A Security Vaccination Passport System Based on Blockchain

Mingdu Huangfu[1(✉)], Yujia Huang[2(✉)], and Ziming Qi[3]

[1] School of Microelectronics, South China University of Technology, Guangzhou, China
duduguonianhao@outlook.com
[2] Institute of Science and Technology, Wenzhou Kean University, Wenzhou, China
1130094@wku.edu.cn
[3] Beijing Haidian Kaiwen School, Beijing, China

Abstract. After the COVID-19 bursts out, all the world has been affected and the worldwide economy is struck because people cannot go out freely and more people tend to stay home due to the coronavirus. Therefore, it is important to think about some solutions to let the citizens travel freely as well as keep them safe. That's one of the reasons why the vaccination passport occurs. Although there are some quite successful vaccination passports, there still exist different problems for the passport. Privacy protection, less complexity, less consumption are the main advantages of our vaccination passport. Because most scruples of the vaccination passport are that whether citizens can use it without submitting much personal information or whether it can prove that people have been vaccinated simply, our vaccination passport aims to increase these parts compared to other vaccination passports. We use blockchain technology which is a kind of decentralized technology to keep individual privacy. Meanwhile, we need less information from the user but a picture. To simplify our vaccination passport, there only are 2 main parts which are the user part and the hospital part. To show the identity that you have been vaccinated, people just need to show the QR code generated by the system and the color of the system will show whether you have the right to go out. All in all, our vaccination passport realizes privacy protection, less complexity, less consumption based on the blockchain and p2p network technology.

Keywords: Blockchain · vaccine passport · p2p network · QR code · health certification

1 Introduction

Coronavirus has made a huge crash to the world's economy since COVID-19 burst out in 2020 [7]. The development speed of the economy of the country which has been affected generally slows down, most of which even declines. The epidemic situation has made every country's economic activity not work properly. Companies stop working and producing, and social unemployment rate increases sharply and capacity decreases,

M. Huangfu, Y. Huang and Z. Qi—Contributed equally.

Z. Zeng et al. (Eds.): ECIT 2022, AHE 11, pp. 796–804, 2023.
https://doi.org/10.2991/978-94-6463-005-3_80

contributing to the recession. According to Moody's analytics, the whole world's actual GDP will decrease about 4.5% in 2020 due to the coronavirus [10]. As the researches for vaccine of COVID-19 advanced, economic conditions had revived since early 2021. People are beginning to focus on developing medical applications, especially the special ecology related to vaccines, to facilitate travel and work in the post-epidemic period.

Vaccination passport, as a special permission for travel, had caught people's attention since the beginning of the epidemic. An authoritative vaccination passport is needed for people who work in specific occupations such as airport workers and flight attendants and work long hours in potentially high-risk areas to certificate their health conditions. But when providing a passport, personal information is at risk of being used maliciously. The main reason for opponents of the vaccine passport is the lack of transparency over the process of registration and information verification. In addition, even with public statements from government departments, most people do not trust the vaccine passport, so absolute technical secrecy is the biggest reason why people are willing to register the vaccine passport.

Unlike most schemes put forward previously used centralized vaccine certification solutions, our study enables the vaccine passport to be both convenient and secure. We manage personal information by hashing algorithms so that it can't be exposed during checks. Benefiting from the characteristics of blockchain technology, the entire information transfer process is immutable, and it is very convenient to supervise the information transformation in blockchain by using the network. That's what optimize the function of our vaccine passport system and make it more complete. The core contribution of the articles are as follows:

1. Designing a vaccination passport system which can help the public go out with the decreasing risk of coronavirus.
2. Implementation of a blockchain-based vaccination passport which can help avoid privacy leaking.

We have discussed the background information in Sect. 2. System functions and design are introduced in Sect. 3 and 4 respectively. In Sect. 5, our vaccination system's advantages and shortcomings are discussed. Finally, we have concluded the article and pointed out our strengths compared with other vaccination passports which already exist.

