A Blockchain-Based Multiple-Parties-Involved Vaccination Passport System

Runzhi Wang[1], Bohan Wu[2(✉)], and Taoyue Xia[3]

[1] Business School, Chengdu University, Chengdu, China
[2] College of Software Engineering, Sichuan University, Chengdu, China
wubohan@stu.scu.edu.cn
[3] University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai, China
xiataoyue@sjtu.edu.cn

Abstract. At the end of 2019, COVID-19 roared out across the horizon. As a contagious and fatal virus, it turned the world into a mess and had a profound impact on everyone. Fortunately, with the emergence of vaccines, human beings can have resistance to the virus, and remain a comparative health status. To consummate the vaccination-associated mechanism and improve portability and security, a BbMpiVP system, which is the abbreviation for our Blockchain-based Multiple-parties-involved Vaccination Passport System, is developed. The programming language Solidity was used to write smart contracts based on Ethereum and JavaScript to launch a website that interacts with the contracts. After testing the system on the Ropsten network, the feasibility, as well as security and portability, were proved. Furthermore, a detailed description will be shown in the Method section to give a general picture and deep understanding of how our system works. Finally, the results show that our system will work properly and provide amenities, especially for those who travel frequently.

Keywords: COVID-19 · Blockchain · digital passport · security

1 Introduction

1.1 Background

COVID-19, after astonishing the globe in winter, 2019, is described as The Sword of Damocles hanging over human beings to some extent. So far, some so-called "positive" measures, such as contact tracing and self-quarantining, only function after detecting contagious resources and are far from satisfactory. Considering the healing of previous smallpox, we pin great hopes on precaution measures and resort to the vaccine. Now related R & D and worldwide launch of vaccines have guided us to the post epidemic era. In most countries, the proportion of vaccinated population Up to May 29th, according to the National Health Commission of the People's Republic of China, the national COVID-19 vaccinations in China had reached 600 million doses.

R. Wang, B. Wu and T. Xia—Contributed equally.

Z. Zeng et al. (Eds.): ECIT 2022, AHE 11, pp. 772–785, 2023.
https://doi.org/10.2991/978-94-6463-005-3_78

Nevertheless, there are no ideal mechanisms or regulations to standardize and supervise the vaccination. Even in the countries with a mitigated epidemic, chances are that the epidemic breaks out again due to sporadic and latent cases traveling across various countries, not to mention the severely affected distinctions.

Therefore, the concept of a digital vaccine passport came into being. Considering the risk of latent travellers carrying pathogens, it seems a must to implement comprehensive, reliable verification over their vaccination or nucleic acid test results to get permission to some arenas.

For instance, in terms of the health status of inspectors, the health code used in China is of great reference significance to epidemic prevention. Tracing trajectories of citizens and travellers with GPS provides warrantable information to gauge whether one is at risk of infection on account of his/her exposure to severe epidemic areas. China's health code, cooperating with other technic mechanisms, play their roles in preventing the further deterioration of the epidemic. Although both have obvious effects on epidemic prevention and control, they still have defects and limitations. There is a possibility of information disclosure in European digital passports, which is a critical concern.

1.2 Technology

"A blockchain is a growing list of records, called blocks, that are linked together using cryptography" [2]. In 2008, a group of people using the moniker Satoshi Nakamoto made the blockchain popular "to serve as the public transaction ledger of the cryptocurrency bitcoin" [9]. Blockchain is a new application model of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. Thus, due to its own cryptographic logic principle, it has made greater contributions in preventing information leakage. A collection of centralized networks interconnected in a distributed manner. All nodes of the network will back up the database and share data with each other. Blockchain is a system composed of multiple interrelated blocks, which is used to store the records of all submitted transactions. The previous block will be automatically connected to the subsequent block due to the hash value [5]. In addition to hash values, these blocks also contain transaction data such as timestamps. Blockchain makes it possible to trade without any intermediaries, so it is indeed a decentralized technology. In the blockchain, all nodes act as peer nodes and are treated equally.

