Immunity Passports

Building a Critical Infrastructure for the Nation-Wide Identification of Recovered COVID-19 Patients

A. Yüksel

K. Kostadinov

L. Verdoner

S. Cirikka

R. Santana Trejo

Contents

1. Introduction

COVID-19, the disease caused by the coronavirus, has affected the entire globe [1]. The negative impact is not only felt by everyone that is currently infected and the healthcare personnel, but the entire world economy suffers the consequences of the disease [2]. Countries around the world have tried several strategies, from informing the public on the virus, enforcing curfews, intensive contact tracing of infected individuals and many more [3].

The decisions taken by governments, which might turn out to be even more harmful than the pandemic itself, are one of the reasons people are witnessing the forming of a global economic crisis. The imposed lockdowns and measures to protect the public from the virus are changing the way our society behaves, which forces many owners to cease their business activities temporarily and in some cases permanently.

As a result, the way cash flows throughout the economy shifts and many people end up struggling with their monthly bills or even losing their jobs. In order to recover from this inevitable crisis, governments have to take into account all trade-offs between rescuing the economy and public safety. This would lead to the imposition of new regulations and rules that people and businesses will be forced to follow.

One of the main ideas is to introduce “immunity passports” and issue them to people that are considered immune to the virus [4]. People who possess them will be allowed to again live their life normally and engage in many sorts of activities, such as working or studying. The main goal is to protect people that are still not resilient to the virus, whilst reopening businesses and providing support for everyone in need. Through the use of immunity certificates, the recovery of the economy is expected to be easier and faster. But, in order for this idea to succeed there has to be a nation-wide testing campaign, which is still impossible, considering the insufficient number of available tests.

The aim of this project is to materialize such an immunity certificate. Delft Blockchain Lab has made this project available, because they wish to extend their current Self-Sovereign Identity library with support for “immunity passports”.

The project plan is built up in the following structure. Chapter 1 will provide some deeper background information. Chapter 2 will go into the technical, legal and operational feasibility of the project, given the duration of this project. Chapter 3 will explain any risks which might be faced during or after the project. Chapter 4 lists the requirements that need to be realized during the project. Chapter 5 describes the team’s communication and workflow strategies. And lastly, chapter 6 contains a roadmap for the coming weeks.

2. Problem Analysis

The project plan begins with background information about the problem. Through the use of reduction techniques, the problem was reduced to deploying a nation-wide system which implements Self-Sovereign Identification.

Building Immunity

Usually, immunity to a disease is proven through a test, which checks for the presence of antibodies associated with this disease inside a person's organism. However, since this is a novel virus, one of the main problems that needs to be taken into consideration is the fact that scientists have not yet proven that the presence of antibodies in someone's organism is solid evidence that this person is immune to the coronavirus [5].

Although repeated infections might turn out to be possible, scientists think that this is highly unlikely and it is generally believed that former patients of COVID-19, that test positive when checked for antibodies, have built immunity [6]. Considering the importance of the project and the fact that the virus is still spreading widely, the possibility of reinfections will not be regarded as a possible hurdle. When the duration of the immunity is later defined, necessary corrections will be applied.

Immunity Passports

The problem with lifting the imposed emergency regulations might be efficiently solved through the use of immunity certificates. They effectively provide people with a "permit" for their usual economic and social activities. Immune people will be extremely valuable in the months after the pandemic is over, because there is always a possibility of a second pandemic, which might have worse consequences than the first one. "Immunity passport" holders may be used as a resource. This would mean that these people could be sent to infection hotspots in order to provide critical support [6].

Unfortunately, immunity certificates need a lot of consideration before deploying them. Since only people that have previously been infected with the virus will become immune and thus have the right to work and ultimately earn money, there will be a majority of people being left behind, possibly without access to food and other supplies. This could be considered as a new kind of discrimination, where the population is split in immune and vulnerable, with the latter having restricted rights. At some point they might try to catch the virus on purpose in order to become immune and get access to their full rights again. Another problem is the duration of the immunity. If everyone has to be regularly tested, there will not be enough tests for everyone [7].

There are several ways in which one could grant such an "immunity certificate". A mere certificate on paper could suffice, however this brings with itself several issues of authentication and authenticity [8]. Furthermore, immunity certificates pose a privacy issue because by using them, people are forced to share their health condition, which might end up in misuse of sensitive information. The "passports" also might make use of mobile technology, which will further exclude parts of the population, currently not having access to such technologies.

