cryptography

MDPI

Article

A Decentralized COVID-19 Vaccine Tracking System Using Blockchain Technology

Atsuki Koyama [1], Van Chuong Tran [2], Manato Fujimoto [1,2], Vo Nguyen Quoc Bao [3] and Thi Hong Tran [1,2,*]

[1] Faculty of Engineering, Osaka City University, Osaka 558-8585, Japan
[2] Graduate School of Informatics, Osaka Metropolitan University, Osaka 558-8585, Japan
[3] Faculty of Telecommunications, Posts and Telecommunications Institute of Technology, Ho Chi Minh City 70000, Vietnam
* Correspondence: hong@omu.ac.jp; Tel.: +81-6-6605-2187

Abstract: Coronavirus disease 2019 (COVID-19) vaccines play a crucial role in preventing the spread of the disease. However, the circulation of low-quality and counterfeit vaccines seriously affects human health and the reputation of real vaccine manufacturers (VMs) and increases the amount of fear concerning vaccination. In this study, we address this problem by developing a blockchain-based COVID-19 vaccine tracking system called "***Vacchain***". Our Vacchain allows users (USERs) to track and trace the route of vaccines. We propose three mechanisms, namely, a system manager (SYS-MAN), a mutual agreement concerning vaccine ownership, and vaccine passports, to enhance the security and reliability of data recorded in the Vacchain ledger. We develop this system on the Substrate platform with the Rust language. Our implementation, evaluation, and analysis have shown that Vacchain can trace and track vaccines smoothly. In addition, data security and reliability are enhanced by the abovementioned three mechanisms. The proposed system is expected to contribute to preventing the spread of COVID-19.

Keywords: COVID-19 vaccine tracking; blockchain for healthcare; decentralized vaccine management; Substrate platform; cryptography

Citation: Koyama, A.; Tran, V.C.; Fujimoto, M.; Bao, V.N.Q.; Tran, T.H. A Decentralized COVID-19 Vaccine Tracking System Using Blockchain Technology. *Cryptography* **2023**, *7*, 13. https://doi.org/10.3390/cryptography7010013

Academic Editor: Kentaroh Toyoda

Received: 18 January 2023
Revised: 1 March 2023
Accepted: 1 March 2023
Published: 6 March 2023

1. Introduction

Coronavirus disease 2019 (COVID-19) has spread quickly and changed the way of life of people all over the world. Building community immunity through vaccination has become mandatory in most countries for the purpose of overcoming the COVID-19 pandemic. Under such circumstances, numerous counterfeit vaccines are circulating because a large amount of money is generated by the global distribution of vaccines. The global market for vaccines is worth approximately 14 trillion Japanese yen [1], and vaccines are commanding enormous sums of money. In July 2021, approximately 2500 people in India received counterfeit COVID-19 vaccines—rather than the real vaccine, these individuals received saline solution [2]. Counterfeit COVID-19 vaccines have also been smuggled across borders, from China to South Africa [3]. In some middle- and low-income countries, where the vaccine supply is insufficient but people can only afford a low-priced vaccine, the probability of inexpensive counterfeit vaccines is relatively high. The circulation of counterfeit vaccines seriously affects human health, the reputation of real VMs, and the effectiveness of the prevention of the spread of COVID-19. Therefore, a strategy for preventing the circulation of counterfeit vaccines is needed.

In addition, resistance to the COVID-19 vaccine remains high because of its rapid production and the early time frame for vaccination. As a result, the circulation of fake vaccine passports to take advantage of loopholes regarding behavioral restrictions placed on those who are unvaccinated is even an issue. One cunning method through which individuals obtain counterfeit vaccine passports involves them colluding with doctors to get them to illegally issue vaccine passports, despite these individuals not having been

vaccinated, in exchange for the doctors receiving a bribe. Such fake passports are actually being traded via the dark web for approximately $250 [4]. This circulation of counterfeit vaccine passports has caused a variety of problems, including nonimmunized people spreading the virus and people who think about getting vaccinated believing that they do not have to face the risk of getting vaccinated and, thus, do not do so. As a result, the ultimate goal of vaccination, which is to achieve population immunity, becomes difficult to achieve. Thus, a strategy to prevent the distribution of fake vaccine passports is needed.

In this study, to address the abovementioned serious problems, we propose a COVID-19 vaccine tracking system, named "***Vacchain***", by utilizing the characteristics of blockchain technology, such as decentralization, immutability, and transparency. The notable feature of our proposed Vacchain is that it is able to not only prevent the circulation of counterfeit vaccines but also trace the origin and route of transactions relating to a vaccine before it is even used. Our Vacchain also provides a trusty vaccine passport solution to prevent the circulation of fake vaccine passports.

The rest of this paper is organized as follows. Section 2 presents the research background related to our study. In Section 3, we describe our proposed Vacchain in detail. Section 4 shows how the system is implemented. In Section 5, we analyze and discuss the effectiveness of Vacchain in preventing the circulation of counterfeit vaccines and fake vaccine passports. Finally, Section 6 concludes the paper.

2. Background

In this section, we describe the research background. First, we explain the characteristics of blockchain as preliminary work. Then, we present several well-known blockchain development platforms. Finally, we describe the existing research related to our study and our focus based on such research.

2.1. Characteristics of Blockchain

Blockchain came into existence with Bitcoin [5] cryptocurrency. The blockchain system records all transactions in a distributed ledger. Moreover, blockchain is a peer-to-peer (P2P) type of network, which means that all nodes share information by communicating directly with each other, without having a specific server or client. Data are stored in the ledger, and the ledger is decentralized and stored in many computers distributed all around the world. This structure results in one of the important characteristics of a blockchain network, being *distributed*. Data stored in the ledger cannot be deleted or modified by anyone, which results in the second characteristic, being *immutable*. Being *immutable* allows blockchain data to become trustworthy and reliable evidence for many kinds of services. The blocks of the ledger are connected via cryptography hash values to form a chain of blocks [6]. Concretely, each block stores its hash value and that of the previous block. Anyone is able to verify whether the ledger has been tampered with by quickly analyzing the hash value of the final block only, which results in the third characteristic, being *transparent*, which helps enhance data reliability since data are transparent and cannot be tampered with. Consensus algorithms such as Proof of Work [7], Proof of Stake [8], and Byzantine Fault Tolerance [9], are required to govern the operation of the blockchain network and to guarantee the three abovementioned characteristics: *decentralized, immutable, and transparent*.

2.2. Blockchain Development Platforms

Several development platforms are available for developing blockchain-decentralized networks without requiring sophisticated knowledge on the network infrastructure. The first well-known platform is Ethereum [10], which allows the deployment of smart contracts for developing a distributed application (Dapp). Smart contracts are computer programs that are processed on a virtual computer known as an Ethereum Virtual Machine (EVM). Individuals are able to develop and deploy a Dapp on the existing EVM platform quickly. However, the disadvantage of the Ethereum platform is the high gas fee with a low processing rate. More importantly, the developer is not able to modify the consensus

governing the network, meaning that the developer does not have the freedom to upgrade the network's scalability and power consumption.