1.3 Our Contribution

Due to the cryptographic hash function adopted by blockchain to encrypt data, hackers can get nothing but messy sequences when directly attacking the blockchain. Taking this technology as the basis for mutual trust among multi-parties involved, the blockchain not only ensures the security of personal information but also simplifies the verification procedure and improves work efficiency. The BbMpiVP system not only makes full use of the advantages of the former factors but also tries utmost to fill the previous gaps of other digital vaccine passport systems. The DApp (Decentralized Application) has the following advantages.

- A timestamp is attached to the QR code to prevent the QR code used for verification from being stolen.
- The DAPP adopts the method of two-step verification, as illustrated in detail in the METHODS section.

2 Methods

2.1 Main Procedure

The main idea of the paper is to design a technique for a convenient and secure Vaccination Passport system shared by everyone. After all, "Despite knowing the privacy drawbacks of online access of their healthcare records, 90% of the Americans still prefer online access" [3, 10]. We will use special terminology, BbMpiVP, which is the abbreviation for our blockchain-based multiple-parties-involved Vaccination Passport, in the following introduction. The system works as Figs. 1, 2, 3 and 4 show.

2.1.1 Parties Involved

Figure 1 shows the parties involved. We applied a multiple-party-involved system which strengthens the supervision, compared to those previous Vaccination Passports of which functions include "reading for patients and writing for CDCs (Centers for Disease Control)" [6]. The following figures are illustrations of the procedure.

2.1.2 Passport Delivery and Authorization

Application (Fig. 2): The users will deliver a physical application to the authority to get a blank passport, which is bonded to the user's account. The hospitals will also deliver some materials to get qualified to vaccinate. As a consequence, the authority will give them the certificate as granted.

2.1.3 Vaccination and Validity Verification

Vaccination and Validity Verification (Fig. 3): After the passport is delivered, each time a user goes to the hospital to get a vaccination, the information of the dose as well as part of his personal information needed will be submitted to one of the authorities to get verified. The authority will check that vaccination and decide whether valid or not. The basis of determination includes information, such as the unique ID number of each dose, dates of vaccination, and so on. Also, if necessary (e.g., after a specific number of vaccinations, the user reaches the total pseudo-healthy standard. If some vaccination goes out of date, the health status is not guaranteed), the authority will change the user's health status depending on the information submitted.

Fig. 1. Different parties involved in the vaccine passport project

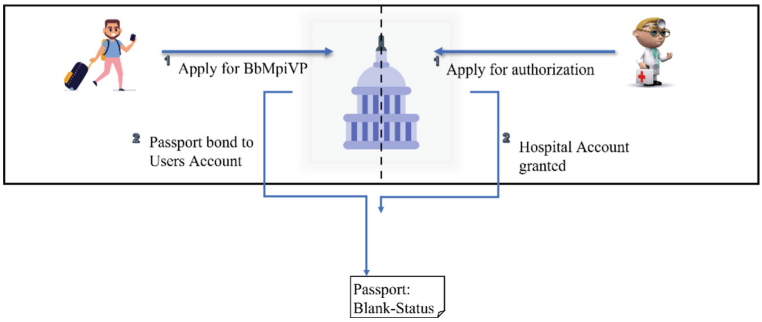

Fig. 2. Passport delivery and hospital granting

2.1.4 Health Status Verification

Health Status Verification: Fig. 4 shows the procedure when the user goes to a public arena that requires him to show verification, he can show this passport on our website. The passport is shown as a QR code with the following information:

- Validation time stamp
- Personal Info
- Total health status

The staff will compare information on the user's physical license and the personal information shown by the QR code. When the information tallies with each other, we can say that the "user" is actually the user. The following health status segment acts as proof of the user's vaccination. Plus, we use validity timestamp, which renders the information time-based, to prevent some malicious deception, such as using screenshots. Also, to reach higher level verification, the staff can input a series of personal information and obtain the user's passport through another entry.

