Designing a blockchain-enabled cross-border COVID-19 vaccination certificate management system

Sean A.
RMIT University
Melbourne, Australia
s3893785@student.rmit.edu.au

***Abstract*—This electronic document is a "live" template and already defines the components of your paper [title, text, heads, etc.] in its style sheet. **CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.* (*Abstract*)**

Keywords*—*Blockchain, Digital Health Certificate, COVID-19 Pandemic, Public Key Infrastructure, Proof of Work, Self-Sovereign Identity

I. Introduction

During the COVID-19 pandemic, existing healthcare systems presented limitations in handling the public health crisis. Digital Health Certificates were implemented during the period of governments attempting to establish economies and return to everyday life. Developing new or existing secure digital health certificates is necessary to reduce losses by ensuring data integrity and privacy and facilitating COVID-19 proof with verified credentials (Gelb & Mukherjee, 2021). This report proposes a solution that addresses existing system disadvantages through blockchain technology and various privacy-preserving techniques.

II. Analysing Existing systems

A. The Requirements

In 2021 the World Health Organization outlined recommended design criteria for constructing Digital documentation of COVID-19 certificates (DDCC:VS) (World Health Organization, 2021). The design criteria accounted for ethical considerations and data protection principles outlined in the 'Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance' (World Health Organization, 2021). The specifics of the design criteria are as follows:

1. "Implementation of the DDCC:VS should not increase health inequities or increase the digital divide.
2. Everyone who has been vaccinated to protect against COVID-19 has the right to obtain and hold a DDCC:VS.
3. The DDCC:VS needs to be in a format that can be accessible to all, for example, in paper and digital formats. Any solution should also work in online and offline environments across multiple
platforms – paper and digital.
4. Individuals should not be treated differently or given different levels of trust due to the format of
the DDCC:VS they are using (e.g. there should be no discrimination based on whether someone is
presenting a DDCC:VS on a smartphone or a paper card).
5. Any solution should not be at an additional cost to the vaccinated person. The interoperability specifications used in DDCC:VS solutions should be based on open standards to ensure equitable
access to a range of non-proprietary digital tools.
6. The Infrastructure that the DDCC:VS solution is built on should ensure that individuals and Member States are not locked into a commitment with only one vendor.
7. Any solution should be as environmentally friendly as possible. The most environmentally sustainable options should be pursued to reduce any additional undue harm to the environment.
8. Any solution should be designed to augment and work within the context of existing health information systems, as appropriate.
9. Any solution should not share or store more data than is needed to successfully execute its tasks.
10. Minimization of health content for purposes not related to health care, and privacy-protecting features, should be built into the system and be respected accordingly.
11. Anti-fraud mechanisms should be built into any approach.
12. Digital technology should not be the only mechanism available for verification. There should always be possible ways to revert to a paper-only manual verification of vaccination certificates. For example, a paper representation may be printed from the DDCC:VS or captured in the International Certificate of Vaccination and Prophylaxis (ICVP) and combined with an identity verification as outlined within the policy set by the public health authority."

(World Health Organization, 2021)

B. Requirements in Action

The systems being used and implemented by governments, precisely that of China, the United States, Italy, Germany, France, Chile, and Estonia, provide few in the way of technical specifications surrounding the operation of the systems (Fraser, 2020), (Iacus et al., 2020), (Mozur et al., 2020), (A COVID-19 Health Passport Secured by Blockchain to Enable Deconfinement, 2020), (staff, 2020). Estonia uses a centralised system (staff, 2020). Additionally, others use a system that relies on a third party (A COVID-19 Health Passport Secured by Blockchain to Enable Deconfinement, 2020). The inclusion of third parties and centralised systems in the context of a Vaccination Certificate Management System is but one example that presents several security and privacy-preserving issues along with failing to follow the suggested design criteria outlined by the World Health Organization (World Health Organization, 2021), (Fraser, 2020), (Iacus et al., 2020), (Mozur et al., 2020), (A COVID-19 Health Passport Secured by Blockchain to Enable Deconfinement, 2020), (staff, 2020), (Abid et al., 2021