Nevertheless, there are already more than 60 companies working on defining immunity certification. Most of them are using blockchain technology, as it provides some of the required privacy and security properties [9].

Privacy and Security

As discussed above, there is a risk of personal information misuse cases, which poses an enormous privacy threat. This might mean that people are less likely to trust the technology and they might choose not to use it, which will make it obsolete. Most of the companies that are working towards a solution, use blockchain technologies to address these caveats. Historically, Bitcoin was created to allow people to have full control over their information, ultimately trying to solve the privacy and security issues. But, since 2009 there have been many cases in which personal privacy was breached [10].

Recently, the World Wide Web Consortium released a new standard called "Verifiable Credentials Data Model", which claims to provide security and anonymity to its users. This model allows users to prove each other claims about themselves without revealing sensitive information [11]. The problem that remains is that such a system is not widely deployed yet.

Self-Sovereign Identity

One approach which has gained a lot of traction recently is the usage of a Self-Sovereign Identity (SSI). This is an implementation of the "Verifiable Credentials Data Model", discussed above. The idea behind SSI is that citizens have full control over their own identity. Instead of the government issuing identification documents, every person could claim information about himself voluntarily and organizations could then attest these claims if they are correct. For example, holders of SSI could claim that they are above a certain age and request a responsible organization to attest this claim after which the holders could use this proof by showing the appropriate attestation without revealing any other sensitive information about themselves (e.g. exact age or date of birth) [12].

Client

The task set is to combine these two topics, namely the granting of an immunity certificate through the use of a Self-Sovereign Identity. The client, Delft Blockchain Lab, is TU Delft's initiative for research, education, and training in blockchain technology and trust in the internet. In cooperation with the Ministry of the Interior and Kingdom Relations it has developed a library for SSI that is set to provide passport-grade identities in the future [13]. The outcome of this project is adding the COVID-19 "immunity passport" feature to the library as it could prove very useful in the coming months. Furthermore, if this project is successful and ends up becoming a nation-wide deployed system, it could possibly be the first step towards mass adoption of Self-Sovereign Identity.

3. Feasibility Study

The issue of user privacy and data sovereignty is one of the most hotly debated topics of the 21st century. In a world where big tech companies such as Google and Facebook are having to pay multibillion euro settlements, research shows that the world is looking for change [14].

The project aims to further popularise a solution to this pressing issue by implementing a user friendly application that abides by the well tested and researched SSI principles, which provide user privacy by placing individuals in control of their data. All projects using innovative technologies give place to several doubts. Can this work in the real world? Will uncertainty challenge on-time completion? Is such a product even possible? This section aims to answer these questions.

Legal Feasibility

When dealing with user data, privacy protection laws are a major concern but there is one advantage to this project, it is all about user privacy and data protection.

The purpose of this project is to showcase the usability of the SSI principles, which are designed to protect user data by giving them ownership of their information. By placing the sensitive data in the hands of the owner most privacy concerns, which relate to a centralized data point owned by a third party, are circumvented.

By using the IPv8 framework and TrustChain as the backbone of the data transfer and validation processes, the hard work of dozens of researchers and specialists is going to be put into use to guarantee safe data transfer and integrity. Safe storage combined with safe data transfer allows the application to be secure and legally safe.

Operational Feasibility

Another important point is whether or not the product would be attractive and practical for the common user. It will take the form of a mobile application, which is a tried and tested platform to get users engaged with a product, it is also a platform that many people are familiar with which improves ease of use.

In terms of practicality the numbers do not lie. So many court cases, debates, legal settlements and outright protests have been conducted on the base of data ownership that there is little room to deny that individuals are looking for more control over their data. People do not trust big corporations anymore, they want control and knowledge of where their data is and who can access it, and such is their right based on article 12 of the UN charter of human rights [15].

SSI provides what people want in an intuitive way, they own their data and only they can give access to it. The application is expected to become the first SSI experience for many users, and allow citizens to acquaint themselves with the concept of owning their internet identity. The concept of proving COVID-19 immunity is an isolated and privacy-sensitive issue, its sensitivity supports the choice of SSI implementation, while its isolation allows us to create a useful application within the allocated time.

Scheduling and Technology

New technologies lead to new problems, and new problems lead to unpredictable solution times, so how can project completion within ten weeks be guaranteed? The project will involve some relatively new technologies including blockchain and decentralized data ownership. Building all of these systems would greatly extend the project lifetime, but the work is simplified by making use of many systems already in place.

