Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5721212, 11 pages
https://doi.org/10.1155/2022/5721212

Research Article

An Immunity Passport Scheme Based on the Dual-Blockchain Architecture for International Travel

Hancheng Gao,[1,2] Haoyu Ji,[1,2] Haiping Huang,[1,2] Fu Xiao,[1,2] and Luo Jian[1]

[1]*College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
[2]*High Technology Research Key Laboratory of Wireless Sensor Network of Jiangsu Province, Nanjing 210023, China*

Correspondence should be addressed to Haiping Huang; hhp@njupt.edu.cn

Received 18 October 2021; Revised 9 December 2021; Accepted 20 December 2021; Published 10 January 2022

Academic Editor: Jinguang Han

The implementation of immunity passport has been hampered by the controversies over vaccines in various countries, the privacy of vaccinators, and the forgery of passports. While some existing schemes have been devoted to accelerating this effort, the problems above are not well solved in existing schemes. In this paper, we present an immunity passport scheme based on the dual-blockchain architecture, which frees people from the cumbersome epidemic prevention process while traveling abroad. Specially, the dual-blockchain architecture is established to fit with the scenarios of immunity passport. Searchable encryption and anonymous authentication are utilized to ensure users' privacy. In addition, the performance and security evaluations show that our scheme achieves the proposed security goals and surpasses other authentication schemes in communicational and computational overheads.

1. Introduction

The Coronavirus Disease 2019 (COVID-19) pandemic is undoubtedly an unprecedented disaster for human society [1–3]. The pandemic is rapidly spreading and getting worse in many countries and regions of the world, which has caused a large number of infections and deaths. Countries around the world are doing their utmost to curb the spread of the pandemic, enacting strict policies such as quarantine for infected people, prohibitions on mass gatherings, and restrictions on entry-exit and so on.

Vaccination, in combination with personal protection, is the most effective measure to prevent the COVID-19 [4]. However, the effectiveness of some vaccines remains controversial in countries because of differences in policies, technical standards, and religions. As shown by recent publications, not everyone holds a positive attitude towards the COVID-19 vaccine [5, 6]. There are even discriminations against unvaccinated people in some areas, which is called stigmatization of vaccination [7, 8].

Restoring the order of human society in the postepidemic era is one of the most important issues, among which lifting restrictions on people's entry-exit is particularly significant. The restrictions on the people who have been vaccinated could be relaxed [9]. Therefore, a number of countries and organizations have launched the immunity passport that allows them to work and travel abroad without compromising personal or public health [8, 10]. However, some serious issues remain unresolved: (1) traditional passports are easy to falsify. (2) There are controversies about the effectiveness of some vaccines among different countries. (3) Under the premise of stigmatization, vaccinators' privacy is still at risk.

To effectively ensure the privacy of people traveling during the COVID-19 pandemic, we propose an immunity passport scheme in this paper. In our scheme, vaccinated people can show their passports to a staff of customs without compromising their privacy for entry and exit. Our contributions are summarized as follows:

(1) In order to adapt our scheme to the international travel scenarios, we designed a dual-blockchain architecture with two different types of blockchain, domestic and international. Different countries participate in the consensus of the international

blockchain, which is conducive to solving the controversies about vaccines.

(2) We leveraged the use of the inherent characteristics of blockchain to make the immunity passport traceable and nonrepudiable. And for the purpose that users can have control over their data, we combined searchable encryption and anonymous authentication with blockchain.

(3) Our scheme allows users to participate in vaccination, authentication, and other processes using legitimate pseudonyms, which can well solve the stigmatization of vaccination.

(4) To prove the feasibility and reliability of our scheme, we conducted a complete security analysis and simulation experiments, including computational overheads, communication overheads, and energy overheads.

The rest of this paper is organized as follows. Section 2 discusses some related research achievements. Section 3 describes the preliminary knowledge and introduces the design details of the system model. The immunity passport scheme is proposed in Section 4. Section 5 presents the correctness and security analysis. Section 6 presents the performance evaluation, and Section 7 concludes this paper.

2. Related Work

Due to its outstanding characteristics, blockchain technology has attracted widespread attention in many fields including medical care, identity authentication, and finance [11–13]. Recently, there have been some studies applying blockchain technology to meet the challenges of COVID-19. Xu et al. [14] proposed a blockchain-enabled privacy preserving contact tracing scheme, in which users' privacy is ensured by the pseudonym. However, their scheme has a high demand for the intensive computation of blockchain nodes. In order to control the spread of COVID-19, a privacy anonymous IoT model using blockchain was presented in [15]. In this scheme, people who wear RFID tags will be notified if they are near to the possible or confirmed "hotspot" area. But the authors did not give a security analysis of the scheme in this paper. Song et al. [16] using Bluetooth technology designed a tracing and notification system based on blockchain and smart contract to ensure users' privacy. However, there is an unreasonable assumption that people always honestly upload their health status to the blockchain. Jacob and Lawarée [17] pointed out that apps such as to StopCovid (France), NHS Covid-19 (UK), and Coronalert (Belgium) have security, political, and other issues. Although these schemes and applications are focused on addressing the issues of privacy, the public is still reluctant to disclose their personal data for privacy reasons [18, 19]. Moreover, contact tracing is a passive defense against the COVID-19 pandemic.

Hasan et al. [20] proposed a digital health passport system combining blockchain, proxy reencryption, and smart contracts. In this system, the data owner grants access to other entities so that the user has control over his data. Based on blockchain, a framework was proposed in [21] to ensure users' privacy, which uses a locality-sensitive hash function to generate a secure identifier. The identifier can only be derived if the user provides his biometric and personal information, whereas, although the authors give details of the pseudoidentity generation, the description of the vaccination certificate is very brief. Angelopoulos et al. [22] presented a framework that used a private blockchain to store the digital health passport. But the authors did not give details about how to ensure users' privacy, and the characteristics of private blockchain did not apply to the scenarios where people travel among multiple countries.

