BID-HCP: Blockchain Identifier Based Health Certificate Passport System

Yuwen Zhang, Yang Liu(✉), and Cheng Chi

China Academy of Information and Communications Technology, Beijing 100191, China
liuyang7@caict.ac.cn

Abstract. The COVID-19 outbreak severely affected daily life. The World Health Organiza-tion stated that quarantine was the most effective way to control the spread of the epidemic before the vaccine was developed, but this also led to economic recession. At present, there is an urgent need for solutions to ensure the normal schedule of life while reducing the spread of the epidemic. Several contact tracking solutions have been proposed in the market, but they all have certain limitations, such as health certificates do not recognize each other, and user information is leaked. This paper proposes a health passport system based on blockchain identifier (BID-HCP), which ensures that uninfected people travel normally through a unified health certificate passport. What's more, the method separates the user's location information from the user's identity effectively, which protects the user's privacy and efficiently analyzes the high-risk areas of the epidemic.

Keywords: Blockchain · Health certificate passport · Digital identity

1 Introduction

Coronavirus disease 2019 (COVID-19) is a serious infectious disease. The disease has spread globally, with a surge in the number of confirmed cases and deaths from COVID-19 in Europe, Asia, North America and other countries. As of June 20, 2020, 8,776,456 people have been diagnosed and 492,910 have died worldwide. According to the current epidemiological investigation, the incubation period of COVID-19 is 1–14 days. It also has the characteristics of incubation period infection, asymptomatic infection and infection in the general population. In addition, it can be spread through respiratory droplets, close contact and aerosols. All the above shows that COVID-19 is extremely spreading and difficult to control. According to the characteristics of infectious diseases, isolation, and restrictions on the movement of people are the most effective means to control the spread of the epidemic as the world has not yet developed a relevant vaccine. Affected by the epidemic, schools, shopping malls, companies and large enterprises have ceased their normal activities. The suspension of production and economic activities has seriously affected economic development, causing economic halt or even regression. The prolonged epidemic has caused many companies to close. Recently, Hermes Worldwide (HERMS), Chanel, Gucci and other famous luxury goods companies have also

© Springer Nature Switzerland AG 2021
J. Cheng et al. (Eds.): CSS 2020, LNCS 12653, pp. 197–209, 2021.
https://doi.org/10.1007/978-3-030-73671-2_18

announced the suspension of production. According to Moody's Analytics, the global real GDP will fall by 4.5% this year due to COVID-19 [1].

In order to accelerate economic recovery and reproduction, most countries have adopted contact tracing technology to prevent and control the spread of the epidemic. Early tracking was mainly carried out through personnel investigations, which was time-consuming and labor-intensive and may be inaccurate in tracking. Nowadays, the widespread application of smart phones provides convenience for tracking activities [2]. The user's trace can be tracked through the Bluetooth technology and GPS positioning technology of the smart phone, but this method has problem of leaking user privacy. This paper proposes a blockchain identifier based heath certificate passport solution (BID-HCP) to protect citizens' healthy travel and gradually realize economic recovery while reducing the risk of information leakage.

2 Related Work and Demand Analysis

The current international economic development is highly dependent on global tourism and global trade, but with the outbreak of the epidemic, related activities must be suspended. The WHO has given that when no effective vaccine has been developed, the most effective way to control the spread of the epidemic is contact tracing and isolation. Contact tracing refers to tracing potential patients who have been in contact with a confirmed patient to help them obtain care and treatment, thereby preventing the further spread of the virus. Many countries have stopped commercial activities to control the spread of the epidemic [3]. For example, during the outbreak of the epidemic, China adopted a total blockade of Wuhan, an area where the epidemic was severe, and prohibited the entry and exit of people in Wuhan. This measure of isolating infected people has controlled the spread of the epidemic to a certain extent. Subsequently, this measure was adopted almost nationwide to restrict the movement and gathering of people by stopping commercial activities. Therefore, China's epidemic prevention and control work has achieved great results. However, such measures have severely affected production and economic activities, causing companies to suspend production, and the economy has experienced a serious economic downturn. How to ensure normal economic activities while effectively controlling the epidemic is an important issue currently facing. Many countries and companies around the world have taken corresponding measures to help resume production and realize the recovery of economic activities.

