Blockchain Technology for Tourism Post COVID-19

Mohd Norman Bin Bakri
Faculty of Information Science and Technology, Multimedia University, Malaysia

Han-Foon Neo
Faculty of Information Science and Technology, Multimedia University, Malaysia

Chuan-Chin Teo
Faculty of Information Science and Technology, Multimedia University, Malaysia

Abstract: During the pandemic, the tourism industry was one of the most severely impacted sectors. As vaccines are now widely available, each government is working to develop a system that can generate a digital vaccine certificate and PCR lab test result to verify that a person has been fully vaccinated or has a negative PCR test result, in order to allow them to enter business premises, travel overseas or cross state borders. However, the use of centralised systems in the development of the digital COVID-19 pass system results in a number of challenges, including the system's high susceptibility to failures, sluggish and inefficient information transmission, and vulnerability. The goal of this research is to offer a new digital COVID-19 pass based on the proposed "SmartHealthCard" blockchain technology. SmartHealthCard is a decentralised application (dApp) encrypting and hashing user data and safely storing it in a distributed database. Privacy preservation, GDPR compliance, self-sovereignty, KYC compliance and data integrity are featured. This initiative has the potential to benefit the public, healthcare professionals, service providers and the government. SmartHealthCard enables quick verification of tamper-proof COVID-19 tests/vaccines, aiding in COVID-19 transmission control while respecting the user's right to privacy.

Keywords: blockchain, tourism, COVID-19, decentralised, privacy.

Introduction

The worldwide pandemic of Coronavirus Disease 2019 (COVID-19) has caused tremendous negative effects on the lives of billions of people, with substantial health, societal, and economic implications. Despite the deployment of effective restrictive public health measures, such as tight travel restrictions, the spreading of COVID-19 persists (Pavli & Maltezou, 2021).

http://doi.org/10.18080/jtde.v11n3.764

Tourism is one of the most important economic sectors in the world, accounting for 7% of global commerce in 2019. Overall, tourism is the world economy's third largest export industry. This amounts to more than 20% of the Gross Domestic Product (GDP) in some countries. It is the most heavily impacted industry hit by the COVID-19 pandemic, which caused a global effect on economies, lives, public services and opportunities. International tourism has dropped by an astounding 73 percent in 2020 due to the COVID-19 pandemic, and demand for international travel remained low at the start of 2021 (Pavli & Maltezou, 2021).

The impact of the COVID-19 pandemic on the travel tourism business has been greatly underestimated since the sprouting of COVID-19 in China. Up until this day, tourism agencies and policymakers still do not have a comprehensive understanding of the crisis's consequences and potential, which can have a serious influence on the industry (Škare *et al.*, 2021). According to the World Travel and Tourism Council (WTTC), COVID-19 might put up to 75 million workers at risk of losing their jobs. The GDP loss from travel tourism might be as high as US$ 2.1 trillion in 2020. WTTC also expects a daily loss of one million jobs in the travel tourism sector (Škare *et al.*, 2021).

Even though the COVID-19 pandemic threat is receding, surges in the number of cases and new variants are on-going. Governments all around the globe are still dealing with the threats that have wreaked havoc on people's lives and economies in over 190 countries, resulting in over 82 million illnesses and 1.8 million deaths (Abid *et al.*, 2021).

Apart from mitigation strategies for COVID-19, the economic reopening plan has risen to the top of the priority list for all governments, businesses, and individuals. One of the problems facing public officials and governments is to efficiently govern their respective economies, open workplaces, permit travel, and avoid new outbreaks of disease.

Different technical alternatives, such as movement papers and tracking applications, are being investigated. However, all are vulnerable to deception and fabrication, and can have an impact on essential freedoms or be socially undesirable. More specifically, because of the nature of trackable applications, public concerns about privacy have been a roadblock to existing solutions. Because of Google/Apple contact tracing capabilities, privacy and secrecy of personal information are jeopardised. Furthermore, apps for Bluetooth-based traceability require the user's gadget to stay in an active broadcasting mode, which drains the battery. In the meantime, Bluetooth technology includes security flaws, such as a weak wireless interface and the identification and disclosure of physical hardware (Abid *et al.*, 2021). Furthermore, there is a considerable possibility of replay attacks on the trackable network that can generate widespread panic.

http://doi.org/10.18080/jtde.v11n3.764

Using a supposed "risk-free certificate"/"immunity passport"/"health certificate" or other secure health document is a potential option. The main concept is that a proof of vaccination may be used to create a certificate that exempts a person from the most stringent government requirements. Its goal is to provide a credential in a digital yet printable format that is tamper-proof and globally provable to anybody who has been vaccinated or has received an authorised PCR/antibody test result. This health credential enables public authorities to control access to sensitive or critical facilities, such as airports, schools, hospitals, workplaces, and other public places, while taking into account the remaining uncertainties about the virus, changing health policies, and the validity period of the test result. As compared to traceability applications, the health credential protects user privacy and will only be checked at frontiers (such as schools, hospitals and airports), saving the battery life of devices because it works offline and consumes no energy.

France, Italy, United States, United Kingdom, China, Estonia, Chile and Germany have all stated that they want to test such credentials. Unfortunately, many government-tested and deployed solutions give little technical specifics, making them difficult to fully comprehend or evaluate (Abid *et al.*, 2021). It is generally known, however, that some of the systems are centralised or dependent on third parties, posing security and privacy concerns.

In light of certain governments' interest and the emergence of a number of commercial alternatives, a scholarly examination of COVID-19 health credentials is required. It is critical, in particular, to give precise technological solutions and to identify existing limits in order for healthcare authorities to be properly informed. Furthermore, a large percentage of developing nations lack the technological and economic capabilities for such developments.

To aid in the fight against this global health crisis, blockchain technology has the advantage of playing a critical role in COVID-19 prevention and assisting in the implementation of government rules and standards while maintaining confidence among all parties. Indeed, due to its characteristics of resilience, integrity and transparency, the emerging Blockchain solution, which is an immutable, distributed, and tamper-proof record database with global computational groundwork (i.e., smart contracts), tends to provide effective COVID-19 solutions based on a great amount of trust and accuracy (Abid *et al.*, 2020).

Blockchain Technology

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every

http://doi.org/10.18080/jtde.v11n3.764

participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash. This means, if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers tried to corrupt a blockchain, they would have to change every block in the chain, across all of the distributed versions of the chain. Blockchains such as Bitcoin and Ethereum are constantly and continually growing as blocks are added to the chain, which significantly adds to the security of the ledger.