III. Background

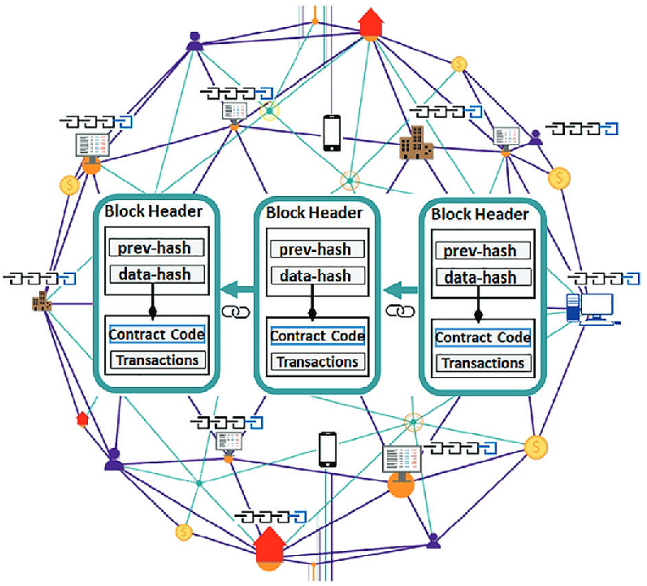
A. Blockchain

Blockchain can be defined as an "open and distributed ledger taking the form of a list of blocks originally designed for recording transactions in cryptocurrency systems" (Meng Shen et al., 2020, p. 2). As part of a P2P network, the ledger's data is shared, duplicated, and synced among its users in an ordered blockchain (Abid et al., 2021). A block's header, which contains the data's SHA-256 hash, is separate from the block's data. To further support and validate the information in its preceding block, each block also carries the hash of the previous block header in its header (Abid et al., 2021). As seen in Figure 1 (Abid et al., 2021).

Blockchain's primary benefits for exchanging digital health certificates include the following:

- Tamper-resistant - Employs Proof of Work (PoW) consensus techniques to control the ability to create new blocks (Meng Shen et al., 2020, p. 2). Data alteration is, therefore, computationally inefficient, making the data stored in the block immutable (Meng Shen et al., 2020, p. 2).
- Decentralised – Peer-to-peer networks are used without the need for a central administration or a trusted third party (Meng Shen et al., 2020, p. 2). Furthermore, multiple copies of the data are stored in the ledger, preventing data loss at a single point of failure (Meng Shen et al., 2020, p. 2).
- Traceability - Any transaction in a blockchain system may be recorded, and participants can readily authenticate transactions between two parties (Meng Shen et al., 2020, p. 2).

Illustration of Blockchain



From "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates" by Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. 2021. *NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Software: Practice and Experience*, p. 4. (https://doi.org/10.1002/spe.2983)

It is impossible to retroactively change data in a single block without changing the subsequent data blocks in the chain, thanks to the cryptographic links between the blocks (Abid et al., 2021).

B. W3C Verifable Credentials

The W3C Verifiable Credentials standards objective is "to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable" (Sporny et al., 2022). Based on the principles of Public Key Infrastructure (PKI) used in digital signatures, it is also intended to standardise document formats making them machine-readable (Sporny et al., 2022). However, as opposed to the centralised PKI, W3C VC operates where every public key can have its distinct address thanks to a decentralised/distributed registry for cryptographic keys typically found in a Blockchain (Abid et al., 2021). This address is a Decentralised Identifier (DID) (Sporny et al., 2022).

C. uPort

The uPort system is an open-source identity management tool that gives users, organisations, and entities self-sovereign identity (Pelle Braendgaard, 2017). A simple, smart contract called an "uPort identity" is used by users, organisations, or other entities to represent themselves digitally on the Ethereum blockchain and make identity-related claims when dealing with other smart contracts, either on-chain or off-chain (Pelle Braendgaard, 2017). In addition to the Selective Disclosure concept and other techniques that limit user exposure to personal information, uPort is based on the W3C VC standard. Using this idea, the user can choose which parts of their VC to divulge to a verifier while keeping the rest a secret (Abid et al., 2021).

D. FogBus

Fog/edge computing is a new computing paradigm where computing resources are available via fully dispersed fog/edge nodes adjacent to end devices (Yoo et al., 2021). Data processing and storage are heavily reliant on local devices in a fog computing concept rather than a cloud infrastructure (Yoo et al., 2021). Fog/edge computing can drastically cut processing time and network traffic by performing analysis, filtering, and processing at neighbourhood fog/edge resources rather than sending massive amounts of data to centralised cloud servers (Yoo et al., 2021). FogBus secures activities on sensitive data by utilising Blockchain, authentication, and encryption mechanisms (Tuli et al., 2018). It is simple to implement, scalable, and reasonably priced thanks to its cross-platform software systems and lightweight design (Tuli et al., 2018).

E. Existing Systems

As previously mentioned, the systems being used and implemented by governments provide few technical specifications surrounding the operation of the systems. This also applies to the commercial systems utilised by governments.