China introduced a health code system during the resumption of work and production [4–6]. The health code system determines the user's health information by collecting key data elements in various scenarios. In order to realize the unification of the nationwide code system, the health code system defines a set of unified identification code mapping rules to realize mutual recognition between different systems and ensure that residents are recognized by one code nationwide. The health code uses the user registration method to complete the user information. When registering, the user first needs to fill in some of their own key information in the health code system, and then the health code system relates to the hospital information, and finally combines the first two to determine the user's health status. User information mainly contains four parts. One is the user's own health information, including current body temperature, whether he has fever, cough and

other symptoms related to COVID-19. The second is whether the user has been in contact with people with abnormal physical conditions recently. The third is to directly contact the information of confirmed patients, including whether they have been in contact with confirmed patients or suspected patients of the new crown within 14 days. The fourth is the user's trace. The system collects the user's trace automatically, and through the mobile phone number to confirm whether the user has visited high-risk areas. The above four aspects of information can basically determine the status of the user's own health code. Finally, the above-mentioned health information is entered into the information system, a unified interface is provided to connect with the hospital, and the hospital determines the user's health status. The health code displays the user's health status in the color of the QR code. The QR code of people who are the COVID-19 virus carrier is displayed in red. The QR code of potential patients who have been in contact with the virus patient is displayed in yellow, and the QR code of ordinary residents is displayed in green. Only the people with green QR code can pass through the pre-set checkpoint. This method can only ensure that healthy residents can travel normally and carry out economic activities, but it cannot predict high-risk areas, and the privacy protection of user information is not strong enough.

Singapore launched the TraceTogether solution [7], which uses Bluetooth technology to detect nearby users within a short distance, and exchanges the TraceTogether ID of users in the nearby range. Then the record stores in the mobile terminal to realize contract tracking. This solution requires users to download and install the application. The mobile terminal always needs to keep the Bluetooth device open, actively broadcast and discover nearby device information, and store the close contact record information in the user's mobile terminal. The program introduces encryption technology, all recorded data is encrypted, and it is not uploaded through the network casually. Only those who test positive for COVID-19 will share information with the Ministry of Health to track close contacts, which ensures the privacy of users to a certain extent. The Ministry of Health can quickly trace the close contacts of the patient through the ID information saved in the terminal of the confirmed patient, and notify those who have been in close contact with the patient through TraceTogether. So the user who have been contact with patients can receive treatment as soon as possible, which also blocks the source of infection to a certain extent. The TraceTogether solution does not collect the user's location information, records the user with a random ID, and does not disclose personal identification information. The phone number bound to the ID is stored on a dedicated server and only read when necessary. The ID information stored in the phone will be automatically deleted after 21 days. This method has a certain protective effect on the user's privacy, but from a technical point of view, the Bluetooth device interface has security risks such as eavesdropping and interference. Furthermore, it's power consumption, because Bluetooth is in a long-term communication state.

The world's two major technology giants Google and Apple also adopted a Bluetooth short-range communication solution, which is similar to TraceTogether [8]. Google and Apple created COVID-19 exposure tracking apps for mobile phones to help track the spread of the COVID-19 virus. The application can be used on android and IOS mobile phones, and realizes the mutual detection of Bluetooth between different systems. The solution also relies on Bluetooth technology to identify the device information of

other people who have been in contact with residents, and directly anonymously records and exchanges device information within the Bluetooth range through smart phones insteading of the central database. Finally, ID comparisons are used to confirm whether the user has been in contact with patients carrying the Covid-19 virus, and to conduct contact investigations to reduce the spread of the virus. According to a poll conducted by the "Washington Post", nearly three-fifths of Americans said that they are unwilling or unable to use Google or Apple contact tracking technology because of concerns about privacy leakage. Both of the above methods use Bluetooth to exchange identity IDs to achieve close contact tracking of COVID-19 patients. The program seems to be feasible, but according to experts, the program must ensure that more than 60% of the population are using the program to achieve the purpose of prevention and control effectively. Moreover, this solution has technical problems, high power consumption, and it is impossible to infer the susceptible area.