The second well-known platform is Substrate [11] provided by Polkadot [12]. In Substrate, components such as the consensus model and governance methods are modularized. One may combine the elements appropriate for their specific requirements. Therefore, the Substrate is characterized by its flexibility in the development process. Developers can utilize open-source Substrate to build their own blockchain network and may choose either to develop applications with the above-provided consensus for saving development time or even to develop a new consensus algorithm for enhancing network scalability, interoperability, and security.

The development of a blockchain network requires knowledge in many research fields, such as cryptography, data encryption, decentralized networking, and P2P communication. Therefore, it is very difficult to create such a platform from scratch. In this study, we develop our system from an open-source Substrate. We do not choose the Ethereum platform because, in the near future, we plan to enhance network scalability, interoperability, and security, which is not relevant to applications on the Ethereum platform. Therefore, Substrate is our best choice at the moment.

2.3. Related Work & Preliminary Idea

Many people are hesitant to be vaccinated [13]. It has been reported that people are hesitant to receive vaccines because of the negative information that they have been presented with on social media sites about the side effects of vaccines. In other words, anxiety and the fear of foreign-made, fake, and low-quality vaccines have discouraged vaccination [14]. Thus, employing blockchain technology to allow users (USERs) to easily track the origin and quality of vaccines before vaccination is necessary to conduct successful vaccination campaigns. Currently, blockchain is being adopted to address many social issues. For example, Ref. [15] proposed a system to stop the spread of COVID-19 at an early stage. This system provides tokens as an incentive for infected people to voluntarily quarantine themselves. In [16], the authors developed an Aura blockchain platform to provide proof of authenticity for luxury brand goods, such as Louis Vuitton Moet Hennessy (LVMN). Another study scored the quality of goods and the trust and reputation of entities in the supply chain [17]. In addition, there have been several studies on the integration of Internet of Things (IoT) and Point of Care Tools (POCT) using blockchain. For example, the work in [18] summarized how blockchain technology is being applied to the healthcare system. The work in [19] developed a blockchain model for the IoTs in healthcare. The authors in [20] proposed a high secured blockchain-based Internet of Medical Devices (IoMT) platform for healthcare. The STAMINA platform described in [21] monitoring and mitigating pandemic outbreaks, which provides the information and tools necessary to take prompt and effective countermeasures in the outbreak period. Regarding vaccine management, the authors in [22,23] proposed a blockchain system that detects expired vaccines and uses machine learning to perform vaccine evaluation functions and vaccine demand forecasting; however, these authors have not yet discussed any secure method of transferring vaccines through blockchain systems. Therefore, it is necessary to develop a system that allows for the secure transfer of vaccine ownership and the distribution of legitimate vaccines in a feasible manner.

In this study, we propose the use of an SYS-MAN that operates as a guardian to protect vaccine quality. Moreover, we propose a mutual agreement on the transfer of ownership to ensure that vaccine ownership is securely controlled. Furthermore, we employ vaccine passports issued on the blockchain to prevent unjustified vaccine distribution.

3. Our Proposed Vacchain System

3.1. System Overview

An overview of our proposed system is shown in Figure 1, which shows several entity roles, such as SYS-MAN, VM, vaccine authorized organization (VAO), vaccine authorized

distributor (VAD), and USER. Information on the abovementioned entities and vaccines is stored in a distributed ledger—the Vacchain ledger. The VM represents the company that manufactures the vaccine. Only the VM is able to record information on vaccines such as vaccine name, type, and ingredients into the Vacchain ledger. The VAO is the organization that approves the vaccine and is assumed to be a government agency of a country. The VAD may be an organization that buys and distributes vaccines, an express company that transports the vaccine, or a hospital that administers the vaccine. The USER is the vaccine beneficiary. The SYS-MAN is the manager of the system, which verifies the trust of other entities such as the VM, VAO, and VAD. The SYS-MAN acts as a guardian that protects the reliability of the data recorded in the Vacchain ledger and thus plays an important role in securing the network. The system is supposed to have multiple SYS-MANs, VMs, VAOs, VADs, and USERs.

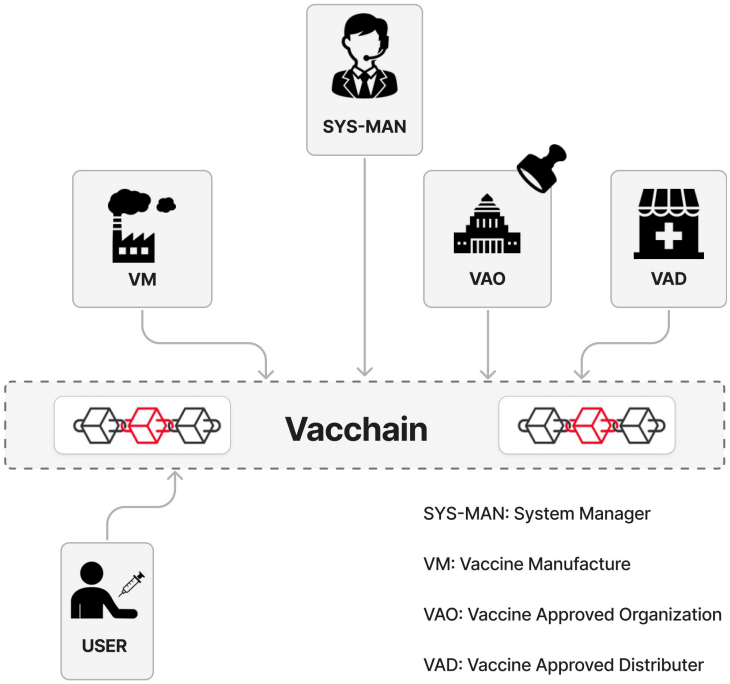

Figure 1. Overall view of the proposed Vacchain system.

Figure 2 shows a general scenario in which the proposed Vacchain system can be used. Processing is commonly carried out in 8 steps as follows. In step 1, the entities create accounts for themselves and decide their role; then, they may submit the necessary documents to the SYS-MAN for role verification. In step 2, the SYS-MAN checks the documents; if there is no issue, then the SYS-MAN confirms the role of the entities and records the confirmation in the Vacchain ledger. In step 3, the confirmed VM registers information on its manufactured vaccines into the Vacchain ledger. In step 4, the VAO approves the registered vaccines for use in their country or area. The approved status is recorded in the Vacchain ledger. In step 5, the vaccine is sent from the VM to the VAD, which can be an express company, hospital, or distributor. In step 6, the VAD confirms its receipt of the vaccine. To represent the changing status of the vaccine, the ownership information is updated from the VM to the VAD and then recorded in the Vacchain ledger.

