Covid-19 VaccinePassport Management System on Blockchain Platform

Gengzao Wu

Master of Cybersecurity, University of Monash
**Corresponding author. Email: Gwuu0007@student.monash.edu*

ABSTRACT
In the context of the COVID-19 pandemic, people's travel has been severely impacted. Proof of vaccination must be quickly linked to travel passports to facilitate people's travel, but its success will depend on the availability of a platform that enables data sharing. This platform needs to enable data sharing and protect users' private data. This paper discusses how blockchain technology can enable these requirements in the VaccinePassport initiative, which provides a transparent and tamper-proof solution for vaccination applications. Considering the anonymous nature of blockchain, VaccinePassport provides an authentication feature for verifying the hash address of the applicant's account.

Keywords: *Blockchain, COVID-19, Authentication, Vaccine, RSA.*

1. INTRODUCTION

Blockchain is a tamper-proof distributed ledger technology born in 2008 that can be treated as a decentralized database [1]. Once a transaction is posted and recorded on the blockchain, it cannot be changed. Various transactions are recorded in blocks, each of which has a hash value as an address, and each block records the hash address of the previous block.

The impact of Covid-19 on the global economy and health of life is enormous, and the use of technology plays an essential role in the fight against the outbreak. With hundreds of people needing to be vaccinated every day, the need to protect users' privacy based on efficiency has become a pressing technical issue. In the healthcare field, trust is an issue that has always existed, and blockchain can be a future direction in healthcare by sharing data between different subjects without the need for trust through its tamper-evident and stealthy nature [2]. In this paper, the author hopes to be able to associate vaccination certificates with passports for travel through blockchain technology in an untrusted environment, by which people's travel is facilitated, and their privacy is protected.

2. PREVIOUS WORK

A traceable epidemic smart contract that can address vaccine expiration and vaccine record fraud was published by Yong et al. in 2020 [3]. In addition, a two-tier blockchain vaccine regulatory system was published by Peng et al. in 2020 to both protect the private data of vaccine manufacturers and to record and monitor the quality information of vaccines [4]. A blockchain system was published by Antal, Cioara, Antal and Anghel in 2021. This system is a blockchain-based vaccine supply system with smart contracts to automate vaccine delivery and register and manage waiting lists for vaccination sites [5].

3. INTRODUCTION OF VACCINEPASSPORT

The VaccinePassport system in this article is designed to combine proof of vaccination with a passport for travel. Nowadays, many public places or public transportation require people to show vaccination certificates for vaccination prevention purposes. The consensus mechanism of the blockchain determines that the records recorded in the blockchain cannot be tampered with because the blockchain is decentralized, and to modify the records on the blockchain requires the consent of more than half of the nodes in control to pass, which cannot be done in reality [6]. So the hash encryption and tamper-proof properties of blockchain combine the inoculation information and passport information well in an untrusted environment.

3.1 Parts of VaccinePassport

The VaccinePassport consists of four parts: person, hospital, government, and checkpoint. Different parts'

functions are as follows:

The person represents people who go to the hospital with the intention of getting vaccinated, and each person has his or her own account on the blockchain, where each account has a unique hash address and holds basic personal information, including vaccination information and passport information.

The hospital stands for an institution that has the ability to provide vaccines, and people usually go to hospitals to get vaccinated. Hospitals can also test patients for the virus and provide isolation treatment for those infected with the virus.

The government stands for the institution that can provide proof of passport, a function generally provided by the government. The government also stores the citizen's identification information in a database and can provide hospitals with the service of verifying the information.

The checkpoint stands for an organization that needs to test passports and vaccinations, usually at various transportation checkpoints, such as airplane terminals and highway access points.

3.2 VaccinePassport's processing flow

As shown in Figure 1, this is the relationship among Person, Hospital, Government and Checkpoint.