Bitcoin's blockchain is used in a decentralized way. However, private, centralized blockchains, where the computers that make up its network are owned and operated by a single entity, do exist. In a blockchain, each node has a full record of the data that has been stored on the blockchain since its inception. For Bitcoin, the data is the entire history of all Bitcoin transactions. If one node has an error in its data, it can use the thousands of other nodes as a reference point to correct itself. This way, no one node within the network can alter information held within it. Because of this, the history of transactions in each block that make up Bitcoin's blockchain is irreversible. If one user tampers with Bitcoin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This helps to establish an exact and transparent order of events.

Because of the decentralized nature of Bitcoin's blockchain, all transactions can be transparently viewed by either having a personal node or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added. Blocks on Bitcoin's blockchain store data about monetary transactions. It turns out that blockchain is actually a reliable way of storing data about other types of transactions too. Some companies that have already incorporated blockchain technology include Walmart, Pfizer, AIG, Siemens and Unilever.

Blockchain technology has the potential to be utilized in various industries. By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of holidays or the time of day or week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if trading internationally), meaning that the money and shares are frozen for that period of time. Health-care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal

http://doi.org/10.18080/jtde.v11n3.764

health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy.

Blockchain-related applications

This section describes four blockchain-related mobile apps to create a digital health/vaccine/immunity passport for users, healthcare providers and service providers.

AOKpass

AOKpass (ICC United Kingdom, 2021) is a blockchain-based platform and mobile app that allows a user to securely validate his or her health status with any third parties while maintaining the privacy of his/her underlying personal health data. Users retain complete control over their personal health data, such as health credentials and test results, which are solely saved on the user's smartphone that does not involve any external database or centralised system. This app is built on the Ethereum permissionless blockchain and employs distributed ledger technology. To secure user data and preserve system security, the AOKpass platform also uses hashing and encryption techniques.

AOKpass is based on the Ethereum public Blockchain network ("Ethereum"), which is a worldwide, open-source decentralised computing platform. Unlike centralised computing networks, which are supported and secured by a single or small number of private databases and/or servers (or "nodes"), Ethereum is supported and secured by a global decentralised public network of discrete nodes (the total number of nodes at any given time).

Ethereum is a platform for the deployment of decentralised applications (dApps), which are programs that operate and access the appropriate functional advantages of Blockchain technology through decentralised Blockchain networks.

A cryptographic 'hash' is a sophisticated digital signature, often known as a cryptographic 'proof', that is a crucial part of a Blockchain. The key characteristics of a hash are that it is obtained precisely from the certificate information; nevertheless, the certificate information cannot be derived backwards from the hash. The hash acts as a secure signature that can be confirmed by anybody who has been given an AOKpass. AOKpass uses the SHA 256 hashing algorithm, which is generally acknowledged as an industry standard.

AOKpass uses Amazon Web Services (AWS) as a third-party service provider to securely store a restricted set of data, which does not include AOKpass users' personal health information. The AOKpass security paradigm is built on two principles, simplicity and the storing and management of as little data as feasible. The backend infrastructure of the AOKpass system is made up of serverless AWS functionality and other provisioned AWS cloud services, effectively offloading any infrastructure-level security threat to AWS operations. The only possible threat

http://doi.org/10.18080/jtde.v11n3.764

is the compromise of the AWS credentials, or the credentials of a few other infrastructure services (AWS, Google Play, Apple Developer Account, Pulumi, Cloudflare). These credentials are kept on secure management platforms and only shared with those who have a need to know.

For the sensitive information that AOKpass does keep (such as attestor emails and names), AOKpass encrypts it utilising a cold encryption key that is not stored anywhere on the network. Without access to a cold private key, which is required to sign possible attestation sources, approval of attestors is likewise impossible. AOKpass's design, in addition to the security of its infrastructure, permits "third party" attestation providers to host their own attestation infrastructure if extra regulatory needs require it.

CommonPass

CommonPass (HandyVisas, 2020) is a digital health software application that allows users to show standardised, provable documentation where they have been vaccinated against COVID-19 or have tested negative for the virus. CommonPass creates a digital health pass that a user produces for border crossings and travel, or to indicate compliance with the venue or destination's health admission regulations, using secure and private processes.

The CommonPass app is free to download from Google Play Store or Apple App Store. It may be used by anybody to keep track of their test results and immunization status. If travelling with CommonPass, the destination may require a unique invitation code to certify that the user fulfils all of the relevant travel regulations.

For pass generation, CommonPass only uses the most current laboratory results from a particular supplier. If a CommonPass was produced during a previous test, it will remain available until the user deletes it. Other than the most recent test results, other test results may be retrievable and used in future editions of the program.

Only the mobile device has access to the CommonPass. Outside healthcare professionals, partners, contractors, or vendors are not allowed to share or store anyone's CommonPass. For troubleshooting purposes, only a de-identified (HIPAA compliant) version of the information is temporarily retained on the systems (two weeks for test results, and 30 days for vaccination records).

Because Personally Identifiable Information (PII) is just stored on the user's own device, the user has control over it. When a particular airline or venue needs to verify the user's status, CommonPass servers save it using a cryptographic algorithm that allows the system to react on the user's behalf only to people who know the user, not to strangers. After two weeks, the status is automatically removed from the servers.

http://doi.org/10.18080/jtde.v11n3.764

IBM Digital Health Pass

The use of the IBM Digital Health Pass (2021) helps to manage and regulate the sharing of COVID-19 health credentials. It only allows for the verification of COVID-19 immunisation records issued digitally by Digital Health Pass participants, including pharmacies, laboratories and clinicians. A user may keep track of COVID-19 health certificates stored in the wallet, which is safely encrypted on a smartphone, or print them out as secure QR codes. It is helpful for those who do not have access to a smartphone.

In business, a staff member may use the Digital Health Pass Verifier app to ensure the COVID-19 health certificate is valid when a user visits a participating company. They may also want a picture ID with the user's name and birth date to ensure the pass belongs to the owner. On the same device, adults can keep COVID-19 health certificates for youngsters or seniors under their dependency.

When a participating company scans the encrypted QR code, it should only be able to determine whether or not the pass is still valid, as well as any personal data that the user has given them permission to access for a COVID-19 test result or vaccine verification. It contains data such as the user's name and birth date that is required to validate their identity.

