Hindawi
Security and Communication Networks
Volume 2022, Article ID 4769187, 16 pages
https://doi.org/10.1155/2022/4769187

Research Article

Blockchain-Based Privacy-Preserving Vaccine Passport System

Yangzhou Cao,[1] Jiageng Chen ,[2] and Yajun Cao[3]

[1]*Central China Normal UniversityWollongong Joint Institute, Central China Normal University Wuhan, Wuhan, China*
[2]*School of Computer, Central China Normal University Wuhan, Wuhan, China*
[3]*Yichang Center for Disease Control, Prevention Yichang, Yichang, China*

Correspondence should be addressed to Jiageng Chen; chinkako@gmail.com

Received 11 November 2021; Accepted 13 January 2022; Published 21 March 2022

Academic Editor: Weizhi Meng

In this study, we propose a blockchain-based privacy-preserving vaccine passport system for the global prevention and control of infectious diseases. The system operates a double-chain framework which consists of a public blockchain and a consortium blockchain. Among them, the combination of the immutability of the public blockchain and Internet of Things (IoT) technology in the supply chain ensures the openness and transparency of the cold chain logistics records of the vaccines covering the stages from auditing to the target vaccination hospitals. The system adopts the consortium blockchain to achieve the balance between the protection of users' vaccination privacy and auditing by the government departments. Specifically, a distributed system-based threshold signature is adopted in the vaccine qualification phase to resist collusion between the vaccine manufacturing company and vaccine approval institutions. The cryptographic tools such as the anonymous credentials, zero-knowledge protocols, and range proofs ensure that users do not disclose any private information other than proving that they have a legally valid vaccine passport when users display the vaccine passports to customs. At the same time, customs can apply various vaccine prevention policies based on the conditions on the specific vaccine passports. Regarding the security properties of the system, a formal security model is given along with the corresponding security proofs.

1. Introduction

With the outbreak of COVID-19 in early 2020, the global defense against the spread of COVID-19 has been severely tested. Following the outbreak, scientists, physicians, and vaccine manufacturers in various countries engaged in the development of vaccines for the coronavirus. On January 24, 2020, the Chinese Center for Disease Control and Prevention (CDC) successfully isolated the first coronavirus strain in China [1]. The National Pathogenic Microbial Resource Library released information and electron microscopy photos of this strain (Wuhan strain 01 of the novel coronavirus), as well as important authoritative information such as primers and probe sequences for nucleic acid detection of the novel coronavirus, all of which laid the foundation for vaccine development. On this basis, COVID-19 vaccines in each country were promoted from the R&D stage to the clinical trial stage. In the second half of 2020, COVID-19 vaccines developed in each country gradually were approved for marketing by various national approval authorities.

At the stage when COVID-19 vaccines were introduced into the market and society, vaccination would face social problems in various aspects. With the gradual introduction of COVID-19 vaccines, vaccine management and vaccination become important issues for national governments. Especially in emergency cases when the COVID-19 vaccine is not sufficient, it is vital for the privacy of vaccination information to be protected to prevent social conflicts. As the epidemic is effectively controlled in various regions, the people returning from various countries and regions are also a serious test for the prevention and control of the local epidemic. Therefore, the application of vaccine passports was born.

As countries around the world gradually recovered from the effects of the COVID-19 epidemic, urgent cultural communication and trade between countries led to the implementation of vaccine passports. On July 26, 2021,

municipalities, wards, towns, and villages throughout Japan began accepting applications for the official certificate ("vaccine passport") for COVID-19 vaccine [2]. The key information of the vaccine certificate includes the individual's name, date of birth, passport number, type of vaccine used, and date of vaccination. The idea is that the certificates exempt travelers from Japan from quarantine and other antivirus measures after their arrival in overseas destinations. However, the Japanese government does not make such exemptions for people who enter Japan with vaccine passports issued by other nations for now, and the government is considering making vaccine passports digital. At 1 : 00 p.m. Vancouver time on August 23, the Premier of British Columbia held a press conference to announce the implementation rules for the British Columbia vaccine certificate. Starting from September 13, people attending indoor concerts, sporting events, movie theaters, and other nondiscretionary activities must receive at least one dose of the COVID-19 vaccine and show proof of it. On October 24, the vaccination requirement will be increased to 7 days after completing two doses of the vaccine before being allowed to enter certain public places with a vaccination card [3].

The vaccine passport should be an internationally recognized certificate of vaccination for COVID-19 [4] and possibly other types as well. In February 2021, the concept of the vaccine passport was still in the initial stages of controversy, and international opinion was divided. In the view of proponents, the emergence, use, and popularity of a vaccine passport would significantly mitigate the impact of the COVID-19 pneumonia outbreak on international travel and facilitate global economic recovery. In contrast, in the view of opponents, it is far from simple to establish a globally circulating and mutually recognized certification system that can effectively protect the privacy and ensure fairness.

The purpose of this study is to design protocols to ensure the transparency and privacy of vaccination, as well as the privacy of vaccine passports through the technology of cryptography to address the issues of privacy protection. However, we point out that the vaccine passports are subjected to a global consensus. It assumes that the design, implementation, and operation of the vaccine passport system should be supported and accepted by countries around the world.

1.1. Prior and Related Work. COVID-19 outbreak led to research on vaccine supply chain improvements. Many researchers in cryptography proposed blockchain-based systems for the distribution and management of vaccine supply chains. The idea is to take advantage of the nontamperability of blockchain, and the nature of jointly maintaining a unified ledger to ensure the supply of vaccines is regulated and transparent. Meanwhile, with the update and development of IoT technology, IoT in the field of traditional commodity logistics has been migrated to the field of logistics and transportation of pharmaceutical products. Among them, the monitoring and supervision of environmental conditions of vaccines belonging to biological products in the process of cold chain logistics transportation can combine IoT devices with sensors. Specific sensors feedback to the CDC, which monitors the logistics of biologics, about the humidity, temperature, light protection, and other transport conditions during the cold chain transportation of vaccines. As vaccination users, they also own the right to know that vaccine production and transportation meet quality control. Cui et al. [5] proposed a blockchain-based vaccine tracking system to protect the entire vaccine cycle. The blockchain is used as a global, unique, and verifiable database to store all circulating databases. Antal et al. [6] used Ethernet's smart contract technology to achieve the integrity of guaranteed vaccine data and the immutability of registration for vaccinators, avoiding identity theft and imitation. Yong et al. [7] applied machine learning techniques to analyze and process data in the vaccine blockchain.

Abid's proposed vaccine platform [8] provides a sovereign user identity that gives users full control over their data and encrypts personally identifiable information to enhance privacy. The platform also leverages W3C verifiable credential standards to facilitate instant verification of COVID-19 proofs and allow users to share selected information with trusted parties. However, the platform's privacy is protected by hashing sensitive information and then storing it on the blockchain, which is at risk when the data are broadcasted. Haque et al. [9], the authors proposed an architectural framework of a permission blockchain-based vaccination passport for the European Union's General Data Protection Regulations (GDPR). The scope of this regulation is broad, and any organization that collects, transfers, retains, or processes personal information involving all EU member states is subject to the regulation. Then, the double-chain structured blockchain system proposed by Qiu and Zhu [10] combines a public blockchain and a private blockchain to manage and store data information in different processes of vaccine logistics and vaccination. However, the user privacy of this system relies too much on the authorization mechanism of the private blockchain.

1.2. Contributions. In this study, we propose a double-chain framework with the vaccine cold chain logistics system and vaccination record system. We introduce threshold signature technology at the vaccine audit stage of public blockchain to deal with complicity between vaccine manufacturing companies and vaccine approval institutions. Second, it applies the consortium blockchain to record the information of vaccination hospitals to give vaccination to users. Its process ensures the privacy of vaccination hospitals, vaccination users, and vaccination vaccines and reserves the right to reveal and audit the vaccination information records by government departments under special circumstances.

In the issuance and presenting of the vaccine passport, the use of anonymous credential, ring signature, and range proofs ensures that the validity of the vaccine passport is proven without revealing the user's vaccination hospital and identity information during the process.

1.3. Paper Organization. In the subsequent content of this study, we present the entities and the system threat model in the vaccine passport system in Section 2. We show the cryptographic techniques and tools used to build the system protocol in Section 3. Section 4 of this article provides the structural design of the system and the specific protocol design. We give the security analysis and proof of the protocols in this model in Section 5. We give a system evaluation in Section 6, and we finally conclude this article in Section 7.

2. Assumptions and Threat Model

2.1. Entities and Assumptions. Before presenting the system structure, we introduce the entity participants in the system.

(i) International coalition government, $\mathcal{GV}$: it acts as the system's CA to manage the authorization and authentication of each participant. It acts as a trusted third party for threshold signatures in the vaccine approval process. In exceptional cases, it can audit the encrypted information in the consortium blockchain that records vaccinations.

(ii) Hospital, $\mathcal{HOSP}$: it issues a credential for the user's vaccine passport after completion of the vaccination and uploads the information recording the vaccination to the consortium blockchain.

(iii) User: the user receives a vaccine passport after completion of vaccination at the hospital. When it is necessary to prove the legitimacy and validity of the vaccine passport to the vaccine passport checkpoint, zero-knowledge proof protocol is applied to protect their privacy.

(iv) Vaccine manufacturing company: it sends samples of the vaccine to be tested to the vaccine approval institutions in each country for approval. Once the vaccine is approved, the batch is issued a certificate of authorization.

(v) Vaccine approval institutions, $\mathcal{AI}$: each country's approval body tests the submitted vaccine samples according to its own standards. The approved vaccine approval institution signs a threshold signature for the vaccine. The $\mathcal{GV}$ issues a threshold signature certificate to the vaccine lot after (t, n) vaccine approval institutions have been met and approved simultaneously.

(vi) Vaccine passport checkpoint: it verifies the user's identification and proof of the legitimacy and validity of the vaccine passport. It also takes the appropriate vaccination measures and policies for the fulfillment of the conditions of the user's vaccine passport.

(vii) Vaccine transit centers: they act as a transit point for vaccine shipments connecting vaccine companies to the CDC. Information on storage and transport conditions during cold chain logistics is uploaded.

(viii) CDC: it audits the vaccine cold chain logistics process for compliance with biologics-related regulations. If so, the vaccine is held in temporary storage and eventually shipped to the hospital where it is administered.

Considering the specific prerequisite assumptions for the application of the vaccine passport system to realistic scenarios and specific programs, the system provides the following reasonable assumptions.

(i) The authority of the international coalition government is recognized by every country in the world

(ii) Countries strictly adhere to the normal operation of the system

(iii) The number of corrupted institutions in vaccine approval institutions is less than half of the total number

(iv) Authorized hospitals follow the hospital code of conduct and do not conspire with users

(v) Users do not disclose or share their secret keys

2.2. Threat Model. In this study, we do not consider network-level security attacks, physical hardware-level damage, and software vulnerability penetration during the engineering implementation of the protocol. In this study, we only consider cryptographic attacks towards the protocol design.

(i) In the threat model of this study, we assume that $\mathcal{GV}$ and auditor are completely honest. They operate according to the protocol algorithm and do not disclose the privacy parameters generated.

(ii) In the threshold signature phase, adversary is allowed to corrupt up to $t < n/2\mathcal{AI}$ s. $\mathcal{GV}$ does not disclose institutional audit signatures to vaccine manufacturing companies.

(iii) In the vaccination information record uploading consortium blockchain phase, all peers except the auditor and $\mathcal{GV}$ are assumed to be honest-but-curious; they try to break the privacy by passively eavesdropping on the inputs and outputs of the protocol but not actively violating the protocol process.