None of the above researches [20–22] addressed how the passport holder can verify the legality of inspectors, which is extremely important for users. Some existing authentication schemes are designed for scenarios such as the smart grid, the Internet of Things, and the smart medical [23–26]. Mahmood et al. [23] proposed an anonymous key agreement protocol for the smart grid infrastructure by using the identity-based signature. This protocol empowers the smart meters for anonymous information exchange with utility, which is proved secure under the random oracle model. A mutual authentication scheme focusing on mobile edge computing is proposed by Jia et al. [24], which only needs one massage exchange round to achieve mutual authentication. However, their scheme cannot achieve some security properties. Almadhoun et al. [25] proposed a decentralized and scalable authentication mechanism that utilizes blockchain-enabled fog nodes with connectivity to Ethereum smart contracts, which gives details of smart contracts involved. Although all the above schemes have advantages and highlights, these authentication schemes are not suitable for the scenarios of immunity passport.

It is noteworthy that the above schemes have some shortcomings when applied to epidemic prevention scenarios, which makes the privacy of users cannot be guaranteed well. Therefore, it is meaningful to design a secure, reliable, and efficient immunization passport scheme for the COVID-19 epidemic.

3. System Model and Security Goals

In this section, we give a brief introduction to the basic theoretical knowledge involved in this paper, such as blockchain, searchable encryption, and bilinear mapping. Subsequently, the system model and security goals are presented. The system model is depicted in Figure 1, and the main notations that appear in the scheme are listed in Table 1.

3.1. Preliminaries. Blockchain. Blockchain is a special kind of data structure that arranges a large number of blocks into a chain in chronological order, where each block is composed of certain data [27]. Blockchain is categorized roughly into public blockchain, consortium blockchain, and private blockchain according to the degree of decentralization. Our scheme adopts the consortium blockchain because of the specific advantages: (1) it can be jointly controlled by multiple organizations or countries, which is suitable for the

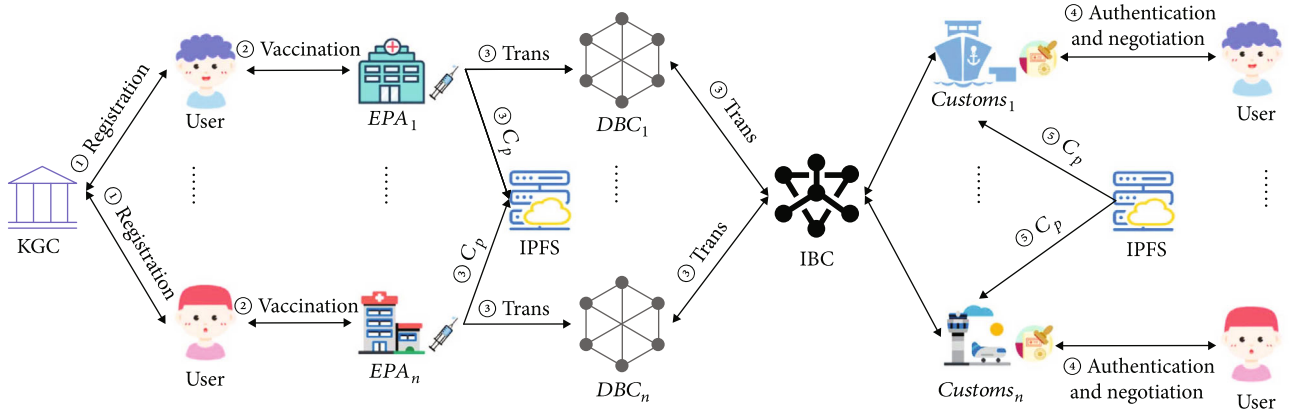

Figure 1: System model of the immunity passport scheme.

Table 1: Notations in the scheme.

Notations	Description
U	User
$\mathbb{G}_1, \mathbb{G}_2$	Multiplicative cyclic groups
$H_i(i = 1, \cdots, 6)$	Secure hash function
PK, SK	Public and private key pair of KGC
PK_c, SK_c	Public and private key pair of IBC
pk_i, sk_i	Public and private key pair of user
D_i	Partial-private key
ID_i'	Pseudoidentity of user
ID_{ctry}	Identity of the country
ID_{DB}	ID of the DBC-block
idx	Index of keyword
C_p	Ciphertext of the passport
Confir	Key confirmation message
K_p	Decryption key
T, T'	Trapdoor

scenarios of our scheme. (2) Only the members of the consortium participate in the consensus, so it has high efficiency. (3) Not everyone can access the data on the consortium blockchain.

Searchable Encryption. Searchable encryption is a cryptographic primitive that supports users to conduct keyword search on encrypted data. It mainly solves how to complete the search for encrypted data when the data is encrypted and stored in the cloud, under the premise that the cloud server is not completely trusted. Similar to searching for plaintext data, a common method for searchable encryption is to establish a secure index for the entire dataset and then use the secure index to complete a secure search for encrypted data on the cloud server. Searchable encryption enhances the scalability of search while saving users a lot of network and computing overhead.

Bilinear Pairings. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups with the prime order as p. Let g be the generator of $\mathbb{G}_1$, which means $\mathbb{G}_1 = \langle g \rangle$. We accept e as bilinear pairing if $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ satisfies the following properties [28]:

(1) Bilinearity. For all $g_1, g_2 \in \mathbb{G}_1$, $a, b \in \mathbb{Z}_p^*$, there is $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

(2) Nondegeneracy. There exists $g_1, g_2 \in \mathbb{G}_1$, such that $e(g_1, g_2) \neq 1$.

(3) Computability. For all $g_1, g_2 \in \mathbb{G}_1$, there exists an efficient algorithm to compute $e(g_1, g_2)$.

3.2. System Model. In the model of the immunity passport scheme, it is assumed that various epidemic prevention agencies (EPAs) in each country form an alliance and jointly maintain a domestic consortium blockchain, that is the "Domestic Blockchain (DBC)." Every country selects an institution with high credibility on behalf of the country to maintain an international consortium blockchain, that is the "International Blockchain (IBC)." Since we use consortium blockchains to design the system model, popular consensus mechanisms adapted to consortium blockchains can be run on our scheme, such as Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS) [29, 30]. Thus, our scheme focuses on how to efficiently authenticate the identity and verify the validity of the passport. The seven entities and two structures of transaction in this model are described in detail as follows:

Key Generate Center (*KGC*). KGC is an organization with high credibility in this system, which is responsible for generating system parameters and distributing partial-private keys for all users.