Digital Health Pass simply uses a unique combination of numbers and characters to represent personal health information, as a QR code. Users have complete control over their data, deciding what to share, with whom, and for what reason. Therefore, the encrypted wallet is inaccessible to IBM and other verifying companies.

Digital Health Pass is not a contact tracker or a location tracking app. It is a secure modern replacement to paper COVID-19 vaccination cards or test results that allows the users to manage and share that they have been tested negative or vaccinated for COVID-19 whenever they want.

CovidPass

During the COVID-19 pandemic, CovidPass (2020) is "health passport" software that promises to resurrect worldwide travel, major events, and gatherings without jeopardising health and safety or privacy. The goal is to allow healthy persons to travel or attend events while avoiding unaffordable total lockdowns. It is safe software that does not expose personal information by relying on insecure Bluetooth technologies. Instead, it uses a closed loop system with end-to-end encryption, making it hard to attack.

CovidPass provides a secure, safe, and long-term solution for re-allowing travel, worldwide tourism and large-scale events. It can assist in addressing the problems that these businesses have faced since the beginning of the pandemic. Indeed, the essential steps implemented thus

http://doi.org/10.18080/jtde.v11n3.764

far to combat the spread of COVID-19 have affected everyone, regardless of whether they are virus-free or infected and have thus had a significant impact on companies and economies throughout the world. This also includes many large-scale events, such as the Tokyo Summer Olympics and the UEFA Euro 2020, that have been postponed as well.

CovidPass provides a smooth and safe encryption solution for results of COVID-19 screening tests from accredited medical laboratories. Individuals who desire to travel or attend large events are provided with these test results, allowing them to offer the same results to the authorities or organisations that have sought access. Those who pass the serological or PCR test receive a secure QR code on their smartphone, which they may show at airline check-in counters, border crossings or event gates to certify their safe status.

Several unique characteristics of CovidPass include:

1) Technology: CovidPass stores encrypted data from COVID-19 screening tests using Blockchain Technology, providing a consistent, inalterable display of PCR or serological test findings.
2) Privacy: CovidPass is not a contact tracing program, but it solves users' privacy concerns. Its goal is to not only aid and promote the economy, but to also resolving people's worries about utilising contact tracing applications.
3) Expertise: CovidPass draws on the knowledge of specialists in the domains of medicine, consumer apps, government relations and tourism to build a complete, flexible solution.

CovidPass is a response to the current problems that the tourist and events industries are facing. It aims to restore trust in safe travel and social interactions by addressing the concerns of governments, corporations, and individuals. Millions of people will be able to return to flights, hotels, stadiums, conferences, and other venues as a result of this.

Research Method

The hardware requirement for this research is a Windows Desktop PC/Laptop, Apple Desktop, or MacBook to build and maintain the SmartHealthCard dApp system. The software requirements needed are draw.io, Node.js, Cloud MongoDB database and uPort Smart Contract.

As for user, the hardware and software needed for users is an Android OS mobile smartphone to install and register the uPort Mobile app. The user also needs to be registered in the SmartHealthCard system by a healthcare provider via the SmartHealthCard dApp.

Equivalent to the user, an issuer or a verifier needs to install and register with the uPort Mobile app. Additionally, they need to install and register with the SmartHealthCard dApp, which works on Windows Desktop PC/Laptop, Apple Desktop, and MacBook. It should be noted that

http://doi.org/10.18080/jtde.v11n3.764

both issuer and verifier must be registered and verified by Local Authorities first in order to install and register with the SmartHealthCard dApp.

Conceptual framework

This research proposes a new Blockchain-based privacy-preserving digital COVID-19 credential platform, SmartHealthCard, for issuing and confirming COVID-19 vaccine and PCR test certificates. SmartHealthCard seeks to stop COVID-19 from spreading while adhering to privacy regulations. For instance, it is compliant with the General Data Protection Regulation (GDPR) and Know Your Customer (KYC), as well as preserving user autonomy. The suggested method will be used not only for COVID-19 testing, but also for COVID-19 vaccinations, which are now accessible in several countries. The characteristics of the proposed conceptual framework are:

1) Privacy preservation: To reserve encrypted user data, including COVID-19 findings, SmartHealthCard uses an off-chain IPFS (Benet, 2014) storage (InterPlanetary File System) Infura (2022). Only the IPFS hash is saved on the Blockchain, ensuring that sensitive data is never exposed to those scanning the Blockchain.
2) General Data Protection Regulation compliance: SmartHealthCard is GDPR-compliant because it uses well-known data-protection standards, including JSON Web Tokens (JWT) (2013), ERC1056 Lightweight Ethereum Identity (Thorstensson, 2018), and W3C verifiable credentials (VC) (2022), ensuring that users remain in charge over their personal data.
3) Self-sovereignty: The user is the owner of his/her identities in SmartHealthCard and has full autonomy over his/her personal information. It enables the selective disclosure idea, which allows the user to exchange specific bits of data with specified trustworthy partners.
4) KYC-compliance: Because it checks the identification of various users before onboarding them, SmartHealthCard is KYC-compliant. This enables more reliable communication and collection of genuine data in real time. As a result, the suggested strategy would act to be the foundation for real-time supervision of the community health condition, as well as the progress of deconfinement and pandemic management.
5) Integrity: This research can confirm the genuineness of the digital COVID-19 credentials by comparing the hash value of the information supplied by the users and the one which is already recorded in the Blockchain ledger, because the hash value of the information is recorded immutably in the Blockchain.

http://doi.org/10.18080/jtde.v11n3.764

Research design

Application's installation, DIDs' generation, and Issuer and Verifier registration