(iv) In the vaccine passport display phase, vaccine passport checkpoint is assumed to be honest-but-curious; it tries to get the user's private data, but it still follows the protocols.

3. Preliminaries

3.1. Bilinear Pairing. Let e: $\mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ a bilinear map where $\mathbb{G}_1$ is a GDH group and $\mathbb{G}_1 \neq \mathbb{G}_2$ in our protocol. $\mathbb{G}_1, \mathbb{G}_2$ are the two multiplicative cyclic groups of prime order q. The bilinear pairing e: $\mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ has the following three properties:

(i) Bilinear: for all $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$, and $\alpha, \beta \in \mathbb{Z}_q$, it holds that $e(g_1^{\alpha}, g_2^{\beta}) = e(g_1, g_2)^{\alpha\beta}$;

(ii) Computability: there exists an efficient algorithm to calculate $e(g_1, g_2)$, where $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$;

(iii) Nondegenerate: $e(g_1, g_2) \neq 1$ for $\exists g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$, where 1 is the unit element in the multiplicative cyclic group.

3.2. q-Strong Diffie–Hellman Assumption. The q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined that for adversary $\mathscr{A}$ on input a $(q+2)$-tuple $(g_1, g_2, g_2^x, g_2^{x^2}, \ldots, g_2^{x^q}) \in \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$

$$\Pr\left[\begin{array}{c} A = g_1^{1/(x+c)}: \\ (A, c) \longleftarrow \mathscr{A}\left(g_1, g_2, g_2^x, g_2^{x^2}, \ldots, g_2^{x^q}\right) \end{array}\right] \leqslant negl(\lambda). \quad (1)$$

3.3. Threshold Signature Scheme. The (t, n) threshold signature scheme allows any t signers among n signers to generate a signature for a message, but less than t signers participate to generate a valid signature. The threshold signature scheme can build a robust signature system to prevent the unlawful behavior of some signers. The threshold signature scheme consists of the following four algorithms:

(i) ThresholdKeyGen (λ, n, t): for distributed systems, threshold key generation algorithm is a protocol that runs interactively among many participants. With the input security parameters λ, number of users n, and threshold t, it outputs the secret share x_i for each participant, such that $(x_1, \ldots, x_n) \longrightarrow (t, n)$ sk.

(ii) Sign (x_i, m): the signers in the participants output the signature share σ_i based on the input secret share x_i and the message m.

(iii) Reconstruction (σ_i): the resulting signature σ can be generated by a trusted third party based on the signature share σ_i of not less than t signers.

(vi) Verify (pk, m, σ): the verification algorithm inputs the verification public key pk, message m, and resulting signature σ and outputs 1 when the signature is successfully verified; otherwise, it outputs 0.

3.4. Ring Signature Scheme. A ring signature is a digital signature that can be executed by any member of a group of users that each have a pair of keys, so that a message with a ring signature is recognized by someone in a particular group. But, it is computationally infeasible to determine which group member's key is used to generate the signature, which is one of the security properties of ring signatures. All possible signers are formed into a ring. Each possible signer is called a ring member. The ring member that generates the signature is called a signer, and each other ring member is called a nonsigner. The ring signature scheme consists of the following three algorithms:

(i) KeyGen (λ, n): let ring $R = \{R_1, \ldots, R_n\}$. With the input security parameters λ, it outputs each user public-secret key pair $(\mathrm{sk}_i, \mathrm{pk}_i)$. Assume that the signing member is R_s.

(ii) Sign $(\mathrm{sk}_s, m, \{\mathrm{pk}_i\}_{i\in\{1,\ldots,n\}, i\neq s})$: the signer R_s generates a ring signature σ_{ring} on message m with its own secret key sk_s and the public keys $\{\mathrm{pk}_i\}$ of other members.

(iii) Verify $(\{\mathrm{pk}_i\}_{i\in\{1,\ldots,n\}}, m, \sigma_{\mathrm{ring}})$: the verification algorithm is with the input of public keys $\{\mathrm{pk}_i\}_{i\in\{1,\ldots,n\}}$, message m, and ring signature σ_{ring} and outputs 1 when the signature is successfully verified; otherwise, it outputs 0.

3.5. Zero-Knowledge Proof. A zero-knowledge proof is a protocol that the prover P can convince the verifier V that an argument is correct without providing any useful information to the verifier. A zero-knowledge proof is essentially an agreement involving two or more parties, i.e., a series of steps that two or more parties need to take to accomplish a task. The prover convinces the verifier that he or she knows or has a certain message, but the proof process cannot divulge any information about the proven message to the verifier. In our system protocol design, we focus on zero-knowledge proof for NP language $L_R = \{y | \exists \omega \ s.t. \ (y, \omega) \in R\}$, where ω is a witness for statement y. A zero-knowledge proof protocol between P and V satisfies the following three properties:

(i) Completeness: if $y \in L_R$, prover P convinces V that his statement is true with probability $1 - \mathrm{negl}(\lambda)$.

(ii) Soundness: if the prover's statement $y \notin L_R$, then any malicious prover P^* convinces an honest verifier of his statement with probability $\mathrm{negl}(\lambda)$.

(iii) Honest verifier zero-knowledge (HVZK): after the proof is executed, the verifier only knows whether the statement of the verifier is true or not, but he does not have access to any other information during the proof. It can also be said that there exists a simulator algorithm Sim that simulates interaction scripts that are nondistinguishable with the real interaction scripts between P and V.

Range proof: range proof is proof that a secret value x, which is encrypted or committed to, lies in a certain interval $[a, b]$. In this study, the secret value x is hidden by Pedersen commitment, such that $C = g^x h^r$. Range proof does not leak any information about the secret value other than the fact that they lie in the interval. The prover needs to provide zero-knowledge proof to the verifier $\mathrm{PK}\{(x, r): C = g^x h^r \wedge x \in [a, b]\}$.

4. Our Proposed System

Before showing the overview of our system model, we present the reasons for choosing the double chain as the basis of the system. The generation of the vaccine passport and the vaccine itself are indivisible. Given the biomedical properties of the vaccine itself, we need a public blockchain to store the production and logistics information of the

vaccine. The choice of the consortium blockchain is that vaccination records are information with privacy properties and are required to be privacy protected and regulated. So, it is uncomplicated to achieve the intended effect in a blockchain under authorization.

4.1. Overview. Our system consists of three main phases in the vaccine cold chain logistics phase, as shown in Figure 1.

Step 1. It is for the vaccine manufacturing company to send a batch of vaccine samples that need to be checked to ensure quality to the vaccine approval institutions in each country.

Step 2. It consists of each country's vaccine approval institution passing its review results through a (t, n) threshold (if a total of n vaccine approval institutions are satisfied with the approval of t vaccine approval institutions, then the batch of vaccine is approved). If the batch meets the audit requirements, a certificate is issued for the batch through the threshold signature.

Step 3. It is that the vaccine manufacturing company entrusts the cold chain logistics company with the approved batch of vaccine to send to the target hospital. The sender is the vaccine production company. The receiver is the first vaccine transit center. The transported goods are batches of vaccines. The logistics information is uploaded to the public blockchain after the logistics are completed.

Step 4. It is the uploading of cold chain logistics information between vaccine transfer centers. The sender is the previous vaccine transfer center. The receiver is the next vaccine transfer center. The transported goods are batches of vaccines with the environmental conditions of the temporary storage of vaccines and the signature of the person in charge.

Step 5. It is when the vaccine is delivered at the last logistics transit center; the CDC under whose jurisdiction the target hospital is located audits the entire cold chain logistics storage and transportation for compliance with the logistics requirements for biologics. If the batch of the vaccine cold chain logistics process meets the requirements, the CDC issues a certificate of conformity signature to the batch of vaccine.

Step 6. It is to upload the logistics information between the last vaccine transfer center and the CDC to the public blockchain after the approval of the vaccine cold chain logistics. The sender is the last vaccine transfer center. The receiver is the local CDC, and the transported goods are batches of vaccines with the CDC's certificate for vaccine cold chain logistics.

Step 7. It is to upload the logistics information of the final vaccine delivery from the local CDC to the target hospital to the public blockchain. The sender is the local CDC, and the receiver is the target vaccination hospital. The transported goods are batch of vaccines with a certificate from the CDC for the cold chain logistics of the vaccine and a threshold signature certificate from the vaccine approval institutions. Users are given the right and ability to know the approval results of vaccinations and vaccine cold chain logistics information by viewing the information recorded on the public blockchain before vaccination in hospitals. This helps to achieve openness and transparency of vaccine information to vaccination users.

In the vaccination phase shown in Figure 2, the local hospital completes the uploading of vaccination information to the consortium blockchain while protecting the privacy of the vaccination information.

Step 8. It is after the last injection of the user's vaccine at the local hospital, the hospital creates vaccination information signed by it and sends the vaccination information to the endorser. The sender of the vaccination information is the local hospital. The receiver is the vaccination user. The information transmitted is the details of the vaccine.

Step 9. It is for the endorser to verify the uploaded vaccination information and generate an endorsement signature.

Step 10. It is that the submitting local hospital broadcasts the collected endorsement signatures and the vaccination information itself to the orderers.

Step 11. It is for orderers to broadcast the sorted set of vaccination information to all peers.

Step 12. It is for the committing peer to check if the vaccination information submitted by the orderers has a legitimate certificate issued by the endorser. The committing peer also detects malicious cases where the same vaccination is included in the vaccination information more than once. In this case, the first valid vaccination information will be accepted. Once the uploaded vaccination information is verified by the committing peer, the vaccination information is submitted and the committing peer maintains the state and a copy of the ledger. For the privacy-preserving vaccination information on the consortium blockchain, it is necessary to audit it in case of special circumstances. Auditors have the ability to open the encrypted vaccination information on the consortium blockchain to audit the vaccination details, such as the time of vaccination and vaccine production date.

In the vaccine passport phase in Figure 2.

Step 13. It is where the local hospital opens the vaccination user's commitment to the vaccine production date, vaccine shelf life, vaccine immunity lasting time, and vaccination date. After the hospital confirms that the commitment is correct, a ring signature is generated for the commitment and the international coalition government-issued user identity card. Finally, the ring signature, commitment, and user identity certificate together form the vaccine passport and are sent to the user.

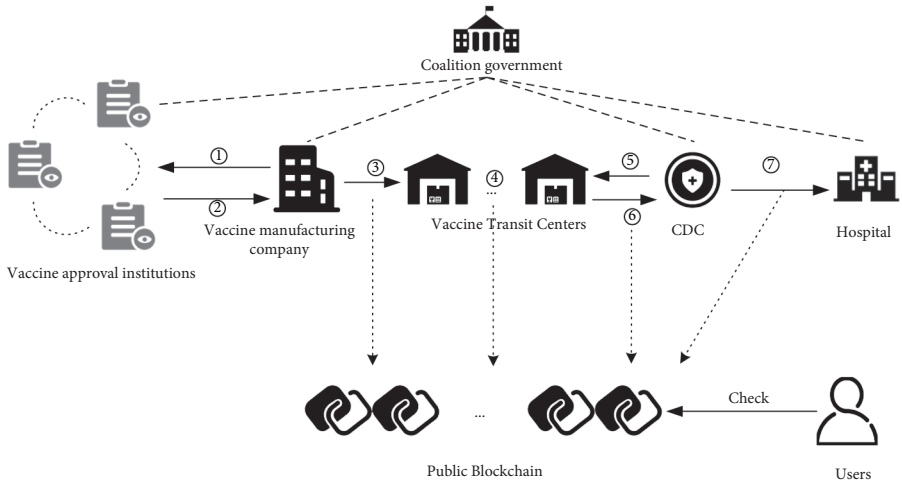

Figure 1: Vaccine cold chain logistics phase.

