Design of a Digital Vaccination Certificate System Leveraging Consortium Blockchains

Shu-Fen Tu, Ching-Sheng Hsu, and Yu-Min Chiang

Abstract—**During the initial outbreak of Covid-19, many countries invested in vaccine research, development, and distribution. Some countries require immigrants to present a vaccination certificate and comply with the country's inspection regulations. Various international methods for inspecting vaccination certificates were proposed. Still, they often had drawbacks such as inconsistent inspection standards, inefficiency, and an inability to verify the authenticity of the inspected individual. Although life has essentially returned to normal, and most countries no longer mandate vaccination certificates for immigrants, such certificates will likely be required again if new influenza viruses emerge. Therefore, addressing the issues related to vaccination certification and developing better inspection methods is crucial. In our research, we have introduced a digital vaccination certification system designed for use among multiple trusted countries, which combines consortium blockchains, digital signatures, QR codes, and facial recognition. Our proposed solution addresses the shortcomings of current vaccine passports and vaccination certification systems, providing significant assistance in managing COVID-19 and potential future pandemics.**

Index Terms—**consortium blockchain, COVID-19, distributed ledger technology, vaccination certificate**

I. Introduction

BEFORE the COVID-19 outbreak, the World Health Organization had issued regulations for the International Certificate of Vaccination or Prophylaxis (ICVP) to prevent the spread of infectious diseases. ICVPs are currently issued and verified on paper. In the early days of the COVID-19 outbreak, the absence of vaccines and treatments led to continued disease spread and numerous infections and deaths. In December 2020, the first internationally recognized Covid-19 vaccine was launched [1]. Research by Syed et al. highlights the positive impact of the Covid-19 vaccine on public health [2]. As more internationally recognized vaccines become available, vaccine coverage gradually increases, and the international demand for vaccine-related passports and vaccination certification systems continues to grow.

Many countries and organizations have launched vaccine passports, certifications, and inspection methods in response to COVID-19. Some countries issue paper-based vaccine passports, while others use digital formats. The different types also lead to variations in certification and inspection methods. For example, China and Israel have implemented vaccine passport systems [3], the European Union has launched an EU digital COVID-19 certificate [4], and the US VCI organization has launched a Smart Health Card (SHC) [5]. Additionally, data formats and approved vaccine lists vary from country to country, hindering the interoperability of vaccination certification systems. Furthermore, the current verification system relies on traditional database storage, which has the risk of a single point of failure and data tampering. Moreover, the current verification method cannot confirm the authenticity of the passport holder's identity, leading to the risk of data forgery and impersonation. These are the challenges faced by the current system.

In response to these challenges, academics have proposed blockchain-based solutions that promise to revolutionize the future of vaccination certification systems. Blockchain technology offers several key benefits, including enhanced security, transparency, and interoperability [6-8]. Hasan et al. proposed a digital medical passport and immunity certificate system based on the Ethereum blockchain 9], which enables more accurate and timely reporting of COVID-19 infection status. In addition, Marbouh et al. [10] have created a trustworthy tracking system based on the Ethereum blockchain and Oracle to help the public receive credible information, including the number of infections, deaths, and recoveries, when responding to the COVID-19 epidemic. These examples highlight the potential of blockchain technology to solve current challenges in vaccination certification systems.

Ethereum is a permissionless public blockchain that provides security against data tampering and single-point system failure. However, it has limitations such as transaction fees, performance, scalability, Transaction Per Second (TPS), and block capacity issues [11]. Another solution is to consider adopting Hyperledger Fabric. Hyperledger Fabric is a permissioned consortium blockchain platform that doesn't require transaction fees and is more efficient than public blockchains while maintaining resistance to tampering [12]. Given the need for trust and independence among countries involved in vaccine passport and certification systems, choosing a more suitable solution like the Hyperledger Fabric consortium blockchain is crucial.

This study aims to design a blockchain-based vaccination certification system that can be used and interoperable among multiple countries that trust each other. The system proposed in this study can verify the completeness and authenticity of relevant data on vaccination certificates and confirm the

Manuscript received October 6, 2024; revised April 9, 2025.

S. F. Tu is a professor at the Department of Information Management, Chinese Culture University, Taipei, 111396, Taiwan (e-mail: dsf3@ulive.pccu.edu.tw).

C. S. Hsu is a professor at the Department of Information Management, Ming Chuan University, Taoyuan, 333321, Taiwan. (corresponding author to provide e-mail: cshsu@mail.mcu.edu.tw).

Y. M. Chiang is a graduate student at the Department of Information Management, Ming Chuan University, Taoyuan, 333321, Taiwan. (e-mail: jack190919jiang@gmail.com).

authenticity of the identity of the person being inspected. Taken together, our research aims to achieve the following goals:

1) Hyperledger Fabric blockchain technology will be employed to establish a digital vaccination certification system suitable for use among multiple trusted countries.
2) Store vaccination certificates in digital format on a decentralized ledger, solving problems associated with potential damage, loss, theft, or counterfeit paper copies.
3) Establish a vaccination certificate issuance mechanism to ensure the legitimacy of the issuing unit.
4) Introduce standardized inspection procedures to enable inspectors to verify the authenticity of personal identities during the inspection process.

II. Literature Review

A. Vaccination Certificate

1) International Certificate of Vaccination or Prophylaxis (ICVP)

The International Certificate of Vaccination or Prophylaxis (ICVP) is a globally recognized vaccination certificate issued by health authorities in various countries in compliance with the World Health Organization's regulations. The ICVP, often called the Yellow Book, may be necessary for inbound and outbound travelers who have received certain vaccinations. It includes personal information and vaccination records and is essential to confirm a traveler's identity. Those who fail to show proof may be subject to compulsory quarantine, isolation, refusal of entry, or other measures by quarantine personnel. Any attempt to alter the certificate will render it invalid, so ensuring that all information matches the passport is essential. If the certificate is lost, it must be reissued at a hospital [13].

2) Digital COVID-19 Health Certificate

This document certifies an individual's novel coronavirus (COVID-19) vaccination status and test results. Different organizations issue certification documents in varying formats. Currently, Taiwan offers two digital vaccination certificate formats: EU DCC and SHC (refer to Table 1). The EU DCC format, initiated by the European Union, is also known as the EU Digital COVID Certificate. It is valid in all EU countries and is available in digital and paper formats. National screening centers or medical institutions issue these certificates. Individuals can store digital vaccination certificates on their mobile devices or request paper certificates, which include a QR code for verification. The QR code also contains a digital signature to prevent forgery. The document's authenticity is confirmed by scanning the QR code and verifying the digital signature. Each issuing institution (such as hospitals, screening centers, medical organizations, etc.) has its digital signature keys securely stored in databases across various countries. Regarding privacy and data security, the EU DCC only contains essential information, such as name, date of birth, date of issuance, and vaccination, screening, and recovery-related details. The SHC format was launched by the Vaccination Certificate Initiative (VCI) and was adopted by Taiwan on July 14, 2022. Compared to the EU DCC format, SHC provides more detailed information, including vaccine type, brand, name, and production lot number.