Users. The user is vaccinated at EPA by virtue of the legal pseudoidentity. The user generates a trapdoor and a decryption key for the staff when he needs the immunity passport; the ciphertext of passport is then searched by the IBC node and returned by the IPFS.

Inter-Planetary File System (*IPFS*). IPFS is a decentralized file storage network used to store the ciphertext of passports generated by the EPAs.

Epidemic Prevention Agency (*EPA*). EPAs maintain a DBC in each country, responsible for vaccinating, generating

Table 2: Structure of transaction on the DBC.

Block header	Timestamp t		Block ID ID_{DB}	Size size	Prehash hash
Transaction	Producer ID_{EPA}	User ID ID'	Keyword-index $\{idx, w\}$	Hash of Ciphertext $\text{hash}(C_p)$	Signature sig_{EPA}

Table 3: Structure of transaction on the IBC.

Block header	Timestamp t	Block ID ID_{IB}	Size size	Prehash hash
Transaction	Producer ID_{ctry}	Search-index $\left(ID_{DB}, ID', \{idx, w\}, \text{hash}(C_p)\right)$		Signature sig_{ctry}

immunity passports, and uploading the ciphertext of passports to the IPFS. And EPAs participate in the consensus of DBC to generate new blocks.

Domestic Blockchain (*DBC*). There are many DBCs in our model. The role of DBC nodes is played by EPAs of each country and the transaction on DBC is broadcast by EPAs.

International Blockchain (*IBC*). Only one IBC exists in our model. The role of IBC nodes is played by institutions on behalf of countries, such as the ministry of health.

Customs. The staff of customs gets the ciphertext of passport and decrypt it after achieving mutual authentication with the user, where a session key is negotiated for transferring the trapdoor and the decryption key.

Structure of Transaction. We deployed two types of blockchain in our scheme, thus we designed different structures of transaction.

The structure of transactions on DBCs is shown in Table 2, including identity of EPA ID_{EPA} that generates the DBC-transaction, pseudoidentity of the inoculator ID', the keyword-index $\{idx, w\}$, hash of the ciphertext of the passport $\text{hash}(C_p)$, and signature of the EPA sig_{EPA}.

The structure of transactions on the IBC is shown in Table 3, including identity of the country ID_{ctry} that generates the IBC-transaction, signature of the country sig_{ctry}, and search-index $(ID_{DB}, ID', \{idx, w\}, \text{hash}(C_p))$. The search-index is composed of ID of the DBC-block, pseudoidentity of the inoculator, the keyword-index, and hash of the ciphertext of the passport.

3.3. Security Goals. We assumed that all blockchain nodes and customs staffs are semihonest, and attackers can eavesdrop on messages while users are communicating with other entities. Based on the assumption, we propose the following security goals.

Confidentiality and Privacy. Our scheme is based on the blockchain, and data stored on the blockchain is shared and transparent. The scheme needs to satisfy user's personal privacy and the confidentiality of immunity passports.

Mutual Authentication. In the proposed scheme, users need to communicate with customs staff. In order to ensure the legitimacy of two parties, they need to achieve mutual authentication before communication.

Traceability and Nonrepudiation. The EPA is responsible for user's health after vaccination. Accordingly, the goals of traceability and nonrepudiation should be achieved in our scheme.

Other Attacks. Furthermore, our scheme should also be able to resist other attacks, such as impersonation attack and insider attack.

4. The Proposed Scheme

In order to facilitate readers to better understand the application scenario, we have made a brief overview of the scheme before describing the details. For the convenience of presentation, it is assumed that the entire process takes user U_1 as an example, referring to Figure 1.

(1) Firstly, U_1 will get his legal pseudoidentity and his full public-private key pair by interacting with KGC.

(2) Then, U_1 is vaccinated at the EPA_1 after mutual authentication with the EPA_1.

(3) Subsequently, EPA_1 generates an immunity passport for U_1 and stores the ciphertext of the passport in IPFS, and two different transactions will be uploaded to DBC_1 and IBC, respectively.

(4) When U_1 travels through the customs, send the decryption key and trapdoor to the staff through the negotiated session key after mutual authentication. The staff will issue a request to the IBC node to search for the corresponding transaction.

(5) Finally, IPFS sends the ciphertext of the passport to the staff, who can verify user's vaccination information.

The detail scheme mainly contains the following phases.

4.1. System Setup and User-Registration. In this phase, KGC generates system parameters and its public-private key pair. The user obtains a legal pseudoidentity and generates his full public-private key pair through the partial-private key generated by KGC (as shown in Figure 2).

System-Setup. To generate system parameters, KGC chooses two multiplicative cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with a prime order p, an element g, which is the generator of $\mathbb{G}_1$, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$. KGC chooses a secret value $SK = x \in \mathbb{Z}_P^*$ and calculates PK as

$$PK = g^x. \tag{1}$$

The IBC node chooses a secret value $SK_c = x_c$ and calculates PK_c as

$$PK_c = g^{x_c}. \tag{2}$$

Then, KGC selects some secure hash functions $H_1 : \{0,1\}^* \times \mathbb{G}_1 \longrightarrow \{0,1\}^{n_a}$, $H_2 : \{0,1\}^* \times \mathbb{G}_1 \longrightarrow \mathbb{Z}_p^*$, $H_3 : \{0,1\}^* \times \mathbb{G}_1^2 \longrightarrow \mathbb{Z}_p^*$, $H_4 : \{0,1\}^* \longrightarrow \{0,1\}^{n_b}$, $H_5 : \mathbb{G}_2^2 \times \{0,1\}^* \longrightarrow \{0,1\}^{n_c}$, $H_6 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1^3 \longrightarrow \{0,1\}^{n_d}$. The system parameters $params = <\mathbb{G}_1, \mathbb{G}_2, p, e, g, PK, H_1, H_2, H_3, H_4, H_5, H_6>$ are published.