The IPv8 framework will be used to handle most of the complications concerning decentralization, SSI and data integrity. This project is also heavily inspired by other health-related SSI systems [16] as a guide in what components the project will involve, reducing design time. The frontend is going to be built as a mobile application, which has many tools to quickly prototype and deploy the product. While most of the complications reside in the backend, they are handled by external frameworks with several times the development time that this project will have, allowing for achieving more in less time.

By focusing solely on the COVID-19 immunity verification pipeline, using the SSI principles to handle user privacy, and using well established frameworks and technologies wherever possible, ten weeks of development time look achievable, this is also backed by the Roadmap which sets out exactly how those weeks are going to be spent.

4. Risk Analysis

The integration of an immunity passport feature into a Self-Sovereign Identity solution is not without risks. A discussion follows about the risk factors involved in the introduction of a large-scale immunity passport on top of an SSI implementation and the use of it, concerning both the individual and the public. Here, only the risks revolving around immunity passports are being considered, but not the risks revolving around the SSI library itself.

Faulty immunity test

At this point in the pandemic, there is not enough evidence about the effectiveness of antibody-mediated immunity to guarantee the accuracy of an “immunity passport” or “risk-free certificate” for COVID-19 [17]. From this, it can be concluded that the immunity passport may thus induce a false sense of security to the relatively carefree holder. The passport of people who now wrongfully think they are immune allows them to do social activities, such as going to work or to meet-ups, while the holders are ignorant to the fact that they are exposing themselves and those around them to great danger. Therefore, the immunity passport may have the unintended side effect of increasing the number of active cases in the areas it is introduced to.

Expiration of the passport

It is unknown how long a person can keep the antibodies in their body after recovering from COVID-19 [18]. So, even if a person is declared immune and gets the immunity passport they are officially eligible for, it is not certain until when those passports should be valid. This might cause a second wave of infections from novel coronavirus, as people who might no longer be immune will also use their passports to gain access to social activities.

However, the coronavirus causing COVID-19 has not rapidly mutated so far, which could indicate that immunity confers long-term protection [19]. This means that immunity passports may actually last for as long as is necessary.

Segregation of those without

As was stated in the problem analysis section of this report, there is a nonzero probability that society will be divided into two groups: those who do have an immunity passport and those who do not. If this happens, antagonization of those with and/or those without passports may occur. This will likely result in great social stigma on people with immunity passports from those without and vice versa.

Purposeful infection

The privileges the immunity passport grants to its holders may prove attractive to those who have not been infected by the coronavirus. As a result, people may want to purposefully contract the coronavirus for a chance to gain immunity and with that eligibility for an immunity passport, which in turn will allow them to be able to return to their daily lives as they were before the outbreak. Thus, immunity passports could again increase the number of infections in the places in which they are introduced.

Privacy and security concerns

The immunity certificate support is going to be built as an extension to a privacy-preserving and secure SSI framework. However, failure to convince the potential user of the safety with regard to privacy may cause the product to not be used. As these technologies are rather new, scepticism by the general public is not out of the question. Thuss, the final product should be as user-friendly as possible.

5. Requirements and Solution Proposal

During the process of requirements engineering, the team made use of two scientific papers, which describe a possible implementation of an “immunity passport” [20] and some properties that such an application should hold [21]. There were also two meetings with the client, which tremendously helped with narrowing down the list of specific requirements which need to be implemented before the end of the project.

Elicitation and Analysis of the Requirements

The following section depicts the requirements analysis process of the team.. This analysis was conducted with the help of user stories.

Three main roles were introduced:

- Holder of SSI
- Attester
- Verifier

User Story 1: “Application startup before configuration”

- When any of the three users wants to start using the application, they should be able to click on the application icon and if this is their first usage, they should be prompted to complete a setup process. It contains a password configuration and local blockchain instance initialization. Then the main menu should appear.

User Story 2: “Application startup after configuration”

- When any of the three users wants to start using the application, they should be able to click on the application icon and if this is not their first usage, they should be prompted to enter their password. Then the main menu should appear.

User Story 3: “Claim creation”

- After a holder has requested a claim, an attester should be able to pick a form from a list. He should then be able to fill in the contents of the claim. All claims should be in user-readable format (e.g. json, that will be rendered on screen later to allow for easy reviews).

User Story 4: “Sending a claim”

- After an attester learns the key identifier of a holder and creates a claim, he should be able to sign it, save it to his blockchain and send it to a holder using his key.

User Story 5: “Receiving a claim”

- When a holder receives a claim for review, he should be able to see it in his inbox.