TABLE I
Comparison Between EU DCC and SHC

Format	EU DCC	SHC
Sponsored by	European Union (EU)	U.S. VCI
Type	Digital and Paper	Digital and Paper
QR code supported	Yes	No
Digital signature supported	Yes	No
Records	Name Birth Date of issue Proof of vaccination, screening, and recovery	Name Birth Date of issue Vaccine type, brand, vaccination, and batch number Proof of vaccination, screening, and recovery
Eligible Area	Countries in the EU	Japan, U.S., Canada, Australia, Taiwan

B. Related Works

The COVID-19 pandemic has posed significant challenges to information transparency. Some studies have suggested utilizing blockchain-based tracking systems for COVID-19 data collection [10] and vaccine distribution [14]-[15]. These systems leverage blockchain's traceability and immutability features to enhance transparency and trustworthiness within the supply chain. Additionally, the widespread use of paper vaccine certificates has raised concerns regarding their authenticity and convenience. Consequently, several studies have designed blockchain-based systems to manage digital vaccine certificates effectively. Jafari et al. [16] developed a digital vaccine certificate system using the Ethereum blockchain. In their system architecture, vaccine injection stations are responsible for recording patient information, issuing digital vaccine certificates, and maintaining a list of vaccine verification units. When a patient presents the digital vaccine certificate to a verification unit, the unit will compare the hash of the patient's data with the hash from the vaccine certificate to verify its legitimacy. Some researchers have suggested using the InterPlanetary File System (IPFS) [17] to enhance data storage security and Ethereum's smart contracts for automating vaccine certificate issuance, verification, and management. In the blockchain-based solution Hasan et al. proposed [9], the owner encrypts their COVID-19 medical records using a symmetric key. The hash of these encrypted records and the symmetric key encrypted with the owner's public key are stored on the blockchain platform. To ensure the confidentiality of the encryption key, Hasan developed a re-encryption proxy mechanism. Interested parties must first request a re-encrypted key from the re-encryption proxy before accessing the encrypted data on IPFS. With this re-encrypted key, they can retrieve the original symmetric key, which enables them to decrypt the medical record data. Additionally, they can re-hash the medical records and compare the resulting hash with the one stored on the blockchain to verify the authenticity and immutability of the data. According to the design proposed by Hasan et al., it appears impossible to retrieve the original symmetric key using the re-encrypted key. This is because the symmetric

key stored on the blockchain is encrypted with the owner's public key, which can only be decrypted with the owner's private key. Furthermore, even if there was a way to obtain the original symmetric key using the re-encrypted key, anyone possessing the original symmetric key could bypass this mechanism and access the encrypted data on IPFS without any restrictions. Therefore, maintaining confidentiality with this mechanism seems to be problematic. Alreshidi's system [18] records an individual's test report on the Ethereum blockchain to ensure authenticity and immutability. The Digital Passport of Health (DPoH) certificate issued to the individual is stored on IPFS, and a unique hash that serves as a reference point for the passport is recorded on the blockchain alongside the user's identity number. Anyone with the user's identity number can request a copy of the DPoH certificate. Additionally, advanced encryption mechanisms are employed to ensure data security. Alreshidi asserts that connecting identities in an encrypted manner helps maintain data integrity. Sharma and Rohilla [19] stored users' vaccination records off-chain using IPFS, while the hashes of these records were saved on the Ethereum blockchain. To ensure data integrity, the data retrieved from IPFS was verified against the corresponding hash. They emphasized that their system utilizes the Proof of Authority (PoA) consensus mechanism, which is more cost-effective than the Proof of Work (PoW) consensus mechanism. Similarly, Trong et al. [20] proposed a vaccine certificate management system combining blockchain technology and IPFS. Unlike other related studies, their system is specifically designed for children, meaning the initial electronic vaccine logbooks must be created by their parents rather than by the kids. After this, the vaccine center will update and maintain these logbooks. The digital vaccine certificate issued by the vaccine center will be linked to the child's vaccine logbook. A notable feature of Trong et al.'s system is that the vaccine logbook is encapsulated in a non-fungible token (NFT) to ensure the data's confidentiality and integrity. The NFT was recorded simultaneously on the IPFS and the Ethereum blockchain platforms.

The digital vaccine certificate management systems mentioned above primarily emphasize data authenticity and immutability. However, a comprehensive digital vaccine certificate system should also address two additional factors: the authenticity of the certificate's source and its relevance to the individual. This means the system must be able to verify the legitimacy of the certificate issuer and confirm that the person presenting the certificate is indeed the rightful holder rather than an impersonator. In addition, the system should offer an easy way to verify certificates for efficient border checks. Furthermore, all these blockchain-based vaccine management systems are built on the Ethereum platform. Ethereum's public chain system has its limitations. Firstly, there are several issues with Ethereum's data uploading. Transactions on Ethereum require payment of handling fees. While Hasan et al. have shown in their research that the cost of their designed system is minimal, Marbouh et al. mentioned that transaction fees vary based on timing, days, and the number and type of characters. Additionally, Ethereum's performance and scalability are potential concerns. Ethereum's transactions per second (TPS) are only about 10-15 [21]. The limited capacity of each Ethereum block causes miners to prioritize transactions with higher fees, which can lead to delays for small transactions. One significant problem is that while the vaccination certificate on the blockchain may be secure and tamper-resistant, it does not guarantee a connection to personal identity.

C. Security Requirements

The research proposes a system to control global infectious diseases by establishing a mechanism for issuing and verifying vaccination certificates. The issuing units are medical institutions in various countries, and the users are vaccinated. In their research on the electronic ticket system proposed by Hsu et al., they mentioned several security requirements [22]:

1) Authenticity: It should be possible to verify the authenticity of the certificate issuer.
2) Integrity: Any alterations to vaccination certificates should be detectable.
3) Non-replicability: A vaccination certificate can only have one valid holder.
4) Non-repudiation: The relevant country or organization cannot deny issuing and verifying the vaccination certificate.
5) Identity authenticity: The examiner should be able to verify that the person presenting the vaccination certificate is the owner.

The research by Hsu et al. also involves adding relevant organizations and individuals who have electronic tickets to the Hyperledger Fabric blockchain platform to ensure the credibility of electronic tickets. It is believed that the proposed digital vaccination certificate system in this study can be used internationally. The vaccination certificate system should also consider the above security requirements.