2 Related Work

A Singapore App named TraceTogether can identify the people who have close contact with the sick people who contract the virus through the user's trip recorded by the Bluetooth connection. Then, the App can upload the data to the government to take action preventing the diseases without collecting the information from the user [2]. TraceTogether adopts a crypto technology to generate random ID to record users without disclosing users' personal information. The phone number bound to the ID is stored on a dedicated server and can only be read when necessary. The ID information stored in the phone will be deleted after 21 days, which protects user privacy to a certain extent. However, APP requires the device to maintain a Bluetooth-communication

state all the time, resulting in high power consumption. Moreover, the Bluetooth device interface has security risks; for example, it may be eavesdropped or interfered. Generally speaking, TraceTogether is a feasible solution for the epidemic situation, but there still are some drawbacks which need to improve. Google and Apple have also adopted short-range Bluetooth communication solutions like TraceTogether [1]. Although there is no centralized database, the device will transmit user information during Bluetooth communication. In general, this is a solution very similar to TraceTogether. Unfortunately, 60% of Americans told a survey that they wouldn't use the APP because the App may leak their personal information. Both solutions have similar problems, such as high consumption, privacy disclosure, and the final effect is also not stable.

In terms of epidemic prevention effect, the health code program adopted by China has achieved more significant results [3–5] This is a complex health system mechanism that does not adopt a blockchain solution. While this ensures that outbreaks are contained, it does a poor job of protecting users' privacy. First of all, users are required to provide a lot of identification information when registering, including name, ID number, home address, mobile phone number, and other key information, to ensure that it can be corresponding to each specific person. Base stations set up by China's major telecom operators can locate the whereabouts of a user with a mobile phone number, and other information is provided to hospitals for further identification and comparison of vaccination information. Such a solution might be perfect in China, but it would be difficult to implement similar solutions in a country like the United States. The main problem is that Chinese people are far less concerned about personal privacy protection than American citizens, for whom such a scheme would be disastrous because they would need to provide a lot of private information. According to a survey in the United States, about 60% of those surveyed explicitly said they would not use a centralized vaccine passport. What is sorely needed, it seems, is a decentralized solution.

None of these solutions seems to take into account the enormous power that blockchain technology can bring. Blockchain technology seems to be tailored to the needs of privacy protection and information security. Let's take a look at some of the solutions that use blockchain and distributed technologies.

Shirajus Salekin Nabil et al. proposed a feasible solution based on the actual situation in Bangladesh [8]. They implemented a solution based on blockchain and QR codes. This solution was instructive to us, but their solution had obvious flaws, wasn't fully functional and, most importantly, wasn't suitable for the application scenario we needed. The participants of the solution are divided into five entities, Authorities, Issuers, Holders, Verifiers, and Vaccine providers. We think we don't need so many entities, and a lot of content can be implemented very well with the features of blockchain. Second, they put a big part of the focus on vaccination priorities. Considering the national conditions of Bangladesh, this is indeed necessary, but the system has already used a large number of computing resources to determine the user's vaccination priority, which is not necessary for some other developed countries [7].

Mohaned Toky proposed a scheme framework based on blockchain and P2P network [9]. The system is divided into the infection verification system, blockchain platform, P2P mobile application and mass monitoring system. The infection verification system simulates the infection mode of virus by digital simulation technology. Blockchain acts

as a database, storing infection model data for each case; P2p mobile application system provides infection risk assessment results and other information; Mass surveillance systems are used to track users' movements and determine whether they are close contacts of infected people. The operation process of the system is rough as follows: through creating a new block in the blockchain (the transaction contained in the block is a new case), an interactive query of P2P mobile application data, and finally automatic detection of unknown infection cases. This approach makes perfect sense in principle, but such systems cannot produce health credentials that allow healthy users to travel normally. That is, it is a good way to track infected and close contacts, but it cannot be used for travel. Moreover, the solution is still under development, and the working mode and incentive mode of the crowd detection system are not clear.

Yuwen Zhang et al. proposed a Blockchain Identifier Based on Bid-HCP (Blockchain Identifier Based) at the International Symposium on (Cyberspace Safety and Security Health Certificate Passport System) [11]. They adopted the W3C's recently proposed DID rule to provide digital identities for registered entities and ensure their authenticity, and worked with nucleic acid testing agencies to issue health certificates to users, so that users without the virus could obtain health certificates and travel with them. And cooperate with global positioning service providers to locate the routes of infected users according to their device terminals [10]. The problem of the scheme proposed by them lies in that the standard of DID is too new, and there are few projects that really apply the standard. There are almost no well-known projects, and no one knows the effect of the final implementation. And the people who came up with it didn't start implementing it, so we don't know when we'll be able to use it.