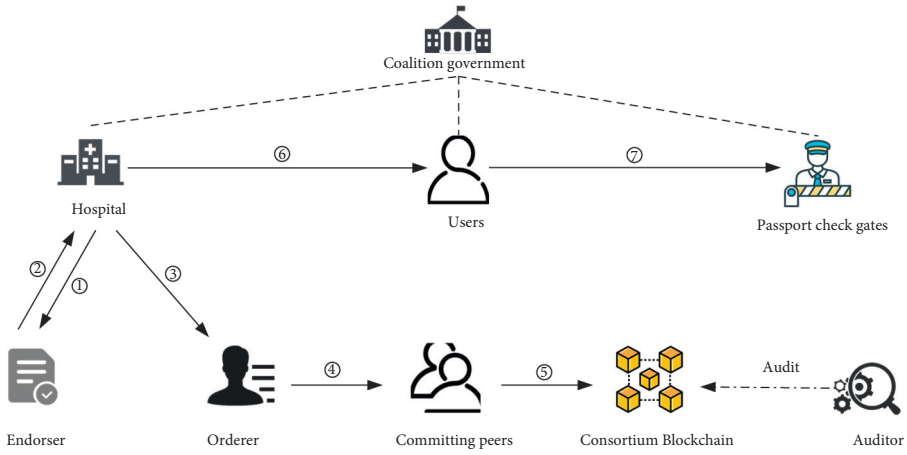

Figure 2: Vaccination and vaccine passport phase.

Step 14. It is for the user to first present the vaccine passport to the passport checkpoint. The passport checkpoint verifies the legitimacy of the user's identity and vaccine passport. Next, the user proves the validity of the vaccine passport to the passport checkpoint. This includes the following three items:

(i) The vaccine injected by the user is within the shelf life. If the vaccine injected by the user does not meet this condition, then first, the passport checkpoint needs to report this medical issue to a government authority. This requires a request for an audit of the vaccination information for the batch (including the local vaccination hospital) and a traceability audit of the vaccine batch. Also, the user needs to be reimbursed for the corresponding vaccination.

(ii) The user produces high titers of antibodies to create effective protection. This corresponds to the last date of vaccination plus 14 days [11], which needs to be greater than the current date. If the user's vaccination information does not meet this condition, the passport checkpoint needs to take a quarantine for 14 days before allowing the user to pass.

(iii) The vaccinated user is in the duration of immunization for the vaccine. This is equivalent to the last date of vaccination plus the vaccine immunity lasting time that needs to be less than the current date. If the user's vaccination information does not meet this condition, the passport control point will need to adopt the vaccine again to stimulate an effective antibody prevention strategy.

None of the above proofs will reveal any information about the user's vaccination, including the production date and shelf life of the vaccine.

4.2. Vaccine Cold Chain Logistics. This study adds Boldyreva's [12] threshold signature technique to other blockchain-based vaccine distribution management systems. Vaccine approval institutions in each country that adopt different standards act as participants in the threshold signature. The international coalition government acts as a trusted third

party as the group administrator in the threshold signature group. This vaccine approval protocol effectively prevents collusion and corruption between vaccine approval institutions and vaccine manufacturing companies. The vaccine approval institutions approve samples of vaccines to be submitted for review in a distributed structure on a per-share basis. The distributed protocol allows for up to half of the vaccine approval institutions to be malicious. Once the approval of the submitted vaccine is complete, the vaccine manufacturer receives only the results of whether the submitted vaccine batch was approved or not and does not know the respective review opinions of the individual vaccine approval institutions. This prevents the vaccine manufacturing company from influencing the outcome of the approval, thereby, achieving fairness and equity in vaccine approval. Details are outlined as follows.

Setup (1^λ): on input 1^λ, where $\lambda \in \mathbb{N}$ is a security parameter, let e: $\mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$, a bilinear map, where $\mathbb{G}_1$ is a GDH group and g is the generator of $\mathbb{G}_1$. $\mathbb{G}_2$ and $\mathbb{G}_T$ are the cyclic groups. The participants in our scheme are the set of n vaccine approval institutions $\{\mathscr{AI}_1, \ldots, \mathscr{AI}_n\}$. All $\mathscr{AI}$s are connected by a broadcast channel as well as by secure point-to-point channels including the international coalition government $\mathscr{GV}$. Let H: $\{0,1\}^* \longrightarrow \mathbb{G}_2$ be collision-resistant hash function.

Generating x $(f_i(y), f_i'(y))$: $\mathscr{AI}_i$ chooses $a_{i0}, \ldots, a_{it} \xleftarrow{R} \mathbb{Z}_p$ and $a_{i0}', \ldots, a_{it}' \xleftarrow{R} \mathbb{Z}_p$ to form the polynomials $f_i(y)$ and $f_i'(y)$ of degree t: $f_i(y) = a_{i0} + a_{i1}y + \cdots + a_{it}y^t$ and $f_i'(y) = a_{i0}' + a_{i1}'y + \cdots + a_{it}'y^t$. $\mathscr{AI}_i$ broadcasts commitment to polynomial coefficients $C_{ik} = g^{a_{ik}}h^{a_{it}'} \bmod p$ for $k \in \{0, \ldots, t\}$. $\mathscr{AI}_i$ computes $s_{ij} = f_i(j)$ and $s_{ij}' = f_i'(j) \bmod q$ for $j \in \{1, \ldots, n\}$ and sends s_{ij} and s_{ij} to $\mathscr{AI}_j$ to verify. Then, each $\mathscr{AI}_j$ verifies if

$$g^{a_{ik}}h^{a_{it}'} = \prod_{k=0}^{t} (C_{ik})^{j^k}. \tag{2}$$

If the above equation is not satisfied, $\mathscr{AI}_j$ will broadcast the complaint against $\mathscr{AI}_i$. According to the conditions satisfied by the distributed key generation protocol DKG for discrete-log based systems of Gennaro et al. [13], each $\mathscr{AI}_i$ sets his share of the secret as $x_i = \sum_{j \in \mathrm{QUAL}} s_{ij} \bmod q$. The distributed secret value x equals $x = \sum_{i \in \mathrm{QUAL}} a_{i0} \bmod q$ from the distributed secret polynomial:

$$F(y) = \sum_{i \in QUAL} a_{i0} + \left(\sum_{i \in QUAL} a_{i1}\right)y + \cdots + \left(\sum_{i \in QUAL} a_{it}\right)y^t. \tag{3}$$

Vaccine approval (x_i): $\mathscr{AI}_i$ decides whether to approve the batch of vaccine according to the criteria. If $\mathscr{AI}_i$ approves it, a signature $\sigma_i = H(\text{vaccine})^{\text{xi}}$ and $\mathrm{pk}_i = g^{x_i}$ are generated and sent to $\mathscr{GV}$. $\mathscr{GV}$ verifies the signature by $e(g, \sigma_i) = e(\mathrm{pk}_i, H(\text{vaccine}))$. If the verification passes, $\mathscr{AI}_i$ is assigned to the set APPR.

Threshold signature (σ_i): if the number of $\mathscr{AI}_i$s in set APPR is greater than t,

$$LB_j(y) = \prod_{k=0,k!=j}^{t} (y - y_k)/(y_j - y_k), \tag{4}$$

is public Lagrange coefficient for the set APPR according to the Lagrange interpolation method [13].

$$\begin{aligned} x &= \sum_{i \in \mathrm{QUAL}} a_{i0} = \sum_{i \in \mathrm{QUAL}} \left(\sum_{j \in \mathrm{APPR}} \mathrm{LB}_j(0) \cdot s_{ij} \right) \\ &= \sum_{j \in \mathrm{APPR}} \mathrm{LB}_j(0) \cdot x_j. \end{aligned} \tag{5}$$

According to the above equation, the resulting signature is that $\sigma_{\text{vaccine}} = \prod_{i \in \mathrm{APPR}} (\sigma_i^{\mathrm{LB}_i(0)}) = H(\text{vaccine})^x$ and public key is that $\mathrm{pk} = \prod_{i \in \mathrm{APPR}} (\mathrm{pk}_i^{\mathrm{LB}_i(0)}) = g^x$.

User verification $(\sigma_{\text{vaccine}}, \mathrm{pk}, \text{vaccine})$: the user checks that $e(g, \sigma_{\text{vaccine}}) \stackrel{?}{=} e(\mathrm{pk}, H(\text{vaccine}))$ for the vaccine. The user accepts the signature if $e(g, \sigma_{\text{vaccine}}) = e(\mathrm{pk}, H(\text{vaccine}))$ holds or rejects it otherwise.

Logistics consignment $(\sigma_{\text{vaccine}}, \text{vaccine})$: structure of vaccine includes the following attributes: ID = H(manufacturer, batch number, serial number), manufacturer, batch number, serial number, vaccine certificate σ_{vaccine}, production date x_p, shelf life x_s, and the duration of immunization x_d. The vaccine manufacturing company broadcasts the vaccine properties, the entrusted logistics company, and the certification certificate $\sigma_{vaccine}$ as a package to the public blockchain.

Cold chain logistics transit $(\sigma_{\text{vaccine}}, \text{vaccine}, \sigma_r)$: the responsible person for the cold chain logistics staging area broadcasts to the public blockchain the vaccine, the vaccine storage environment, its signature σ_r, and the logistics destination package.

Distribution of CDC $(\text{public blockchain}, \mathrm{sk}_{\mathrm{CDC}})$: after checking that the cold chain logistics on the public blockchain meets the standards for transporting biologics, the CDC attaches a signature $\sigma_{C\ DC}$ and broadcasts the distribution to the destination vaccination hospital to the public blockchain.

4.3. Vaccination Record. The framework of the vaccination record system is based on Hyperledger Fabric [14], which is a permissioned blockchain. The privacy protections of the identity of the vaccination hospitals and vaccination users in the vaccine record system are referred to the technique of one-time sender and receiver public key in PAChain [15]. The certificate of authority for the long-term public key (representing the identity of the hospital and the user) of the vaccination hospital and the vaccination user uses the BBS + signature [16] issued by the international joint government. However, in the vaccination record system of this study, the identity of the user and hospital is anonymous to the endorsement node. The endorsement of the vaccination record by the endorsing node uses the anonymous credential technique based on the Boneh-Boyen signature [17]. Vaccination information is encrypted with the auditor's public key using ElGamal encryption [18] to ensure that the

information is hidden. If necessary, the auditor can reveal the encrypted vaccination information with his or her secret key. Details are outlined as follows.

(param)$\longleftarrow$ **Setup** (1^λ): on input 1^λ, where $\lambda \in \mathbb{N}$ is a security parameter. Suppose H_1: $\{0,1\}^* \longrightarrow \{0,1\}^{128} \in \mathbb{Z}_p$ and H_2: $\mathbb{G}_1 \longrightarrow \mathbb{Z}_p$ are collision-resistant hash functions. It randomly picks generators $g_0, g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_u, g_h \in G_1, \widehat{g}_1, \widehat{g}_2, \widehat{g}_e \in G_2$.