Figure 2: *Comparative Table of COVID-19 Vaccination Certificate Systems*

	Infrastructure			Security Features			
Approach	**No Centralisation**	**No Third Party**	**Blockchain**	**Privacy-Preserving**	**Self-Sovereignty**	**GDPR-Compliant**	**KYC-Compliant**
Corona Pass	-	+	-	-	-	-	+
China Alipay App	+	-	-	-	-	+	-
ImmuPass	+	+	+	-	-	-	+
CERTUS	+	+	+	-	-	-	+
DigiLocker	+	+	+	+	+	+	+
Secure ABC	+	+	-	+	+	+	-
CATC App	+	-	+	-	+	-	+
Digital Health Pass	+	+	+	+	+	+	+
VaccineGuard	+	+	+	+	+	+	+

Note. (Bizagi, n.d.), (DigiLocker Free, n.d.). (Eisenstadt et al., 2020). (Estonia, Hungary, and Iceland, Together with AstraZeneca Estonia Are Participating in a Pilot of Guardtime's VaccineGuard — Guardtime, n.d.). (Hicks et al., 2020). (IBM Watson Health Is Now Merative, n.d.). (IMMUPASS - Immunity Certificate, n.d.). (Mozur et al., 2020). (SICPA, n.d.)

IV. Proposed System

The aim is to design a system that assures data immutability and integrity, enables consumers to fully manage and control their data, increases privacy by encrypting personally identifiable information, enables fast verification of COVID-19 proof using credentials standards, and the notion of selective disclosure, which allows users to disclose certain information to reliable third parties.

The system will be designed to meet strong levels of personal data security that are in line with General Data Protection Regulation (GPDR) and know your customer (KYC) standards ensuring the user's self-sovereignty while guaranteeing the user's right to privacy and the protection of populations.

A. Objectives

By eliminating the usage of Third Parties, Centralization, and Central Points of Failure, existing blockchain system solutions may be used and expanded upon while maintaining the privacy standards required by many existing systems. The ultimate goal is to protect users' right to privacy without sacrificing the system's overall security and integrity.

B. Infrastructure

Off-chain storage and a private permissioned blockchain are both parts of the Infrastructure. By limiting access to the system to just authorised users who can prove their cryptographic key, the Ethereum-based private permissioned is utilised to address privacy concerns. The end result is a verifiable data registry that is impervious to tampering. The second is off-chain storage, in particular an IPFS storage that saves user data (Benet, 2014). Sensitive information can never be disclosed to third parties who are scanning the Blockchain because there is nothing else saved on-chain outside the IPFS (Interplanetary File System-IPFS storage) hash. Secure COVID-19 Off-chain storage is where data is kept apart from the Blockchain, and the Blockchain just retains a pointer to the encrypted data that is kept there. This ensures the GDPR requirements. Between the suggested system and the government's private cloud platform, there is an intermediary layer. Over the edge network, fog nodes are installed and are managed by healthcare authorities. The Fog nodes' closer proximity to the user data sources reduces network congestion and the time it takes for services to be delivered. To further secure data integrity, confidentiality, and privacy, FogBus uses authentication, encryption, and blockchain technologies.

C. Those Involved

The following actors are involved in the system:

- Governments and health authorities - Authorize the administration of COVID-19 vaccinations and issue certificates (Abid et al., 2021).
- Healthcare providers - COVID-19 test vaccinations are controlled and used by healthcare providers (Abid et al., 2021). Approved by healthcare and governmental agencies and are transparently recognisable (Abid et al., 2021).

- Users - those who have received vaccinations (Abid et al., 2021).
- Service Providers - Verify and authenticate COVID-19 Certificates that have been issued (Abid et al., 2021). Authorised by neighbourhood authorities and transparently recognisable (Abid et al., 2021).

D. Main Proccess and Operation

The below section will illustrate the operation for the proposed system solution.

Registration of Healthcare Providers and Service Providers

1. Request for authorisation as a COVID-19 Certificate Issuer by a healthcare provider.
2. The healthcare provider provides the blockchain wallet's public key.
3. Following the verification and confirmation of eligibility, the healthcare authority registers the blockchain address, medical ID, and name of the requesting healthcare provider.
4. Following the completion of this procedure, the healthcare professional may issue COVID-19 certifications.
5. The service provider submits their blockchain account address, service ID, and name to the local authority to become an approved verifier, after which they receive authorisation from them.