User Story 6: “Claim review”

- After a holder receives a claim, he should be able to access it through his inbox and manually review its contents. Then he should be able to decide whether to accept the form or not.

User Story 7: “Claim acceptation”

- After a holder has reviewed a claim and has decided to accept it, he should be able to sign it, save it to his blockchain and send it to the attester who originally created the claim.

User Story 8: “Claim decline”

- After a holder has reviewed a claim and has decided to decline it, he should be able to remove it from his inbox. He does not need to notify anyone about his decision.

User Story 9: “Claim time out”

- After a certain amount of time, an attester should be able to remove an outstanding claim if it is not signed and returned by its holder.

User Story 10: “Receiving an old claim”

- When an attester receives a claim that is not on his blockchain anymore, he should notify the holder that this claim is no longer valid.

User Story 11: “Receiving a claim”

- When an attester receives a claim that is on his blockchain, he should check automatically if both claims are still the same (verify the claim).

User Story 12: “Invalid claim”

- When a claim turns out to be invalid, an attester should notify the holder that sent it.

User Story 13: “Valid claim”

- If a claim turns out to be valid, an attester should be able to save it to his own chain instance.

User Story 14: “Receiving a notification - Holder”

- A holder should be able to see any notifications about claims that he has made.

User Story 15: “Showing attestation for verification”

- A holder should be able to choose from a list of all his attestations, the one he needs for verification. After picking it, the attestation is shown in appropriate format for verification (e.g QR code). Attestations may also be sent using bluetooth or other networks.

User Story 16: “Reviewing an attestation”

- A verifier should be able to enter into state for verification. This is accomplished through a click of a button in the main menu. There may be different states,

depending on the medium that is going to be used for the verification. For example, if the holder presents the attestation using a QR code, the verifier should be able to use his camera for verification. After scanning the attestation, the verifier should be able to manually review it.

User Story 17: “Reviewing a specific attestation”

- A verifier should be able to enter into state for verification. This is accomplished through a click of a button in the main menu. Then he should be able to pick the type of form, he is going to verify. There may be different states, depending on the medium that is going to be used for the verification. For example, if the holder presents the attestation using a QR code, the verifier should be able to use his camera for verification. After scanning the attestation, the verifier should be able to automatically review it.

User Story 18: “Verifying an attestation”

- After reviewing the attestation either automatically or manually, both parties get notified by either showing a pass or fail notification.

All functional and non-functional requirements will be listed in the backlog once the project repository is configured. For this process, the MoSCoW method is going to be used.

Application Restrictions

Because there are some restrictions posed by the bill [21], some additional features are being considered. If the project duration is not sufficient to implement them, they are going to be listed as recommendations in the final report of the project.

First, there is a portion of the citizens, which are considered technologically excluded. They either do not have access to devices with internet connection or they do not possess sufficient knowledge to handle such devices. In this case, there might be a feature which allows for the issuance and usage of paper certificates.

Second, holders which are not carrying their device at all times or which device is not working, should not be penalised. A possible solution is the introduction of “smart bracelets” which are going to contain their owner’s attestations. This will allow for verification on demand.

Solution Proposal

The problem analysis has shown that “immunity passports” might turn out to be obsolete if implemented now, since there is no proof that people build immunity against COVID-19. The specific regulations about those certificates will also become available only if immunity exists. That is why the solution should not solely focus on implementing “immunity passports”.

A better solution is to create a framework which will allow for the issuance and verification of many kinds of certificates. The idea is to provide a framework that makes use of the attestation model implemented by the Delft Blockchain Lab. The main feature of this framework is the support for any kind of certificate. This will be done by the developer that

implements an application that uses the framework. Later, those applications may be united in a single supper app. Also, by giving control over certificate creation to the developer, the holders will not be required to constantly update their application since all certificates will follow a specific data model and when holders receive certificates, the application will render them in human-readable format for the manual check.

In order to have a specific implementation of a certification service, interested stakeholders can create their own applications. That is why earlier the process of establishing communication between a holder and an attester or a verifier was vaguely described. This process should be a part of the application which implements the framework. The idea behind this is that for some certificates, holders will personally go to the attester and ask for a certificate. In other cases, holders might approach attesters over the phone, Internet or through a video calling service, which might also be implemented as a part of the application.

As a proof of concept, an Android application is going to be delivered which will allow for the creation, attestation and verification of immunity certificates. This fulfills the needs of the client. It will be assumed that patients will have to personally go to a healthcare expert in order to get tested and receive a certificate. That is why the process of requesting an immunity certificate will not be implemented. If later the government approves home testing, the application might be extended with a video calling service in order to provide supervision, which is just an implementation of the certificate requesting process.