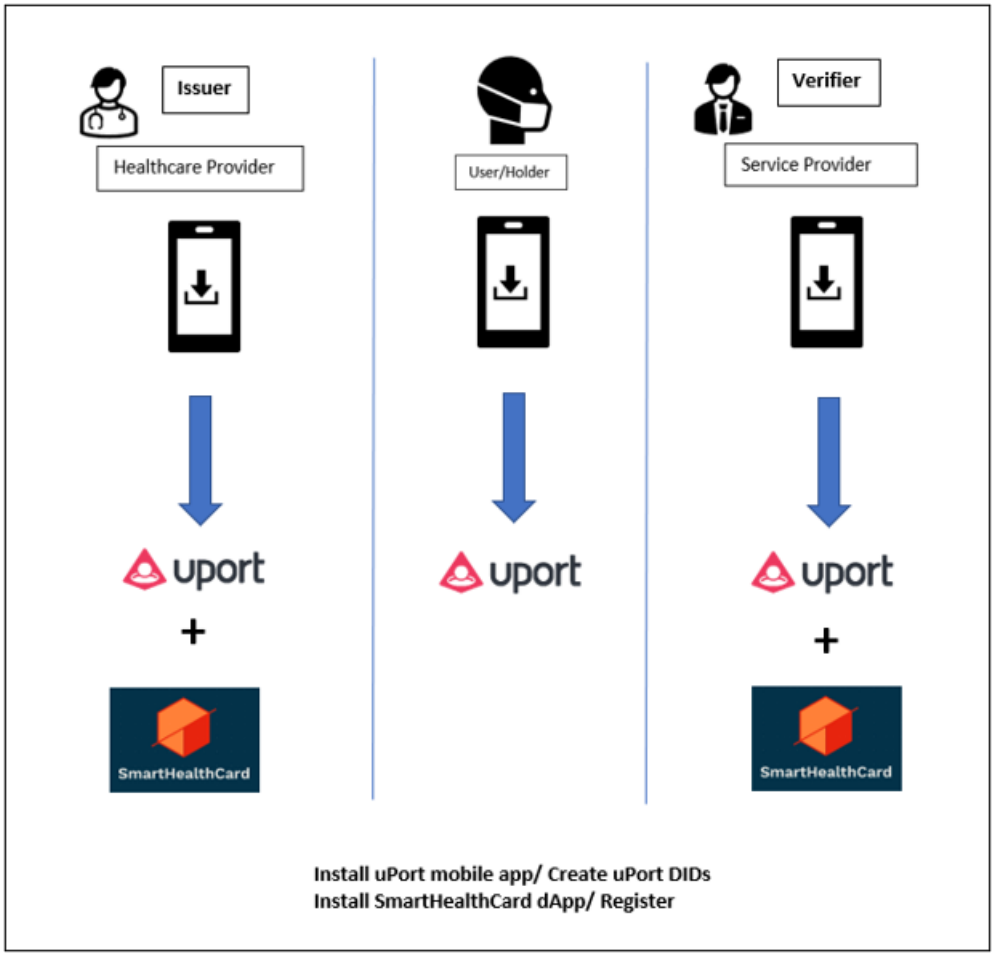

Figure 1. App configurations

Figure 1 depicts several SmartHealthCard configurations, including the generation of Decentralized IDs (DIDs) and registration of the verifier and issuer. This research assumes that all main actors have the SmartHealthCard and uPort mobile (Braendgaard, 2018) applications loaded before the COVID-19 vaccine/test and COVID-19 credential issuing steps:

- Both the verifier and issuer install and download the uPort Credential Mobile Wallet app, the self-sovereign identity Wallet, and give the authority with the personal information and uPort DID. After that, the authority verifies the issuer's or verifier's eligibility and registers the service/medical ID, uPort DID, and other personal information on the Ethereum Blockchain.
- Installing the SmartHealthCard dApp and logging in with his/her uPort DID enables the healthcare provider to obtain the "Issuer" role. The same steps are applied for the service provider to get authorisation for "Verifier" role.

http://doi.org/10.18080/jtde.v11n3.764

- The holder additionally downloads and registers for the uPort app from the Apple App Store or Google Play Store. Creating a uPort Identity is as simple as generating a standard Ethereum key pair account, where there are no gas charges and all Ethereum accounts are legitimate identities. Furthermore, uPort enables identities to be denoted as an object capable of doing tasks like validating messages from other DIDs, signing communications, and updating their DID-document. It enables the holders to regain access to their identity in the event of a broken or lost phone.

The holder retains full autonomy over his or her identity and all related information and will not lose access due to the loss of the private key. It is worth noting that, because the ERC-1056 standard is utilised, a holder just has to construct an Ethereum key pair and not a smart contract for key management or a transaction. As a result, the identity generation procedure is very quick and easy, whereby millions of identities may be generated in one day, guaranteeing strong alignment with a government-sponsored identity initiative.

Holder's access to SmartHealthCard

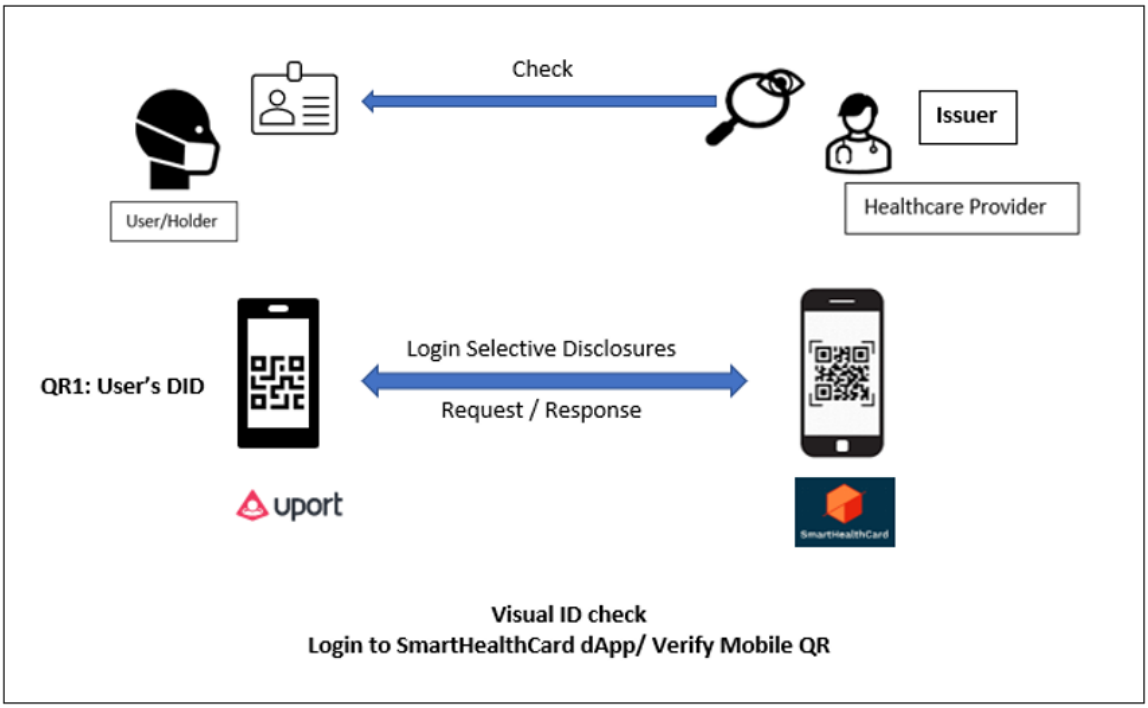

Figure 2. Interaction between holder and the apps

Figure 2 shows the holder's initial interaction with the SmartHealthCard dApp, which takes the form of a login selective disclosure response/request. A holder has now generated his or her uPort DID and is ready to go to the healthcare provider for the COVID-19 vaccine/test and get registered on the SmartHealthCard platform.