User-Registration. KGC randomly picks $\mu \in \mathbb{Z}_P^*$, calculates g^μ, and sends g^μ to the user. The user chooses a secret value $x_i \in \mathbb{Z}_P^*$ and calculates X_i and his pseudo-identity ID_i' as

$$X_i = g^{x_i}, \tag{3}$$

$$ID_i' = H_1(ID_i \| (g^\mu)^{x_i}), \tag{4}$$

then sends ID_i' and X_i to KGC. KGC checks whether formula (5) is valid.

$$ID_i' = H_1\left(ID_i \middle\| X_i^\mu\right). \tag{5}$$

If the equality holds, KGC picks $r_i \in \mathbb{Z}_P^*$ and calculates R_i, k_i, and d_i according to

$$R_i = g^{r_i}, \tag{6}$$

$$k_i = H_2\left(ID_i' \| R_i\right), \tag{7}$$

$$d_i = g^{r_i + k_i x}. \tag{8}$$

KGC sends the partial-private key $D_i = (R_i, d_i)$ to the user through a secure channel. The user sets his full public-private key pair to: $pk_i = (R_i, X_i)$ and $sk_i = (x_i, d_i)$.

Once the user has his legal pseudoidentity and full public-private key pair, he will use the pseudoidentity to participate in the next phases.

4.2. Passport Generation and Storage. In this phase, the EPA vaccinates the user and generates an immunity passport after authenticating user's pseudoidentity, then stores the ciphertext of the passport on IPFS. Subsequently, different types of transaction will be uploaded to IBC and DBC.

User-Authentication. The user chooses a secret value $u_i \in Z_q^*$, calculates U_i, h_i, and V_i according to

$$U_i = g^{u_i}, \tag{9}$$

$$h_i = H_3\left(ID_i' \| U_i \| X_i\right), \tag{10}$$

$$V_i = g^{h_i x_i + h_i u_i} \cdot d_i, \tag{11}$$

and sends a signature $\text{sig}_i(U_i, V_i)$ to EPA. EPA calculates k_i, h_i as

$$k_i = H_2\left(ID_i' \| R_i\right), \tag{12}$$

$$h_i = H_3\left(ID_i' \| U_i \| X_i\right), \tag{13}$$

and checks Equation (14). If the equation holds, the user is considered legitimate.

$$e(V_i, g) = e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g\right) e\left(U_i^{h_i}, g\right). \tag{14}$$

Passport-Storage. EPA generates the immunity passport passpt $\in \{0,1\}^*$ for the user, randomly picks $l_i \in Z_q^*$, and calculates L_i, the ciphertext of the passport C_p according to

$$L_i = X_i^{l_i}, \tag{15}$$

$$C_p = \left\{ e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g^{l_i}\right) \times \text{passpt}, L_i \right\}, \tag{16}$$

and the hash of the ciphertext $\text{hash}(C_p) = H_4(C_p)$. EPA gets sig_{EPA} by signing the $\text{hash}(C_p)$, extracts the ID of vaccine $ID_v \in \{0,1\}^*$ as the keyword $w = ID_v$, and calculates the index of keyword idx as

$$idx = H_5\left(e\left(g^{l_i}, g\right) \| w\right). \tag{17}$$

EPA stores C_p in IPFS and broadcasts $\{ID_{EPA}, ID_i', \{idx, w\}, \text{hash}(C_p), \text{sig}_{\text{EPA}}\}$ as a new transaction. Then, the transaction is uploaded to DBC after being verified by other EPAs. After a new block is generated on the DBC, the IBC node sets $(ID_{DB}, ID', \{idx, w\}, \text{hash}(C_p))$ as the search-index and broadcasts $\{ID_{\text{ctry}}, (ID_{DB}, ID', \{idx, w\}, \text{hash}(C_p)), \text{sig}_{\text{ctry}}\}$ as a new transaction. After being verified by other countries, the transaction is uploaded to IBC.

After the end of this phase, the ciphertext of user's passport is stored in IPFS, the corresponding keyword-index and search-index are also uploaded to the blockchain as transaction information.

4.3. Identity Authentication and Key Agreement. In this phase, the user and customs staff perform identity authentication to confirm both of them are legitimate, and a secure session key is negotiated for subsequent data transmission, as depicted in Figure 3.

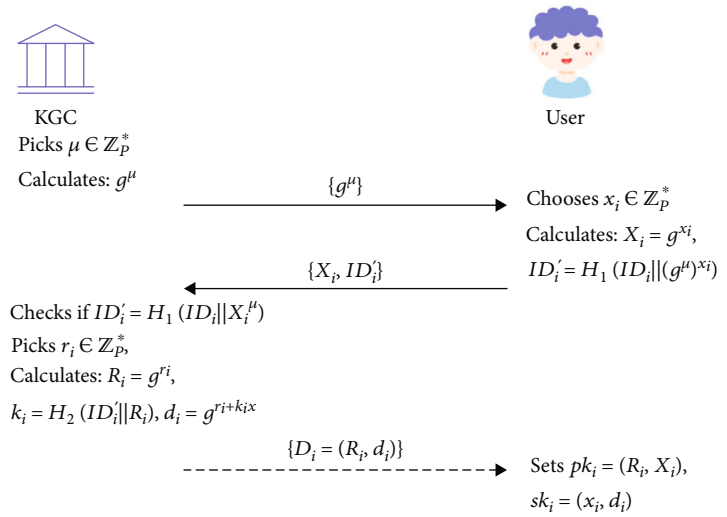

Figure 2: Generation of pseudoidentity and public-private key pair.