D. Hyperledger Fabric

Hyperledger Fabric is an open-source blockchain platform tailored for enterprise use. Supported by the Linux Foundation, it allows enterprises to deploy and operate permissioned blockchains [12]. Its highly modular and adjustable architecture allows for diverse applications, including in healthcare [23]. Systems utilized in enterprises or across multiple organizations must consider numerous conditions to ensure controllable risks. For instance, crucial factors include participant verification, permissioned networks, high transaction throughput, low transaction delay, transaction record privacy and confidentiality, and system stability. In a permissionless blockchain, members are anonymous and untrustworthy, and significant updates or hard forks can occur. Additionally, each transaction requires a handling fee with an unpredictable amount, leading to heavy transaction traffic and several other issues. These uncontrollable risks make permissionless blockchains unsuitable for enterprises. Moreover, ensuring different levels of data privacy is difficult in permissionless blockchains, typically requiring other mechanisms. Therefore, permissioned blockchains are more suitable for application scenarios involving enterprises or multiple organizations. The vaccine passport and certification systems related to COVID-19 comprise numerous trusting and independent countries, so the Hyperledger Fabric consortium

blockchain is believed to be better positioned to assist.

III. The Proposed System

This section will offer a comprehensive overview of the key participants involved in our system, the system operation process, and a thorough description of the system architecture design. Also, to ensure clear understanding, we will begin by explaining the symbols used in this section.

- X: a nation
- Y: a nation
- B: blockchain
- u: a user
- *DB/FS*: database or file system
- pk(X): EC public key of X
- sk(X): EC private key of X
- pk(u): EC public key of u
- sk(u): EC private key of u
- vc(u): the vaccination certificate of user u
- h(vc(u)): the SHA256 hash value for the vaccination certificate of user u
- face(u): the facial features of user u
- req(vc(u)): the request of a vaccination certificate of user u
- ds(vc(u), sk(X)): the digital signature of vc(u) signed by X using ECDSA with SHA256
- verify(vc(u), ds(vc(u), sk(X)), pk(X)): verification of the digital signature

A. The System Process

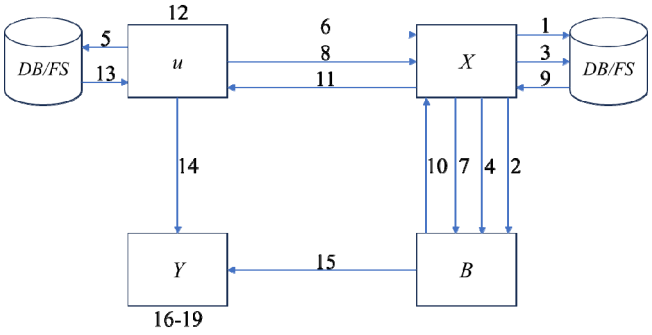


Fig. 1. System flowchart

Figure 1 shows the system flow designed in this study. The rectangular diagram in the figure represents the process, the variable name in it represents the entity that performs the processing, the numbers next to it represent the execution sequence and processing method, and the arrow segments represent data flow, the numbers next to it represent the execution sequence and data content. The detailed description of the system flow chart of this study is as follows.

1) pk(X), sk(X)
2) pk(X)
3) vc(u)
4) h(vc(u))
5) pk(u), sk(u)
6) pk(u), face(u)
7) pk(u), face(u)
8) req(vc(u))
9) vc(u), sk(X)
10) pk(X)
11) vc(u), pk(X), ds(vc(u), sk(X))
12) verify(vc(u), ds(vc(u), sk(X)), pk(X))
13) sk(u)
14) vc(u), ds(vc(u), sk(X)), ds(vc(u), sk(u))
15) pk(X), pk(u), face(u), h(vc(u))
16) verify(vc(u), ds(vc(u), sk(X)), pk(X))
17) verify(vc(u), ds(vc(u), sk(u)), pk(u))
18) compare the recomputed h(vc(u)) with that from blockchain
19) face verification

B. The System Architecture

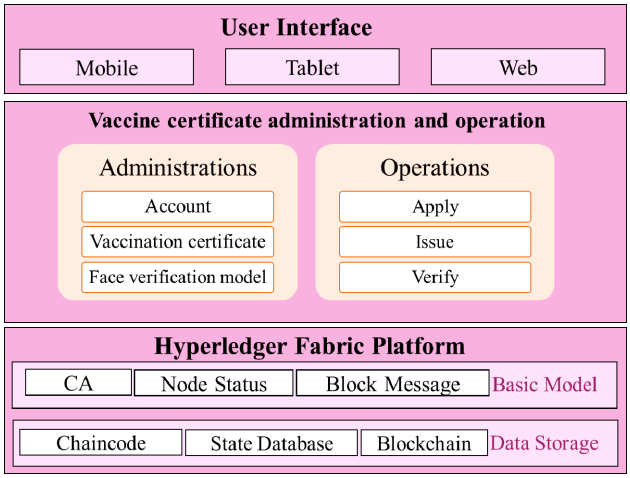


Fig. 2. System architecture

Figure 2 represents the architecture of the system module as designed in this research. The architecture comprises several layers: data storage, a foundational model, a vaccination certificate administration and operation system, and a user interface.

Data Storage

The Hyperledger Fabric consortium blockchain platform is designed to securely store data and exploit the blockchain's tamper-resistant properties. It enables the implementation of smart contracts to manage vaccination certificate data effectively and provides access to relevant information through the status database.

Basic Model

The foundational framework is established upon Hyperledger Fabric and encompasses integral functions such as CA management, node status oversight, and block message surveillance. This setup offers a robust infrastructure for deploying and managing blockchain networks. By carefully orchestrating these features, organizations are empowered to maintain high security and

operational efficiency. This foundation supports the development of applications that can leverage blockchain's potential for fostering transparency, accountability, and streamlined processes in various industries.

Vaccination Certificate Administration and Operation System

Implementing blockchain technology in developing a vaccination certificate system allows medical institutions to efficiently manage accounts related to vaccination certificates and their associated verification functions. This sophisticated system grants individuals the ability to secure their vaccination certificates and facilitates the process of identity verification through facial recognition technology.

User Interface

The system presented in this study is designed to provide distinct user interfaces tailored to the specific needs of different user groups. Medical institutions engage with the system through a web browser interface, while general individual users utilize the system via mobile phones or tablets, thereby ensuring widespread accessibility and user convenience.