$(\mathrm{sk}_{\mathrm{vc}}, \mathrm{sk}_{\mathrm{re}}, \mathrm{sk}_{\mathrm{sd}}, \mathrm{pk}_{\mathrm{vc}}, \mathrm{pk}_{\mathrm{re}}, \mathrm{pk}_{\mathrm{sd}})\longleftarrow$ **AuditorKeyGen():** auditor picks random secret keys $\mathrm{sk}_{\mathrm{vc}}, \mathrm{sk}_{\mathrm{re}}, \mathrm{sk}_{\mathrm{sd}} \xleftarrow{R} \mathbb{Z}_p$ and outputs their public keys $\mathrm{pk}_{\mathrm{vc}} = g_1^{\mathrm{sk}_{\mathrm{vc}}}, \mathrm{pk}_{\mathrm{re}} = g_2^{\mathrm{sk}_{\mathrm{re}}}, \mathrm{pk}_{\mathrm{sd}} = g_3^{\mathrm{sk}_{\mathrm{sd}}}$.

$(\mathrm{sk}_{\mathrm{CA},U}, \mathrm{pk}_{\mathrm{CA},U}, \mathrm{sk}_{\mathrm{CA},H}, \mathrm{pk}_{\mathrm{CA},H})\longleftarrow$ **CAKeyGen():** CA picks random secret keys $\mathrm{sk}_{\mathrm{CA},U}, \mathrm{sk}_{\mathrm{CA},H} \xleftarrow{R} \mathbb{Z}_p$ and outputs their public keys $\mathrm{pk}_{\mathrm{CA},U} = \widehat{g}_1^{\mathrm{sk}_{\mathrm{CA},U}}, \mathrm{pk}_{\mathrm{CA},H} = \widehat{g}_2^{\mathrm{sk}_{\mathrm{CA},H}}$.

$(\mathrm{sk}_e, \mathrm{pk}_e)\longleftarrow$ **EndorserKeyGen():** endorser picks random a secret key $\mathrm{sk}_e \xleftarrow{R} \mathbb{Z}_p$ and outputs its public key $\mathrm{pk}_e = \widehat{g}_e^{\mathrm{sk}_e}$.

$(\mathrm{sk}_{U,1}, \mathrm{sk}_{U,2}, \mathrm{pk}_{U,1}, \mathrm{pk}_{U,2})\longleftarrow$ **UserKeyGen():** the user randomly picks a pair of long-term secret keys $\mathrm{sk}_{U,1}, \mathrm{sk}_{U,2} \xleftarrow{R} \mathbb{Z}_p$ and computes a pair of long-term public keys $\mathrm{pk}_{U,1} = g_4^{\mathrm{sk}_{U,1}}, \mathrm{pk}_{U,2} = g_4^{\mathrm{sk}_{U,2}}$. $\mathcal{HOSP}$ is also a type of user, so it follows the same algorithm to generate $(\mathrm{sk}_{H,1}, \mathrm{sk}_{H,2}, \mathrm{pk}_{H,1}, \mathrm{pk}_{H,2})$.

$(\mathrm{Cert}_{\mathrm{CA},U})\longleftarrow$ **CACertIssue** $(\mathrm{sk}_{\mathrm{CA}}, \mathrm{pk}_{U,1})$: first, the user needs proof to CA: $\mathrm{PoK}\{(\mathrm{sk}_{U,1})\colon \mathrm{pk}_{U,1} = g^{\mathrm{sk}_{U,1}}\}$. After passing CA verification, CA computes $A_{\mathrm{CA},U} = (g_u \cdot \mathrm{pk}_{U,1} \cdot g_5^{s_u})^{1/(\mathrm{sk}_{\mathrm{CA},U}+\omega_u)}$ using randomly selected $s_u, \omega_u \xleftarrow{R} \mathbb{Z}_p$ and its own $\mathrm{sk}_{\mathrm{CA},U}$. Then, CA issues a certificate $\mathrm{Cert}_{\mathrm{CA},U} = \{A_{\mathrm{CA},U}, s_u, \omega_u\}$ to the user's $\mathrm{pk}_{U,1}$. $\mathcal{HOSP}$ is also a type of user, so it follows the same algorithm to generate $(\mathrm{Cert}_{\mathrm{CA},H} = \{A_{\mathrm{CA},H} = (g_h \cdot \mathrm{pk}_{H,1} \cdot g_5^{s_h})^{1/(\mathrm{sk}_{\mathrm{CA},H}+\omega_h)}, s_h, \omega_h\})\longleftarrow$ **CACertIssue** $(\mathrm{sk}_{\mathrm{CA},H}, \mathrm{pk}_{H,1})$.

$(E_i, R_i, E, R_v, \pi_{\mathrm{enc}})\longleftarrow$ **VaccInfoEnc**(vaccination, $\mathrm{pk}_{\mathrm{vc}}$)**:** vaccination information includes ID = H (manufacturer, batch number, serial number), vaccine certificate $\sigma_{\mathrm{vaccine}}$, production date x_p, shelf life x_s, the date of vaccination x_v, and the duration of immunization x_d. Let $M = H_1$(vaccination), and it divides 128-bit M into 8 segments of 16-bit messages m_i by $M = \sum_{i=0}^{7} m_i \cdot (2^{16})^i$. It encrypts each m_i into $E_i = g_0^{m_i}\mathrm{pk}_{\mathrm{vc}}^{r_{v,i}}$ and $R_i = g_6^{r_{v,i}}$, where $r_{v,i} \xleftarrow{R} \mathbb{Z}_p$. The encryption E on M can be generated by $E = \prod_{i=0}^{7} E_i^{(2^{16})^i} = g_0^M \mathrm{pk}_{\mathrm{vc}}^{r_v}$ and $R_v = g_6^{r_v}$, where $r_v = \sum_{i=0}^{7} r_{v,i} \cdot (2^{16})^i$. The user sends E_i to the auditor. Then, it proves in zero-knowledge proof that the knowledge of $(m_i, r_{v,i})$ and (M, r_v): $\mathrm{PoK}\{(\{m_i, r_{v,i}\}_{i\in\{0,\ldots,7\}}, M, r_v)E_i = g_0^{m_i}\mathrm{pk}_{\mathrm{vc}}^{r_{v,i}} \wedge R_i = g_6^{r_{v,i}} \wedge E = g_0^M \mathrm{pk}_{\mathrm{vc}}^{r_v} \wedge R_v = g_6^{r_v}\}$.

Details of the zero-knowledge proof is as follows:

(1) The $\mathcal{HOSP}$ randomly picks $a_i, b_i \in \mathbb{Z}_p$ for $i \in \{0, \ldots, 7\}$ and $a, b \in \mathbb{Z}_p$ and then computes commitments: $C_{v,i} = g_0^{a_i}\mathrm{pk}_{\mathrm{vc}}^{b_i}, D_{v,i} = g_6^{b_i}$ and $C_v = g_0^a \mathrm{pk}_{\mathrm{vc}}^b, D_v = g_6^b$.

(2) It computes $c = H(\{E_i, R_i, C_{v,i}, D_{v,i}\}_{i\in\{0,\ldots\}}, E, R_v, C_v, D_v)$ and for $i \in \{0, \ldots 7\}$ computes challenge response: $z_{1,i} = a_i + \mathrm{cm}_i, z_{2,i} = b_i + \mathrm{cr}_{v,i}$, $z_1 = a + \mathrm{cM}$, $z_2 = b + \mathrm{cr}_v$.

(3) Then, it outputs $\pi_{\mathrm{enc}} = \{\{C_{v,i}, D_{v,i}, z_{1,i}, z_{2,i}\}_{i\in\{0,\ldots 7\}}, C_v, D_v, z_1, z_2, c\}$

$(\mathrm{otpk}_U, R_U)\longleftarrow$ **OTpkGen** $(\mathrm{pk}_{U,1}, \mathrm{pk}_{U,2})$: $\mathcal{HOSP}$ randomly picks $r_u \xleftarrow{R} \mathbb{Z}_p$ and outputs $(\mathrm{otpk}_U = \mathrm{pk}_{U,1} \cdot g_4^{H_2(pk_{U,2}^{r_u})}, R_U = g_4^{r_u})$. $\mathcal{HOSP}$ uses the same algorithm to generate $(\mathrm{otpk}_H = \mathrm{pk}_{H,1} \cdot g_4^{H_2(pk_{H,2}^{r_h})}, R_H = g_4^{r_h})\longleftarrow$ **OTpkGen** $(\mathrm{pk}_{H,1}, \mathrm{pk}_{H,2})$. $\mathcal{HOSP}$ encrypts user's long-term public key $\mathrm{pk}_{U,1}$ and long-term public key $\mathrm{pk}_{H,1}$ of $\mathcal{HOSP}$ to the auditor by picking random $r_{\mathrm{re}}, r_{\mathrm{sd}} \xleftarrow{R} \mathbb{Z}_p$ and computing $(E_{\mathrm{re}} = \mathrm{pk}_{U,1} \cdot \mathrm{pk}_{\mathrm{re}}^{r_{\mathrm{re}}}, R_{\mathrm{re}} = g_2^{r_{\mathrm{re}}})$ and $(E_{\mathrm{sd}} = \mathrm{pk}_{H,1} \cdot \mathrm{pk}_{\mathrm{sd}}^{r_{\mathrm{sd}}}, R_{\mathrm{sd}} = g_3^{r_{\mathrm{sd}}})$. Then, $\mathcal{HOSP}$ runs the following proof of knowledge for ensuring:

(i) $\mathrm{pk}_{U,1}$ and $\mathrm{pk}_{H,1}$ are issued a valid certificate of identity by CA.

(ii) otpk_U is generated by $\mathrm{pk}_{U,1}$. otpk_H is generated by $\mathrm{pk}_{H,1}$. otpk_U is the one-time public key identity of the user whose public key is $\mathrm{pk}_{U,1}$. otpk_H is the one-time public key identity of $\mathcal{HOSP}$ whose public key is $\mathrm{pk}_{H,1}$.

(iii) The user's long-term public key $\mathrm{pk}_{U,1}$ and $\mathcal{HOSP}$'s long-term public key $\mathrm{pk}_{U,1}$ are encrypted by the auditor's public key $\mathrm{pk}_{\mathrm{re}}$ and $\mathrm{pk}_{\mathrm{sd}}$.

$\mathcal{HOSP}$ needs to use proof of knowledge to endorser:

$$\mathrm{PoK}\Big\{\Big(A_{\mathrm{CA},U}, s_u, \omega_u, \mathrm{pk}_{U,1}, r_{\mathrm{re}}, H_2\big(\mathrm{pk}_{U,2}^{r_u}\big)\Big)\colon e\Big(A_{\mathrm{CA},U}, \widehat{g}_1^{\omega_u} \cdot \mathrm{pk}_{\mathrm{CA}}\Big) = e\Big(g_u \cdot \mathrm{pk}_{U,1} \cdot g_5^{s_u}, \widehat{g}_1\Big) \wedge \mathrm{otpk}_U = \mathrm{pk}_{U,1} \cdot g_4^{H_2\left(\mathrm{pk}_{U,2}^{r_u}\right)} \wedge R_U = g_4^{r_u} \wedge E_{\mathrm{re}} = \mathrm{pk}_{U,1} \cdot \mathrm{pk}_{\mathrm{re}}^{r_{\mathrm{re}}}\Big\}. \tag{6}$$

The details of the zero-knowledge proof is as follows:

(1) $\mathcal{HOSP}$ randomly picks $r_a, r_b, r_c, r_d, r_e, r_\alpha, r_\beta \xleftarrow{R} \mathbb{Z}_p$ and makes $\theta = A_{\mathrm{CA},U}^{r_a}$. It computes commitments: $C_{U,1} = e((g_u \cdot E_{\mathrm{re}})^{r_e} g_5^{r_\beta} \theta^{-r_c} \mathrm{pk}_{\mathrm{re}}^{-r_d}, \widehat{g}_1)$, $C_{U,2} = g_{\mathrm{re}}^{r_\alpha}$, $C_{U,3} = R_{\mathrm{re}}^{r_e} g_{\mathrm{re}}^{-r_d}$, $C_{U,4} = \mathrm{pk}_{\mathrm{re}}^{r_\alpha} g_4^{-r_b}$.