In order to do so, the issuer examines the holder's official physical ID (identity card or passport) and scans the uPort DID's QR code, "QR1", to engage with the holder's identification

http://doi.org/10.18080/jtde.v11n3.764

for the first time. Alternatively, the issuer examines to see if the holder already has a valid credential, because each holder may only have one valid certificate at a time. The holder must then log in to SmartHealthCard. The holder's uPort DID and personal information (for example, passport or identity card number) are requested, and the holder has the ability to accept or reject the request using his/her uPort mobile application. Thus, a selective disclosure response/request is triggered. It is the primary way of validating a holder's credentials, and therefore provides total authority over the personal data. After successfully logging in, the healthcare professional can run PCR or antibody tests, as well as administer a COVID-19 vaccination.

Issuing COVID-19 certificates

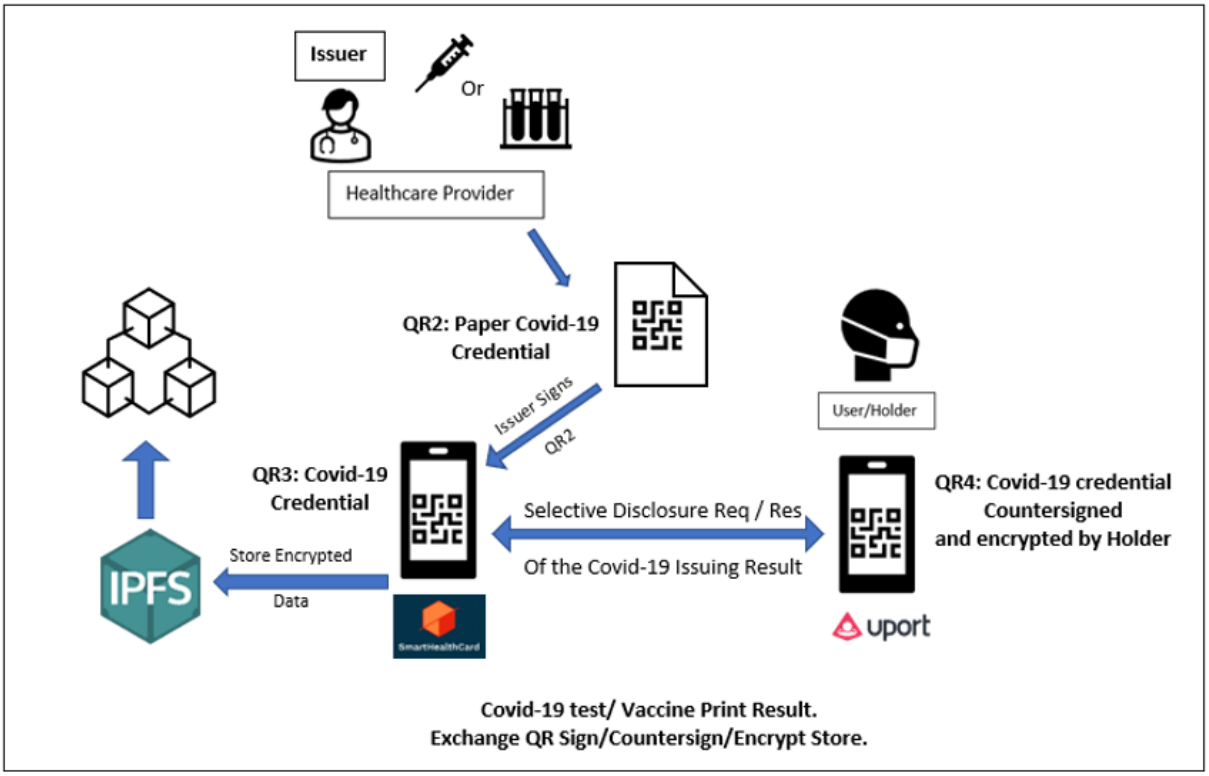

Figure 3. Interaction between holder and the apps

The process of issuing COVID-19 certificates is illustrated in Figure 3, where the issuer performs the COVID-19 vaccination or test. The result of a COVID-19 test is obtainable in about 48 hours for a PCR test and 15 minutes for an antibody test. In this case, a positive result indicates the absence of the virus or the existence of antibodies over a certain threshold. The issuer issues a printed paper version of the COVID-19 certificate once the result is ready. The issuer then uses the SmartHealthCard dApp to scan the printed QR code, "QR 2", to create a digitally signed vaccine/test result as a new QR code, "QR 3". Next, the "QR 3" is sent to the holder, who scans it using the uPort mobile app and digitally countersigns it as a recipient acceptance, resulting in the holder generating and owning a new QR code, "QR 4". To be more

http://doi.org/10.18080/jtde.v11n3.764

specific, this information is transmitted via a selective disclosure response/request, in which the user can confirm or deny.

Meanwhile, the COVID-19 credentials and signatures are encrypted by the holder. The holder also signs the request with his/her device's private key and transmits the result. When the issuer receives the selective disclosure answer, it preserves encrypted personal information, together with COVID-19 digital certificates, in a secure off-chain IPFS storage (Benet, 2014). Only the IPFS hash (SHA-256 hash) is saved on-chain as a data pointer, ensuring that sensitive information is never disclosed to anyone scanning the Blockchain. Lastly, the hash of the encrypted information reflects the QR code "QR 4", which belongs to the holder.

It is worth noting that the "QR 2" code and the printed QR code, which is not digitally signed, may act as a fallback version, backup or rescue version in the event of a lost or stolen mobile phone or a specific desire of the verifier or holder, particularly during initial familiarisation with the digital COVID-19 credential.