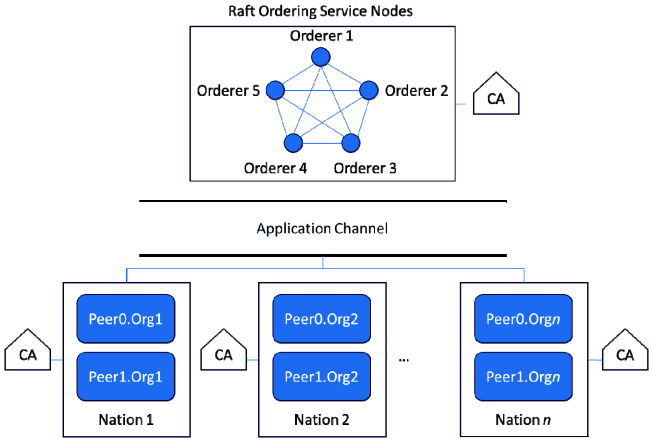


Fig. 3. Deployment of the consortium blockchain network for the vaccination certificate system

The consortium blockchain network vaccination certificate system deployment involves the Raft ordering service cluster and an international alliance comprising various countries, as illustrated in Figure 3. The participants in the blockchain network consist of four types of service nodes: ordering node (orderer), certificate node (CA), endorsement node (endorser), and commitment node (committer). The ordering node is tasked with ordering transactions, packaging blocks, and implementing crash fault tolerance (CFT) functions. The number of nodes of the Raft ordering service must be odd numbers such as 3, 5, 7, etc. Theoretically, the ordering service can operate normally when more than half of the sorting nodes are available. The CA is responsible for issuing, managing, and revoking digital identities and public and private keys. The endorsement node oversees smart contract operations, transaction review, and endorsement, while the commitment node handles transaction validation, commitment, and blockchain maintenance. In this study, alliance members operate and manage endorser and committer services, specifically national medical authorities. All alliance members have the right to review transactions and access the blockchain, preventing any member from monopolizing transaction review and data access rights, thereby achieving decentralization. Hyperledger Fabric manages blockchain access rights through the application channel mechanism. Participants within the same application channel possess identical blockchain copies and access rights, while those outside the channel do not have such permissions. Moreover, private data serves as another data privacy protection mechanism in Hyperledger Fabric, further defining data access permissions for participants in the same application channel. Through application channels and private data mechanisms, alliance members can flexibly define subsets of members who can share private and confidential transactions, thus ensuring data privacy protection.

IV. Implementation Results

Following the framework outlined in this study, we have developed and implemented a simulation system. In this section, we will provide an in-depth introduction to the system's implementation results, specifically from the perspectives of the medical institution, verifier, and regular user. This comprehensive review will shed light on the operational aspects of the system across these three primary stakeholders.

A. Medical Institution

Medical institutions can log in to the system via the web. Once they reach the homepage (refer to Figure 4), they should choose "Medical Institution" as the login identity, which will then direct them to the Medical Institution user login screen (see Figure 5). Upon successful login, they can access the medical institution's home page (see Figure 6). Four main functions are available: adding new injection records, viewing recent ones, searching previous ones, and registering facial images. Users must input relevant information when adding new vaccination records (see Figure 7). To check a person's most recent vaccination record, they need to enter the individual's passport number (refer to Figure 8). If there is a need to access a person's past vaccination record, it can be done through the previous vaccination record query page (refer to Figure 9). Lastly, medical institutions can capture individuals' facial images using cameras for registration purposes (see Figure 10).

B. Verifier

Healthcare professionals can log into the system via a web page. Once logged in, they will visit the home page and select Verifier as the login identity, directing them to the Verifier login screen (Figure 11). After logging in, they can navigate to a webpage prompting them to scan a QR code (Figure 12). Once prompted, they can use the QR code scanner to scan the QR code presented by the person (Figure 13). After successfully scanning the QR code, the person's vaccination certificate and digital signature verification will be displayed (Figure 14). Press the "Go to Face Recognition" button at the bottom of the screen to enter the face recognition system, and the verification results will be displayed directly on the screen (Figure 15).

C. Regular User

Regular users can log in to the system using mobile phones or tablets (Figure 16). Upon entering the home page, they can access the facial image login/verification and QR code verification functions (Figure 17). Upon entering the facial image login/verification page, the system will automatically capture the user's facial image from the screen. Users can then log in or be verified using this facial image (Figure 18). In the QR code verification screen, users will find their personal vaccination certificate information and a QR code for verification (Figure 19).

V. Discussions

A. Security Analysis

This study proposes a system to help control global infectious diseases by establishing a mechanism for issuing and verifying vaccination certificates. Section 2.3 mentioned several security requirements that this system should meet. This section will conduct a security analysis of this system based on these requirements.

Authenticity

In our system, two key roles are responsible for verifying the authenticity of vaccination certificates: the regular user and the verifier. Each vaccination certificate sent to the regular user or the verifier includes a digital signature from the medical institution. The user and the verifier can verify the digital signature using the medical institution's public key, which is stored on the blockchain. Additionally, only authorized medical institutions can add their public keys to the blockchain, ensuring that the system can reliably verify the authenticity of the certificate issuer.

Integrity

In this system, users and verifiers receive vaccination certificates with a digital signature from the medical institution. They can retrieve the public key of the medical institution from the blockchain to decrypt the digital signature and obtain the hash value. Next, they can re-hash the vaccination certificate and compare it with the previously obtained hash value. If the comparison matches, the integrity of the vaccination certificate can be confirmed. The system uses a highly collision-resistant algorithm, SHA-256, meaning the chances of two different messages producing the same hash value are extremely low. Therefore, any differences in the comparison results indicate tampering or falsifying the vaccination certificate.

Non-replicability

The QR code generated by this system for verification is time-sensitive. If someone obtains the QR code through any means, it will not pass the verification if it has expired. This means that only one valid vaccination certificate can exist at a time. Only legitimate vaccination certificate holders can generate a new QR code for verification after the expired validity period. Therefore, individuals with non-legitimate vaccination certificates cannot replicate a valid vaccination certificate.

Identity Authenticity

In our system design, verified individuals will use their vaccination certificate, the medical institution's digital signature, and their digital signature to create a QR code. They will then present the QR code to the verifier for scanning. After the verifier scans the QR code, the system will query the blockchain for the public keys of the medical institution and the individual to verify their respective digital signatures. Once the verification is successful, the verifier will use a camera to take a photo of the holder's face and obtain the holder's facial image from the medical institution for comparison. If the pictures match, the verifier can confirm the authenticity of the individual's identity.