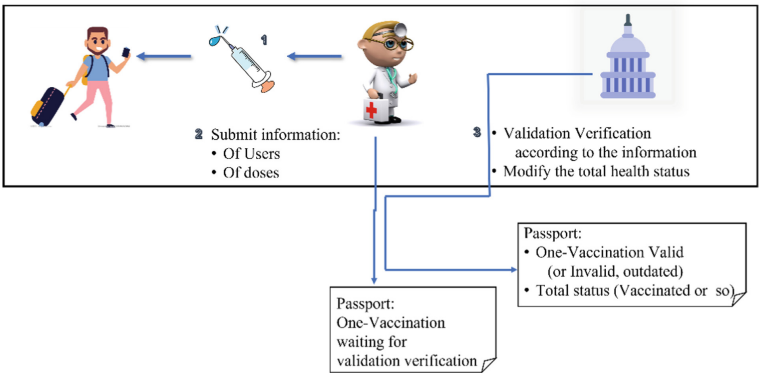

Fig. 3. Vaccination, information submission, and validity verification

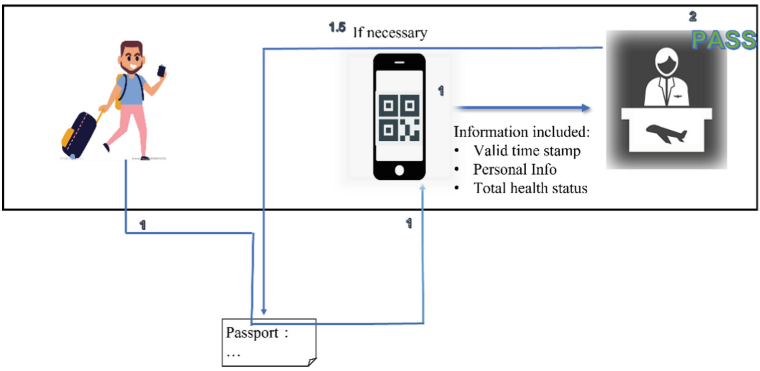

Fig. 4. Passport verification at the verifier

2.2 Smart Contract

Figure 5 shows the functions and classes we implemented in Solidity to realize our blockchain-based vaccine passport with smart contract.

At first, we created a map from ETH (Ethereum) address to identity to bound distinctive parties with different identities. Also, a map from users' addresses to their passports is used for them to view their passports, or for verifiers to search and judge the validity.