(2) It computes challenge $c = H(E_{\mathrm{re}}, R_{\mathrm{re}}, \theta, C_{U,1}, C_{U,2}, C_{U,3}, C_{U,4})$ and computes challenge response: $z_b = r_b + c \cdot H_2(\mathrm{pk}_{U,2}^{r_u}), z_c = r_c + c \cdot \omega_u$, $z_d = r_d + c \cdot r_f r_a$, $z_e = r_e + c \cdot r_a$, $z_\alpha = r_\alpha + c \cdot r_{re}$, $z_\beta = r_\beta + c \cdot r_a s_u$.

(3) It outputs $\pi_{\text{re}} = \{\text{otpk}_U, E_{\text{re}}, R_{\text{re}}, c, \theta, z_b, z_c, z_d, z_e, z_\alpha, z_\beta\}$

Likewise, $\mathcal{HOSP}$ proofs the above relationship to the endorser. The proof process π_{sd} is very similar to that of the user, so it will not be explained in detail here.

$(\text{otsk}_H) \longleftarrow$ **OTskGen** $(\text{sk}_{H,1}, \text{sk}_{H,2}, R_H)$: with $\text{sk}_{H,1}$, $\text{sk}_{H,2}$, and R_H, $\mathcal{HOSP}$ calculates $\text{otsk}_H = \text{sk}_{H,1} + H_2(R_H^{\text{sk}_{H,2}})$ and lets $\text{otpk}_H = g_4^{\text{otsk}_H}$. At the same time, $\mathcal{HOSP}$ sends R_U to the vaccination user over a secure channel. The user then generates his own one-time secret key $\text{otsk}_U = \text{sk}_{U,1} + H_2(R_U^{\text{sk}_{U,2}})$.

$(0/1) \longleftarrow$ **EndorserVerify** $(\pi_{\text{re}}, \pi_{\text{sd}}, \pi_{\text{enc}})$: the endorser verifies the legitimacy of the vaccination information and the legitimacy of the one-time public key of the sender ($\mathcal{HOSP}$) and the receiver (user).

The details of the zero-knowledge proof is as follows:

(1) First $\mathcal{HOSP}$ needs proof to endorser: PoK $\{(\text{otsk}_H)\text{: } \text{otpk}_H = g_4^{\text{otsk}_H}\}$.

(2) On input π_{enc}, for $i \in \{0, \ldots, 7\}$, endorser computes $c = H(\{E_i, R_i, C_{v,i}, D_{v,i}\}_{i\in\{0,\ldots7\}}, E, R_v, C_v, D_v)$ and checks $C_{v,i} \stackrel{?}{=} E_i^c g_0^{z_{1,i}} \text{pk}_{vc}^{z_{2,i}}, D_{v,i} \stackrel{?}{=} R_i^c g_1^{z_{2,i}}$, $C_v \stackrel{?}{=} E^c g_0^{z_1} \text{pk}_{\text{vc}}^{z_2}, D_v \stackrel{?}{=} R_v^c g_1^{z_2}$.
It outputs 1 if the above equation holds or 0 otherwise.

(3) On input π_{re}, endorser computes $C'_{U,1} = e((g_u \cdot E_{\text{re}})^{z_e} g_5^{z_\beta} \theta^{-z_c} \text{pk}_{\text{re}}^{-z_d}, \widehat{g}_1) \cdot e(\theta, \text{pk}_{\text{CA}})^c$, $C'_{U,2} = g_{\text{re}}^{z_\alpha} R_{\text{re}}^{-c}$, $C'_{U,3} = R_{\text{re}}^{z_e} g_{\text{re}}^{-z_d}$, $C'_{U,4} = \text{pk}_{\text{re}}^{z_\alpha} g_4^{-z_b} (\text{otpk}_U / E_{\text{re}})^c$.
Then, endorser computes $c' \stackrel{?}{=} H(E_{\text{re}}, R_{\text{re}}, \theta, C'_{U,1}, C'_{U,2}, C'_{U,3}, C'_{U,4})$ and checks $c' \stackrel{?}{=} c$. It outputs 1 if $c' = c$ holds or 0 otherwise.

(4) On input π_{sd}, endorser does same as (3). The initiator of the vaccine record upload operation can only be the hospital. Therefore, at this step, the endorser needs to verify that the initiator of the upload operation has a valid hospital identification credential.

If all four of the above verifications output 1, then $(1) \longleftarrow$ **EndorserVerify** $(\pi_{\text{re}}, \pi_{\text{sd}}, \pi_{\text{enc}})$.

$(\text{Cert}_e) \longleftarrow$ **EndorserCredIssue** $(\text{otpk}_H, E, \text{sk}_e)$: after verifying the legitimacy of the vaccine information commitment and the legitimacy of the one-time public key of $\mathcal{HOSP}$ and the user, the endorser generates a certificate Cert_e by endorsing the vaccination record (otpk$_H$ and E). The endorser picks some random $l, k \xleftarrow{R} \mathbb{Z}_p$ and uses secret key sk_e to compute $\text{Cert}_e = \{A_e = (g_7 \cdot g_8^l \cdot E \cdot \text{otpk}_H)^{1/(\text{sk}_e + k)}, l, k\}$ to $\mathcal{HOSP}$.

$(1/0) \longleftarrow$ **EndorserCredProof** $(\text{Cert}_e, \text{otsk}_H, M, r_v)$: after obtaining the endorser's certificate Cert_e, $\mathcal{HOSP}$ needs zero-knowledge proof to the verifier that the vaccination record has a valid certificate. First, $\mathcal{HOSP}$ computes the tag $T = f^{\text{otsk}_H}$ for detecting double recording. $\mathcal{HOSP}$ needs to use proof of knowledge to verifier:

$$\text{PoK}\left\{(\text{otsk}_U, M, r_v, A_e, l, k)\text{: } e\left(A_e, \text{pk}_e \cdot \widehat{g}_e^k\right) = e\left(g_7 \cdot g_8^l \cdot g_0^M \cdot \text{pk}_{\text{vc}}^{r_v} \cdot g_4^{\text{otsk}_H}, \widehat{g}_e\right) \wedge T = f^{\text{otsk}_H}\right\}. \tag{7}$$

The details of the zero-knowledge proof are as follows:

(1) $\mathcal{HOSP}$ randomly picks $r_a, r_b, r_c, r_d, r_e, r_s, r_\alpha, r_\beta \xleftarrow{R} \mathbb{Z}_p$ and makes $S_1 = A_e \cdot u_1^{r_a}, S_2 = g_8^{r_a}$. It computes commitments: $C_{e,1} = e(u_1^{r_d} \cdot S_1^{-r_e} \cdot g_8^{r_\beta} \cdot g_0^{r_s} \cdot \text{pk}_{\text{vc}}^{r_\alpha} \cdot g_4^{r_b}, \widehat{g}_e) \cdot e(u_1, \text{pk}_e)$, $C_{e,2} = g_8^{r_c}, C_{e,3} = S_2^{r_e} g_8^{-r_d}, C_{e,4} = f^{r_b}$.

(2) It computes challenge $c = H(T, S_1, S_2, C_{e,1}, C_{e,2}, C_{e,3}, C_{e,4})$ and computes challenge response $z_b = r_b + c \cdot \text{otsk}_H, z_c = r_c + c \cdot r_a$, $z_e = r_e + c \cdot k$, $z_d = r_d + c \cdot r_a \cdot k$, $z_\alpha = r_\alpha + c \cdot r_v$, $z_\beta = r_\beta + c \cdot l$, $z_s = r_s + c \cdot M$.

(3) It outputs $\pi_e = \{\text{Cert}_e, c, S_1, S_2, z_b, z_c, z_d, z_e, z_s z_\alpha, z_\beta\}$

(4) On input π_e and pk_e, verifier computes $C'_{e,1} = e(u_1^{z_d} S_1^{-z_e} g_8^{z_\beta} g_0^{z_s} \text{pk}_{\text{vc}}^{z_\alpha} g_8^{a_b} g_7^c, g) \cdot e(u_1^{z_c} S_1^{-c}, \text{pk}_e)$, $C'_{e,2} = g_8^{z_c} S_2^{-c}$, $C'_{e,3} = S_2^{z_e} g_8^{-z_d}$, $C'_{e,4} = f^{z_b} T^{-c}$.

Then, verifier computes $c' = H(T, S_1, S_2, C'_{e,1}, C'_{e,2}, C'_{e,3}, C'_{e,4})$ and checks $c' \stackrel{?}{=} c$. It outputs 1 if $c' = c$ holds or 0 otherwise.

$(1/0) \longleftarrow$ **Link** (T_1, T_2): on input, two vaccination records with two tags T_1, T_2. If $T_1 = T_2$, it outputs 1. Otherwise, it outputs 0.

$(1/0) \longleftarrow$ **Audit** $(E_{\text{re}}, R_{\text{re}}, E_{\text{sd}}, R_{\text{sd}}, \{E_i, R_i\}_{i\in\{0,\ldots,7\}})$: on input a ciphertext $(E_{\text{re}}, R_{\text{re}})$, $(E_{\text{sd}}, R_{\text{sd}})$ and $\text{sk}_{\text{re}}, \text{sk}_{\text{sd}}$, auditor has the ability to reveal long-term public keys of users and $\mathcal{HOSP}$ by computing $\text{pk}_{U,1} = E_{\text{re}} / R_{\text{re}}^{\text{sk}_{\text{re}}}, \text{pk}_{H,1} = E_{\text{sd}} / R_{\text{sd}}^{\text{sk}_{\text{sd}}}$. On input a ciphertext $\{E_i, R_i\}_{i\in\{0,\ldots,7\}}$ and sk_{vc}, auditor has the ability to reveal vaccination information by computing $g^{m_i} = E_i / R_i^{\text{sk}_{\text{vc}}}$. The auditor uses a precomputation table containing $(g^0, g^1, \ldots, g^{(2^{16}-1)})$ to find out the message of m_i and reveal vaccination information $M = (m_7 \| \ldots \| m_0)$. The auditor uses the secret keys $\text{sk}_{\text{re}}, \text{sk}_{\text{sd}}$ to reveal the long-term public key $\text{pk}_{H,1} = E_{\text{sd}} / R_{\text{sd}}^{\text{sk}_{\text{sd}}}$ of the vaccination hospital and the long-term public key $\text{pk}_{U,1} = E_{\text{re}} / R_{\text{re}}^{\text{sk}_{\text{re}}}$ of the vaccination user.

4.4. Vaccine Passport. The signing of the vaccine passport is accomplished by the vaccination hospital. This process uses ring signature [19] to ensure the anonymity of the vaccination hospital when issuing the authorization. During the presentation of the vaccine passport, the vaccination properties are proven using the Bulletproofs scheme [20] in range proofs to guarantee the validity of the vaccine without exposing the vaccine information. Before using Bulletproofs, it uses interactions to transform the relationships of vaccine attributes into relationships suitable for Bulletproofs range proofs [21]. The identity privacy of the owner of the vaccine

passport is protected using the same one-time public key technique as that used to protect the identity of the user in the previous vaccination record system.