Users logging into System

1. The user creates a blockchain wallet and account.
2. The healthcare provider checks the user's physical ID and scans the QR code of the user's blockchain account address.
3. Alternatively, the healthcare provider checks if the user already has a valid certificate.

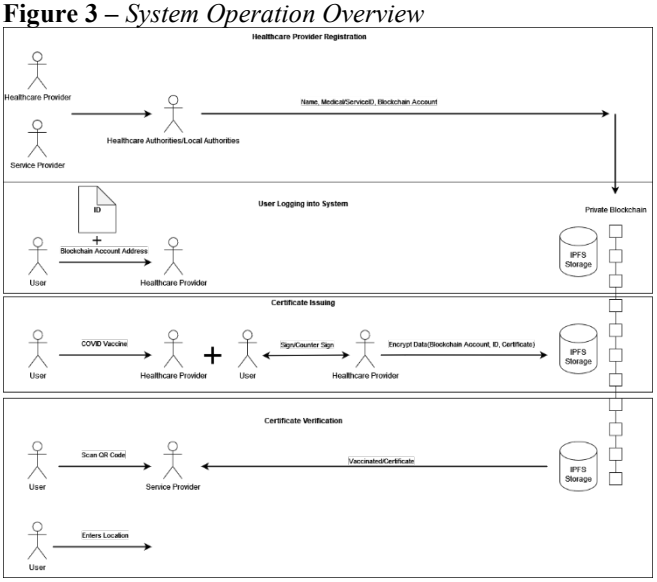
Certificate Issuing

1. Healthcare provider conducts COVID-19 vaccination for the user.
2. Healthcare provider registers personal details, blockchain account address, and validity date in the off-chain storage after signing and encrypting the data.
3. A hash of encrypted data is stored in Blockchain.
4. The user acquires a digitally signed and counter-signed COVID-19 certificate.

Certificate Verification

1. A user presents a QR code and physical ID used in registration.
2. The service provider checks the certificate presented by the user by scanning the QR code.
3. The service provider compares the physical ID number on the certificate against the ID number that is presented.
4. Service provider compares the hash stored in the Blockchain against the hash of the encrypted, signed data as a QR code.
5. Allows or doesn't allow entrance to area, state, or territory.

Figure 3 – *System Operation Overview*



E. Australian and Overseas Benefits

The existing technology enables governments to make use of a system with desired security characteristics including binding, uniqueness, peer indistinguishability, and forge/tamper proof. These features assist create a system that enables tamper-proof and rapid verification of COVID-19 immunisation certificates, aiding Australian and foreign governments in stopping the unnecessary spread of the disease while defending the users' basic privacy rights. Additionally, this helps public health authorities and governments manage access to facilities and crucial sites while enabling people to move around safely (Abid et al., 2021).

F. Advantages

- Authorized users can only access the system using cryptographic keys, and users retain full control over their login information and personal information.
- Blockchain is not used to store COVID-19 data.
- Allows for Instant Verification.
- Tamper-Proof.
- Enables paper copies as a backup.
- COVID-19 Certificates that have been signed and countersigned.
- The Ethereum Blockchain does not charge a transaction fee for acts that involve hash verification.
- With regard to existing and alternative solutions, Fog (Edge) & Cloud Computing handles latency and reaction time problems.

G. Disadvantages

- Certain actions on the Ethereum Blockchain require a transaction fee.
- Reliant on the Ethereum Blockchain's response time and latency

The bulk of current or proposed solutions fall short in one or more areas of privacy preservation systems or in defining the

system's technological requirements (Fraser, 2020), (Iacus et al., 2020), (Mozur et al., 2020), (A COVID-19 Health Passport Secured by Blockchain to Enable Deconfinement, 2020), (staff, 2020). These systems are also centrally controlled or substantially dependent on outside parties (Mozur et al., 2020). (Bizagi, n.d.). As a result, the suggested solution in this document provides compliance with GDPR, KYC standards, and user self-sovereignty.

V. Conclusions

This report offered a system solution for a cross-border COVID-19 vaccination certificate management system for issuing and verifying certificates that uses blockchain technology. To reduce the dangers and spread of the COVID-19 pandemic, the system provides the quick verification of tamper-proof COVID-19 certificates. This is done while maintaining the users' right to privacy thanks to cutting-edge technologies like IPFS storage, Blockchain, and uPort Self-Sovereignty Identity, which satisfies GDPR and KYC regulations. The report includes a technical description of the operation, a comparative analysis, and a high-level overview. In terms of future development and expansion, there is space to offer further and more thorough specifications, tests, and proofs of concept.