Based on the existing research results and practical application, it can be seen that there are some good solutions to the huge impact of COVID-19 on the social life and economic development of all countries. But there are some problems. For example, the scheme of using Bluetooth to realize the user's movement tracking requires that the device carried by the user always maintains the Bluetooth communication state, which will undoubtedly lead to high power consumption, neither environmental-friendly nor convenient. In addition, in terms of user privacy protection, these schemes are not completely reassuring to users. Although they achieve a certain degree of decentralization, they are not thorough enough. There are some schemes although the idea is very ingenious, but did not fall for a long time, and cannot be put into practice. Our program is not only convenient and practical, saving energy, but also can ensure that users can travel normally after vaccination.

3 System Functions

3.1 Record Vaccination Information of Users

The system should have the function of accurately recording user inoculation information, and can ensure that the information will not be maliciously modified. We can record vaccination using transactions in blocks of the blockchain. Every piece of personal vaccination information is included in a transaction, and we take advantage of the immutable nature of blockchain to ensure that vaccination information cannot be maliciously modified.

3.2 Provide Travel Vouchers for Healthy Users

The QR code displayed on the DAPP of individual users is a proof of their health status, and the green code is equivalent to a health certificate recognized by the authority. Users can use QR codes to travel easily.

3.3 Protect Users' Privacy

We have achieved the protection of user privacy to the greatest extent. First of all, we don't collect any personal information other than a photo. And user-provided photos are hashed together with the user's ID before being recorded on the blockchain. We don't keep a copy of the user's photo, just a hash to verify the user's identity. And according to the unidirectional characteristics of hash calculation, the current computing power is not enough to support the original data through the calculated hash value. This also ensures that the attacker of the system cannot obtain the real information of the user in any case. Can be described as a complete protection of user privacy.

4 System Design

First, we need authorities to bear the cost of deploying the contract code onto the blockchain. Authorities do not need to register, but their role in the system is to authorize hospitals, verify the authenticity of registered hospitals and give them the power to change individual users' vaccination records. It is worth mentioning that in reality, there are cases where hospitals add vaccination information incorrectly. Due to the immutable property of blockchain, once the vaccination information of individual users is incorrectly recorded, the existence of these erroneous records will lead to a series of problems. Therefore, a confirmation mechanism is set up in our system: when confirming to add user vaccination information, the hospital will send an authentication message to the corresponding individual user address, which contains all the information to be added by the hospital. Individuals receive and confirm the verification message before passing the verification, and the vaccination information is recorded on the blockchain. Individual users cannot actively initiate the addition of vaccination records. The addition of records is initiated by the hospital, but whether it can be successfully added is not entirely dependent on the hospital. This ensures the authenticity of vaccination records and reduces the risk of incorrect records. Moreover, you can find more details in Fig. 1, after the user owns his vaccination passport, when he goes to public places, the QR code generated by the vaccination passport can help prove his safety.

In general, as shown in Fig. 2, our vaccine passport system is used by only two entities: hospitals and individuals. At the time of registration, we need users to confirm whether they are hospital users or individual users. If the user is a hospital user, the relevant information of the hospital must be provided, and the authority will verify the authenticity of the information. Hospitals that pass the test are certified and have the right to add vaccination information to the blockchain. In addition, hospital information will also be provided to all users in the system, including other hospital users and individual users. If you are an individual, you only need to submit a portrait of yourself. The system