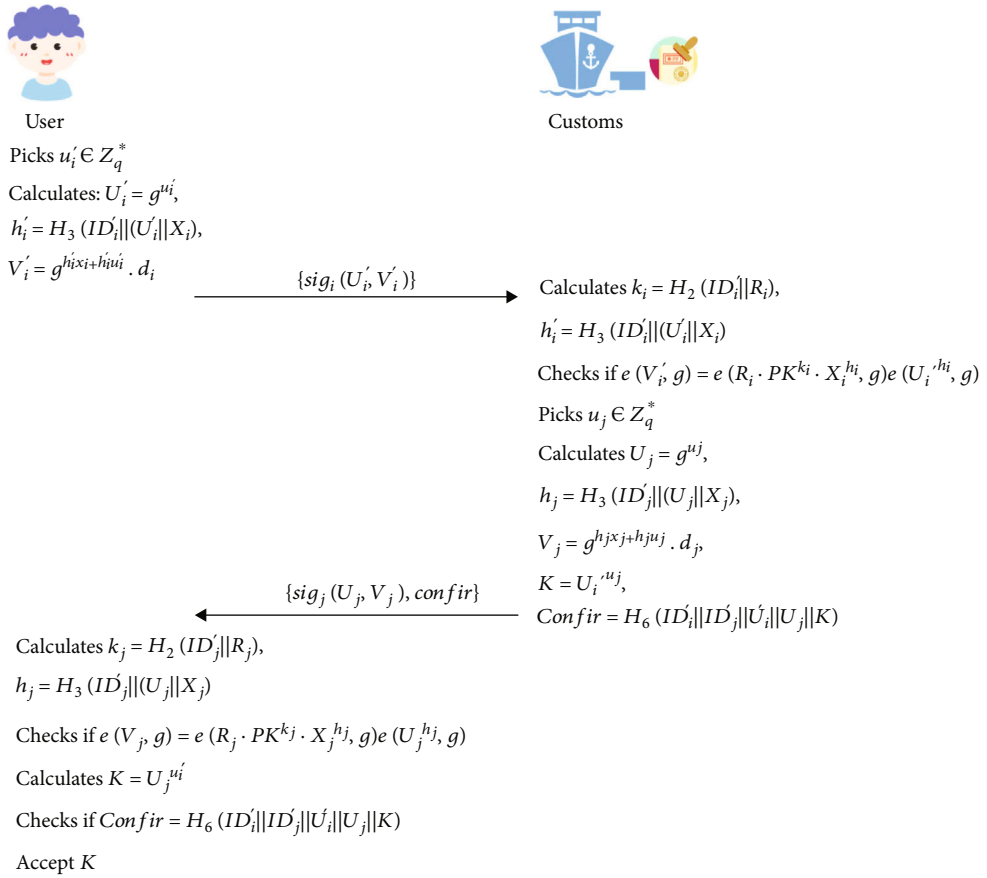

Figure 3: Identity authentication and key agreement for user and customs staff.

Authentication and Negotiation. The user randomly picks $u_i' \in Z_q^*$ and calculates U_i', h_i', V_i' to authenticate with the customs staff as in the "User-Authentication". After authenticating user's identity, the staff picks $u_j \in Z_q^*$ and calculates U_j, h_j, and V_j to obtain the signature $sig_j(U_j, V_j)$ according to

$$U_j = g^{u_j}, \tag{18}$$

$$h_j = H_3\left(ID_j'||U_j||X_j\right), \tag{19}$$

$$V_j = g^{h_j x_j + h_j u_j} \cdot d_j. \tag{20}$$

Table 4: Comparisons of functional properties.

	[20]	[21]	[22]	Ours
Anonymity	×	√	√	√
Universal	×	×	√	√
Mutual authentication	×	×	×	√
Access control	√	√	√	√

Then, the staff calculates the session key K, the key confirmation message Confir, and sends $\{sig_j(U_j, V_j), Confir\}$ to the user. K and Confir can be computed as

$$K = U_i^{'u_j}, \tag{21}$$

$$\text{Confir} = H_6\left(ID_i' \middle\| ID_j' \middle\| U_i' \| U_j \| K\right). \tag{22}$$

The user calculates k_j, h_j according to

$$k_j = H_2\left(ID_j' \| R_j\right), \tag{23}$$

$$h_j = H_3\left(ID_j' \| U_j \| X_j\right), \tag{24}$$

checks Equation (25). If the equation holds, the staff is considered legitimate.

$$\left(V_j, g\right) = e\left(R_j \cdot PK^{k_j} \cdot X_j^{h_j}, g\right) e\left(U_j^{h_j}, g\right). \tag{25}$$

The user then calculates K and verifies whether Equation (22) is established. And the session key K is accepted if the equation is established. The K can be computed as

$$K = U_j^{u_i'}. \tag{26}$$

The user has completed the mutual authentication with the staff, and both of them have obtained the same session key for the transmission of important information.

4.4. Passport Search and Access. In this phase, the staff gets a trapdoor and a decryption key from the user through the session key and uses the trapdoor to get the ciphertext of passport from IPFS. Then, with the decryption key, the staff decrypts the ciphertext to obtain the passport.

Passport-Search. The user calculates the trapdoor T, and the decryption key K_p according to

$$T = g^{1/x_i} \cdot PK_c^{u_i}, \tag{27}$$

$$K_p = e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, L_i\right)^{1/x_i}, \tag{28}$$

sends $\{T, K_p\}$ to the staff with the support of K. The staff sends $\{T, U_i\}$ to an IBC node. The IBC node calculates T' as

$$T' = \frac{T}{U_i^{SK_c}}, \tag{29}$$

and checks Equation (30), and locates the specific block on the DBC according to the ID_{DB} if the equation holds. Then, IPFS searches corresponding C_p according to the hash(C_p) and sends it to the staff.

$$idx = H_5\left(e\left(L_i, T'\right) \| w\right). \tag{30}$$

Passport-Access. The staff decrypts the C_p with the decryption key K_p, where passport $= C_p/K_p$.

At this point, the staff uses user's trapdoor to search for the ciphertext of the passport. Through the decryption key, user's passport is finally obtained by the staff.