After the user received the last vaccination at the hospital, the hospital uploads the vaccination record information to the consortium blockchain. The hospital then issues a vaccine passport to the user.

4.4.1. Vaccine Passport Issue

(1) The user commits the date of vaccination x_v, production date x_p, shelf life x_s, and the duration of immunization x_d by selecting $r_v, r_p, r_s, r_d \xleftarrow{R} \mathbb{Z}_p$ and generates commitments $C_v = g^{x_v} h^{r_v}, C_p = g^{x_p} h^{r_p}, C_s = g^{x_s} h^{r_s}, C_d = g^{x_d} h^{r_d}$. The user sends $C_v, C_p, C_s, C_d, r_v, r_p, r_s, r_d$ to the vaccination hospital. For the user identity certificate $\mathrm{Cert}_{\mathrm{CA},U} = \{A_{\mathrm{CA},U} = (g_u \cdot \mathrm{pk}_{U,1} \cdot g_5^{s_u})^{1/(\mathrm{sk}_{\mathrm{CA}}+\omega_u)}, s_u, \omega_u\}$ issued by the CA, the user randomly selects $r_a \xleftarrow{R} \mathbb{Z}_p$ to send $A_{\mathrm{CA},U}^{r_a}$ to $\mathcal{HOSP}$.

(2) $\mathcal{HOSP}$ receives the user information and opens the commitment and checks:

$$\begin{aligned} C_v &\stackrel{?}{=} \mathrm{Commit}(x_v', r_v), \\ C_p &\stackrel{?}{=} \mathrm{Commit}(x_p', r_p), \\ C_s &\stackrel{?}{=} \mathrm{Commit}(x_s', r_s), \\ C_d &\stackrel{?}{=} \mathrm{Commit}(x_d', r_d). \end{aligned} \tag{8}$$

If one of the equations does not hold, $\mathcal{HOSP}$ refuses to issue a vaccine passport to its user. Otherwise, $\mathcal{HOSP}$ accepts to issue a vaccine passport for the user.

(3) $\mathcal{HOSP}$ generates a ring signature σ_{ring} for the vaccine passport information $(C_v, C_p, C_s, C_d, A_{\mathrm{CA},U}^{r_a})$. First, it lets $m = H(C_v, C_p, C_s, C_d, A_{\mathrm{CA},U}^{r_a})$ and selects $(n-1)$ public keys of other hospitals. Then, it randomly picks seed $\alpha \xleftarrow{R} \mathbb{Z}_p$ and $x_i \xleftarrow{R} \mathbb{Z}_p$. Suppose that f is a trapdoor one-way function such as RSA. It computes $y_i = f(x_i, \mathrm{pk}_i)$ and $v_{(i_s+1)} = H(m \| \alpha)$ to go along the ring from signer index i_s. It closes the ring by computing $v_{(i_s)} = H(m \| y_{(i_s-1)} \oplus \cdots \oplus H(m \| y_{(i_s+1)} \oplus H(m \| \alpha)))$ and uses secret key sk_H of signing $\mathcal{HOSP}$ to compute $x_{i_s} = f^{-1}(v_{(i_s)} \oplus \alpha)$. $\mathcal{HOSP}$ randomly selects an index i_0 and outputs the ring signature $\sigma_{\mathrm{ring}} = (i_0, v_{i_0}, x_1, \ldots x_n, \mathrm{pk}_1, \ldots, \mathrm{pk}_n)$.

(4) $\mathcal{HOSP}$ outputs vaccine passport $\{C_v, C_p, C_s, C_d, A_{\mathrm{CA},U}^{r_a}, \sigma_{\mathrm{ring}}\}$

4.4.2. Vaccine Passport Proof

(1) User generates new one-time public and secret keys pair by $(\mathrm{otpk}_U', R_U') \longleftarrow$ **OTpkGen** $(\mathrm{pk}_{U,1}, \mathrm{pk}_{U,2})$ and $(\mathrm{otsk}_U') \longleftarrow$ **OTskGen** $(\mathrm{sk}_{U,1}, \mathrm{sk}_{U,2}, R_U')$. The user needs proof to vaccine passport checkpoint:

$$\mathrm{PoK}\left\{(\mathrm{otsk}_U'): \mathrm{otpk}_U' = g^{\mathrm{otsk}_U'}\right\}, \tag{9}$$

$$\begin{aligned} &\mathrm{PoK}\Big\{\big(A_{\mathrm{CA},U}, s_u, \omega_u, \mathrm{pk}_{U,1}, r_{\mathrm{re}}, H_2(\mathrm{pk}_{U,2}^{r_u})\big): e\big(A_{CA,U}, g_5^{\omega_u} \cdot \mathrm{pk}_{\mathrm{CA}}\big) = e\big(g_u \cdot \mathrm{pk}_{U,1} \cdot g_5^{s_u}, \widehat{g}_1\big) \wedge \mathrm{otpk}_U' \\ &= \mathrm{pk}_{U,1} \cdot g_4^{H_2\left(\left(\mathrm{pk}_{U,2}^{r_u}\right)\right)} \wedge R_U' = g_4^{r_u} \wedge E_{\mathrm{re}} = \mathrm{pk}_{U,1} \cdot \mathrm{pk}_{\mathrm{re}}^{r_{\mathrm{re}}}\Big\}. \end{aligned} \tag{10}$$

(2) Vaccine passport checkpoint verifies the legitimacy of the ring signature σ_{ring}. The verification is straightforward; the vaccine passport checkpoint starts at index i_0 with value v_{i_0}. If $v_{i_0} = H(m \| y_{(i_0-1)} \oplus \cdots \oplus H(m \| v_{i_0} \oplus y_{i_0}))$, it verifies that the vaccine passport has the hospital's valid ring signature.

(3) The vaccine injected by the user is within the shelf life. It requires that the inequality $(x_v - x_p - x_s) > 0$ be satisfied.

The user produces high titers of antibodies to create effective protection. This corresponds to the last date of vaccination plus 14 days [11], which needs to be greater than the current date. It requires that the inequality $(x_v + x_d) < t$ be satisfied, where t is the current date.

The vaccinated user is in the duration of immunization for the vaccine. This is equivalent to the last date of vaccination plus the vaccine immunity lasting time needs to be less than the current date. It requires that the inequality $x_v > (t - 14)$ be satisfied.

$$\begin{aligned} &\mathrm{PoK}\Big\{\big(x_p, x_s, x_d, x_v, r_p, r_s, r_d, r_v\big), \big(C_p, C_s, C_d, C_v\big): C_p = g^{x_p} h^{r_p}, C_s = g^{x_s} h^{r_s}, C_d = g^{x_d} h^{r_d}, C_v = g^{x_v} h^{r_v} \\ &\wedge \big(x_v - x_p - x_s\big) > 0, \big(x_v + x_d\big) < t1, x_v > (t - 14)\Big\}. \end{aligned} \tag{11}$$

(4) After vaccine passport checkpoint returns $g^t, g^{(t-14)}, g^{2^l}$, the above range proof translates to

$$\begin{aligned}&\mathrm{PoK}\Big\{\big(x_p, x_s, x_d, x_v, r_p, r_s, r_d, r_v\big), \big(A_1 = C_v/\big(C_pC_s\big),\\ &A_2 = C_vC_dg^{2^l}/g^t, A_3 = C_v/g^{(t-14)}\big)\colon A_1 = g^{x_v-x_p-x_s}h^{r_v-r_p-r_s}, A_2 = g^{x_v+x_d-t+2^l}h^{r_v+r_d}, A_3 = g^{x_v-t+14}h^{r_v}\wedge\big(x_v-x_p-x_s\big)\\ &\in\big[0,2^l\big), \big(x_v+x_d-t+2^l\big)\in\big[0,2^l\big), \big(x_v-t+14\big)\in\big[0,2^l\big)\Big\}.\end{aligned}\tag{12}$$

5. Security Analysis

Definition 1. Threshold signature scheme is called secure robust threshold signature scheme if the following two conditions hold:

(i) Unforgeability: for every PPT adversary A, it is allowed to corrupt up to t participants in the threshold system and is given the oracle channel to ask a finite number of messages m_i and threshold signatures σ_i. Eventually, it forges with negligible probability a valid (m, σ), and m is not in the set of previous queries (m_i, σ_i).

(ii) Robustness: for every PPT adversary A, it is allowed to corrupt up to t participants in the threshold system, and threshold signature protocol runs successfully.

Theorem 1. *(t, n)-threshold signature scheme under the GDH group is a secure threshold signature scheme in the random oracle model against an adversary which is allowed to corrupt any $t < n/2$ participants.*

Definition 2 (Soundness). The vaccination information privacy protocol is sound if for all PPT adversary $\mathscr{A}$ with oracle to query polynomial level times $(E_i, R_i, E, R_v) \longleftarrow$ **VaccInfoEnc** (vaccination, $\mathrm{pk}_{\mathrm{vc}}$), and then,

$$\Pr\left[\begin{array}{c}1\longleftarrow\mathbf{EndorserVerify}\left(\pi_{\mathrm{enc}}\right):\\ \left(\pi_{\mathrm{enc}}\right)\longleftarrow\mathscr{A}\left(\left\{E_i, R_i, E, R_v\right\}\right)\end{array}\right]\leqslant\mathrm{negl}\left(\lambda\right).\tag{13}$$

Theorem 2. *The vaccination information privacy protocol is sound if DLP is hard, and the protocol provides knowledge of soundness.*

Proof. It rewinds $c' = H\left(\left\{E_i, R_i, C'_{v,i}, D'_{v,i}\right\}_{i\in\{0,\ldots,7\}}, E, R_v, C'_v, D'_v\right)$, where $c \neq c'$ and computes $\left\{z'_{1,i}, z'_{2,i}\right\}_{i\in\{0,\ldots,7\}}, z'_1, z'_2$. It extracts the knowledge of

$$\begin{aligned}m_i &= \left(z'_{1,i} - z_{1,i}\right)/\left(c' - c\right),\\ r_{v,i} &= \left(z'_{2,i} - z_{2,i}\right)/\left(c' - c\right),\\ M &= \left(z'_1 - z_1\right)/\left(c' - c\right),\\ r_v &= \left(z'_2 - z_2\right)/\left(c' - c\right).\end{aligned}\tag{14}$$

□

Definition 3 (Privacy). The vaccination information is private in the protocol if for all PPT adversary $\mathscr{A}$:

$$\left|\Pr\left[\begin{array}{c}b = b'\colon\\ \left(\left\{\pi_{\mathrm{enc}}\right\}_{(0),(1)}\right)\longleftarrow\mathbf{VaccInfoEnc}\left(\left\{\mathrm{vaccination}\right\}_{(0),(1)}\right),\\ b\overset{R}{\longleftarrow}\{0,1\}, b'\longleftarrow\mathscr{A}\left(\pi_{\mathrm{enc}}\right)_{(b)}\end{array}\right] - 1/2\right| \leq \mathrm{negl}\left(\lambda\right).\tag{15}$$

Theorem 3. *The vaccination information is private in the protocol if DDH is hard in $\mathbb{G}_1$, and the protocol is HVZK.*

Proof. The encryption $(E_i = g_0^{m_i}\mathrm{pk}_{\mathrm{vc}}^{r_{v,i}}, R_i = g_6^{r_{v,i}})$ used in this protocol is the ElGamal encryption algorithm. The security of this encryption is based on the DDH assumption. If the DDH assumption is difficult on $\mathbb{G}_1$, the vaccination information of this protocol is private during transmission.