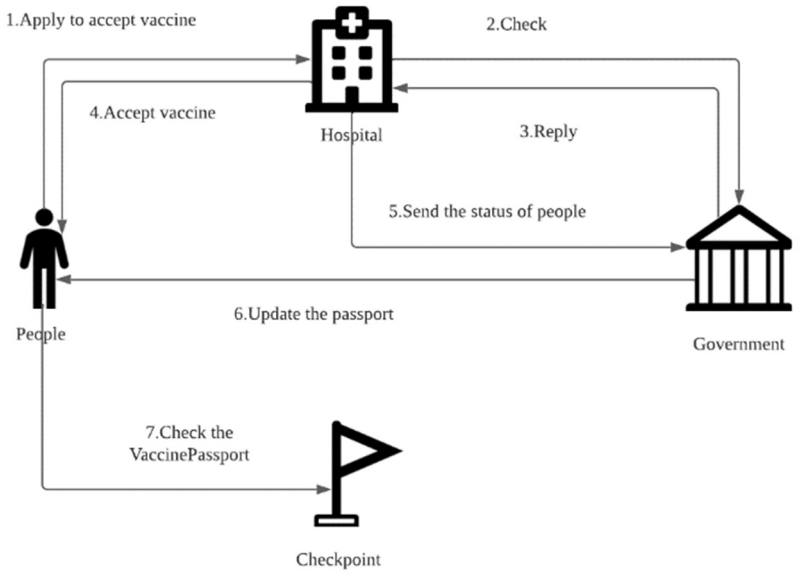

Figure 1 Relationship of different parts.

The specific process is shown in Figure 2. One person goes to the hospital to request a vaccination and needs to provide the address of his or her personal account.

When the hospital receives the application, the hospital needs to determine if the person has been vaccinated. If the person has been vaccinated, the request will be rejected. If not, the hospital needs to verify the authenticity of the account information.

The hospital needs to send the address of the account to the government and request verification from the government. The government matches the information corresponding to the address with the database to verify the existence of the account and gets back to the hospital with the results. Once the hospital gets the results, if it does not exist, the hospital will reject the request. If it exists, the hospital will perform a nucleic acid test on the patient after receiving the response, and if infected with the virus, the hospital will reject the application and quarantine the patient. At the same time, for the tested people who are not infected with the virus, the hospital will accept the vaccination request and notify the government that the person has been vaccinated. The government will instantiate a VaccinePassport on the blockchain according to the smart contract and send the VaccinePassport as a transaction record to the person's account to update the original passport.

When people need to travel and arrive at the testing point, they just need to provide their personal account addresses. The detection point finds the account on the blockchain and checks the transaction records to know if the user has a vaccine passport. This is convenient for the testing point and also protects the user's privacy.

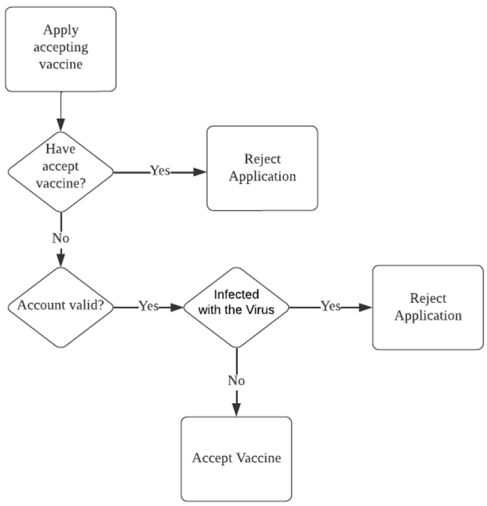

Figure 2 Process of Applying for Vaccination.