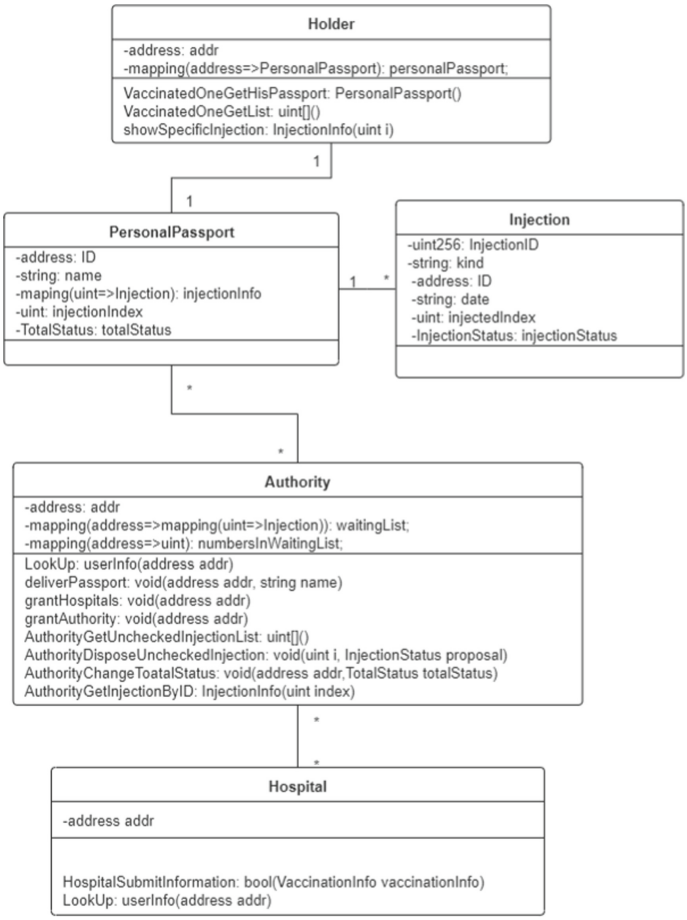

Fig. 5. Smart contract implemented in Solidity

Once the smart contract is deployed, the initiator will automatically be the dominant authority, who has the privilege to grant hospitals, other authorities, deliver passports to users and update health status in a specific passport.

Once a personal user goes to a granted hospital for vaccination, the detailed information of that vaccination will be submitted to the authority for validation verification by calling the HospitalSubmitInformation function, whose logic is shown in Algorithm 1.

Algorithm 1: Hospital Submit Information (Alg. 1)

Input: Authority address ***addr***, vaccination kind ***k***, user ID ***ID***, vaccination date ***d***, waiting list of Authority ***wl***
Output: No output

```
1   if caller's identity is not a granted hospital then
2       return;
3   end
4   n ← length of wl
5   idx ← passport[ID].vaccinationNumber
6   vac ← {VaxNum,k,ID,d,idx,injected(status)}
7   passport[ID].vaccination[idx] ← vac
8   wl[addr][n] ← vac
9   n ← n + 1
10  idx ← idx + 1
11  passport[ID].vaccinationNumber ← idx
12  TotalVaccinationNumber ++
13  Return
```

The detailed vaccination information will be uploaded into the waiting list of a prescribed authority for validity check, and also into the user's vaccination attribute of his passport simultaneously.

After that, the authority should check the waiting list, and determine the specific vaccination whether valid or not. The procedure is shown in detail in Algorithm 2.

After getting a list containing indexes, the prescribed authority can choose an index, and present an appraisal to that vaccination, which will be updated in the user's passport.

For the verifiers, they just need to input some personal information of the user who is required to show proofs of their vaccination, and the corresponding yielded information would be compared to what is shown on the user's screen. If the two match, then the user can pass the verification check.

Algorithm 2: Authority dispose of vaccination (Alg. 2)

```
Input: Authority's address addr, waiting list wl
Output: No output
/*First, get a list of vaccinations needed to be handled */
Function GetWaitingList(addr, wl):
    l ← an empty list
    cnt ← 0
    for i = 0 to wl.length – 1 do
        push i into l
        cnt ← cnt + 1
    end
    return l
end
/* Then, choose an index from the list, and dispose of
thatvaccination */
/* Proposal stands for the verification of the vaccination,
valid or not */
Function DisposeVaccination(addr,wl,i,proposal):
    Vac ← wl[addr][i]
    Ad ← vac.ID
    Vn ← vac.VaccinationNum
    Vi ← vac.VaccinationIndex
    Passport[ad].vaccination[vi].status ← proposal
Pop vac from wl
End
List ← GetWaitingList(addr,wl)
I ← a chosen index from list
DisposeVaccination(addr,wl,I,proposal)
```

2.3 Our Website (DApp)

Since it's a web app so far, we implemented the front-end with React and ES6 technology. It does well in interacting with our contracts and generating the final QR code. The pictures below will show some key features of our DApp.

2.3.1 Hospital Submit Vaccination Information

From Fig. 6, we can see that the granted hospitals just need to enter four contents: The authority's address, the vaccine type, the ID of the user, and the date of vaccination, then the form will be submitted onto the web, and interact with our contract. Then the waiting list of that authority will update, and so will the user's passport.