B. Performance Analysis

This study simulates the batch reading of 50 vaccination records and measures the execution time in milliseconds (ms). To ensure fairness, 30 reading simulations were conducted, with the vaccine records accessed from the state database. Figure 20 illustrates the execution time for each simulation, with a horizontal line indicating the average execution time. This study also simulates the batch writing of 50 vaccination records and measures the execution time in milliseconds (ms). In Hyperledger Fabric, transactions are not immediately packaged into blocks upon arrival. Instead, blocks are created and written to the blockchain ledger after collecting a batch of transactions. Consequently, the writing performance is influenced by two parameters: BatchTimeout (BT) and MaxMessageCount (MMC). The BT parameter indicates the maximum waiting time before a batch of transactions is packaged into a block, and the MMC parameter sets the upper limit on the number of transactions allowed in each batch—essentially, the maximum number of transactions a block can contain. This study tested the execution time for four combinations of these parameters: BT = 100 ms, 500 ms, and MMC = 5, 10. Each parameter combination was simulated 30 times to maintain fairness. Figure 21 shows the execution time for each simulation, with a horizontal line indicating the average execution time. Table 2 presents relevant statistical data on the execution time for reading and writing vaccination records, including the maximum, minimum, average, and standard deviation of the execution times from the 30 simulations. The results indicate that the time required for data reading is significantly less than that for data writing, demonstrating excellent time efficiency. The primary focus of this study is to perform vaccination record verification, which is a data-reading operation. Therefore, the vaccination record verification process proposed in this study is practical for real-world applications.

TABLE II
Statistical Data on the Execution Times for Reading and Writing Vaccination Records

	Read	Write			
		BT=100 MMC=5	BT=100 MMC=10	BT=500 MMC=5	BT=500 MMC=10
Max	381	9810	9765	29918	29972
Min	329	9577	9511	29499	29494
Average	353.37	9681.73	9625.10	29681.10	29700.90
Standard deviation	11.89	61.30	62.99	92.78	96.44

C. Comparison with related works

COVID-19 did not emerge long ago, so there are limited studies on blockchain-based COVID-19 digital vaccine certificate systems [9], [16], [18]-[20], which we have reviewed in Section 2. These studies primarily focus on utilizing blockchain technology and hashing to ensure the authenticity and immutability of digital vaccine certificates. Our system also employs blockchain and hashing to achieve these purposes. However, our design considers several factors as follows for verifying digital vaccine certificates that are often overlooked in existing research.

Ensuring the legitimacy of the issuer

In our system, the issuer of the vaccine certificate must add a digital signature to the vaccine certificate. This allows the verifier to use the issuer's public key to confirm the legitimacy of the issuer's identity. In contrast, other related systems do not include the issuer's digital signature, making it impossible to verify if a vaccine certificate is from a legitimate source.

Ensuring the legitimacy of the owner

The systems developed by Alfreshidi, Jafari et al., and Sharma and Rohilla rely solely on personal identification information, such as passport IDs, to access vaccine certificates. However, they do not technically verify the legitimacy of the ownership of these certificates. In contrast, the systems designed by Trong et al. and the one proposed in this study technically address the ownership verification issue. Trong et al. encapsulated the vaccine certificate into an NFT and used it as electronic proof of ownership. Meanwhile, the system proposed in this study adds the owner's digital signature to the vaccine certificate, enabling verifiers to confirm ownership legitimacy using the owner's public key.

Ensuring confidentiality and privacy of vaccine certificates

Vaccine certificates contain personal privacy information, and ensuring their confidentiality is crucial. Verifiers should only view these certificates with the owner’s authorization. This system records the hash value of the vaccine certificate on a blockchain while the original certificate is kept in the issuer's private database. This approach prevents blockchain participants from accessing the vaccine certificate without proper authorization. In the work of Jafari et al., vaccine certificates were not encrypted before storage, which means that all blockchain participants could potentially view them without the owner's consent since blockchain functions as an open ledger. Meanwhile, Hasan et al.'s system does encrypt vaccine certificates, and the encryption key is maintained privately by the owner. However, as discussed in Section 2, their system provides a method for others to obtain this key. If the key were to be compromised, the encryption of the vaccine certificate would no longer be effective.

Avoid fake vaccine certificate holders

The individual presenting the vaccine certificate may not be the actual owner, and merely verifying ownership does not entirely eliminate the risk of impersonation. Previous studies have not provided a solution to this issue. Our system addresses this problem by incorporating biometric verification. The owner's biometric data are securely stored on the blockchain. During the verification process, the biometrics of the certificate holder are compared with the owner's biometrics stored on the blockchain. If the two sets of biometrics match, it confirms that the holder is indeed the owner, helping to prevent counterfeiting.

Facilitating vaccine certificate verification

Our system utilizes mobile devices and QR codes to streamline verification [15]. Alreshidi noted that using passport numbers can expedite and simplify cross-border verification. However, any convenient verification method must prioritize the key security factors previously discussed. Unfortunately, passport numbers or similar personal identification codes alone do not guarantee these security measures.

The summary of the previous comparative analysis is presented in Table 3.

TABLE III
COMPARISON OF OUR SYSTEM WITH PREVIOUS WORK

Factors	Ours	[9]	[16]	[18]	[19]	[20]
Legitimacy of the issuer	Yes	No	No	No	No	No
Legitimacy of the owner	Yes	No	No	No	No	Yes
Confidentiality and privacy	Yes	No	No	Yes	Yes	Yes
Impersonation prevention	Yes	No	No	No	No	No
Verification facilitation	Yes	No	No	No	No	No

VI. CONCLUSIONS

The digital vaccination certificate system proposed in this study is built on the Hyperledger Fabric consortium blockchain platform and is specifically tailored for transnational applications across mutually trusting nations. The blockchain's inherent security features make it challenging to alter vaccination certificates once they are recorded. In addition, we ensure the authenticity of the issuing unit by verifying the digital signature of the medical institution. Moreover, we ensure that the issuing unit cannot repudiate the vaccination certificate it has issued. The integrity of the vaccination certificate is maintained through the user's digital signature. Additionally, we have incorporated facial recognition to confirm the person's identity and utilize QR codes to simplify the verification process, eliminating the need to compare paper vaccination certificates with passports manually. When the QR code is scanned, the system automatically completes the required comparison, and the verified person's vaccination certificate and digital signature verification results are shown, significantly enhancing the verification process's efficiency. This study also demonstrates the practical application of the system through Web and mobile interfaces. The system addresses the need for vaccination certification and can be applied to other infectious diseases to prepare for future global health challenges.

While this study has developed a vaccination certification system with various considerations, there are still some research limitations. Firstly, the analysis assumes that the public will be willing to provide facial images for facial recognition technology without considering the possibility of rejection. Additionally, there is no consideration for the potential of facial recognition misjudgment within the system.

Moreover, the system relies on mobile devices to display QR codes as proof of vaccination without considering individuals without access to mobile devices.

New concepts and technologies, such as blockchain interoperability and oracles [24], have emerged recently. However, there is limited relevant information, and researchers have different opinions. Therefore, in future studies, we will reference the research results of various researchers and integrate the distributed oracle network into this system. This will enable the system to achieve cross-chain and cross-system communication.