The simulator of this protocol randomly picks $\left\{E_i, R_i, z_{1,i}, z_{2,i}\right\}_{i\in\{0,\ldots,7\}}, c', z_1, z_2 \overset{R}{\longleftarrow}$ corresponding domain. Then, it computes

$$\begin{aligned}C_{v,i} &= E_i^{c'}g_0^{z_{1,i}}pk_{vc}^{z_{2,i}},\\ D_{v,i} &= R_i^{c'}g_1^{z_{2,i}},\\ C_v &= E^{c'}g_0^{z_1}\mathrm{pk}_{\mathrm{vc}}^{z_2},\\ D_v &= R_v^{c'}g_1^{z_2},\end{aligned}\tag{16}$$

where they are indistinguishable from real protocol interactions. The simulator sets c' as $H\left(\left\{E_i, R_i, C_{v,i}, D_{v,i}\right\}_{i\in\{0,\ldots,7\}}, E, R_v, C_v, D_v\right)$ in the random oracle model. Therefore, this protocol provides zero-knowledge of vaccination information. □

Definition 4 (Soundness). The users (including hospitals and vaccination users) privacy protocol is sound if for all PPT adversary $\mathscr{A}$ with oracle to query polynomial level times $(\mathrm{Cert}_{\mathrm{CA},U}) \longleftarrow$ **CACertIssue** $(\mathrm{pk}_{U,1})$, and then,

(i) The public key of the user (including hospital and vaccination user) is issued a valid certificate $(A_{\mathrm{CA},U}, s_u, \omega_u)$:

$$\Pr\left[\begin{array}{c} 1 \longleftarrow \mathbf{EndorserVerify}\left(\pi_{\mathrm{re}}\left(\mathrm{or}\ \pi_{\mathrm{sd}}\right)\right): \\ \left(\mathrm{Cert}_{\mathrm{CA},U}{}'\right) \longleftarrow \mathscr{A}\left(\mathrm{pk}_{U,1}\right) \\ \mathrm{where}\left(\mathrm{Cert}_{\mathrm{CA},U}{}', \mathrm{pk}_{U,1}\right) \notin \text{oracle queries}, \\ \left(\mathrm{otpk}_U, \pi_{\mathrm{re}}\left(\mathrm{or}\ \pi_{\mathrm{sd}}\right)\right) \longleftarrow \mathbf{OTpkGen}\left(\mathrm{pk}_{U,1}, \mathrm{pk}_{U,2}\right) \end{array}\right] \leqslant \mathrm{negl}\left(\lambda\right). \tag{17}$$

(ii) otpk_U is computed from a public key $\mathrm{pk}_{U,1}$ and the public key $\mathrm{pk}_{U,1}$ is encrypted to the auditor:

$$\Pr\left[\begin{array}{c} 1 \longleftarrow \mathbf{EndorserVerify}\left(\pi_{\mathrm{re}}{}'\left(\mathrm{or}\ \pi_{\mathrm{sd}}{}'\right)\right): \\ \left(\mathrm{Cert}_{\mathrm{CA},U}\right) \longleftarrow \mathbf{CACertIssue}\left(\mathrm{pk}_{U,1}\right), \\ \left(\mathrm{otpk}_U{}', \pi_{re}{}'\left(\mathrm{or}\ \pi_{\mathrm{sd}}{}'\right)\right) \longleftarrow \mathscr{A}\left(\mathrm{pk}_{U,1}{}', \mathrm{pk}_{U,2}{}'\right) \\ \mathrm{where}\ \mathrm{pk}_{U,1}{}' \neq \mathrm{pk}_{U,1} \end{array}\right] \leqslant \mathrm{negl}\left(\lambda\right). \tag{18}$$

Theorem 4. *The users (including hospitals and vaccination users) privacy protocol is sound if the q-SDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$ *in the random oracle model, where q is the maximum number of* ***CACertIssue*** *oracle queries, and the protocol provides knowledge of soundness.*

Proof. It rewinds $c' = H\left(E_{\mathrm{re}}, R_{\mathrm{re}}, \theta, C_{U,1}{}', C_{U,2}{}', C_{U,3}{}', C_{U,4}{}'\right)$, where $c \neq c'$, and computes $z_b', z_c', z_d', z_e', z_\alpha', z_\beta'$. It extracts the knowledge of

$$\begin{aligned} r_a &= \left(z_e' - z_e\right)/\left(c' - c\right), \\ s_u &= \left(z_\beta' - z_\beta\right)/\left(r_a\left(c' - c\right)\right) \\ \omega_u &= \left(z_c' - z_c\right)/\left(c' - c\right), \\ r_{re} &= \left(z_\alpha' - z_\alpha\right)/\left(c' - c\right), \\ H_2\left(\mathrm{pk}_{U,2}^{r_u}\right) &= \left(z_b' - z_b\right)/\left(c' - c\right), \\ \mathrm{pk}_{U,1} &= \mathrm{otpk}/g_4^{H_2\left(\mathrm{pk}_{U,2}^{r_u}\right)} \\ A_{\mathrm{CA},U} &= \theta^{1/r_a}. \end{aligned} \tag{19}$$

BBS + signature is unforgeable against adaptively chosen message attack under the q-SDH assumption. □

Definition 5 (Anonymity). The anonymity of users (including hospitals and vaccination users) is enabled in the protocol if for all PPT adversary $\mathscr{A}$,

$$\left|\Pr\left[\begin{array}{c} b = b': \\ \left(\left\{\mathrm{otpk}_U, R_U\right\}_{(0),(1)}\right) \longleftarrow \mathbf{OTpkGen}\left(\mathrm{pk}_{U,1}\right), \\ b \xleftarrow{R} \{0,1\}, b' \longleftarrow \mathscr{A}\left(\left\{\mathrm{otpk}_U, R_U\right\}_{(b)}\right) \end{array}\right] - 1/2\right| \leqslant \mathrm{negl}\left(\lambda\right). \tag{20}$$

Theorem 5. *The anonymity of users (including hospitals and vaccination users) is enabled in the protocol if CDH is hard in* $\mathbb{G}_1$*, and the protocol is HVZK.*

Proof. The encryptions $(E_{\text{re}} = \text{pk}_{U,1} \cdot \text{pk}_{\text{re}}^{r_{\text{re}}}, R_{\text{re}} = g_2^{r_{\text{re}}})$ and $(E_{\text{sd}} = \text{pk}_{H,1} \cdot \text{pk}_{\text{sd}}^{r_{\text{sd}}}, R_{\text{sd}} = g_3^{r_{\text{sd}}})$ used in this protocol are the ElGamal encryption algorithm. The security of this encryption is based on the DDH assumption. The one-time public key $(\text{otpk}_U = \text{pk}_{U,1} \cdot g^{H_2(pk_{U,2}^{r_u})}, R_U = g_4^{r_u})$ and $(\text{otpk}_H = \text{pk}_{H,1} \cdot g^{H_2(pk_{H,2}^{r_h})}, R_H = g_4^{r_h})$ generation algorithm is based on the CDH assumption. If the CDH assumption is difficult on $\mathbb{G}_1$, the anonymity of users (including hospitals and vaccination users) is enabled during transmission.

The simulator of this protocol randomly picks $c', \theta, z_b, z_c, z_d, z_e, z_\alpha, z_\beta \xleftarrow{R}$ corresponding domain. Then, it computes

$$\begin{aligned} C_{U,1} &= e\left((g_u \cdot E_{\text{re}})^{z_e} g_5^{z_\beta} \theta^{-z_c} \text{pk}_{re}^{-z_d}, \widehat{g}_1\right) \cdot e(\theta, \text{pk}_{\text{CA}})^c, \\ C_{U,2} &= g_{re}^{z_\alpha} R_{\text{re}}^{-c}, \\ C_{U,3} &= R_{\text{re}}^{z_e} g_{\text{re}}^{-z_d}, \\ C_{U,4} &= \text{pk}_{\text{re}}^{z_\alpha} g_4^{-z_b} (\text{otpk}_U / E_{\text{re}})^c, \end{aligned} \tag{21}$$

where they are indistinguishable from real protocol interactions. The simulator sets c' as $H(E_{\text{re}}, R_{\text{re}}, \theta, C_{U,1}, C_{U,2}, C_{U,3}, C_{U,4})$ in the random oracle model. Therefore, this protocol provides zero-knowledge of CA certificate for the user's long-term public key and the user's long-term public key. □

Definition 6 (Soundness). The vaccination information endorsement protocol is sound if for all PPT adversary $\mathscr{A}$ with oracle to query polynomial level times $(\text{Cert}_e) \longleftarrow$ **EndorserCertIssue** (otpk_H, E), and then, this vaccination information $E = g_0^M \text{pk}_{\text{vc}}^{r_v}$ and otpk_H is issued a valid certificate (A_e, l, k) by the endorsement nodes:

$$\Pr\left[\begin{array}{c} 1 \longleftarrow \textbf{EndorserCredProof}(\text{Cert}_e', \text{otpk}_H, E) \vee \\ 1 \longleftarrow \textbf{EndorserCredProof}(\text{Cert}_e, \text{otpk}_H', E'): \\ (\text{Cert}_e') \longleftarrow \mathscr{A}(\text{otpk}_H, E) \vee \\ (\text{Cert}_e) \longleftarrow \textbf{EndorserCredIssue}(\text{otpk}_H, E) \\ \text{where}(\text{otpk}_H', E') \neq (\text{otpk}_H, E) \end{array}\right] \leqslant \text{negl}(\lambda). \tag{22}$$

Theorem 6. *The vaccination information endorsement protocol is sound if the q-SDH assumption holds in* $(\mathbb{G}_1, \mathbb{G}_2)$ *in the random oracle model, where q is the maximum number of* ***EndorserCredIssue*** *oracle queries, and the protocol provides knowledge of soundness.*

Proof. It rewinds $c' = H(T, S_1, S_2, C_{e,1}', C_{e,2}', C_{e,3}', C_{e,4}')$, where $c \neq c'$, and computes $z_b', z_c', z_d', z_e', z_\alpha', z_\beta', z_s'$. It extracts the knowledge of

$$\begin{aligned} r_a &= (z_c' - z_c)/(c' - c), \\ l &= (z_\beta' - z_\beta)/(c' - c), \\ k &= (z_e' - z_e)/(c' - c), \\ M &= (z_s' - z_s)/(c' - c), \\ r_v &= (z_\alpha' - z_\alpha)/(c' - c), \\ \text{otsk}_H &= (z_b' - z_b)/(c' - c), \\ A_e &= S_1 / u_1^{r_a}. \end{aligned} \tag{23}$$

BBS + signature is unforgeable against adaptively chosen message attack under the q-SDH assumption. □

Definition 7 (Privacy). The vaccination information is private in the protocol if for all PPT adversary $\mathscr{A}$,

$$\left|\Pr\left[\begin{array}{c} b = b': \\ (\{\text{Cert}_e\}_{(0),(1)}) \longleftarrow \textbf{EndorserCredIssue} \\ (\{E, \text{otpk}_H\}_{(0),(1)}), \\ b \xleftarrow{R} \{0,1\}, b' \longleftarrow \mathscr{A}(\{E, \text{otpk}_H\}_{(b)}) \end{array}\right] - 1/2\right| \leqslant \text{negl}(\lambda). \tag{24}$$

Theorem 7. *The vaccination information is private in the protocol if the protocol is HVZK.*

Proof. The simulator of this protocol randomly picks $\{c', S_1, S_2, z_b, z_c, z_d, z_e, z_s z_\alpha, z_\beta\} \xleftarrow{R}$ corresponding domain. Then, it computes

$$\begin{aligned} C_{e,1} &= e\left(u_1^{z_d} \cdot S_1^{-z_e} \cdot g_8^{z_\beta} \cdot g_0^{z_s} \cdot \text{pk}_{\text{vc}}^{z_\alpha} \cdot g_8^{a_b} g_7^{c'}, g\right) \\ &\quad \cdot e\left(u_1^{z_c} S_1^{-c'}, \text{pk}_e\right), \\ C_{e,2} &= g_8^{z_c} S_2^{-c'}, \\ C_{e,3} &= S_2^{z_e} g_8^{-z_d}, \\ C_{e,4} &= f^{z_b} T^{-c'}, \end{aligned} \tag{25}$$

where they are indistinguishable from real protocol interactions. The simulator sets c' as $H(T, S_1, S_2, C_{e,1}, C_{e,2}, C_{e,3}, C_{e,4})$ in the random oracle model.