Mohaned Toky proposed a scheme framework based on blockchain [9]. The system consists of four subsystems: infection verification subsystem, blockchain platform, p2p mobile application and Mass-Surveillance System. The infection verification subsystem simulates the epidemic infection mode through digital simulation technology. The blockchain platform serves as a database to store the infection model data of each case. The P2P mobile application system provides information such as visual infection risk assessment results, prediction data, and infection case detection. The Mass-Surveillance System monitors the user's trace and whether have had contact with the COVID-19 patients. Through the creation of new blocks (new cases) in the blockchain and interactive query of P2P mobile application data, unknown infection cases can be automatically detected. This program can be used to automatically detect infection cases in real time and estimate the risk of COVID-19 infection. Based on the private and security advantages of the blockchain system, the program proposes a concept of epidemic prevention measures, control and tracking plans, and combines the advantages of P2P mobile applications to realize the prediction of unknown infection cases. However, the solution is still under development, and it is not clear how the crowd detection system works, and the incentive model is not clear.

The above methods almost have the problem of user privacy leakage. The bluetooth technology itself is vulnerable to malicious attacks and extremely power-intensive. Although the QR code consumes a small amount of power and collects data only when it is used, but the collected data will eventually be concentrated in the hands of a centralized service provider, which may be at risk of leaking user data. Existing technical solutions have certain limitations [10, 11], and they cannot guarantee normal travel, prediction of high-risk areas, and track potential patients while ensuring privacy. Through the comparative analysis of various programs, this article summarizes the existing problems as follows:

(1) Inadequate Interoperability Considerations. In response to the prevention and control of the COVID-19 epidemic, patient tracking through information technology is a commonly adopted measure in most countries. Each country and region have actively proposed corresponding solutions based on existing technologies, but each solution has certain regional applicability and cannot guarantee cross-regional use. There is still no

interoperability between these existing solutions. Therefore, a global health certificate passport system is needed to ensure the normal development of transnational business.

(2) Lack of Privacy Protection. The current solutions may leak user privacy to a certain extent. Currently, users are paying more and more attention to personal privacy protection, but in order to track close contacts, data sharing is necessary, which leads to the leakage of users' personal information. In the above-mentioned scheme, the user is not willing to use it because of concerns about privacy leakage, which makes it difficult to achieve the purpose of tracking. Data sharing and privacy protection are contradictory, but they must exist at the same time. There is no effective means to solve such problems.

(3) Bluetooth Tracking Technology Restricted. Bluetooth tracking technology is an effective tracking method that uses Near Field Communication (NFC) to achieve close contact record. However, like all wireless communication technologies, the technology itself has security vulnerabilities and is vulnerable to various threats. For example, it is easy for communication information to be eavesdropped, and even other personal information in the user's device is stolen. More importantly, the power consumption of Bluetooth is serious.

(4) Health Certificate without Contact Tracking Insufficiency. The health code in the above scheme only provides a health certificate for the user's travel, and lacks tracking of the user's close contact with the patient. Bluetooth technology can effectively track and record close contacts of COVID-19 carriers, but it does not provide users with health certificates, nor can guarantee normal travel. The existing scheme does not have both health certificate and contact tracking functions.

This paper proposes a health certificate passport system based on blockchain identifier (BID-HCP). Specifically, the use of blockchain technology to achieve credible authentication of digital objects, by defining a set of universal health passport data structure and interaction mechanism to ensure that users can carry out economic activities on a global scale. At the same time, it can also analyze high-risk areas through the user's track, and provide notificaiton services for COVID-19 potential carriers through user authorization.

3 System Design

The blockchain identifier based health certificate passport (BID-HCP) can provide users with a globally unified health certificate, which can ensure that residents get back to a normal daily lives, and then realize economic recovery gradually. This solution uses blockchain technology to construct a unified identity authentication system, a permissions management and information interaction mechanism based on the identity, which can provide health status certificates to the demander while minimizing the leakage of user privacy. The method of separating the user's trace data from the user's personal information is adopted to minimize the leakage of user privacy. It then analyzes the risk level of each region by using big data processing and other technologies. At the same time, contact matching can be performed through user-authorized behaviors, which can locate high-risk groups quickly. In this part, we will introduce the architecture, data model, participating roles, and the interaction process between them based on the blockchain.