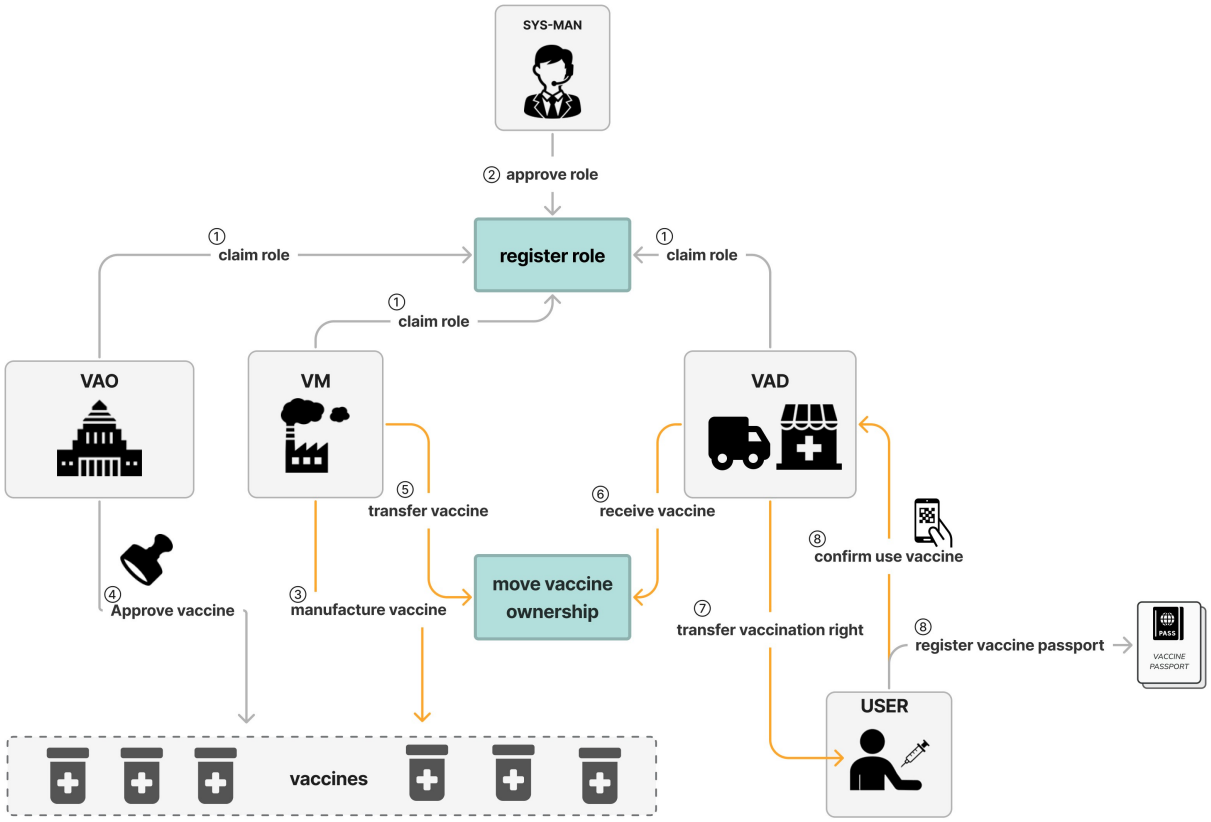

Figure 2. Flowchart of the proposed system from vaccine production to vaccination.

Other information on vaccines, such as manufacturer name and ingredients, cannot be changed. In step 7, the USER decides to receive the vaccine. Vaccine ownership is transferred to the USER and recorded in the Vacchain ledger. In step 8, the USER accepts the vaccination, followed shortly by the vaccination history being registered in the Vacchain system and the vaccine passport being created.

3.2. SYS-MAN

To enhance the data reliability of the tracking system, we propose two approaches. First, only VMs are allowed to register vaccine information in the Vacchain ledger and, thus, take full responsibility for any issue caused by their registered vaccines. However, fake VMs may register fake vaccines to deceive customers. Therefore, we propose a second method that uses an SYS-MAN to verify and filter the identity of not only VMs but also VAOs and VADs. The SYS-MAN approves the role and authority for account-representing organizations such as VMs, VAOs, and VADs after confirming a certain degree of trustworthiness so that organizations can be identified and held accountable.

Figure 3 illustrates a two-step procedure by which the SYS-MAN can accept and approve entity roles. In step 1, accounts such as VMs, VAOs, and VADs claim their role in the Vacchain. These accounts then submit documents to the SYS-MAN for role verification purposes. In step 2, the SYS-MAN verifies the documents, approves the role, and records the approval in the Vacchain ledger.

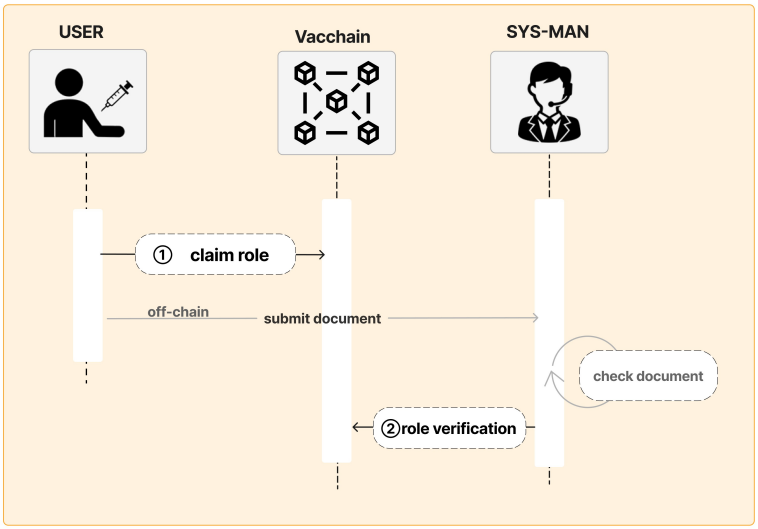

Figure 3. Process from role request to approval

3.3. Mutual Agreement on Transferring Ownership

As mentioned above, only the VM is able to register vaccine information such as ingredients and expiration date. The transfer of the vaccine from the manufacturer to the shipping company, to the hospital, and finally to the beneficiary is represented by a change in the ownership of the vaccine only. Basically, only the current owner of the vaccine is able to transfer vaccine ownership to another account. However, a potential problem exists in which an account may not agree with the transfer of vaccine ownership, which results in a security leakage. To address this problem, we propose a mutual agreement procedure for the secure transfer of vaccine ownership. To achieve this mutual agreement, we introduce an intermedial parameter named *buyerID*, which represents the identity of the potential buyer of the vaccine. We assume that VM A is the current owner of vaccine V. VM A transfers vaccine ownership to VAD B. This transfer of ownership is conducted via two steps, as illustrated in Figure 4. First, the current owner, VM A, transfers the vaccine to VAD B by setting the *buyerID* of vaccine V to VAD B. Second, once the *buyerID* of the vaccine is changed to B, the VAD B decides whether or not to accept the transfer of ownership. If VAD B accepts the change in ownership, then the current owner of the vaccine is transferred from A to B. VAD B now becomes the owner of the vaccine and can thus make decisions to use or resell the vaccine to other entities. Otherwise, the vaccine owner is still A.

