information from the blockchain.

5) *Ethash*: Ethash is the designated proof-of-work function in Ethereum's blockchain network. It belongs to the Keccak hash function family, which also includes the SHA-3 hash functions. Although Ethash is similar to SHA-3 hash functions, it is not identical to them and should not be used interchangeably.

6) *Node JS*: Node JS is a technology used for developing backend systems, handling frontend pages and assets, and managing user authentication through JWT (Json Web Token). It relies on web3 as a dependency, which enables the execution of Solidity code on the frontend.

7) *React JS*: ReactJS is a popular JavaScript library used for building user interfaces (UIs) for web applications. Its main purpose is to provide a way to efficiently update and render components in response to user interactions or changes in application data, without having to reload the entire page.

B. Project Description

We have proposed a system to address the loopholes in the current methodologies. This system will automatically generate and validate certificates with



authenticated, reliable, and unchangeable data using HTML, CSS, React JS for the front end. Blockchain, Solidity for the back end and Node JS, Java script for connectivity and management of our system. The upcoming sections will provide a detailed description of the entire process.

1) *System Actors*

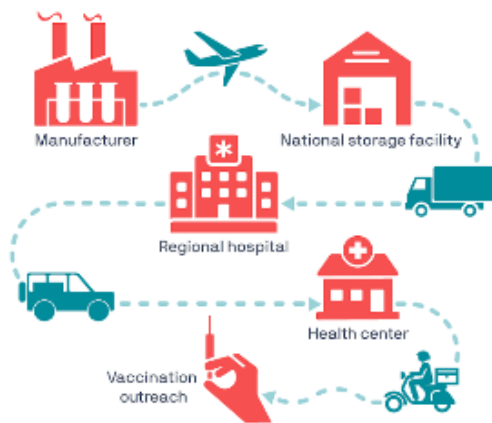


Fig 1. Vaccine Cold Chain

Fig 1. defines the various system actors involved.

- *Manufacturer*: process raw materials into vaccines.
- *Distributor*: transports vaccines between locations.
- *Inspector*: performs quality checks on vaccines and performs quality checks on manufacturing plants.
- *Storage Facility*: store vaccines in cold temperatures.
- *Immunizer*: it includes the doctors, nurses who vaccinates people and provides vaccine certificates.
- *Traveler*: refers to the patient who receives vaccine, vaccine certificate and presents vaccine certificate at the border of the destination country.
- *Border Agent*: verifies the vaccine certificates.

2) *System Design Flow*

- Inspector issues certificate for batch to Manufacturer <batch status updated to MANUFACTURED>
- Manufacturer presents certificate to Distributor and verifies each certificate <batch status updated to DELIVERING_INTERNATIONAL>

- Distributor presents updated certificate to Storage Facility, who verifies each batch certificate <batch status updated to STORED>
- Storage Facility presents certificates to Distributor, who verifies each certificate <batch status updated to DELIVERING_LOCAL>
- Distributor presents updated certificate to Immunizer and he verifies certificates <batch status updated to DELIVERED>
- Immunizer vaccinates Traveler and issues vaccine passport <certificate issued with status VACCINATED>
- Traveler presents vaccine passport to Border Agent Border Agent verifies vaccine passport.

C. *Methodology used to implement the objectives and provide solution.*

TABLE 1. Methodology Implemented

<i>Problem faced</i>	<i>Affected actors</i>	<i>Methodology implemented to provide the solution</i>
Vaccine certificate can be falsified.	Border Agent	Cryptographically verify using on-chain data.
Key facilities may not meet the quality standards	All	Publish inspection results to blockchain and verify presented inspected results.
Vaccine certificate may not be recognized by the designation countries	Distributor, Traveler, Immunizer	Verify the digital signatures in presented certificates.



D. User Classification

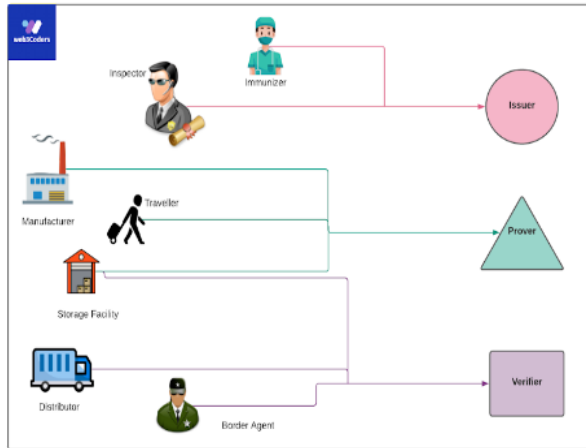


Fig 2. User Classification

- As an Issuer, I can issue a signature representing a digital certificate for a manufacturer’s plant or storage facility.
- As a Prover, I can present a certificate/signature issued to me.
- As a Verifier, I can validate the signature on the blockchain for a vaccine.