2.3.2 Authority Disposing of Vaccination

Figure 7 depicts the interface of the authority's vaccination appraisal presenting procedure. Firstly, by entering the index of the vaccination shown in the waiting list to be handled, A table will pop up to show the detailed information of that vaccination. Then the authority can decide whether it is valid or not, and update the vaccination status.

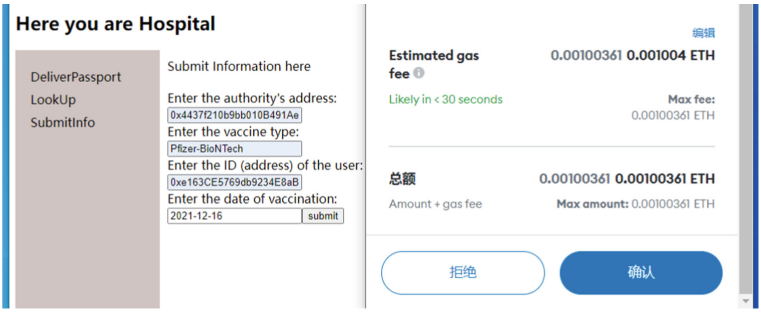

Fig. 6. The interface of hospital submitting

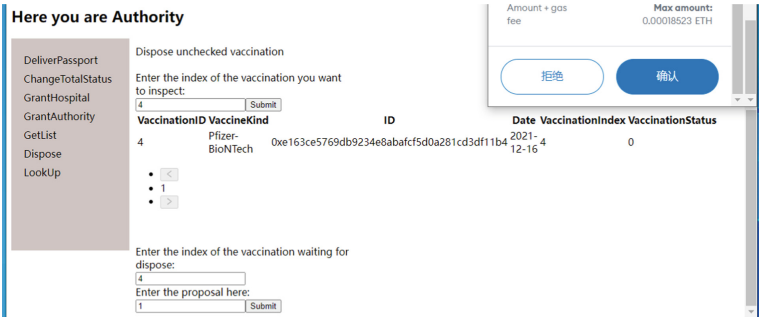

Fig. 7. The interface of authority presenting appraisal

Fig. 8. Personal QR code

2.3.3 Personal QR Code

After getting a vaccination and receiving the verification of the authority, the user's passport will contain all the information needed for passing a checkpoint (verifier). Therefore, we create a dynamic QR code in users' interface for them to show, as displayed in Fig. 8. When the code is scanned, the verifier will get some necessary information for them to check the user's identity and the validity of his/her vaccination.

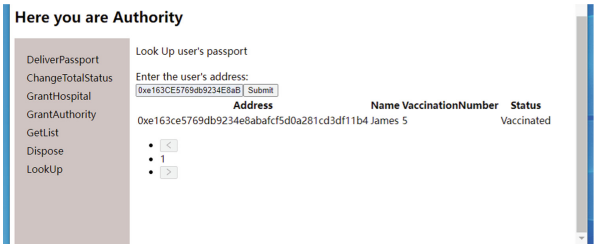

Fig. 9. The interface of looking up information

2.3.4 Verifier Looking Up

Then it comes to the possible final step, Fig. 9 shows validity checking for verifiers. After scanning the QR code shown by a user, the verifier can enter the necessary information of that user into the input box, and a table with the contents included in his/her passport will show up. This kind of verification processing ends up in our two-step authentication method. Not only does it maintain the reliability of the information, but security is also preserved since the verifier can only access the health status data when inputting a series of precisely matched information, which does not cause any privacy leakage.

2.4 Some Advantages

All in all, to avoid a traditional centralized Identity Management System, in which an identity provider has control over the user's identity data, the whole system is based on the blockchain platform. Normally with distributed ledger technology, data stored in the blockchain is immutable which means we can trace the source of malpractice crime and whichever party cannot shield criminals. We fully took advantage of Ethereum and its unique smart contract mechanism as the means to implement our BbMpiVP system. Smart contracts will carry out transactions automatically and certainly speed up the transaction process.