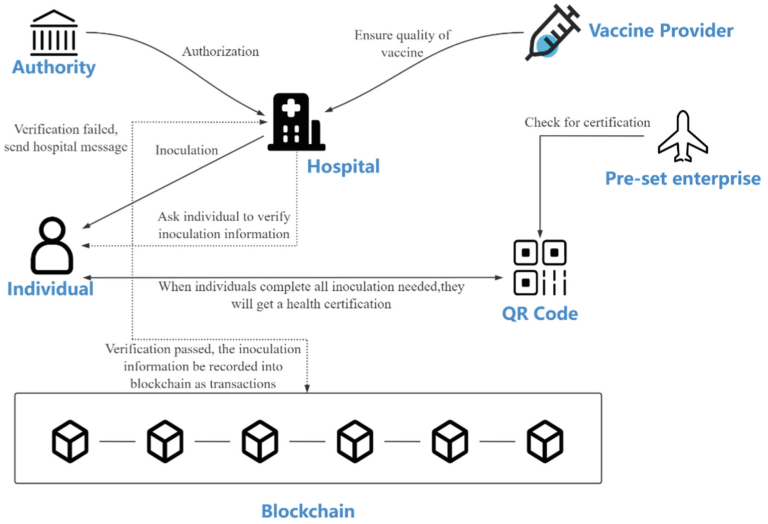

Fig. 1. Workflow of vaccination and certification model

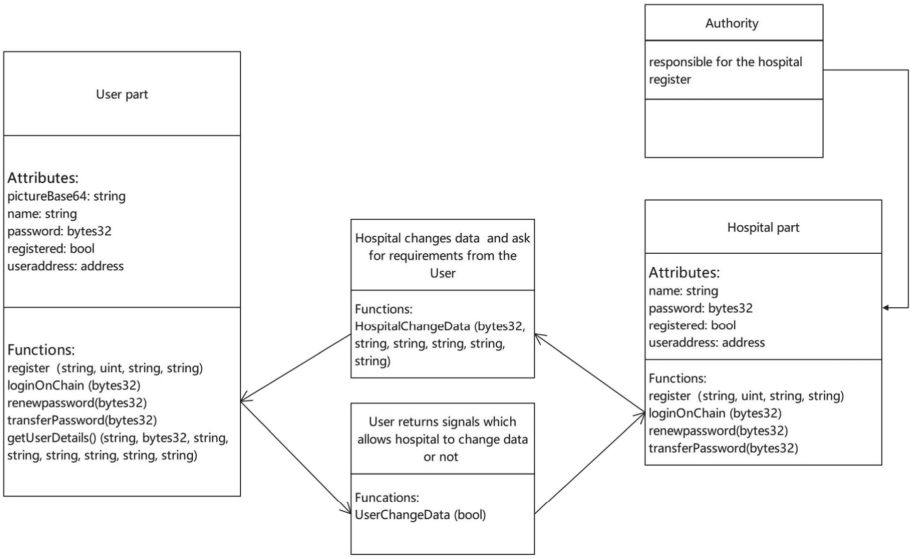

Fig. 2. Class Diagram of the Proposed System

will use the photo provided by the user and the user ID (i.e., the address of the wallet that the user uses to connect to the blockchain) to automatically generate a QR code for verification. The photo information and ID provided by the user will be hashed once, and the hash value obtained will be recorded on the blockchain for further verification. The color of the QR code represents the user's health status: red indicates confirmation of virus infection; Yellow represents those who have not been vaccinated or have not

Fig. 3. Startup layout of proposed system

completed inoculation. These two conditions are not allowed to travel. The green QR code indicates that the user has completed the vaccination and is in good health. Users in this state can use the green code to travel normally. The system will automatically determine and generate the QR code according to the user's vaccination record. The verifier can scan the QR code to confirm whether the user of the vaccine passport is the person holding the passport.

In the login interface, both hospital users and individual users need to enter their private keys to enter the system. After logging in to the hospital, the user can modify the hospital information, such as contact information, address, and hospital name. However, the modification can only take effect after being sent to the authority for certification. After logging in, the hospital can add the information of the inoculator. When adding, the hospital needs to input the wallet address of the inoculator and relevant information of the inoculator. After adding, the hospital will send the confirmation information to the user. If the individual user refuses to confirm, the vaccination will not take effect and hospital-initiated vaccination information will not be added.

There are also a few points worth mentioning: to reduce the amount of data recorded on the blockchain, users' vaccination information is recorded on the chain, and personally identifiable information and hospital-related information are not. Data volume amplification will affect the performance of the blockchain.

We implement our algorithms with html and published them as an open source on github [6]. The initial web interface is as shown in Fig. 3.

5 Discussion

The QR code health certificate does not fully represent the user's real health status. The vaccine passport system we have implemented is aimed at the point of vaccination to judge the user's health status. In other words, our vaccination passport system does a good job of recording and assessing the user's vaccination status, but it is not enough to determine whether the user is healthy or not.