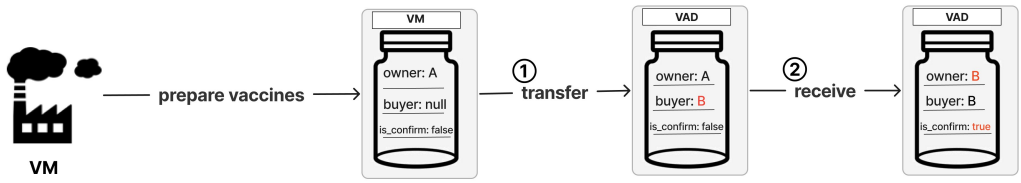

Figure 4. Transfer of ownership according to 3 parameters.

3.4. Vaccine Passport

The reality is that the vaccines that are handled around the world and exist on the blockchain may not all be trustworthy. Our proposed system can guarantee that the available vaccines have been manufactured and distributed through traceable channels. Blockchain technology itself does not guarantee vaccine trustworthiness. Therefore, the Vacchain system should be structured in such a way that counterfeit vaccines cannot be distributed or that there is no longer any motivation to distribute fake vaccines. Here, we believe that issuing vaccine passports on the Vacchain system eliminates the benefit of distributing counterfeit vaccines and thus addresses the fake vaccine issue. A vaccine pass-

port, which includes the tracking information of the vaccine and the verifiable information of the vaccine beneficiary, is automatically created once vaccination occurs.

Figure 5 illustrates an assumption that a fake vaccine is created by illegally copying the quick response (QR) label of the real vaccine. Because both fake and real vaccines with the same QR code cannot be sold in the same Vacchain system, one must decide whether to sell either only fake or only real vaccines in Vacchain while selling the others in other marketplaces. If a legitimate vaccine is sold at a lower price, without passing through the proposed Vacchain system, then the history of vaccination cannot be registered in the vaccine passport at the time of vaccination. Proof of vaccination cannot be performed, even though the vaccine has been administered. Thus, the advantage of creating counterfeit (or fake) vaccines is eliminated. Therefore, we believe that the demand for counterfeit vaccines can be lowered and, thus, that their distribution can be reduced.

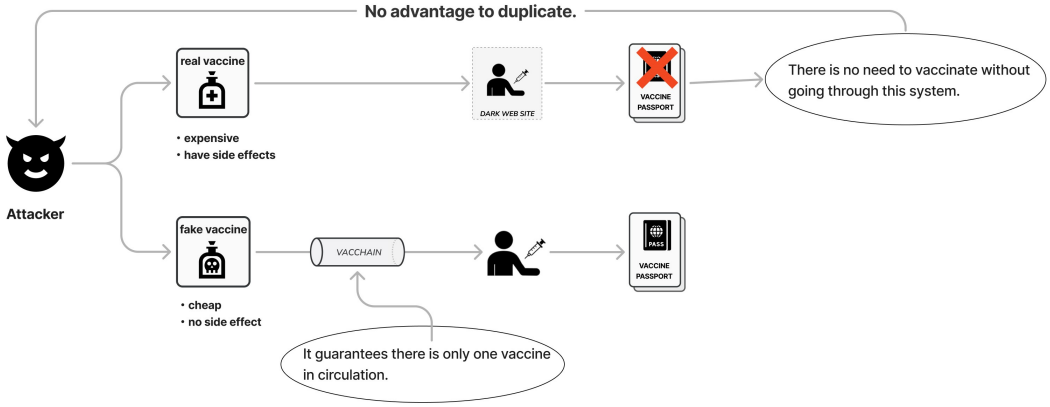

Figure 5. Counterfeit vaccine registration scenario by a dishonest attacker.

As a concrete example, we consider the case where the beneficiary, USER C, is issued a vaccine passport and the vaccination history is verified by USER D, who may be a quarantine officer at the airport or a clerk at a store (see Figure 6). The information recorded in the vaccine passport of USER C includes the address of the beneficiary, USER C, and a list of those vaccines that USER C has received. When USER D needs to check the vaccination history of USER C, he or she may use USER C's address as a search key to search for the vaccine passport of USER C in the Vacchain ledger, where the vaccine passport is decentralized and stored in a hash map structure.

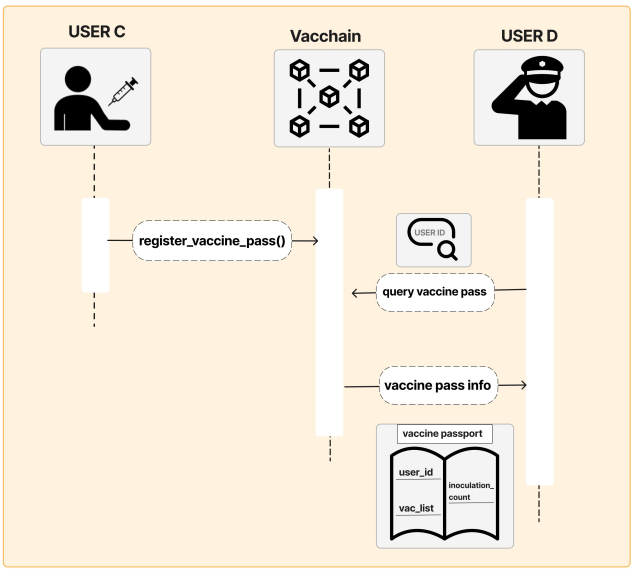

Figure 6. Vaccine passport registration and information available through search.

4. System Implementation

4.1. System Overview

The overall diagram of the proposed system is shown in Figure 7. The system is comprised of three parts: frontend, blockchain, and backend. The frontend part provides an intuitive and user-friendly interface that allows USERs to interact with data in the blockchain and backend parts. We develop the frontend part mainly by using the JavaScript language.