Sharing of User Health Information. The global health certificate passport system based on the blockchain requires all participants to register a digital identity, including public keys, encryption protocols and service endpoints. The digital identity is used to identify the user uniquely. The public key is used to authenticate the user's identity, and the user with the corresponding private key is the owner of the identity. The service endpoint is used for interactive sharing of information. Then, the health certificate signed by the testing agency is transferred among different participants in the form of authorized access, thereby realizing the credible health information sharing on a global scale.

Privacy Protection and Contact Trace. The COVID-19 testing agency obtains the trace information of users who are carriers of the COVID-19 virus and publishes it to the service endpoint. The authorized location service provider subscribes and synchronizes the data from the service system controlled by testing angency. After that, the location service provider analyzes the trace data based on big data technology to predict high-risk areas and infer people who may be infected. Finally, the user can submit their own trace information stored on the mobile phone to the location service provider for determining whether they are high-risk infection group, and accept the COVID-19 nucleic acid testing as soon as possible.

3.1 The Functional Architecture of BID-HCP

BID-HCP system provides a reference functional architecture for the mutual recognition of health certificates among different systems, including a common data model and an interaction method (see Fig. 1). In order to ensure that the health certificate can be used on a global scale, the World Health Organization (WHO) is introduced to release the information of the globally recognized COVID-19 nucleic acid testing agency and the health certificate data model.

The BID-HCP system consists of a blockchain layer, an information service layer, and an entity layer. The blockchain layer is the base of the entire system, and each

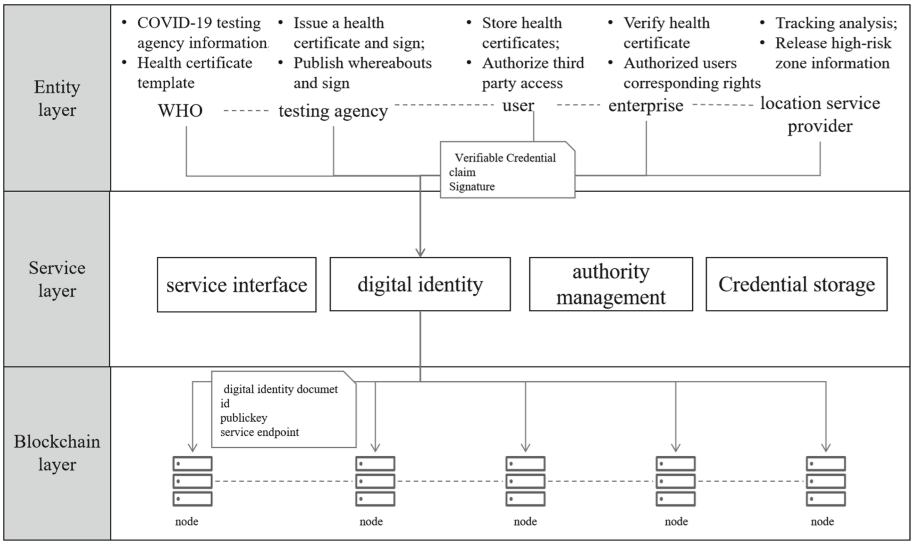

Fig. 1. The functional architecture of BID-HCP

blockchain node stores the digital identity document. The most important thing in the document is the correspondence between the digital identity and the public key, which is mainly used for digital identity verification. The information service layer establishes a secure identity authentication and data exchange mechanism for each participant, which is composed of information service interface, digital identity, data authority management and credential storage modules. The entity layer is composed of health certificate passport participants, and defines the role and data template of each participant.

In this article, the participants in the BID-HCP system are composed of user, WHO, testing agency, enterprise, and location service provider. Each of the participants has an identifier and associated identity description documents on the blockchain. The identity documents include four elements: identity ID, public key, service information URL, and self-declared signature. The public key is used for identity verification and credential verification when interacting with other roles.

The user (terminal) is the applicant for the health passport. Generally, it is a mobile phone application through which the user can register a digital identity. At the same time, the mobile terminal has the ability to communicate with the location service provider, and record trace information. The trace information is mainly used for contact trace analysis.

The World Health Organization (WHO) mainly conducts qualification assessment of COVID-19 nucleic acid testing agency. Only agencies with corresponding qualifications can provide users with COVID-19 nucleic acid testing services, and have the right to issue health certificates. As well, WHO provides a universal health certificate data template to ensure that the health passport can be used globally.