3 Copyright Form

For the mutual benefit and protection of Authors and Publishers, it is necessary that Authors provide formal written Consent to Publish and Transfer of Copyright before publication of the Book. The signed Consent ensures that the publisher has the Author's authorization to publish the Contribution.

The copyright form is located on the authors' reserved area.

The form should be completed and signed by one author on behalf of all the other authors.

4 Result and Discussion

The primary purpose of this paper is to introduce a solution based on cloud blockchain to handle vaccination efficiently and safely, as well as prove the validity of one's vaccination. For testing purposes, we deploy our contract on the Ropsten test network of

Ethereum. As much as we have expected, the website works well and each party can use this website-based DApp properly and easily while preserving security. The result indicates that our design can work as a decentralized solution for vaccination processing.

Nowadays, some countries have restricted their borders unless they show valid negative covid-19 test certificates or proofs of vaccination. However, some fraud and unauthentic vaccination, as well as maliciously stolen proofs caused trust issues. To address the problem, vaccination, validation verification, and proving process should be seamlessly connected and the relevant data, including information of stakeholders and manipulating records, will be logged on the public chain forever and immutably, and our BbMpiVP system works well under this kind of mutual mistrust condition. These trajectories make it warrantable to investigate and affix the responsibility for negligent and malicious crimes, no matter in which procedure they take place. Wielding the power to grant hospitals according to their qualification, supervise every dose, and revise users' status of vaccination and health condition, authorities seem to have a superior privilege. Nevertheless, their manipulations will be tracked as well.

Also, the smart contract regulates the procedure and each stakeholder is obliged to stick to it automatically, the results of which include standardization and improved efficiency.

Kelvin K. Tsoi et al. [4] in their research "The way forward after COVID-19 vaccination" also conceived the QR code mechanism. However, they applied static code printed on their physical passport, which could be exploited by malicious attackers, thus disguise becomes possible. Our innovation of the dynamic QR code prevents the unvaccinated from embezzling others' BbMpiVP. The timestamp within the QR code implies an expiry time, for example, 5 min. Once a timeout BbMpiVP is shown, the holder is required to refresh the page and get a new one, which is impossible to perform only with a solid QR code on screenshots.

Another work, "Towards a GDPR-compliant blockchain-based COVID vaccination passport" done by AKM Bahalul Haque et al. [1] constructs a similar structure of three-party participation as ours. However, due to the high cost of storing data on the chain, they introduced an off-chain database which was designed to relieve the pressure of data storage. Without the immutability, the off-chain database may be at high risk of data divulge, thus causing security loss. In this case, we decide to store all data on the chain, which means that every user should take his/her own expense on data storage and update.

Since users and staffs of checkpoints lack basic mutual trust, we implement a two-step verification. The first step refers to the phase during which users show their valid QR code with health status information. If the public place requires a high-level and more strict verification, such as nursing homes where susceptible aging men concentrate, the staff there can obtain users' health status directly through another entry by inputting a set of users' information. This phase is the second verification. Note that the information must strictly match each other, or they will retrieve nothing, preserving privacy and security.

However, there are still some limitations listed as follows.

Firstly, since we directly store all of our passports on the chain instead of an off-chain database, it costs too much Ether to deliver transactions. As Fig. 1 shows, the estimated gas per transaction can reach 0.000621 Ether, amounting to $ 2.94. The silver lining is

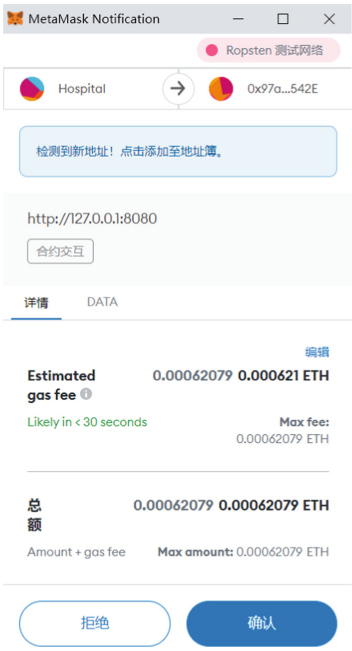

Fig. 10. The pop-up MetaMask window to confirm a transaction

that users don't have to pay to generate QR codes since the "LookUp" function serves as a pure function (Fig. 10).