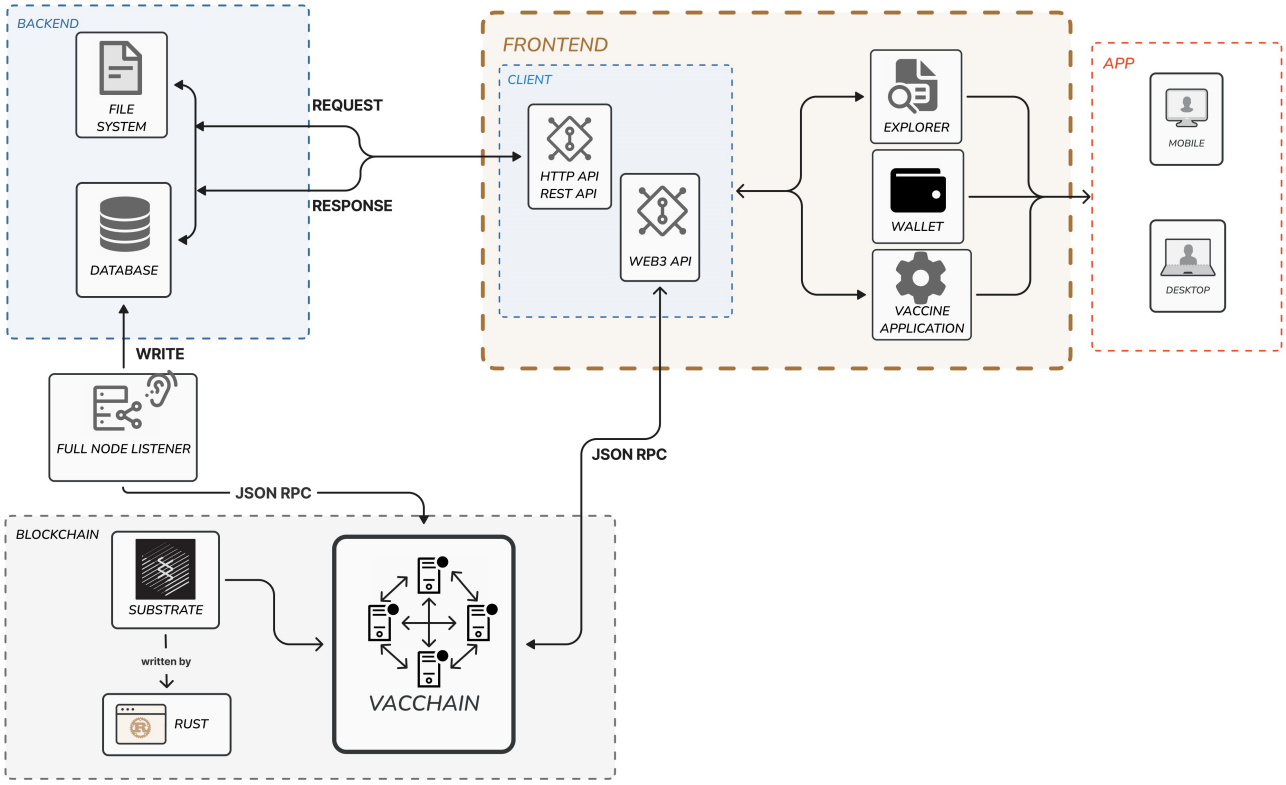

Figure 7. Overall view of the proposed system.

The backend is responsible for storing the data registered on the blockchain in a local database through a full-node listener. Storing blockchain data in an off-chain backend database enables not only faster access to the data but also the searching, filtering, and sorting of on-chain data quickly. The backend part of our Vacchain system is used to manage USER accounts and sign-in and sign-out tasks. We develop the backend part mainly by using the Typescript language.

The blockchain part is the most important part of our system, as it stores and manages the distributed Vacchain database. We develop the blockchain part on the Substrate platform by using the Rust language. We utilize the Aura + GRANDPA consensus, which is the default consensus on the Substrate platform. Aura is actually a simple version of Proof of Stake by a round-robin process concerning the tasks of validators, whereas GRANDPA is a block finality mechanism that has been proven to be secured by Polkadot public networks. The nodes join the system as evaluators to secure the network and receive the reward coins in return for their hard work. Most of our original ideas are implemented in the blockchain part. The following subsections describe in more detail how we implement the blockchain part as well as new ideas such as the *SYS-MAN* and *mutual agreement on transferring ownership*.

4.2. Substrate-based Decentralized Blockchain Engine

The Substrate platform [11] used in the proposed system consists of two major elements: the *outer node* and *runtime*. The *outer nodes* play a role in communicating with other

nodes to establish a P2P network and reach a consensus. *Runtime* is responsible for determining whether a transaction is legitimate and for transitioning the state of the blockchain and includes a combination of runtime logic called pallets, which make blockchain development more flexible and relatively easier. These pallets are coded in the Rust language, which is fast, portable, and memory safe. Each pallet includes multiple logic functions that allow entities to perform specific tasks.

Figure 8 shows an overall diagram of the pallets and functions of the proposed system. There are five pallets corresponding to five entities: the SYS-MAN, VM, VAD, VAO, and USER. Each pallet includes a number of functions that can be executed by the corresponding entity, as shown in Figure 8. The *claim_role* function can be executed by all types of entities to determine the role of the account expected to be assigned. The SYS-MAN then verifies the role request from USERs and executes the *approve_role* function to confirm the role.