5. Correctness and Security Analysis

5.1. Correctness and Security Analysis. In this section, we analyse the correctness of critical steps in our scheme.

Authentication-Correctness:

$$\begin{aligned} e(V_i, g) &= e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g\right) e\left(U_i^{h_i}, g\right) \\ &= e\left(g^{h_i x_i + h_i u_i} \cdot d_i, g\right) = e\left(g^{h_i x_i + h_i u_i} \cdot g^{r_i + k_i x}, g\right) \\ &= e\left(g^{r_i + k_i x + h_i x_i + h_i u_i}, g\right) = e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i} \cdot U_i^{h_i}, g\right) \\ &= e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g\right) e\left(U_i^{h_i}, g\right). \end{aligned} \tag{31}$$

Decryption-Correctness:

$$\begin{aligned} \text{passport} = \frac{C_p}{K_p} &= \frac{C_p}{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, L_i\right)^{1/x_i}} \\ &= \frac{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g^{l_i}\right)}{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, L_i\right)^{1/x_i}} \times \text{passpt} \\ &= \frac{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g^{l_i}\right)}{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, X_i^{l_i}\right)^{1/x_i}} \times \text{passpt} \\ &= \frac{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g^{l_i}\right)}{e\left(R_i \cdot PK^{k_i} \cdot X_i^{h_i}, g^{x_i l_i}\right)^{1/x_i}} \times \text{passpt} = \text{passpt}. \end{aligned} \tag{32}$$

Table 5: Comparison of computational complexity.

Scheme	Users	Other devices	Total
[23]	$3T_h + 2T_m + 1T_e + T_p$	$4T_h + 2T_m + 1T_e + 2T_p$	$7T_h + 4T_m + 2T_e + 3T_p$
[24]	$5T_h + 4T_m + 1T_e + T_p$	$5T_h + 5T_m + 3T_a + T_p$	$10T_h + 9T_m + 1T_e + 3T_a + 2T_p$
Ours	$4T_h + 3T_m + 3T_e + T_p$	$4T_h + 3T_m + 3T_e + T_p$	$8T_h + 6T_m + 6T_e + 2T_p$

Search-Correctness:

$$\begin{aligned} idx &= H_5\left(e\left(L_i, T'\right)\|w\right) = H_5\left(e\left(X_i^{l_i}, \frac{T}{U_i^{SK_c}}\right)\|w\right) \\ &= H_5\left(e\left(g^{x_i l_i}, \frac{g^{1/x_i}\cdot PK_c^{u_i}}{g^{u_i SK_c}}\right)\|w\right) \\ &= H_5\left(e\left(g^{x_i l_i}, \frac{g^{1/x_i}\cdot g^{SK_c u_i}}{g^{u_i SK_c}}\right)\|w\right) \\ &= H_5\left(e\left(g^{l_i}, g\right)\|w\right) = idx. \end{aligned} \tag{33}$$

5.2. Security Analysis. Confidentiality and Privacy. In our scheme, the user interacts with other entities by virtue of a legal pseudoidentity. The attacker cannot infer user's real identity through the ID' unless he cracks user's secret key x_i or the random number μ picked by the KGC. The attacker also cannot obtain effective data even if the IPFS is hacked, because the IPFS stores the ciphertext of passport. In the step of "Passport-Search," only the user can generate a trapdoor and send it to the staff for searching, and then, IPFS returns the corresponding C_p to the staff. Thus, users have full control over their data.

Mutual Authentication. In the phase of "Authentication and Negotiation," the user signs his identity information with the private key $sk_i = (x_i, d_i)$ to get $\text{sig}_i(U_i, V_i)$, where $V_i = g^{h_i x_i + h_i u_i}\cdot d_i$. The customs staff verifies V_i with user's public key $pk_i = (R_i, X_i)$. The correctness of this step has been given above. Therefore, the scheme achieves the goal of mutual authentication.

Traceability and Nonrepudiation. In our scheme, the information of each user's vaccination is uploaded to DBC and IBC. Each transaction contains the identity of the producer, known as ID_{EPA} or ID_{ctry}. Once the user has a health problem due to the vaccine, it can be traced back to the corresponding country or EPA, and the corresponding sig_{EPA} and sig_{ctry} can avoid producer repudiation.

Impersonation Attack. It is impossible for an attacker to pose as a legitimate user unless he cracks user's private key sk_i, and the attacker cannot impersonate the staff as well. Assume that an attacker wants to impersonate a legitimate entity, he must sign with user's private key in the "Authentication and Negotiation" phase, which is hard because only the user knows the secret value x_i.

Insider Attack. KGC cannot reveal the private key sk_i of users because it is only responsible for generating partial-private keys in the phase of "User-Registration." In addition, all the vaccination records will be uploaded to blockchain, and the traceability and nonrepudiation characteristics ensure that blockchain nodes will not upload fake information.

6. Performance Evaluation

In this section, we make a functional property comparison between the proposed scheme and the existing immunity passport schemes [20–22]. Then, the proposed scheme is compared with the existing authentication schemes [23, 24] in terms of computational overheads, communicational overheads, and energy overheads.

6.1. Functional Comparison. Table 4 shows the comparison of the functional properties of our scheme with other immunity passport schemes. From Table 4, we can see that all four schemes achieve access control of user data. Hasan et al.'s scheme [20] cannot provide anonymity, although blockchain is used in their scheme. Schemes in [21, 22] did not consider the issue of coordination between different departments in multiple countries in the scenarios of immunity passport. Moreover, schemes in [20–22] all cannot provide mutual authentication between the user and the passport inspector. Our scheme achieves these functions well.

6.2. Overheads Comparison. The computational complexity comparison of our scheme and schemes [23, 24] in the phase of authentication is shown in Table 5. Among them, T_h, T_m, T_e, T_a, and T_p, respectively, represents the time of hash function, point multiplication, modular exponentiation, point addition, and bilinear mappings.

For comparing the computational overheads, we conducted simulations on a PC with an Intel Core i5-7300HQ CPU at 2.50 GHz and 8 GB RAM, running Windows 10 Home (64 bit). Simulations show that the operation time of T_h, T_m, T_e, T_a, and T_p, which are about 0.0018 ms, 0.0012 ms, 0.0021 ms, 0.0127 ms, and 2.7737 ms, respectively. The computational overhead comparison of the user, other devices, and the total are shown in Figures 4, 5, and 6.