Table 1: Comparison of COVID-19 vaccine systems.

	Blockchain structure	Vaccine supply chain	Vaccination record	User privacy	Vaccination hospital privacy	Vaccination privacy	Auditable	Vaccination certificate
[7]	Public blockchain	√	√	√	×	×	√	×
[10]	Public chain and private blockchain	√	√	√	√	√	√	×
[6]	Public blockchain	√	×	×	×	×	√	×
[8]	Private blockchain	×	√	√	×	√	×	√
[5]	Public blockchain	√	×	×	×	×	√	×
[22]	Consortium ethereum-based blockchain	×	√	√	×	√	×	√
[23]	Consortium blockchain	×	√	√	×	√	?	√
[24]	Permissioned blockchain	×	√	√	√	√	√	√
China health code system	No blockchain	×	√	×	×	×	√	√
This study	Public blockchain and consortium blockchain	√	√	√	√	√	√	√

"√" represents that the privacy protection of this attribute of the vaccine system is based on stronger assumptions, such as storing the private data in a private database off-chain or increasing the restriction of database access, thus having a higher probability of privacy leakage. "?" represents that this attribute of the vaccine system is not mentioned from the open-source code or references.

Therefore, this protocol provides zero-knowledge of vaccination information. □

Lemma 1 (Ring lemma). *Ring signature is unforgeable if the DL assumption holds. The anonymity of the ring signature is unconditional.*

Lemma 2. *The Bulletproof has perfect completeness, perfect special honest verifier zero-knowledge, and computational witness extended emulation.*

6. System Analysis

6.1. Security and Privacy. We compare the vaccine system proposed in this study with other solutions proposed in academia and platform systems that have been applied in practice, as given in Table 1. The main aspects of comparison are the blockchain structure, the domain covered by the system, the properties of user privacy protection, and auditability.

In terms of vaccine system structure, the non-blockchain-based vaccine system is represented by the China health code system, a digital vaccine certificate implemented by the Chinese government based on Alipay, a trusted third party. The authentication of the vaccine certificate is done by the verifier through the QR code in the Alipay wallet app. Another blockchain-based vaccine system mainly takes advantage of the immutability and decentralized property of blockchain to create a more credible and secure vaccine system, which is also the trend of vaccine system research. The main types of blockchains in vaccine systems are public blockchains, private blockchains, and consortium blockchains. In this study and [10], a double-chain structure is used. However, under the assumption of global recognition, the consortium blockchain has an advantage over the private blockchain in terms of use coverage.

In terms of privacy protection, we divide user privacy into user identity privacy, vaccination hospital privacy, and privacy of vaccination records. Systems with a single public blockchain structure, for example [5, 6], are not user privacy protected. The blockchain of vaccination records in [7] keeps sensitive information of users out of the blockchain and protects user privacy to some extent. The [8, 10, 22, 23] schemes use private blockchain or consortium blockchain for participant's identity authentication to protect user privacy. Qiu and Zhu [10] stored all the vaccination records in a private blockchain and Alabdulkarim et al. [24] stored the private data on the private database of the authorized specific peer. However, this does not guarantee the leakage of user vaccination privacy by the nodes in the private blockchain, and the storage of vaccination records would be centralized. In the study by Abid et al. [8], the vaccination certificate is issued by the healthcare provider (issuer) with a signature. Therefore, this process can expose the privacy of the user's vaccination hospital. Also, this scheme cannot audit the vaccination information because it uses a private blockchain and a certain degree of information encryption. Both [22, 23] used consortium blockchains structure, but do not have any encryption of user privacy information, so these two schemes guarantee the privacy of user personal information only to some extent. However, the privacy of vaccination hospitals cannot be guaranteed.

6.2. Performance Analysis. The main objective of this study is to propose a framework for a double-chain-based vaccine passport system and to refine the design of the protocol between specific participants. This goal of this study is to provide a systematic solution to the vaccine passport which focuses more on the theoretical aspect. Therefore, only a qualitative analysis of the system's performance is presented here.

The additional performance overhead of the public blockchain-based vaccine cold chain phase is mainly in the approval phase. For each approval process of vaccines sent for review, the approval institutions in each country need to participate in the distributed setting of threshold secret sharing of the value x. For each distributed key generation protocol, it is assumed that there are n approval institutions, and each institution needs to generate 2 random polynomials. At the same time, each approval authority broadcasts the commitment of polynomials to the other $(n-1)$ approval authorities. The communication data volume of the whole broadcast channel is $O(n^2)$.

The permission blockchain framework for the vaccination record phase of this study is based on the Hyperledger Fabric architecture. By referring to the idea of PAChain [15], the privacy of the vaccination records is protected among the endorsers, orderers, and committing peers. This study removes the trust in the endorser compared to PAChain, thus increasing the authentication protocol. Therefore, the system latency in this phase is slightly higher than PAChain.

The performance bottleneck in the passport identification phase is mainly due to the range proof of the vaccine attributes. Benefiting from the efficiency and aggregability of Bulletproofs [20], the proof size of vaccine passports in the presentation phase is $O(\log(\mathrm{mn}))$ for a batch size of n users and the vaccine attribute length of m bits. For the specific case where the vaccine attribute is 64 bits $(m = 64)$, the proof size for a single user is $3 \times 675 = 2025$ bytes; while, the aggregated proof size for 512 users is $3 \times 1253 = 3759$ bytes.

Based on the results of the above system performance analysis, we believe that the vaccine passport system proposed in this study is feasible for development and implementation. In future implementations, sacrificing acceptable system performance loss in exchange for abundant privacy-preserving security properties is to be considered in advance.

7. Conclusion

This study makes improvements to the vaccine approval part of the previous vaccine distribution and management system. The introduction of a threshold signature scheme in distributed vaccine approval institutions has a certain degree of deterrence against collusive corruption between vaccine approval institutions and vaccine manufacturing companies. Second, the privacy protection in the previous double-chain system is optimized. In this study, the privacy protection of vaccination hospitals, vaccine trusts, and vaccination users is added to the audit function, which increases the controllability and auditability of the vaccination record system in practice. Finally, the vaccine passport proposed in this study protects the privacy of the user's vaccination hospital, the vaccine, and the user's identity while proving the validity and legitimacy of the passport to the vaccine passport checkpoint. Moreover, it is possible to differentiate and adopt targeted measures and policies for different conditions of the vaccine passport. Future work in this study lies in weakening the authority of local vaccination hospitals in the system. It can increase the link between the double chains using corresponding cryptographic techniques.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. Tan, X. Zhao, X. Ma et al., "A novel coronavirus genome identified in a cluster of pneumonia cases—wuhan, China 2019- 2020," *China CDC weekly*, vol. 2, no. 4, pp. 61-62, 2020.

[2] "Vaccination certification to be digitized by the end of this year for use in Japan," 2021, https://www.nikkei.com/article/DGXZQOUA264980W1A820C2000000/.

[3] L. Byers, "BC launches proof of vaccination to stop spread of covid-19," 2021, https://news.gov.bc.ca/releases/2021HLTH0053-001659.

[4] M. A. Hall and D. M. Studdert, "Vaccine passport" certification—policy and ethical considerations," *New England Journal of Medicine*, 2021.

[5] L. Cui, Z. Xiao, J. Wang et al., "Improving vaccine safety using blockchain," *ACM Transactions on Internet Technology*, vol. 21, no. 2, pp. 1–24, 2021.

[6] C. Antal, T. Cioara, M. Antal, and I. Anghel, "Blockchain platform for covid-19 vaccine supply management," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 164–178, 2021.

[7] B. Yong, J. Shen, X. Liu, F. Li, H. Chen, and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management*, vol. 52, Article ID 102024, 2020.

[8] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "Novidchain: blockchain-based privacy-preserving platform for covid-19 test/vaccine certificates," *Software: Practice and Experience*, 2021.

[9] A. B. Haque, B. Naqvi, A. K. M. N. Islam, and S. Hyrynsalmi, "Towards a gdpr-compliant blockchain-based covid vaccination passport," *Applied Sciences*, vol. 11, no. 13, p. 6132, 2021.

[10] Z. Qiu and Y. Zhu, "A novel structure of blockchain applied in vaccine quality control: double-chain structured blockchain system for vaccine anticounterfeiting and traceability," *Journal of Healthcare Engineering*, vol. 2021, Article ID 6660102, 10 pages, 2021.

[11] F.-C. Zhu, Y.-H. Li, X.-H. Guan et al., "Safety, tolerability, and immunogenicity of a recombinant adenovirus type-5 vectored covid-19 vaccine: a dose-escalation, open-label, non-randomised, first-in-human trial," *The Lancet*, vol. 395, no. 10240, pp. 1845–1854, 2020.

[12] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group

signature scheme," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 31–46, Springer, Miami, FL, USA, 6 January 2003.

[13] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 295–310, Springer, Prague Czech Republic, 2 May 1999.

[14] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, pp. 1–15, ACM, Porto Portugal, 23 April 2018.

[15] T. H. Yuen, "Pachain: private, authenticated & auditable consortium blockchain and its implementation," *Future Generation Computer Systems*, vol. 112, pp. 913–929, 2020.

[16] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-taa," in *Proceedings of the International conference on security and cryptography for networks*, pp. 111–125, Springer, Maiori, Italy, 6 September 2006.

[17] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proceedings of the International conference on the theory and applications of cryptographic techniques*, pp. 56–73, Springer, Interlaken, Switzerland, 2 May 2004.

[18] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[19] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Proceedings of the Annual International Cryptology Conference*, pp. 465–480, Springer, Santa Barbara, CA, USA, August 2002.

[20] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: short proofs for confidential transactions and more," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, pp. 315–334, IEEE, San Francisco, CA, USA, 20 May 2018.

[21] J. Camenisch, R. Chaabouni, and abhi shelat, "Efficient protocols for set membership and range proofs," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 234–252, Springer, Melbourne, VIC, Australia, 7 December 2008.

[22] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third, and J. Domingue, "Covid-19 antibody test/vaccination certification: there's an app for that," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148–155, 2020.

[23] "A simple and secure certificate of covid-19 immunity," 2020, https://www.immupass.org/.

[24] Y. Alabdulkarim, A. Alameer, M. Almukaynizi, and A. Almaslukh, "Spin: a blockchain-based framework for sharing covid-19 pandemic information across nations," *Applied Sciences*, vol. 11, no. 18, p. 8767, 2021.