Some people may have contracted the virus before they took to complete a round of inoculations, or even before they were vaccinated. This requires preliminary examination

by the hospital. Once people are diagnosed with infection, they should be recorded in our system, strictly restricting their travel. And all infected people will be marked as red QR code in our system. In addition, there is an immunization rate, not all people who finish the vaccine, 100% will not be infected with the virus. In fact, there are a number of people who get infected after finishing the vaccine, there were such cases happened in China. How to follow up users' infection status in real time, which needs to be combined with other products or technologies. That's not taken into our consideration.

What we want to implement is a completely decentralized, blockchain-based and distributed network-based system that can accurately record users' vaccination status. At this point, we're pretty much there.

It is also worth noting that these features are not sufficient to limit the spread of the disease, as users are not tracked. Chances are that the user has been infected, but not detected in the first place, and in the time between infection and detection, the infected people travelled to other places and came into contact with other people. This can lead to the spread of the epidemic. There are already some solutions on the market, but none of them don't require large amounts of users' personal information, which led to a conflict between the need for immunization and the need for privacy.

In theory, this could be done in conjunction with blockchain while collecting minimal personal information. But if we want to track users without collecting information, that's much more difficult at all. This requires further breakthroughs in blockchain technology.

6 Conclusions

To prevent contagion of COVID-19, there were lots of solutions that had been published on the market. Some of them adopted blue-tooth communication to track people, meanwhile, the system will save traces of people to web service providers. People's information will be submitted to the government when necessary, especially for those who were infected by COVID-19. There were also some solutions that utilized communication base stations to locate and trace people. But they required users to offer a bunch of their private information, like their ID number and phone number, to make sure the system operate well when a user registered. None of these solutions mentioned above don't collect the private information of users. It's obviously unacceptable for those who are privacy-conscious. There also exist solutions designed only for developing countries, which put their emphasis on the priority of vaccine inoculation. It will cost lots of calculation resource of their web service, and it's inconvenient as well. Given that countries have different conditions and requirements, obviously, this sort of scheme will not apply to the developed country like American. In fact, the developing country like China, which has a robust and stable economy will not adopt this kind of scheme, either.

There are other schemes that put forward good frameworks based on blockchain and P2P networks, but none of them have been implemented yet. They are just ideas and pictures. Such solutions are not convincing in terms of functional integrity and performance stability. Unlike the schemes mentioned above, our scheme targets the pain spots of privacy protection requirements, realizing a complete and convenient vaccination passport scheme which is capable enough for accurate recording of vaccination information. We have implemented a completely anonymous way to record personal vaccination information on the blockchain and provide users with health certificates with the right to travel

normally. It greatly facilitates people's travel and provides the greatest convenience for people's economic life, trade and tourism. All in all, we think our plan is worth adopting.

References

1. Apple Inc, Google LLC (2020) Exposure notification-bluetooth specification
2. Bay J et al (2020) BlueTrace: a privacy-preserving protocol for community-driven contact tracing across borders. Government Technology Agency-Singapore, Technical report
3. GBT 38961–2020 (2020) Personal health information code-reference model. Standards Press of China, Beijing
4. GBT 38962–2020 (2020) Personal health information code-Data format. Standards Press of China, Beijing
5. GBT 38963–2020 (2020) Personal health information code-Application interface. Standards Press of China, Beijing
6. https://github.com/polo001107/VaccinePassport_Dapp (2022)
7. McKibbin W, Fernando R (2020) The economic impact of COVID-19. Economics in the Time of COVID-19 45.10.1162
8. Nabil S, Pran Md, Haque A, Chakraborty N, Chowdhury M, Ferdous MdS (2021) Blockchain-based Covid vaccination registration and monitoring
9. Torky M, Hassanien AE (2020) COVID-19 blockchain framework: innovative approach. arXiv preprint arXiv:2004.06081
10. Zandi M (2020) Handicapping the paths for the pandemic economy. Moody's Analytics
11. Zhang Y, Liu Y, Chi C (2020) BID-HCP: blockchain identifier based health certificate passport system. In: International symposium on cyberspace safety and security. Springer, Cham