References

1. World Health Organization. (2021). Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, 27 August 2021. Www.who.int. https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1
2. Gelb, A., & Mukherjee, A. (2021, February 11). *A COVID Vaccine Certificate: Building on Lessons from Digital ID for the Digital Yellow Card*. Center for Global Development | Ideas to Action; Center for Global Development. https://www.cgdev.org/publication/covid-vaccine-certificate-building-lessons-digital-id-digital-yellow-card
3. Meng Shen, Liehuang Zhu, & Ke Xu. (2020). *Blockchain : empowering secure data sharing* (p. 2). Springer Nature.
4. Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Software: Practice and Experience*, 4–6. https://doi.org/10.1002/spe.2983
5. Yoo, S., Kim, T., & Kim, Y. (2021). *Edge/Fog Computing Technologies for IoT Infrastructure*. MDPI. https://doi.org/10.3390/books978-3-0365-1455-0
6. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2018). FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. *ArXiv:1811.11978 [Cs]*. https://arxiv.org/abs/1811.11978
7. Sporny, M., Longley, D., & Chadwick, D. (2022). *Verifiable Credentials Data Model v1.1*. World Wide Web Consortium (W3C). https://www.w3.org/TR/vc-data-model/
8. Pelle Braendgaard. (2017, February 27). *What is a uPort identity?* Medium; uPort. https://medium.com/uport/what-is-a-uport-identity-b790b065809c
9. staff, E. editorial. (2020, May 20). *Estonia tests first digital immunity passports for workplaces*. Eandt.theiet.org. https://eandt.theiet.org/content/articles/2020/05/estonia-tests-first-digital-immunity-passports-for-workplaces/
10. *A COVID-19 health passport secured by Blockchain to enable Deconfinement*. (2020, June 29). SICPA. https://www.sicpa.com/news/covid-19-health-passport-secured-blockchain-enable-deconfinement
11. Fraser, B. (2020). Chile plans controversial COVID-19 certificates. *The Lancet*, *395*(10235), 1473. https://doi.org/10.1016/s0140-6736(20)31096-5
12. Iacus, S. M., Natale, F., Santamaria, C., Spyratos, S., & Vespe, M. (2020). Estimating and projecting air passenger traffic during the COVID-19 coronavirus outbreak and its socio-economic impact. *Safety Science*, *129*, 104791. https://doi.org/10.1016/j.ssci.2020.104791
13. Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *The New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
14. *Customer identification: Know your customer (KYC) | AUSTRAC*. (n.d.). Www.austrac.gov.au. https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-know-your-customer-kyc
15. GDPR. (2019). *GDPR.eu*. GDPR.eu. https://gdpr.eu/
16. Bizagi. (n.d.). *CoronaPass™ FAQ*. Retrieved January 31, 2023, from https://resourcesbizagi.azureedge.net/docs/coronapass/CoronaPass-FAQ.pdf
17. DigiLocker Free. (n.d.). *secure, flexible and easy-to-use application*. DigiLocker Free. https://digilocker.gov.in/
18. Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A., & Domingue, J. (2020). COVID-19 antibody Test/Vaccination certification: There's an app for that. *IEEE Open Journal of Engineering in Medicine and Biology*, *1*, 148–155.
19. Estonia, Hungary, and Iceland, together with AstraZeneca Estonia are participating in a pilot of Guardtime's VaccineGuard — Guardtime. (n.d.). Guardtime.com. https://guardtime.com/blog/estonia-hungary-and-iceland-together-with-astrazeneca-estonia-are-participating-in-a-pilot-of-guardtime-s-vaccineguard
20. Estonia, Hungary, and Iceland, together with AstraZeneca Estonia are participating in a pilot of Guardtime's VaccineGuard — Guardtime. (n.d.). Guardtime.com.

https://guardtime.com/blog/estonia-hungary-and-iceland-together-with-astrazeneca-estonia-are-participating-in-a-pilot-of-guardtime-s-vaccineguard
21. Hicks, C., Butler, D., Maple, C., & Crowcroft, J. (2020). SecureABC: Secure AntiBody certificates for COVID-19. In *arXiv.org*. Cornell University Library, arXiv.org.
22. *IBM Watson Health is now Merative*. (n.d.). Www.ibm.com. https://www.ibm.com/watson-health/merative-divestiture
23. *IMMUPASS - Immunity Certificate*. (n.d.). Immupass.org. Retrieved January 31, 2023, from https://www.immupass.org/
24. Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *The New York Times*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
25. *SICPA*. (n.d.). SICPA. https://www.sicpa.com/