The testing agency with COVID-19 testing qualification can issue a global health certificate passport.

Enterprise is the user of the health certificate passport. The user presents the health certificate issued by the testing agency to the enterprise. After the enterprise has passed the verification, the user will be granted the right to applied for, such as taking an airplane.

Location service providers have the ability to provide geographic location record. In order to protect user privacy, the location information generated by the user during the activity needs to be returned to the user and stored in the user's mobile terminal. Generally, the geographic location service providers need to register on the chain before communicating with the user terminal,, which can prevent malicious attacks.

3.2 BID: Digital Identity Code and Data Structure Model

The identification coding scheme of this scheme (BID) adopts the Decentralized Identifiers (DIDs) [12, 13] scheme formulated by the International World Wide Web Consortium (W3C), and the coding rule is did:bid:specification. Among them, did is the identification prefix specified by the W3C, bid is a self-developed blockchain registration method, and specification is a customized identification coding scheme for bid. In this scheme, the custom part is the first 12 bits of the hash value of the public key. Each role verified by KYC before registering as a corresponding role to ensure the authenticity of the information. The BID is consist by the BID document and verifiable credential (see Fig. 2). The BID document is used to describe how to use BID credibly, which consist

by publick key, authentication protocol and service endpoint. The verifiable credential are used to indicate the different identities possessed by the entity.

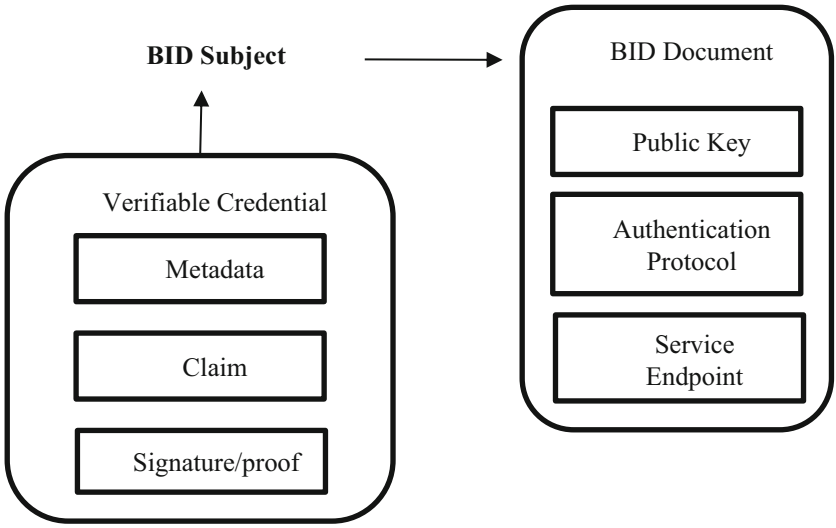

Fig. 2. The structure of BID

The following are the digital identity data model, health certificate data model, and travel data model.

The Digital Identity Data Model:

```
      "id":"did:bid:6cc796b8d6e2fbebc9b3cf9e",
      "type": "Secp256k1",
      "publicKeyHex":
"4b4042665b3235a12fb49730ff620fef1c96e9efa5c90119abd2e8acfe856053"
      "service":
      {
         "id": "did:bid:6cc796b8d6e2fbebc9b3cf9e#resolver",
         "type": "DIDResolve",
         "serviceEndpoint": "https://who.covid-19"//Data exchange interface
      }
      "proof":
      {
         "type": "Secp256k1",
         "creator": "did:did:bid:6cc796b8d6e2fbebc9b3cf9e#keys-1",
         "signatureValue": "QNB13Y7Q9...1tzjn4w=="
      }
```

The Health Certificate Data Model:

id: did:bid:hash(covid-19 passport data)
covid-19 passport：
{
id: did:bid:6cc796b8d6e2fbebc9b3cf9e #Indicates the owner of the health certificate
passport NO: 12345678
covid-19 test result: health
test date: 20200620
Expiry date: 7days
inspection institution: Peking Union Medical College
}
Signature: QNB13Y7Q9...1tzjn4w #Signed by the testing agency to prove that the health certificate is authentic