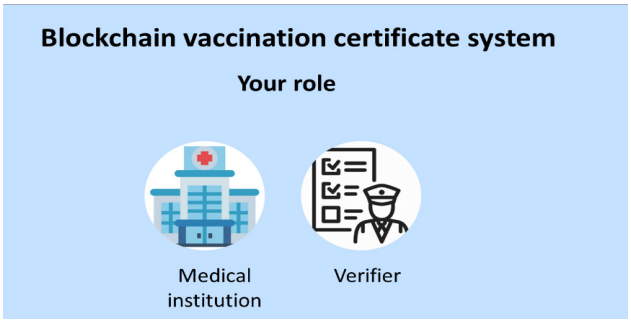


Fig. 4. The website for a medical institution and verifier

Fig. 5. Medical Institution user login page

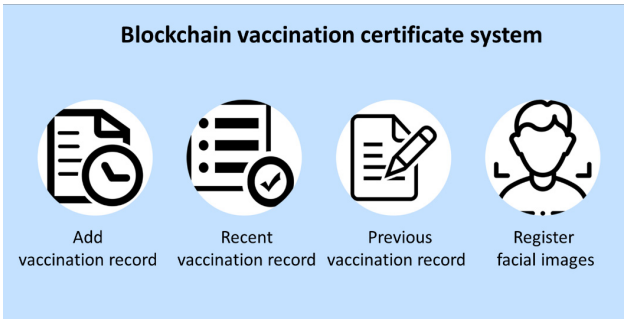


Fig. 6. Medical institution's homepage

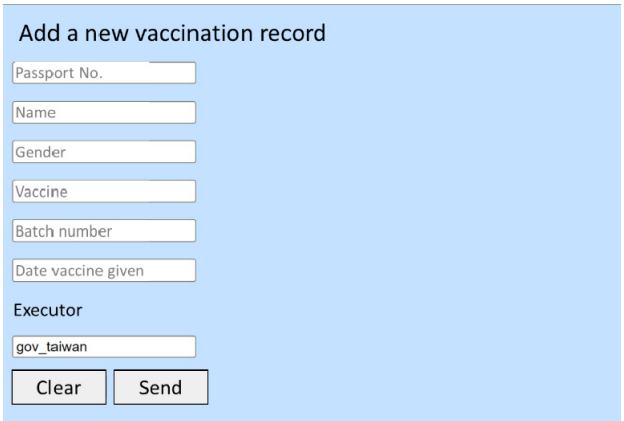


Fig. 7. Adding a new vaccination record

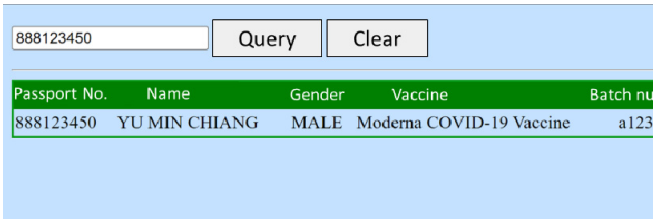


Fig. 8. Querying the most recent vaccination record

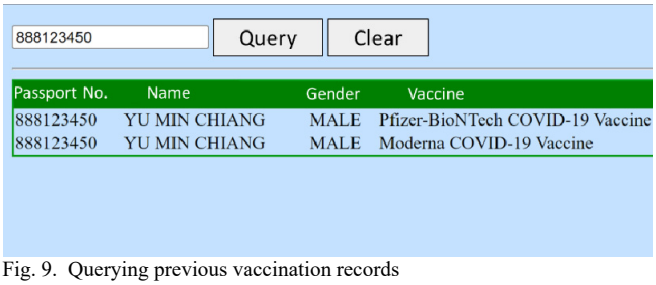


Fig. 9. Querying previous vaccination records

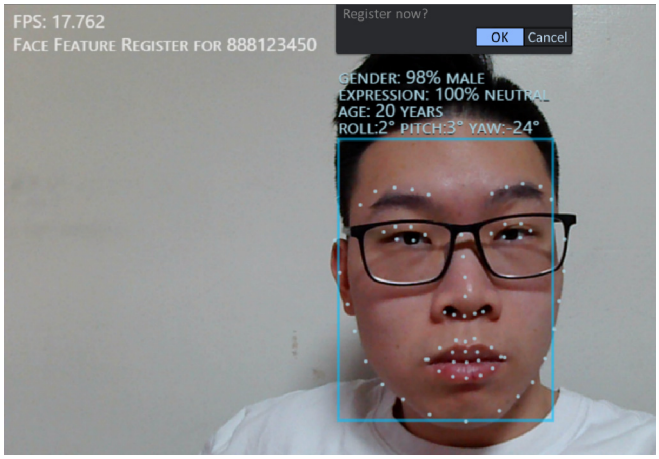


Fig. 10. Facial image registration

Fig. 11. Verifier login page

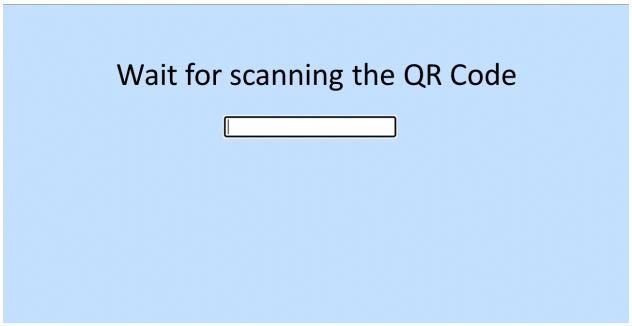


Fig. 12. Webpage for scanning the QR code

Fig. 13. Scanning the QR code