As for the computation of users, user in our scheme requires to calculate $\{U_i', h_i', V_i', k_j, h_j, e(V_j, g), K\}$, that is $4T_h + 3T_m + 3T_e + T_p$ (2.7908 ms). Similarly, Mahmood et al.'s scheme [23] requires $3T_h + 2T_m + 1T_e + T_p$ (2.7838 ms), and Jia et al.'s scheme [24] requires $5T_h + 4T_m + 1T_e + T_p$ (2.7908 ms). Figure 4 shows that our scheme is similar as other schemes in terms of users' computational overheads. Comparing the computational overheads of other devices, our scheme requires to calculate $\{k_i, h_i', e(V_i', g), U_j, h_j, V_j, K, \text{Confir}\}$, that is $4T_h + 3T_m + 3T_e + T_p$ (2.7908 ms). Similarly, scheme [23] requires $4T_h + 2T_m + 1$

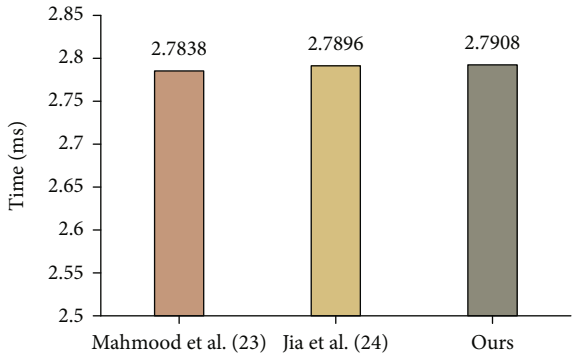

Figure 4: Computational overheads comparison: users.

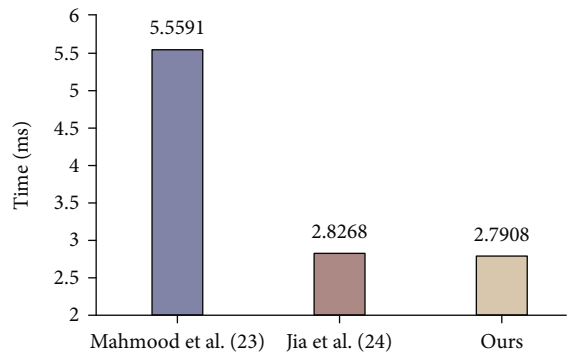

Figure 5: Computational overheads comparison: other devices.

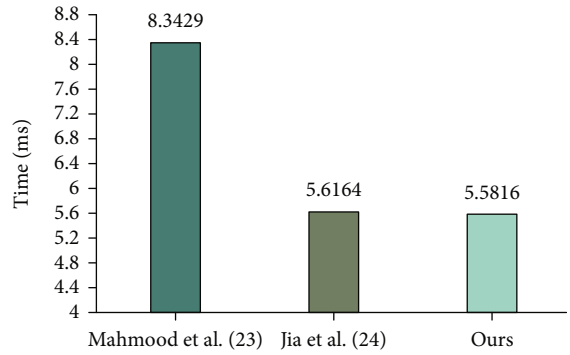

Figure 6: Computational overheads comparison: total.

$T_e + 2T_p$ (5.5591 ms), and scheme [24] requires $5T_h + 5T_m + 3T_a + T_p$ (22.8268 ms). As can be seen from Figure 5, our scheme and scheme [24] are significantly better than scheme [23], because the number of bilinear mappings operation is reduced, which is time-consuming. Furthermore, it can be seen that the computational overheads of our scheme are equal between the users and other devices. As for the total computational overheads, our scheme performs similarly to scheme [24], with a 33.10% reduction compared to scheme [23], which can be seen from Figure 6.

The bit length of a signature, a public key pair, and the hash values are assumed 256 bits. The identity and the timestamp are, respectively, assumed 128 bits and 32 bits, respectively. Our scheme needs to transmit $\{|U_i'|, |V_i'|, |U_j|, |V_j|, |\text{Confir}|\}$,

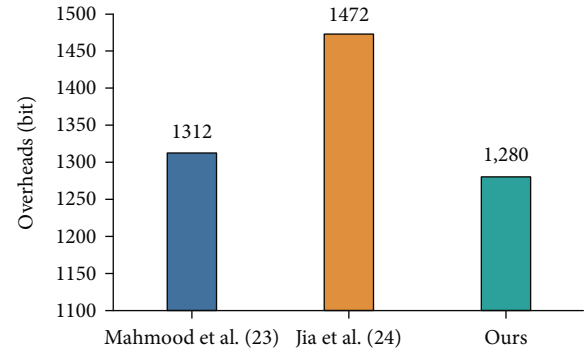

Figure 7: Communicational overheads comparison: total.

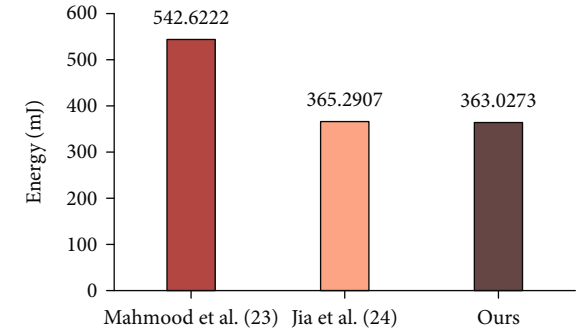

Figure 8: Energy overheads comparison: total.

that is 1280 bits. Similarly, scheme [23] needs to transmit 1312 bits during authentication; scheme [24] needs to transmit 1472 bits. We can see from Figure 7 that the performance of the communicational overhead of our scheme is a little different from scheme [23]. However, our scheme only requires two rounds of massage exchange, whereas scheme [23] requires three rounds. And our scheme reduced 13.04% compared to scheme [24] because the transmission of unnecessary information is reduced in our scheme, such as timestamps.