4. VACCINEPASSPORT'S CERTIFICATION SCHEME

A potential risk with the whole VaccinePassport process is that a patient might provide an account that is not his or her own. Because the data on the blockchain is public, an account on the blockchain can view any other accounts on the blockchain, which means that a person can know the hash address of another account. If an applicant provides the hospital with the address of another person's account, the hospital and the government are unable to discern whether the account belongs to the provider. In addition to this, if a person knows from another source that a person's account has a VaccinePassport, then that person can provide an address with a VaccinePassport to the checkpoint, and when the checkpoint search the VaccinePassport on that address, it will assume that the provider has the conditions to pass, thus allowing the provider without a VaccinePassport to pass the inspection. In this way, the PEOPLE can bypass the detection point's audit. This is a problem that will seriously interfere with the proper functioning of the system and needs to be addressed urgently in order to meet the requirements for proper use in reality.

4.1 Authentication algorithm

To solve this problem, the project requires that the applicant can guarantee that the information he provides is his own, i.e., the information provided by the applicant needs to be resistant to repudiation. This involves the problem about digital authentication, which in cryptography is generally solved by asymmetric encryption. The cryptography scheme published by Memon et al. in 2015 is the authentication function through elliptic curve cryptography, which is an asymmetric encryption algorithm [7]. Asymmetric cryptography has a key pair including a public key and a private key. The public key is public, but the private key is private. The text encrypted by the private key can be decrypted by the public key, and similarly, the text encrypted by the public key can be decrypted by the private key. But it is not feasible to compute the private key by the public key [8].

The asymmetric encryption scheme used in this paper is RSA. RSA is a mod-based asymmetric encryption scheme where p and q are two large prime numbers, n=p*q. φ(n)=(p-1)*(q-1), select e(gcd(φ(n),e)=1; 1<e<φ(n)). Then d=e^-1(modφ(n)). Public key: PU={e,n}, Private key: PR={d}. It is impossible to calculate the private key if people only know the public key, because p and q are private; it is hard to calculate p and q if the attacker only knows n. In encrypt function, C≡M^e mod n, because d≡e^-1, e*d = 1. So, in decrypt function, M≡C^d mod n. The security of RSA is due to the difficulty of factorization of large prime numbers [9]. Li, Jiang, and Sun (2019) proved that the large integer decomposition problem is unable to be resolved nowadays [10].

4.2 RSA in VaccinePassport

Suppose there is a man named Bob. When Bob creates an individual's account, two different but random prime numbers p and q are generated, so n=p*q, and φ(n)=(p-1)*(q-1). Then e(1<e<φ(n)) is randomly generated. This computes d modφ(n) = e^-1 mod φ(n). Bob publishes the public key $PU_{bob} = \{e, n\}$, while the private key PU_{bob} is not disclosed to the outside world. All users of the blockchain know that PU_{bob} is the public key of Bob's account. But it is impossible to calculate PR_{bob} by PU_{bob}.

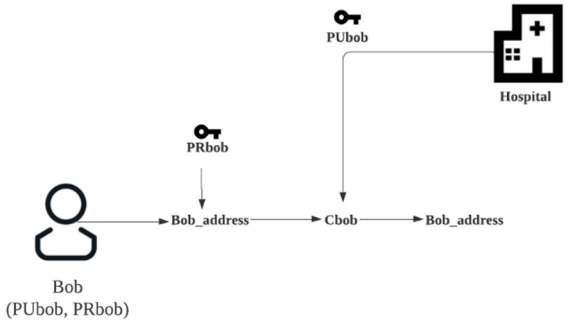

Figure 3 Bob's authentication.

As seen in Figure 3, when Bob goes to the hospital to apply for vaccination, he needs to provide his account address. In order to achieve the effect of digital signature, Bob needs to encrypt his account address with the private key PR_{bob} that only he knows. Bob takes the account hash address bob_address as input, the private key PR_{bob} as the encryption key, and the encryption operation gets the output C_{bob} = bob_address ^ d mod n. When Bob goes to the hospital to apply for vaccination, C_{bob} can be provided to the hospital. Since the account of Bob has broadcasted the public key PU_{bob} of the

account before, the hospital will decrypt C_{bob} with this public key PU_{bob}. Once decrypted, the hospital will get the Bob's account address and send it to the government for verification to authenticate the account, a process that ensures that the account's hash address provided belongs to the applicant. There is a situation that a person named Alice wants to use Bob's account to apply vaccine. Alice needs to know Bob's private key PR_{bob}, but PR_{bob} is only known to Bob, and the RSA algorithm ensures that PR_{bob} cannot be calculated by PU_{bob}. So, Alice cannot get the C_{bob}.