Verification of COVID-19 certificates

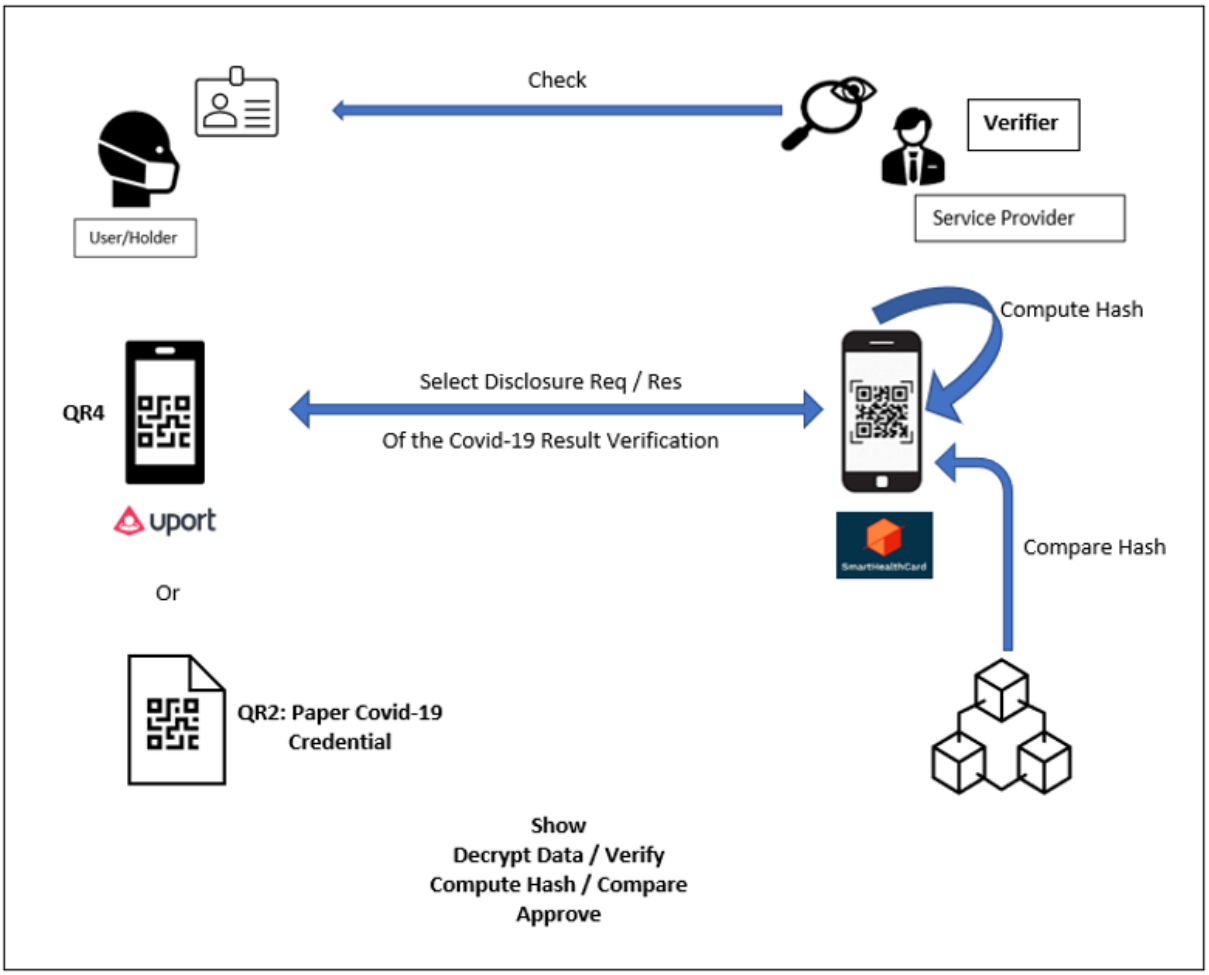

Figure 4. Certificate verification

http://doi.org/10.18080/jtde.v11n3.764

The process of verification of COVID-19 certificates is shown in Figure 4. The holder now possesses the counter-signed and signed COVID-19 vaccine/test certificates (QR 4) as well as a backup/rescue certificate (QR 2), that may offer the verifier with a provably legitimate or valid COVID-19 credential. To stop someone impersonating him or her, the holder must show not only the COVID-19 certificate, but also the evidence of identification. As a result, the holder/user must present the same valid physical ID that were used during the registration stage at the time of verification. The verifier must decode the holder data in order to validate COVID-19 credentials. He or she can then check the COVID-19 result, the physical ID number, the uPort DID and both signatures (holder and issuer).

The uPort process utilises the Box Public Key Authenticated Encryption Algorithm (Ecrypt, 2019) to decrypt holder/user data and offers an ERC-1098 cross-client method (Alabi, 2018) for requesting decryption/encryption, allowing the latest generation of decentralised apps to securely store users' private information in databases. In this technique, Ethereum key pairs must never be utilised directly for encryption; instead, the user must create a random ephemeral key pair for encryption and acquire an encryption key pair from the account's private key for decryption. To decrypt data, the verifier has to acknowledge the holder's secret key and acquire user approval.

Continuing the verification of COVID-19 certificates, the verifier computes the content hash ("QR4"), then matches it up to the hash recorded in the Blockchain, assuring permanence and data integrity. Lastly, the verifier can authenticate COVID-19 credential acceptance and broadcast it in a secure manner. In the end, the verifier/service provider may certify that COVID-19 credentials have been accepted and safely proclaim the user's admittance.

It is worth noting that different verifier institutions, such as hospitals, testing facilities, authorities and airline agents, can do the same operation. This would allow them to not just restrict access to public areas, but also to gain access to accurate data and create anonymised statistics. It would make it easier for the government to keep track of the population's health in real time.