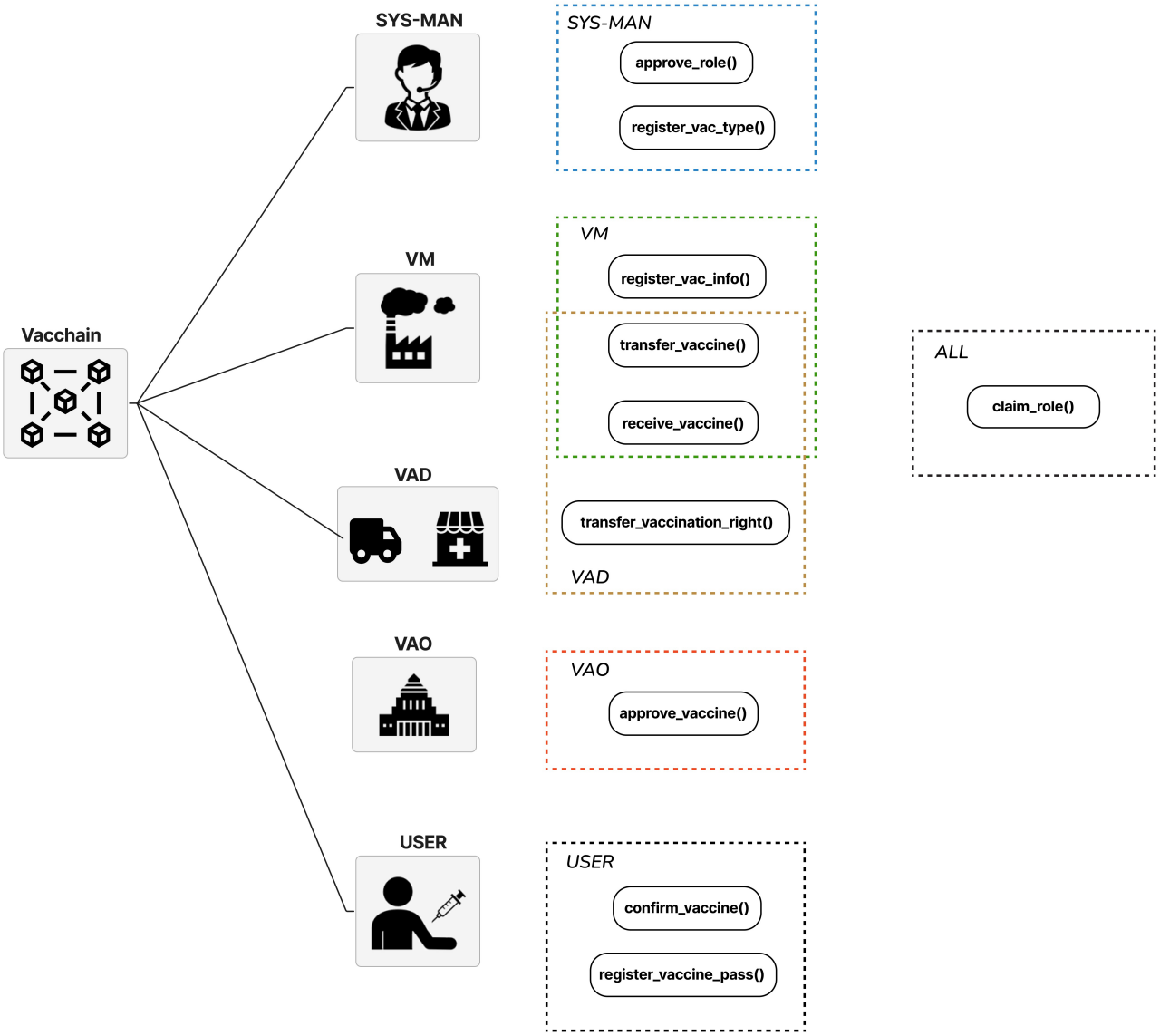

Figure 8. Main smart contract functions of the proposed system.

In vaccine management, the processing flow is as follows. First, the SYS-MAN registers a new type of vaccine into the Vacchain ledger by executing the *register_vac_type* function. The VAO executes the *approve_vaccine* function if it approves a specific type of vaccine to be used in the area. The VM executes the *register_vac_info* function to register the vaccines it has produced; the vaccine information may include the lot number, type of vaccine,

ingredients, original date, expired date, manufacturer ID, owner ID, etc. The VM may then transfer vaccine ownership to the VAD by executing the *transfer_vaccine* function. The vaccine receiver, the VAD, may execute the *receive_vaccine* function to complete the transfer of vaccine ownership. These two functions are described in detail in Section 4.2.2. Finally, the current owner of the vaccine, which may be a hospital or clinic, may decide to inject the vaccine into the final USER by executing the *transfer_vaccination_right* function, and the USER administering the vaccine executes the *confirm_vaccine* and *register_vaccine_pass* functions. The injection information is added to the vaccine passport of the USER.

4.2.1. SYS-MAN

We implement the previously mentioned SYS-MAN by using two functions, *claim_role* and *approve_role*. In addition, two parameters, *role* and *role_status*, are used to indicate the status of an account. Role requests and role approval are processed as follows. In step 1, it is necessary to request a role. The function used in this step is the *claim_role* function, in which the account ID can be obtained from the signature on the transaction to be sent. By using the account ID, one can retrieve the account information stored on the blockchain ledger. Once the *claim_role* function is executed, the account status parameter, *role*, is changed to the role that the account owner wants to play, such as VM, VAD, or VAO. Then, *role_status* is changed to *Pending*, which means that the role is being requested. In step 2, we consider the *approve_role* function, which approves the role request and grants authority and can be executed by the SYS-MAN (see Figure 8). The function retrieves the account status from the specified account ID that has requested the role and checks the account parameter *role_status* to determine whether or not it is *Pending* by executing the abovementioned *claim_role* function. If *role_status* is pending, then the *claim_role* function is successfully activated, and the account parameter *role_status* is then changed to *Approved* and recorded in the blockchain. Not only can the requested account become fully activated in the role it had requested, but it can also execute those functions specific to only that type of role.

4.2.2. Mutual Agreement on Transferring Ownership

In the proposed system, vaccine ownership is transferred between the sender and receiver of the vaccine by mutual agreement. The *claim_role* and *approve_role* functions are used to achieve this end. In addition, we introduce *ownerID*, *buyerID*, and *is_confirm* to indicate vaccine status.

Let us consider an example where ownership is transferred from *VM A* to *VAD B*, as illustrated in Figure 9. Before transferring ownership, *VM A* must execute *register_vac_info*, which records the information of *vaccine V* into the Vacchain ledger. The mutual agreement on transferring ownership of *vaccine V* between *VM A* and *VAD B* is as follows. In step 1, *VM A* executes the *transfer_vaccine* function. Only the current owner of *vaccine V* (*VM A*) is able to execute this function. The verification of the owner is performed by comparing the account ID of the executing account with that recorded in the *ownerID* status of *vaccine V*. Once the *transfer_vaccine* function is successfully executed, the content of *buyerID* is changed to the address of *VAD B*, indicating that only *VAD B* is entitled to accept or not accept the transfer of ownership. In step 2, *VAD B* may execute the *receive_vaccine* function to accept the transfer of ownership. This function can be executed only by *VAD B*, which has its account ID being recorded in the *buyerID* of *vaccine V*. Once this function is successfully executed, the content of the *ownerID* of *vaccine V* is changed to the address of *VAD B*. Furthermore, the *is_confirm* parameter is converted to *true*, which means that the transfer of ownership has been successfully completed. By following these two steps with the confirmation of the vaccine parameters, it is possible to prevent the unauthorized receipt of the vaccine by anyone other than the designated recipient.

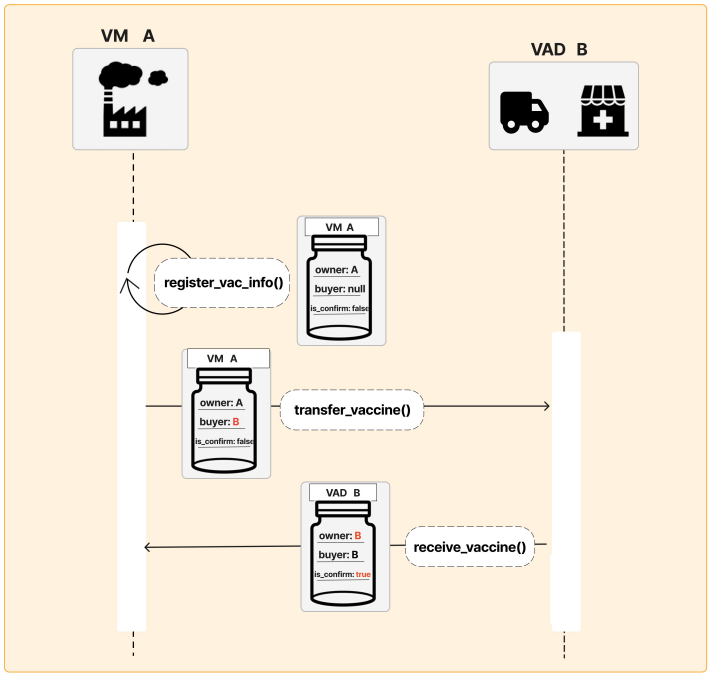

Figure 9. Transition diagram of the parameter until ownership of the vaccine passes from Manufacturer A to Distributor B .