E. High level Architecture of the System

1) 3-Tiered Architecture:

A 3-tiered architecture is a software architecture pattern that divides an application into three interconnected layers or tiers: presentation, application logic, and data storage.

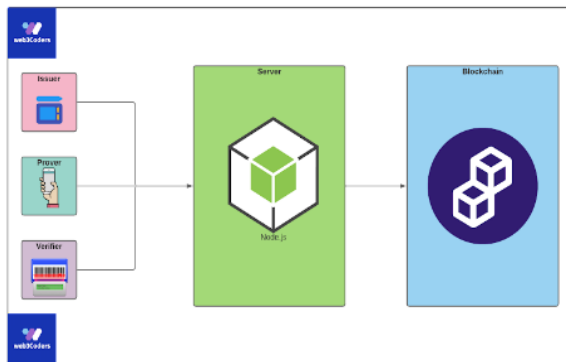


Fig 3. 3-Tiered Architecture

2) 2-Tiered “dApp” Architecture:

2-tiered "dApp" (decentralized application) architecture is a software architecture pattern that consists of two main layers: the frontend or user interface layer and the backend or blockchain layer.

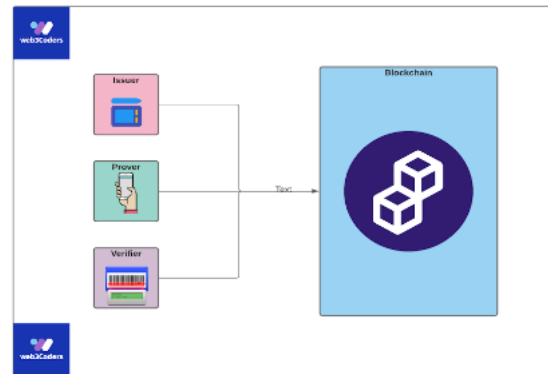


Fig 4. 2-Tiered “dApp” Architecture

F. Conclusion and Future Work

The Blockchain system is a revolutionary technology that allows individuals to record transactions on a public, decentralized ledger without the intervention of a central authority. The application of this technology has the potential to benefit the education sector in numerous ways. With its ability to securely store, exchange, and share sensitive data, Blockchain can greatly enhance various systems. The technology can facilitate faster, simpler, and more efficient operations, while also bridging gaps in areas such as credentialing, copyright protection, and rapid connectivity. As a result, traditional systems in these areas are expected to significantly benefit from Blockchain in the near future.

This project with the implementation of the Block Chain and Solidity will be able to verify and validate the Covid-19 certificates at various levels and thus helps us in achieving a system in which all the process is transparent and unchangeable. This system reduces the manual work needed for the verification of the certificates. The Authorities are also at comparatively low risk of invalid certificate production. By using an additional hashing algorithm, we are decreasing the percentage of data being tampered with hence prevent the forging of vaccine certificates. However, there are few further research and work that is necessary to overcome problems that involves dishonest doctors and immunizers, lack of loyal raw material suppliers and manufacturers, distribution to areas without internet access, IoT, etc.

VI. RESULT AND DISCUSSION

Using blockchain technology, a decentralized application has been created on the Ethereum platform to track the availability of administered vaccine certificates and verify them. The application has two interfaces - the Ministry interface for registering hospitals and the Hospital



interface for administering vaccines and recording information on the blockchain. The verification process is designed for real-world application, and the application is currently deployed on a local machine.

REFERENCES

- [1]. Jieying Chen, Xiaofeng Ma, Mingxiao Du and Zhuping Wang, "A blockchain application for medical information sharing", in Proceedings of the 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), 2018.
- [2]. Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, 2017.
- [3]. Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, "BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability", IEEE International Conference on Blockchain, 2019R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
- [4]. Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.
- [5]. Abhijith L Kotian, Deepa K, "Detection and Classification of Skin Diseases by Image Analysis Using MATLAB", International Journal of Emerging Research in Management & Technology, ISSN: 2278-9359 (Volume-6, Issue-5),pp.779-784, 2017