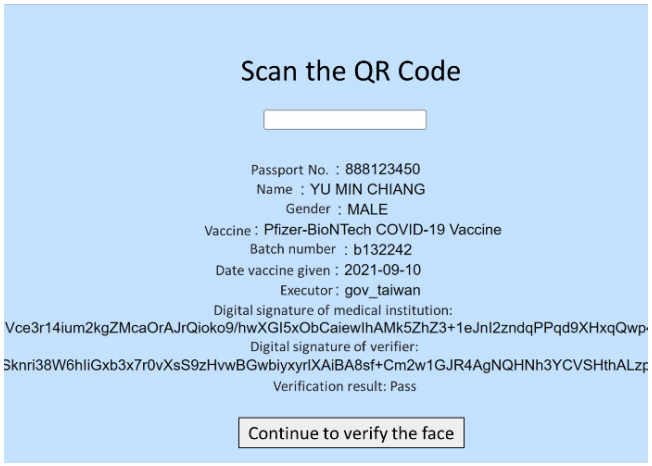


Fig. 14. Verification result of vaccination certificate and digital signature

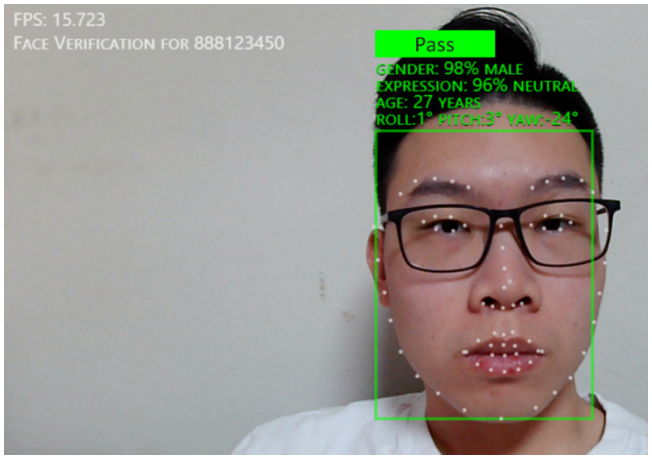


Fig. 15. Verification result of facial image

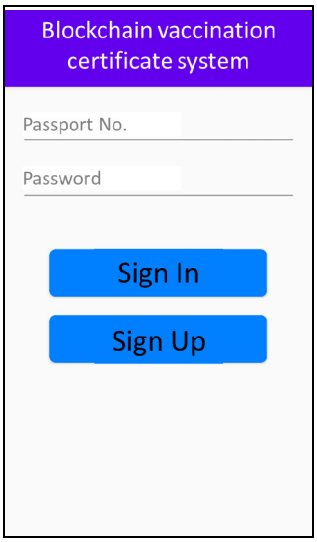


Fig. 16. Regular user login screen

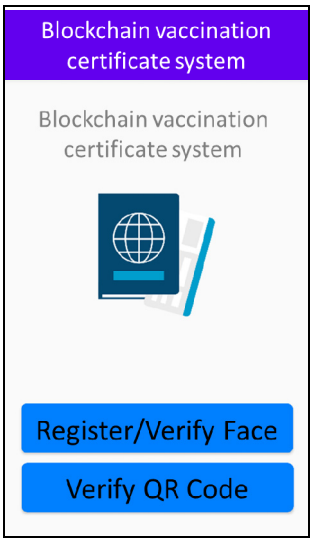


Fig. 17. QR code verification

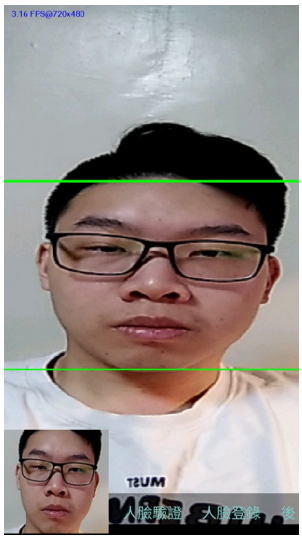


Fig. 18. Facial verification

Fig. 19. Personal vaccination certificate information

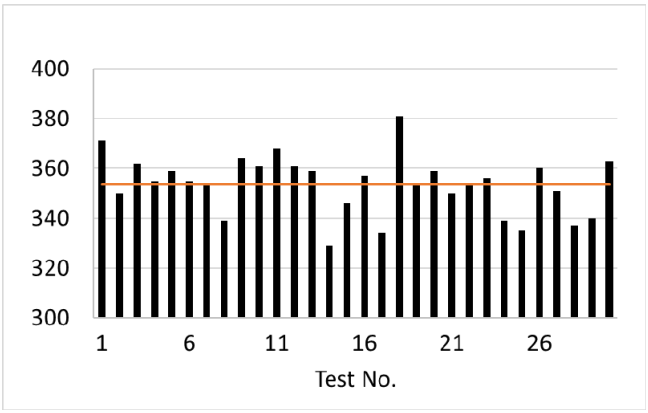
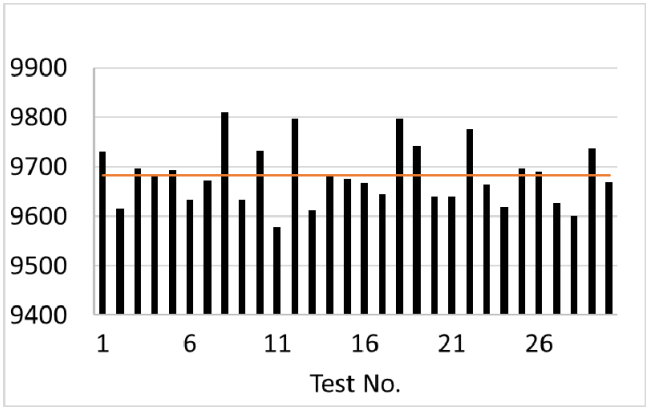
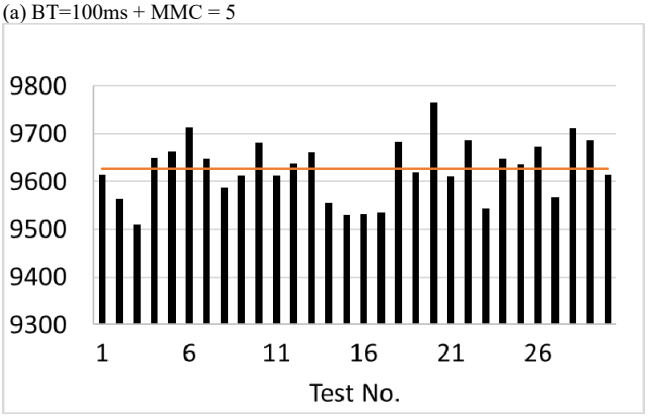


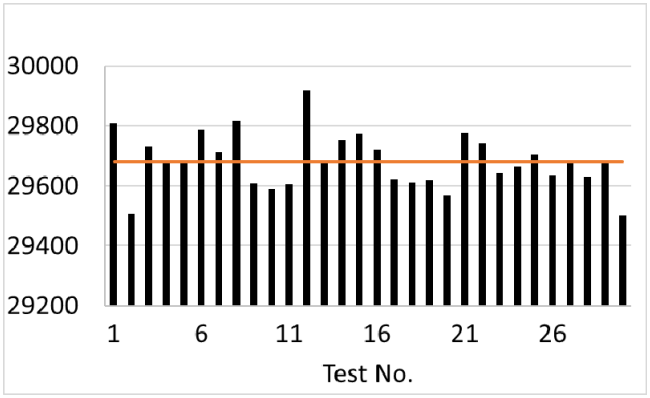
Figure 20. Simulation experiment on reading vaccination records