5. Evaluation

Three new mechanisms are combined to protect legitimate vaccines and vaccine passports on the blockchain ledger. In this section, we first discuss how the data reliability of Vacchain can be enhanced by employing these mechanisms. Second, we compare our work with the related literature.

5.1. Data Reliability of Vacchain

Impact of the SYS-MAN *:*

SYS-MANs operate as guardians of the network; they verify the role requested by entities and allow only trusted entities to update the database according to their confirmed roles. For example, *VM A* is able to execute functions designed for manufacturers only and must take full responsibility for its registration and updated information since every action is immutably recorded as concrete evidence. If an entity works dishonestly, then the SYS-MAN has permission to remove the account from the network by revoking the role of that entity. In other words, the existence of an SYS-MAN helps enhance the data security and reliability of the network. It is worth noting that the SYS-MAN is able to decide only whether to approve or revoke the role of the requested entities. Network miners, not SYS-MANs, are able to create a new block of the blockchain ledger. Therefore, the network still is decentralized in nature.

Impact of the Mutual Agreement of Ownership Transfer*:*

If vaccine ownership could be unilaterally sent without the approval of the recipient, then it would be impossible to assign responsibility when irregularities related to the vaccine are discovered. In other words, even if a defect is found in the vaccine and the proposed system is used to trace the vaccine to identify the cause, it might be difficult to track down the cause because of the imposition of responsibility. The mutual agreement mechanism can be used to address these problems. The transfer of vaccine ownership is done by mutual agreement, making it possible to trace the vaccine and to clearly identify who is responsible for its management. In addition, since the owner of the vaccine at a given point in time is clearly specified, the system can be applied to the implementation of extended functions, such as those functions that can be performed only by the owner of the vaccine.

Impact of Vaccine Passports on Blockchain:

As previously mentioned, a vaccine handled on the blockchain may not always be legitimate. Therefore, we propose the issuance of a vaccine passport to eliminate the advantage of distributing counterfeit vaccines. However, although this mechanism is expected to be effective against fraud involving replicating vaccines, it cannot detect the presence of foreign substances or illegally exported entries. In other words, it is difficult to completely prevent fraud outside the blockchain. However, this system makes it possible to trace vaccines so that if they are found to be counterfeit or deficient vaccines, they can be traced back to the original source. This situation increases accountability while discouraging and deterring fraud.

5.2. Vacchain Comparison

This section discusses and compares the related works that employ blockchain technology for vaccine management. The comparison is shown in Table 1. The first three works, i.e., [15,22,24], are academic works, whereas the last two works, i.e., [25,26], are industrial works (startup projects). Each work has its own strong points in terms of its own approaching problem. Therefore, it is impossible to conclude that one specific work is completely better than the others. Here, we focus on comparing two concepts, "vaccine traceability" and "data reliability", which are our issues of interest. We briefly describe the main points of all works and then prove that our work is the best in terms of these two concepts. The system in [15] allows for vaccine payments through a blockchain network and encourages voluntary testing and quarantining by using token incentives. However, vaccine traceability and data reliability issues have not yet been addressed.

Table 1. Comparison with related studies.

Research	Platform	Main Focus	Traceability	Data Reliability
(Manoj et al., 2020) [15]	public blockchain	Give tokens, encourage legitimate behavior and provide incentives	×	×
(Yong et al., 2020) [22]	Ethereum (public blockchain)	Detecting expired vaccines. Demand forecasting by machine learning	△	△
(Antal et al., 2021) [24]	Ethereum (public blockchain)	Temperature control using Internet of Things (IoT) devices. Side effect reports are also managed on the blockchain	✓	×
VXPASS [25]	BSV (public blockchain)	Protects patient privacy without storing personally identifiable information	×	△
eZVax [26]	Hyper Ledger Fabric (consortium blockchain)	Store, manage, and analyze data throughout the vaccine supply chain	✓	△
Our proposed Vacchain	Substrate (consortium blockchain)	Prevent counterfeit vaccines by making them traceable	✓	✓

✓ : traceability/data reliability are fully provided. △ : traceability/data reliability are partially provided. ×: traceability/data reliability are not provided.

The work in [22] uses machine learning to predict vaccine demand and distribute vaccines efficiently. The system is developed as a Dapp on the Ethereum platform. Vaccine information is written to the blockchain at the time of vaccine production and vaccination only. The transfer of vaccine ownership throughout distribution has not yet been addressed, which means that traceability is partly provided. Each role is assigned by the government, and information about quality assurance is recorded on the blockchain. Data reliability is partly enhanced by employing the role of the government. The work in [24] uses IoT

devices to manage vaccine status, reporting the side effects on the blockchain to provide transparency, and is also being developed on Ethereum. The freezers in which the vaccines are stored and the information about the vaccine are linked and managed and can be traced back to the manufacturer. However, there is no mention of selecting a trusted VM or medical center to enhance data reliability.

The startup project VXPASS [25] is a platform that stores information about vaccines and vaccination records on the Bitcoin SV (BSV) network. The project aims to protect patient privacy by not storing personally identifiable information on the chain. Moreover, the project does not handle vaccine distribution information, and only medical professionals are allowed to update data in the blockchain ledger.

eZVax [26] is a solution that stores and makes traceable data throughout the vaccine supply chain and manages vaccination information. The quality and authenticity of vaccines can be instantly verified. However, there is no mention of who chooses the trusted manufacturers, distributors, etc., which means that data reliability is not yet sufficient.

Our proposed Vacchain focuses on tracking the vaccine and detecting and eliminating counterfeit vaccines. Actions related to vaccine ownership are recorded and traceable, which encourages the organization in charge of the vaccine to act accordingly given its high level of responsibility. Our Vacchain places high priority on enhancing the reliability of the data recorded in the ledger by proposing three mechanisms: an SYS-MAN, the mutual agreement of ownership, and a vaccine passport. It is clear that each related work focuses on solving a specific issue. However, in terms of traceability and data reliability, our work solves the problem in depth to provide the best results in terms of these two concepts.

6. Conclusions

In this study, we develop a highly secure decentralized system for vaccine distribution. To enhance system security and data reliability, we propose three mechanisms: an SYS-MAN, the mutual agreement of vaccine ownership, and a vaccine passport. The SYS-MAN approves or revokes the role of entities who join the system. The mutual agreement manages the transfer of vaccine ownership. The vaccine passport eliminates the need to circulate counterfeit vaccines. We implement and evaluate the network on the open-source Substrate platform. Theoretically, the system is highly secure due to the use of the abovementioned three proposed mechanisms. Our testing also shows that the system operates smoothly.