http://doi.org/10.18080/jtde.v11n3.764

Architecture design

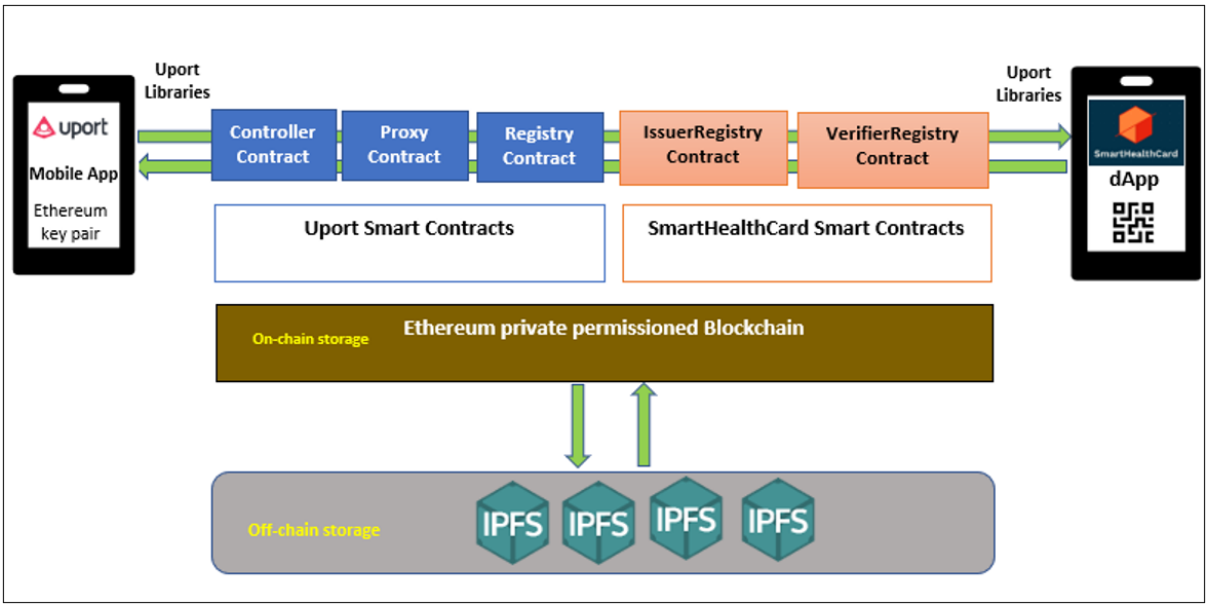

Figure 5. SmartHealthCard's architecture

Figure 5 shows the proposed SmartHealthCard platform architecture, which includes a uPort mobile app, uPort smart contracts, SmartHealthCard dApp and SmartHealthCard smart contracts. The SmartHealthCard system, in particular, uses uPort libraries and tools to build and control identities, as well as exchange and request certified information between them. The Decentralized Identifier (DID) specification is followed by uPort identities. Furthermore, a holder's personal information is encrypted and reserved off-chain in IPFS, with just the hash of the encrypted information being saved on-chain in the Ethereum private permissioned Blockchain, that will be used for confirmation process.

Verifiable credentials

The World Wide Web Consortium (W3C) developed the Verifiable Credentials (VC) standard to sort out digital certificates, authentications and claims in a safe and privacy-preserving way (W3C, 2022). The primary notions are built on the concept of Public Key Infrastructure (PKI). It is intended to standardise document format standards that make them machine-readable and communicative, as well as to generalise PKI, which is often expensive and centralised. The generalisation goes to a distributed or decentralised registry for cryptographic keys, often (not always) stored on a Blockchain since this enables each public key to have its own distinctive address, namely a Decentralized Identifier (DID).

http://doi.org/10.18080/jtde.v11n3.764

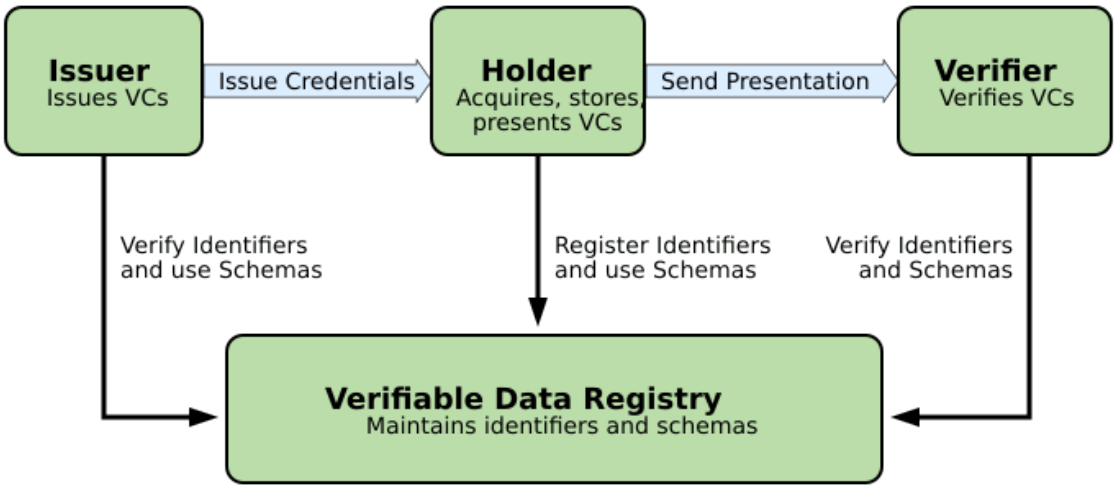

Figure 6. Information flow and responsibilities in Verifiable Credentials Model (adapted from W3C, 2022)

Figure 6 depicts the information flow and many responsibilities in the verifiable credential model (W3C, 2022). Through a verified data registry, the subject should establish globally unique IDs. The holder requests that the issuer create a VC by associating properties with identifiers. The topic of the VC they are preserving is generally, but not always, the holder. A parent, for example, may keep track of their children's VCs. The issuer checks the holder's identities and attributes, as well as its legal authority to hold the subject's VC, before issuing it. The issued VC must be kept by the holder. Finally, the holder may present the verifier with a provable appearance of his or her credentials. The issuer does not know the identities of the verifier in this model, which is a significant change from present identity management systems.

uPort

uPort is an Ethereum Blockchain-based user-centric information and self-sovereign identity platform. The uPort infrastructure consists of a self-sovereign wallet in a mobile app, a modern web application/decentralized application authentication mechanism and associated developer libraries. Figure 7 depicts the overall design and operation of the uPort identity handling system. For identity-related information, any app or user in uPort can communicate with an "Application Contract". This process has an impact on two primary contracts: 1) "Proxy Contract", which serves as an immutable and universal user identifier; 2) "Controller Contract", which manages identity access control logic. The app communicates with the "Proxy Contract" via the "Controller Contract", which transmits a request to the appropriate app. The "Proxy Contract" communicates with all application contracts on the Blockchain as a permanent identification and establishes a layer between application contracts and the user's private key (in the digital wallet).