For the implementation of the attestation and verification phases, IPv8 will be used. For the blockchain, TrustChain will be used, since it is already incorporated into the attestation model provided by the client. Since all this is implemented in Python, a packaging tool for Python apps on Android will be used. The available ones are: BeeWare, Chaquopy and Kivy. There already exists an app which makes use of Kivy, but BeeWare allows for packaging applications on other operating systems too and might be a better choice. Chaquopy on the other hand is lightweight. The GUI is going to be implemented by using React and Expo. For continuous integration either GitHub or GitLab will be used.

In conclusion, the solution provides support for a multiple of certificates, which allows for the definition of many health certificates. They might be used during the COVID-19 crisis to give people different rights, depending on their health condition. Holders are also not required to constantly update their applications, since they do not have to be aware of the available certificate types. Finally, the framework allows for the development of a superapp which will contain many certification services.

6. Project Approach

In the first week of the project there was a long meeting with regards to the approach to this project. In this meeting a working agreement was set up, in which several guidelines that need to be followed were outlined. As most of the group members are not familiar with each other or with how well they can work in a team, a working agreement appeared to be appropriate.

This project has several supervisors. These are the client, the coach, the TA and, if necessary, the Software Project coordinators.

The contact between the group and the client happens on a weekly basis. The client is expecting questions and also posing ones, in order to gauge the progress. The medium used for this meeting is the Discord voice chat. For small inquiries the client may be asked questions by sending messages through Discord.

The communication with the coach happens at certain points in the project. Those meetings are done through Jitsi. The coach will give feedback during these different points throughout the project. For general inquiries the TA is the first point of contact. He should be asked first instead of the coach.

The contact with the TA happens on a weekly basis. This meeting also goes through Jitsi. Furthermore there is a shared Mattermost channel with the group, TA and coach, where small questions at any point in time may be asked. The TA is the first point of contact for day-to-day guidance.

The team itself has two means of communication. There is a WhatsApp group and a Mattermost channel. The Mattermost channel is the primary means of communication. The WhatsApp group is only used in case of heads up if there is an absentee in the Mattermost channel. The Mattermost channel is used to discuss anything in regards to the project.

Lastly, if required, there is a public Mattermost channel for all students in the Software Project to ask their questions regarding the Software Project to the Software Project coordinators.

7. Roadmap

This roadmap is a general guideline of the topics the group will focus on every week, it is both a planning tool and a feasibility check to see how work could be divided in appropriate time slots. It is not a strict project schedule and is subject to change based on unforeseen problems or a change in project direction or scope under the product owner's decision. This can be accomodated thanks to the use of the agile SCRUM process.

The roadmap predicts two main lines of work:

Frontend: focused on designing the interface and making the correct calls to the backend.

Backend: focused on implementing immunity passports through the use of the Delft Blockchain Lab's own SSI framework.

The prediction is that the backend section will take significantly more effort and as such it was given two weeks for implementing most features, it will also receive more developers if required.

The frontend will start with a functionality focused approach, so the application's visual appeal will only be a focus later in development. This allows for prioritization of a functional product, keeping the frontend ahead of the backend, and guaranteeing that time is only invested in styling UI components that are actually necessary in the final product.

Roadmap:

Week 3: 04/05 - 10/05

- Frontend: UI Design
- Backend: Start work on packaging the Python framework for Android
- Project setup: repository, pipeline, dependencies, continuous integration
- Basic mobile application (no SSI functionality)

Week 4: 11/05 - 17/05

- Frontend: Implement all UI components in design for joining the network
    - functionality over style
    - mock methods where the backend is expected
- Backend: Finish pipeline for joining the network
- Incorporate SSI into mobile application (some form of interaction with backend)

Week 5: 18/05 - 24/05

- Frontend: Implement UI components for adding and sending immunity proofs
- Backend: Start work on proof creation by professionals and transmission to user

Week 6: 25/05 - 31/05

- Frontend: Implement UI components for sending proofs to other users (eg: QR code generator + reader)
- Backend: Finish implementing immunity proof creation and transmission

Week 7: 01/06 - 07/06

- Frontend: Overall styling, debugging and testing
- Backend: Finish establishing proof pipeline, debugging and testing

Week 8: 08/06 - 14/06

- Buffer week for unpredicted delays, requirements, problems
- Overall testing, validation, debugging and report writing

Week 9: 15/06 - 21/06

- Overall testing, validation, debugging and report writing

References

[1] D. L. Heymann and N. Shindo, “COVID-19: what is next for public health?,” *Lancet*, vol. 395, no. 10224, pp. 542–545, Feb. 2020.