However, Vacchain still has limitations that should be addressed in the future. For example, Vacchain does not yet focus on solving the fundamental issues of blockchain technology, such as consensus, processing throughput, storage size, and scalability. Our future work will aim to enhance the scalability and processing rate of the system. Furthermore, upgrading the network consensus is our next research theme. We fully expect a bright future where there is no use for counterfeit vaccines.

Author Contributions: Conceptualization, A.K. and T.H.T.; Funding acquisition, T.H.T.; Methodology, A.K., V.C.T. and T.H.T.; Project administration, T.H.T.; Software, A.K. and V.C.T.; Supervision, M.F., V.N.Q.B. and T.H.T.; Validation, A.K. and T.H.T.; Writing–original draft, A.K.; Writing–review & editing, A.K., M.F., V.N.Q.B. and T.H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Japan Science and Technology Agency (JST) under Strategic Basic Research Programs Precursory Research for Embryonic Science and Technology (PRESTO) under grant number JPMJPR20M6.

Data Availability Statement: The developed code of Vacchain is public in our lab on GitHub: Vacchain-Frontend: https://github.com/OMU-BlockchainLab/vaccine-chain-ui.git, accessed on 28 February 2023. Vacchain-Backend: https://github.com/OMU-BlockchainLab/vaccine-backend.git, accessed on 28 February 2023. The demo of Vacchain can be found here: https://www.youtube.com/watch?v=Gy-31vUumZg, accessed on 28 February 2023, showing how we use the system to transfer and track the vaccine.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BSV	Bitcoin Satoshi version
Dapp	distributed application
EVM	Ethereum virtual machine
IoMT	internet of medical devices
IoT	internet of things
POCT	point of care tools
P2P	peer-to-peer
SYS-MAN	system manager
VM	vaccine manufacturer
VAD	vaccine authorized distributor
VAO	vaccine approved organization

References

1. Fighting Counterfeit Pharmaceuticals: New Defenses for an Underestimated-and Growing-Menace. Available online: https://www.strategyand.pwc.com/gx/en/insights/2017/counterfeit-pharmaceuticals.html (accessed on 21 August 2022).
2. Sgueglia, K. 15 People Face Charges in Connection to a Conspiracy with Fake COVID-19 Vaccine Cards, DA Says. Available online: https://edition.cnn.com/2021/08/31/us/manhattan-charges-covid-vaccine-card-scheme/index.html (accessed on 3 August 2022).
3. Shuster, S. 'Tip Of the Iceberg': Interpol Says Fake COVID-19 Vaccines Were Smuggled Across Continents. Available online: https://time.com/5943581/interpol-face-covid-vaccine/ (accessed on 20 June 2022).
4. A Passport to Freedom? Fake COVID-19 Test Results and Vaccination Certificates Offered on Darknet and Hacking Forums. Available online: https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/ (accessed on 11 January 2023).
5. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.
6. Sadeghi, M.; Mahmoudi, A.; Deng, X. Adopting distributed ledger technology for the sustainable construction industry: evaluating the barriers using Ordinal Priority Approach. *Environ. Sci. Pollut. Res.* **2022**, *29*, 10495–10520.
7. Porat, A.; Pratap, A.; Shah, P.; Adkar, V. *Blockchain Consensus: An Analysis of Proof-of-Work and Its Applications*; Stanford University: Stanford, CA, USA, 2017. Available online: https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf (accessed on 11 January 2023).
8. King, S.; Nadal, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-Publ. Pap. August* **2012**, *19* .
9. Gao, S.; Yu, T.; Zhu, J.; Cai, W. T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm. *China Commun.* **2019**, *16*, 111–123. [CrossRef]
10. Buterin, V. Ethereum: A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–36.
11. Substrate Documentation. 2023. Available online: https://docs.substrate.io/ (accessed on 11 January 2023).
12. Wood, G. Polkadot: Vision for a heterogeneous multi-chain framework. *White Pap.* **2016**, *21*, 2327–4662.
13. Willis, D.E.; Andersen, J.A.; Bryant-Moore, K.; Selig, J.P.; Long, C.R.; Felix, H.C.; Curran, G.M.; McElfish, P.A. COVID-19 vaccine hesitancy: Race/ethnicity, trust, and fear. *Clin. Transl. Sci.* **2021**, *14*, 2200–2207. [CrossRef] [PubMed]
14. Bullock, J.; Lane, J.E.; Shults, F.L.R. What causes COVID-19 vaccine hesitancy? Ignorance and the lack of bliss in the United Kingdom. *Humanit. Soc. Sci. Commun.* **2022**, *9*, 1–7.
15. 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 Proceedings of the 2020 IEEE Globecom Workshops, GC Wkshps 2020-Proceedings, Taipei, Taiwan, 7–11 December 2020. Available online: http://xxx.lanl.gov/abs/arXiv:2011.01468v1 (accessed on 12 June 2022).
16. The Aura Blockchain Consortium. Available online: https://auraluxuryblockchain.com/ (accessed on 13 October 2022).
17. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 May 2019; pp. 184–193.
18. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. [CrossRef]
19. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G. Optimized Blockchain Model for Internet of Things based Healthcare Applications. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 135–139. . [CrossRef]
20. Aileni, R.M.; Suciu, G. IoMT: A Blockchain Perspective. In *Decentralised Internet of Things: A Blockchain Perspective*; Khan, M.A., Quasim, M.T., Algarni, F., Alharthi, A., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 199–215. [CrossRef]

21. Bakalos, N.; Kaselimi, M.; Doulamis, N.; Doulamis, A.; Kalogeras, D.; Bimpas, M.; Davradou, A.; Vlachostergiou, A.; Fotopoulos, A.; Plakia, M.; et al. STAMINA: Bioinformatics Platform for Monitoring and Mitigating Pandemic Outbreaks. *Technologies* **2022**, *10*, 63.
22. 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.
23. Abbas, K.; Afaq, M.; Ahmed Khan, T.; Song, W.C. A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry. *Electronics* **2020**, *9*, 852. [CrossRef]
24. Antal, C.; Cioara, T.; Antal, M.; Anghel, I. Blockchain Platform For COVID-19 Vaccine Supply Management. *IEEE Open J. Comput. Soc.* **2021**, *2*, 164–178. [CrossRef]
25. VXPASS Website. 2022. Available online: https://vxpass.com/ (accessed on 31 January 2023).
26. Sim, C.; Zhang, H.; Chang, M.L. Improving End-to-End Traceability and Pharma Supply Chain Resilience with Blockchain. *Blockchain Healthc. Today* **2022**, *5*. [CrossRef]