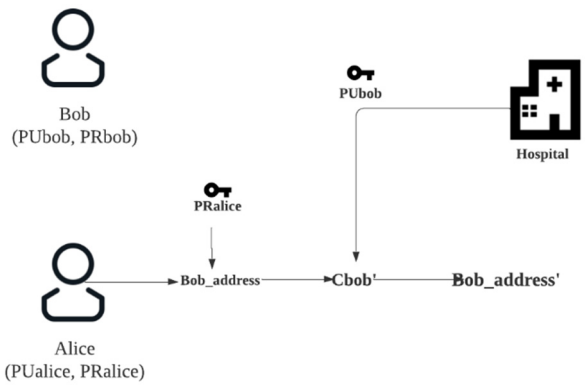

Figure 4 Alice's Disguise.

There is another situation as shown in Figure 4. When Alice encrypts Bob's address with her private key PR_{alice} to get C_{alice}, but Alice claims that it is encrypted with Bob's private key PR_{bob}. The hospital will decrypt it with Bob's public key PU_{bob} and finally get bob_address' = Dec (C_{alice} , PU_{bob}) and bob_address' ≠ bob_address. And bob_address' will be an illegal address that cannot be used. The hospital gets this address and transmits it to the government for verification. There is no doubt that this account's hash address will not pass the government's validation and the hospital will eventually reject the applicant's application.

Again, this authentication function works at the testing point, as both the testing point and the hospital need people to provide the hash address of their accounts on the blockchain. This is how RSA is applied to the VaccinePassport authentication function.

5. CONCLUSION

This paper proposes a blockchain model called the VaccinePassport, which can efficiently share data among applicants, hospitals, governments, and testing sites in an environment of mutual distrust. The VaccinePassport also has the ability to screen data when accepting applicants, and the application of RSA algorithms makes the VaccinePassport be resistant to forgery when reviewing applicant data. In order to ensure the security of the RSA algorithm for private keys in this model, the two prime numbers p and q need to be as large as possible, but this will reduce the speed of computer processing and will have a certain impact on the efficiency of the whole system. Future research can focus on the optimization in the speed of the authentication algorithm, e.g., replacing a more efficient lightweight asymmetric encryption algorithm.

REFERENCES

[1] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[2] Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. Blockchain in healthcare today.

[3] Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. International Journal of Information Management, 52, 102024.

[4] Peng, S., Hu, X., Zhang, J., Xie, X., Long, C., Tian, Z., & Jiang, H. (2020). An efficient double-layer blockchain method for vaccine production supervision. IEEE transactions on nanobioscience, 19(3), 579-587.

[5] Antal, C., Cioara, T., Antal, M., & Anghel, I. (2021). Blockchain platform for COVID-19 vaccine supply management. IEEE Open Journal of the Computer Society, 2, 164-178.

[6] Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial Innovation, 5(1), 1-14.

[7] Memon, I., Hussain, I., Akhtar, R., & Chen, G. (2015). Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme. Wireless Personal Communications, 84(2), 1487-1508.

[8] Khan, A. G., Basharat, S., & Riaz, M. U. (2018). Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. International Journal of Scientific & Engineering Research, 9(10), 992-999.

[9] Kessler, G. C. (2003). An overview of cryptography.

[10] Zhang, X., Li, M., Jiang, Y., & Sun, Y. (2019, July). A Review of the Factorization Problem of Large Integers. In International Conference on Artificial Intelligence and Security (pp. 202-213). Springer, Cham.