Energy overheads is also an important evaluation indicator. We use the voltage and current of the PC used in the simulations for comparing energy overheads, which are 1.2 V and 54.2 A, respectively. A hash function consumes 1.2 V $*$ 54.2 A $*$ 0.0018 ms = 0.1171 mj, a point multiplication consumes 1.2 V $*$ 54.2 A $*$ 0.0012 ms = 0.0780 mj, a modular exponentiation consumes 1.2 V $*$ 54.2 A $*$ 0.0021 ms = 0.1366 mj, a point addition consumes 1.2 V $*$ 54.2 A $*$ 0.0127 ms = 0.8260 mj, and a bilinear mappings consumes 1.2 V $*$ 54.2 A $*$ 2.7737 ms = 180.4014 mj. The total energy overheads comparison can be seen in Figure 8, which shows that the energy overheads of our scheme is almost equal to that of scheme [24] and still better than that of scheme [23].

7. Conclusion

In this paper, we propose an immunity passport scheme to mitigate the impact of COVID-19. This scheme helps people travel between different countries without going through tedious epidemic prevention procedures in this era of postepidemic. The highlight of this scheme is that it combines

searchable encryption and authentication with blockchain, which ensures users' privacy and allows them to have control over their data. According to the security analysis, our scheme can well meet the security requirements of the immunity passport scenarios. Furthermore, the evaluation results show that compared with other schemes, our scheme has better communication and computing performance while achieving the functional properties. In the next, designing an efficient consensus mechanism and detailed smart contracts for this scheme is our future research direction.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors' Contributions

Hancheng Gao and Haoyu Ji are the co-first author.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (grant numbers 62072252 and 61872194).

References

[1] O. E. Awosusi and E. Shaib, "COVID-19 induced changes on lifestyles education and socio-economic activities in West African states: recovery strategies for post Pandemic Era," *International Journal of World Policy and Development Studies*, vol. 6, no. 64, pp. 38–43, 2020.

[2] T. P. Velavan and C. G. Meyer, "The COVID-19 epidemic," *Tropical Medicine & International Health*, vol. 25, no. 3, pp. 278–280, 2020.

[3] R. Padhan and K. P. Prabheesh, "The economics of COVID-19 pandemic: a survey," *Economic Analysis and Policy*, vol. 70, pp. 220–237, 2021.

[4] J. S. Tregoning, K. E. Flight, S. L. Higham, Z. Wang, and B. F. Pierce, "Progress of the COVID-19 vaccine effort: viruses, vaccines and variants versus efficacy, effectiveness and escape," *Nature Reviews Immunology*, vol. 21, no. 10, pp. 626–636, 2021.

[5] J. V. Lazarus, S. C. Ratzan, A. Palayew et al., "A global survey of potential acceptance of a COVID-19 vaccine," *Nature Medicine*, vol. 27, no. 2, pp. 225–228, 2021.

[6] M. Sallam, "COVID-19 vaccine hesitancy worldwide: a concise systematic review of vaccine acceptance rates," *Vaccines*, vol. 9, no. 2, p. 160, 2021.

[7] M. Ansari, A. Mohammad Aghaei, Y. Rezaie, and Y. Rostam-Abadi, "Discrimination in COVID-19 vaccination programs - a possible risk for mental health," *Asian Journal of Psychiatry*, vol. 63, article 102758, 2021.

[8] C. Dye and M. C. Mills, "COVID-19 vaccination passports," *Science*, vol. 371, no. 6535, p. 1184, 2021.

[9] I. de Miguel Beriain and J. Rueda, "Immunity passports, fundamental rights and public health hazards: a reply to Brown et al.," *Journal of Medical Ethics*, vol. 46, no. 10, pp. 660-661, 2020.

[10] J. Pang, Y. Huang, Z. Xie, J. Li, and Z. Cai, "Collaborative city digital twin for the COVID-19 pandemic: a federated learning solution," *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 759–771, 2021.

[11] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[12] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[13] S. Xu, X. Chen, and Y. He, "EVchain: an anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 845–856, 2021.

[14] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, 2021.

[15] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, and G. Garg, "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model," *IEEE Access*, vol. 8, pp. 159402–159414, 2020.

[16] J. Song, T. Gu, X. Feng, Y. Ge, and P. Mohapatra, "Blockchain meets COVID-19: a framework for contact information sharing and risk notification system," 2020, http://arxiv.org/abs/2007.10529.

[17] S. Jacob and J. Lawarée, "The adoption of contact tracing applications of COVID-19 by European governments," *Policy Design and Practice*, vol. 4, pp. 1–15, 2020.

[18] S. Abuhammad, O. F. Khabour, and K. H. Alzoubi, "COVID-19 contact-tracing technology: acceptability and ethical issues of use," *Patient Preference and Adherence*, vol. Volume 14, pp. 1639–1647, 2020.

[19] S. M. Idrees, M. Nowostawski, and R. Jameel, "Blockchain-based digital contact tracing apps for COVID-19 pandemic management: issues, challenges, solutions, and future directions," *JMIR Medical Informatics*, vol. 9, no. 2, article e25245, 2021.

[20] H. R. Hasan, K. Salah, R. Jayaraman et al., "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020.

[21] S. Chaudhari, M. Clear, P. Bradish, and H. Tewari, "Framework for a DLT based COVID-19 passport," *Intelligent Computing*, pp. 108–123, 2021.

[22] C. M. Angelopoulos, A. Damianou, and V. Katos, "DHP framework: digital health passports using blockchain–use case on international tourism during the COVID-19 pandemic," 2020, http://arxiv.org/abs/2005.08922.

[23] K. Mahmood, X. Li, S. A. Chaudhry et al., "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, pp. 491–500, 2018.

[24] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," *IEEE Systems Journal*, vol. 14, no. 1, pp. 560–571, 2020.

[25] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, Aqaba, Jordan, 2018.

[26] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[27] M. Pilkington, "Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, pp. 225–253, Edward Elgar Publishing, 2016.

[28] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," *International Workshop on Public Key Cryptography*, vol. 2947, pp. 277–290, 2004.

[29] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, p. 113385, 2020.

[30] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.