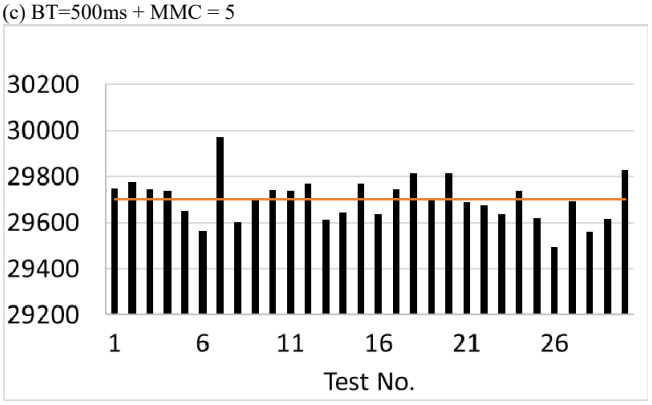
(a) BT=100ms + MMC = 5



(b) BT=100ms + MMC = 10



(c) BT=500ms + MMC = 5



(d) BT=500ms + MMC = 10

Figure 21. Simulation experiment on writing vaccination records

REFERENCES

[1] FDA. (2021, August). FDA approves first COVID-19 vaccine. FDA News Release. (Online). Available: https://www.fda.gov/news-events/press-announcements/fda-approves-first-covid-19-vaccine

[2] Ayesha Ayub Syed, Ford Lumban Gaol, Wayan Suparta, Edi Abdurachman, Agung Trisetyarso, and Tukoro Matsuo, "Prediction of the Impact of Covid-19 Vaccine on Public Health Using Twitter," IAENG International Journal of Computer Science, vol. 49, no.1, pp19-29, 2022

[3] BBC. (2021, July). Covid passports: how do they work around the world? BBC News. (Online). Available: https://www.bbc.com/news/world-europe-56522408

[4] EU. (2022, January). Key documents related to the Digital COVID-19 Certificate. (Online). Available: https://commission.europa.eu/publications/key-documents-related-digital-covid-19-certificate_en

[5] W. S. Ogan and C. A. Longhurst. (2023, March). Lessons learned from digital vaccine records during a pandemic. Mayo Clinic Proceedings: Digital Health. (Online). 1(2), pp.60-62. Available: https://doi.org/10.1016/j.mcpdig.2023.02.002

[6] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq. (2022, November). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*. (Online). *14*(*11*). Available: https://doi.org/10.3390/fi14110341

[7] Chetana Pujari, Chandrakala C B, Sharadruthi Reddy Muppidi, Sanjana Reddy Yalla, and Manjula C Belavagi, "A Novel Method of Secure Child Adoption Using Blockchain Technology," IAENG International Journal of Applied Mathematics, vol. 53, no.4, pp1531-1539, 2023

[8] Ren Gao, Shengqiang Huang, and Baolin Li, "Green Agri-Food Blockchain Technology for Investment Decision-Making under Cost Information Constraints," IAENG International Journal of Applied Mathematics, vol. 54, no. 1, pp82-91, 2024

[9] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham. (2020, December). Blockchain-based solution for COVID-19 digital medical passports and immunity certificates. *IEEE Access*. (Online). *8*. pp. 222093–222108. Available: https://doi.org/10.1109/ACCESS.2020.3043350

[10] D. Marbouh, T. Abbasi, F. Maasmi, I. A. Omar, M. S. Debe, K. Salah, R. Jayaraman, and S. Ellahham. (2020, Octobor). Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arab J Sci Eng.* (Online). *45*(*12*). pp. 9895–9911. Available at: https://doi.org/10.1007/s13369-020-04950-4

[11] A. I. Sanka and R. C. Cheung, "A Systematic Review of Blockchain Scalability: Issues, Solutions, Analysis and Future Research," *Journal of Network and Computer Applications*, vol. 195, pp. 103232, 2021.

[12] Hyperledger Fabric. (2024). A blockchain platform for the enterprise. Hyperledger Fabric Docs. (Online). v.latest. Available: https://hyperledger-fabric.readthedocs.io/en/latest/index.html

[13] Taiwan Centers for Disease Control. (2023, April). International Certificate of Vaccination. (Online). Available: http://at.cdc.gov.tw/g3B379

[14] F. Masood and A. R. Faridi, "Developing a Novel Blockchain-based Vaccine Tracking and Certificate System: An End-to-end Approach," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 1358–1376, 2024.

[15] I. Wahyudi, P. Sukarno, and A. A. Wardana, "Mobile-based Vaccine Tracking System using Ethereum Blockchain and QR Code," in 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), pp. 1-6.

[16] A. M. H. Jafari, R. K. Patchmuthu, and S. T. H. Tajuddin. (2024, April). Immutable COVID-19 vaccination certificate using blockchain. *Procedia Computer Science*. (Online). *233*. pp. 194-203. Available: https://doi.org/10.1016/j.procs.2024.03.209

[17] J. Benet. (2014, July). IPFS - Content addressed, versioned, p2p file system. *arXiv*. (Online). vol. abs/1407.3561. Available: https://doi.org/10.48550/arXiv.1407.3561

[18] A. Alreshidi. (2024, June). Blockchain-based decentralised management of digital passports of health (DPoH) for vaccination records. *International Journal of Advanced Computer Science and Applications*. (Online). *15*(*6*). Available: https://dx.doi.org/10.14569/IJACSA.2024.01506144

[19] N.Sharma and R. Rohilla, "Scalable and Cost-Efficient PoA Consensus-Based Blockchain Solution for Vaccination Record Management," *Wireless Personal Communications*, vol. 135, no. 2, pp. 1177–1207, 2024.

[20] N. D. P. Trong, N. H. Kha, M. N. Triet, K. V. Hong, T. D. Khoa, H. G. Khiem, N. T. Phuc, M. D. Hieu, N. V. Minh, P. D. X. Duy, T. Q. Thuan, L. K. Bang, Q. T. Bao, N. T. K. Ngan, L. K. Tung, and N. T. Vinh, "Blockchain-Enhanced Pediatric Vaccine Management: A Novel Approach Integrating NFTs, IPFS, and Smart Contracts," Lecture Notes in Computer Science: Proceedings of The 20th International Conference on Services Computing 2023, 17-18 December, 2023, Shenzhen, China, pp63-78. Available: https://doi.org/10.1007/978-3-031-51674-0_5

[21] Chainspect. (2024, October). What does TPS stand for in Blockchain Performance? (Online). Available: https://chainspect.app/blog/transactions-per-second-tps

[22] C. S. Hsu, S. F. Tu, and Z. J. Huang. (2020, April). Design of an e-voucher system for supporting social welfare using blockchain technology. *Sustainability*. (Online). *12*(*8*). Available: https://doi.org/10.3390/su12083362

[23] Anass Rghioui, Said Bouchkaren, and Anas Khannous, "Blockchain-based Electronic Healthcare Information System Optimized for Developing Countries," IAENG International Journal of Computer Science, vol. 49, no.3, pp833-847, 2022

[24] S. K. Ezzat, Y. N. Saleh, and A. A. Abdel-Hamid. (2022, June). Blockchain oracles: state-of-the-art and research direction. *IEEE Access*. (Online). *10*. pp. 67551-67572. Available: https://doi.org/10.1109/ACCESS.2022.3184726