The Track Data Model:

id: did:bid:hash(track data)
"id": "bid:6cc796b8d6e2fbebc9b3cf9e", #creater
"version": 1,
"created": "2019-10-23T09:14:17.961Z",
"updated": "2019-10-23T09:14:17.961Z",
"COVID-19 track data":
[
{
"location": "beijing ",
"date": "20200708 8:00-9:00",
}
{
"location": "beijing ",
"date": "20200708 8:00-9:00",
}
...
{
"location": "beijing ",
"date": "20200708 8:00-9:00",
}
]
Signature:QNB13Y7Q9...1tzjn4w #Signed by the testing agency to prove that the track is true and effective

3.3 The Workflow of BID-HCP

The registration and use process of the BID-HCP system is mainly divided into three steps. The first step is the digital identity registration, the second step is the health certificate passport application, and the third step is the use process of the health certificate passport. The specific process is as follows (Fig. 3).

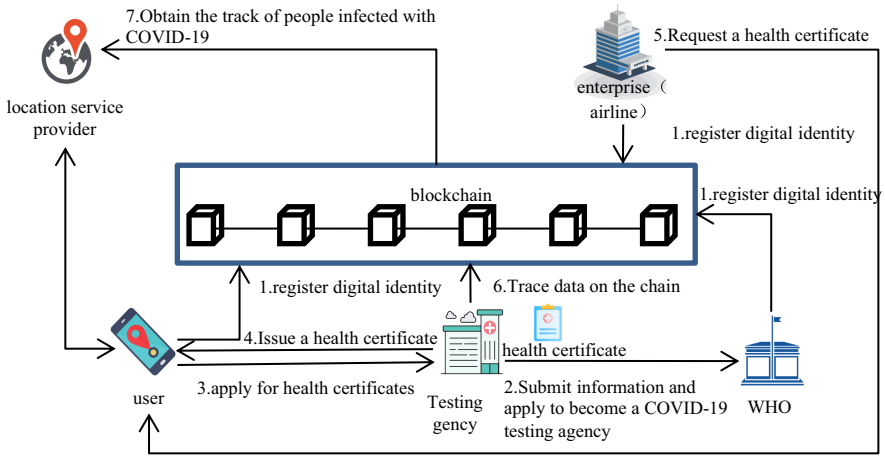

Fig. 3. Flow chart of BID-HCP

(a) **The Process of Registration of Various Roles**
The first step, the user downloads the blockchain wallet through the mobile terminal and generates a public and private key pair, then submits the user information to register the identity through the terminal application, finally publishes the identity and corresponding documents on the blockchain for subsequent interactive verification work. Similarly, other roles also need to register digital identities and publish the corresponding documents on the blockchain.
The second step, the testing agency applies to the WHO to become an international health certification testing agency for COVID-19. After the WHO has reviewed the information of the testing agency, it will expose the testing agency's digital identity to its service information site.

(b) **Health Certificate Passport Application Process**
The third step, enterprises and users query the identity information of testing institutions with COVID-19 testing qualifications through the service information interface of WHO. After obtaining the identity information, the user further queries the detailed information of the testing agency on the chain, including the location of the testing agency, and finally goes to the location for COVID-19 nucleic acid testing.
The fourth step, if the user is a non-virus carrier, the testing agency will issue a health certificate for the user based on the universal health certificate model provided by the WHO and the personal identification information provided by the user for the

user to travel. The health certificate is stored in the service system of the testing agency and the user's mobile phone terminal. In order to protect the user's privacy, the health certificate is stored off-chain instead of on the blockchain.

(c) **Use Process of Health Certificate Passport**
The fifth step, the enterprise requests the user to access the health certificate. The user obtains the company's public key to verify the company's identity by accessing the document on the chain. If the verification is correct, the enterprise can access health certificate owned by user. After obtaining the health certificate, the enterprise queries the public key of the testing agency on the blockchain to verify whether the health certificate is issued by a qualified testing agency. If the verification is passed, the user is granted the corresponding rights, such as taking an airplane.