Secondly, compared to our system whose users have to provide verifiers with the necessary information, a better alternative is to apply ZKP (Zero-Knowledge Proof) mechanisms to avoid information divulging.

Thirdly, including captcha is a good and achievable way to improve the security of login [7].

Also, since our BbMpiVP system is website-based, the intermediate platform, the browsers, can access users' browsing information by the cache. So, it's better to launch our own apps. To some extent, another solution is to release an electronic device, such as a smart bracelet, and attach Bluetooth or LAN functions to it. Thus, users can submit their BbMpiVP automatically whenever and wherever needed and simplify the procedure. To some extent, we can develop it to support a Blockchain and IoT-based vaccine supply system as the Blockchain project suggests [8].

5 Conclusions

This paper puts forward a solution about digital vaccine passports based on blockchain technology. The involved contract has been deployed on the Ropsten test network of Ethereum. We have summarized the existing scientific research achievements and provided a better alternative. In this project, personal information is embedded into the QR code to simplify the operation process, and an additive timestamp is attached to the QR

code to prevent others from stealing BbMpiVP. The Solidity language and JavaScript were used to implement the interaction between contract and web pages. However, storing data on the chain leads to the cost of data manipulating and storing. Two-step verification highlights our innovations. In the first step, the user shows the QR code and the verifiers only need to check his QR code to know whether his health status meets the standard. This process will not disclose the user's privacy. The following step suggests that the verifiers are supposed to access health status directly from the blockchain by entering a sequence of matched information.

To sum up, we have established a distributed application that takes information authenticity and security into account. When it comes to the further consummation of the BbMpiVP system, a PKI (Public Key Infrastructure) mechanism may improve work efficiency and protect privacy as well. Plus, beyond dispute, its benefits outweigh its defects to replace the previous web app with a mobile one.

We hope that our innovations can inspire more people to conceive ingenious solutions regarding digital vaccine passports.

References

1. Haque AKMB, Naqvi B, Islam AK, Hyrynsalmi S (2021) Towards a GDPR-compliant blockchain-based COVID vaccination passport. Appl Sci 11(13):6132
2. Narayanan A (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press
3. Shah H, Shah M, Tanwar S, Kumar N (2021) Blockchain for covid-19: a comprehensive review. Pers Ubiquitous Comput
4. Tsoi KK, Sung JJ, Lee HW, Yiu KK, Fung H, Wong SY (2021) The way forward after COVID-19 vaccination: vaccine passports with blockchain to protect personal privacy. BMJ Innov 7(2):337–341
5. Tajan L, Westhoff D (2020) Approach for GDPR compliant detection of COVID-19 infection chains arXiv:2007.08248
6. de los Santos Nodar MA, Fernández Caramés TM (2021) Covid-19 digital vaccination passport based on blockchain with its own cryptocurrency as a reward and mobile app for its use. Eng Proc 7(1):35
7. Jabed M, Ranjan N (2013) Captcha based on human cognitive factor. Int J Adv Comput Sci Appl 4(11)
8. Mendonça RD, Gomes OS, Vieira LFM, Vieira MAM, Vieira AB, Nacif JAM (2021) lockColdChain: vaccine cold chain blockchain. arXiv:2104.14357
9. The Great Chain of being sure about things. The Economist, 31 October 2015. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things. Accessed 23 Nov 2021
10. Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found Healthcare Intelligence on Blockchain with novel privacy risk control. J Med Syst 40(10)