[2] CPB Netherlands Bureau for Economic Policy Analysis, “Corona crisis scenarios (26 March 2020),” *CPB Netherlands Bureau for Economic Policy Analysis*, 26-Mar-2020. [Online]. Available: https://www.cpb.nl/en/corona-crisis-scenarios#. [Accessed: 29-Apr-2020].

[3] J. H. Tanne, E. Hayasaki, M. Zastrow, P. Pulla, P. Smith, and A. G. Rada, “Covid-19: how doctors and healthcare systems are tackling coronavirus worldwide,” *BMJ*, vol. 368, Mar. 2020, doi: 10.1136/bmj.m1090.

[4] J. Horowitz, “In Italy, Going Back to Work May Depend on Having the Right Antibodies,” 04-Apr-2020. [Online]. Available: https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html. [Accessed: 25-Apr-2020].

[5] “‘Immunity passports’ in the context of COVID-19,” 24-Apr-2020. [Online]. Available: https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19. [Accessed: 26-Apr-2020].

[6] Eichenberger R., Hegselmann R., Savage D. A., Stadelmann D., and Torgler B., “Certified Coronavirus Immunity as a Resource and Strategy to Cope with Pandemic Costs,” *Wiley Online Library*, 15-Apr-2020. [Online]. Available: https://doi.org/10.1111/kykl.12227. [Accessed: 25-Apr-2020].

[7] S. Baker and E. Larson, “The Problem With Immunity Certificates,” 09-Apr-2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-04-09/there-s-a-big-problem-with-coronavirus-immunity-certificates. [Accessed: 26-Apr-2020].

[8] C. N. N. Laura Smith-Spark, “Is this how to get out of lockdown?,” *CNN*, 03-Apr-2020. [Online]. Available: https://www.cnn.com/2020/04/03/health/immunity-passport-coronavirus-lockdown-intl/index.html. [Accessed: 29-Apr-2020].

[9] I. Allison, “COVID-19 ‘Immunity Passport’ Unites 60 Firms on Self-Sovereign ID Project - CoinDesk,” *CoinDesk*, 13-Apr-2020. [Online]. Available: https://www.coindesk.com/covid-19-immunity-passport-unites-60-firms-on-self-sovereign-id-project. [Accessed: 26-Apr-2020].

[10] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[11] “Verifiable Credentials Data Model 1.0,” 19-Nov-2019. [Online]. Available: https://www.w3.org/TR/vc-data-model/. [Accessed: 23-Apr-2020].

[12] Q. Stokkink and J. Pouwelse, “Deployment of a Blockchain-Based Self-Sovereign Identity,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 1336–1342.

[13] J. Pouwelse, “Blockchain-based identity with government support.” [Online]. Available: https://www.blockchain-lab.org/trust/. [Accessed: 29-Apr-2020].

[14] “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,” *Pew Research Center: Internet, Science & Tech*, 15-Nov-2019.

[Online]. Available: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. [Accessed: 02-May-2020].
[15] "Universal Declaration of Human Rights," 06-Oct-2015. [Online]. Available: https://www.un.org/en/universal-declaration-human-rights/. [Accessed: 30-Apr-2020].
[16] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, doi: 10.1109/pimrc.2017.8292361.
[17] "'Immunity passports' in the context of COVID-19," 24-Apr-2020. [Online]. Available: https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19. [Accessed: 26-Apr-2020].
[18] H. Leung, "What to Know About Coronavirus Immunity and Chances of Reinfection," *Time*, 03-Apr-2020. [Online]. Available: https://time.com/5810454/coronavirus-immunity-reinfection/. [Accessed: 02-May-2020].
[19] R. Eichenberger, R. Hegselmann, D. A. Savage, D. Stadelmann, and B. Torgler, "Certified Coronavirus Immunity as a Resource and Strategy to Cope with Pandemic Costs," *Kyklos*. 2020, doi: 10.1111/kykl.12227.
[20] Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury, Allan Third, John Domingue, "COVID-19 Antibody Test Certification: There's an app for that," 20-Apr-2020. [Online]. Available: https://arxiv.org/abs/2004.07376. [Accessed: 27-Apr-2020].
[21] L. Edwards *et al.*, "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates." 22-Apr-2020, doi: 10.31228/osf.io/yc6xu.