(d) **Contract Tracking Process**
The sixth step, if the user is a COVID-19 carrier, the testing agency will issue a COVID-19 virus carrier diagnosis for him. At the same time, the testing agency requires the user to provide its trace information and publish the user's trace without exposing user privacy. In order to prove the authenticity of the trace information, the testing agency will sign the trace data with its own private key.
The seventh step, after the testing agency publishes the track of the COVID-19 virus carrier on the server, the location service provider obtains the track of the COVID-19 virus carrier through the subscriber. Then the location service provider analyzes the trace data base big data technology, infer the high-risk areas of the COVID-19 epidemic, and publish the information on its exposed servers. The location service provider matches the user's trace information with the user's authorization. If the matching is successful, they will be classified as a high-risk group, and remind them to perform nucleic acid testing as soon as possible.

4 Challenges and Analysis

The BID-HCP system solves the problem of information sharing between different subjects to a certain extent. The digital island between each system is opened through the health certificate passport. To a certain extent, this solution also protects the privacy of users. However, in terms of technology and management, there are still certain unresolved problems, and further research work is needed.

Blockchain Performance Challenges. The trace data of COVID-19 carriers is stored on the chain, which will cause data expansion. Later, the mode of on-chain and off-chain storage can be considered. Specifically, the trace data is stored off-chain, and the fingerprint of the off-chain data is stored on the chain. Using the form of data fingerprints can not only save storage space, but also ensure that the off-chain data has not been tampered with through on-chain fingerprint verification.

Mobile Phone Storage Space Challenge. In order to prevent the leakage of private data, the verifiable credentials are stored in the mobile terminal, which occupies a large amount of storage space on the mobile phone. Later, it's available using the proxy storage mode to store the verifiable credentials in the proxy server. However, there is a problem that the proxy server grasps user information, which may leak user information. It's a

new challenge that the agency service provider can save user data but not disclose user information.

Location Information Leakage Challenges. It's obvious that location service provider will store the user's geographic location information when the user application interacts with base station, and there is a risk of user privacy leakage. Therefore, it is necessary to formulate user location information security protection management measures to restrict the behavior of location service providers, and protect user privacy.

5 Conclusion

In order to effectively control the spread of the COVID-9 epidemic, a variety of contact tracking applications based on smart phone terminals have been proposed on the market, but these methods expose users' privacy and leads to low user participation. At present, all countries are on the brink of economic recession, and it is necessary to come up with a method that can effectively prevent and control the spread of the epidemic, as well as protect the lives of residents and restore the economy. This article proposes a blockchain identifier based health certificate passport system (BID-HCP) that protects users' privacy while ensuring users' normal travel and resumption of production. On the other hand, this research saves the user's trace data in the mobile terminal, which is controlled by the user, and the data is shared to the demander through authorization, which protects the user's privacy. At present, the BID-HCP system has been deployed and verified in Hubei and some other places, through integration with the National Industrial Internet identification resolution system.

References

1. Zandi, M.: Handicapping the Paths for the Pandemic Economy. Moody's Analytics, June 2020
2. Li, J., Guo, X.: COVID-19 contact-tracing apps: a survey on the global deployment and challenges. Journal (2020)
3. Salathé, M., Althaus, C.L., Neher, R., et al.: COVID-19 epidemic in Switzerland: on the importance of testing, contact tracing and isolation. Swiss Med Wkly (2020)
4. GBT 38961–2020: Personal health information code-Reference model. Standards Press of China, Beijing (2020)
5. GBT 38962–2020: Personal health information code-Data format. Standards Press of China, Beijing (2020)
6. GBT 38963–2020: Personal health information code-Application interface. Standards Press of China, Beijing (2020)
7. Jason, B., et al.: BlueTrace: a privacy-preserving protocol for community-driven contact tracing across borders. Singapore (2020)
8. Apple Inc, Google LLC.: Exposure Notifification-Bluetooth Specification, May 2020
9. Mohamed, T., Ella, H.A.: COVID-19 Blockchain Framework: Innovative Approach (2020)
10. Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W., Imran, M.: BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond (2020)

11. Angelopoulos, Marios, C., Damianou, A., Katos, V.: DHP Framework: Digital Health Passports Using Blockchain - Use case on international tourism during the COVID-19 pandemic. arXiv:abs/2005.08922 (2020)
12. Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/. Accessed 30 Aug 2020
13. Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/. Accessed 30 Aug 2020