http://doi.org/10.18080/jtde.v11n3.764

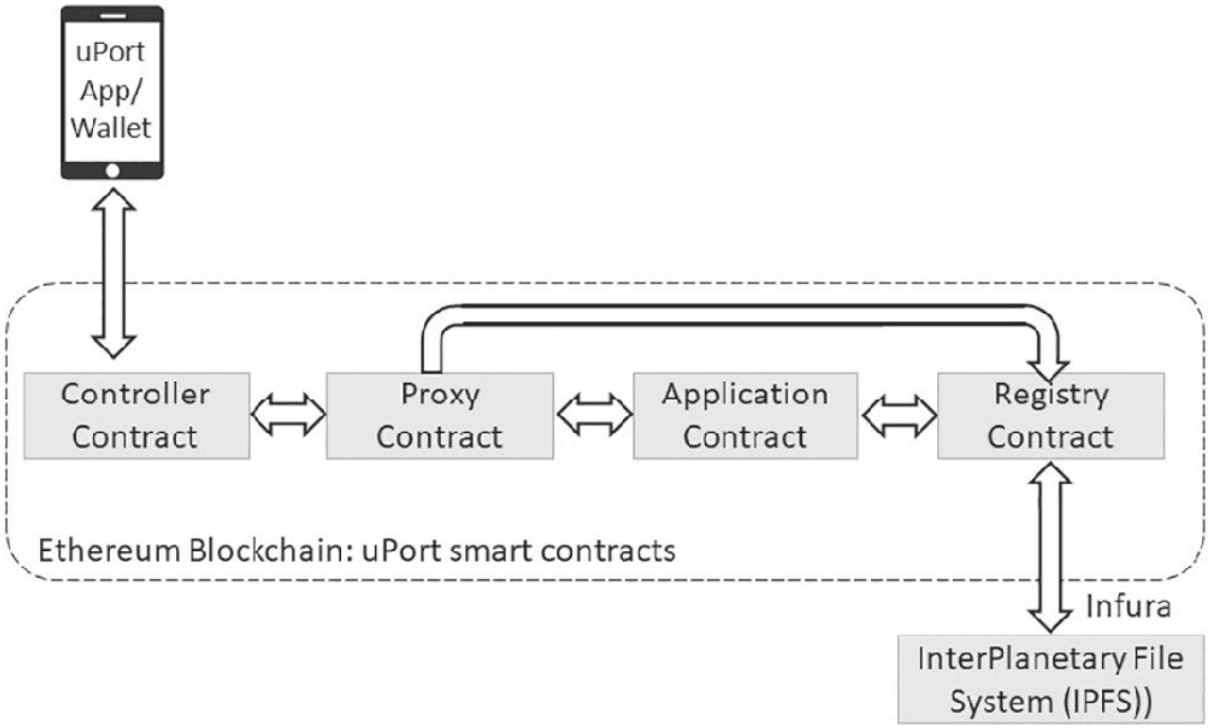

Figure 7. uPort Identity Handling System (adapted from Naik & Jenkins, 2020)

In order to do so, uPort makes use of Infura's standard RPC interface (2022), which provides an infrastructure for communicating with the Ethereum network. Furthermore, by submitting a transaction to the uPort Sensui server, which subsequently supplies appropriate Ether to pay the transaction fee, users can make a transaction without having any Ether in their wallet. Finally, data relating to uPort identification will be encrypted and reserved off-chain (which is on IPFS). This is accomplished by utilising a "Registry Contract" to create a cryptographic connection to an external data structure that can only be changed by the "Proxy Contract". To interact with the off-chain network, uPort requires the Infura interface.

It is worth noting that uPort is based on the W3C VC standard and includes additional methods to assist users to protect their personal information, for instance the notion of Selective Disclosure. Thus, the holder may choose whatever aspects of his or her VC to disclose with a verifier using this approach, while keeping the rest hidden. This is unquestionably a significant step forward in protecting users' rights to personal data privacy.

Implementation

SmartHealthCard dApp system components are shown in Figure 5. There are two forms of smart contracts, the smart contract for SmartHealthCard dApp and uPort Credential Mobile Wallet.

The registration procedure of the Issuer and Verifier is carried out on-chain to ensure transparency. However, only the Holder's data is encrypted and saved off-chain. Two smart contracts are created to accomplish this, the "IssuerRegistry" and the "VerifierRegistry"

http://doi.org/10.18080/jtde.v11n3.764

contract. The fundamental features of both contracts are built on events, which are used to alert authority listeners of what is happening. This also reduces on-chain costs and makes use of the Blockchain's immutable logs.

Furthermore, this research has created a modifier which guarantees that only the authorised Ethereum addresses are permitted to conduct the activities. The modifier is, in fact, a Solidity component that is applied to ensure that specific criteria are satisfied before performing a function. As a result, if access is refused, the function will not be triggered, and the Blockchain transaction that dealt with the call will be revoked.

As for uPort smart contracts, they contain a proxy, controller and registry contract. Proxy contract is the holders' permanent identity that is linked to their private key. This enables the holders to replace their private key without affecting their long-term identification. Controller contract is a component which restricts access to the proxy contract and enables the holders to restore their identity in the event that the holders' private key or mobile devices are lost. Registry contract is to establish a cryptographic connection between the holders' off-chain personal data and uPort identity.

SmartHealthCard dApp

We utilise uPort Credentials in SmartHealthCard to enable the generation and validation of identity data. This is an uPort library that facilitates secure communication between parties by enabling the activity of identity generation within the SmartHealthCard dApp and allowing data to be signed and verified. These bits of information, known as credentials, are presented as signed JSON Web Tokens (JWTs) (autho, 2013) and will be shown as QR codes. The uPort Transports library also helps to transport COVID-19 certificates between the SmartHealthCard dApp and the Holder through the uPort Credential Mobile Wallet app.

Obtaining SmartHealthCard dApp identity

To construct the SmartHealthCard server side using uPort-credentials, the first step is to create an application identity. As the identity is on the Ethereum blockchain, it complies with ERC-1056 protocol (Thorstensson, 2018). Hence, it is applicable to use it for signing requests.

It is important to remember that the private key should remain secret. It is just presented here for reference. This research uses sample application identities (e.g., private keys) to issue and verify credentials on a server. A sample of identity creation is shown in Figure 8.

http://doi.org/10.18080/jtde.v11n3.764

```
webpack 5.26.0 compiled with 8 warnings in 10429 ms
PS F:\Degree-3year-sem1\FYP\Report\Source Code\SmartHealthCard_Version2\dApp> node
Welcome to Node.js v16.13.2.
Type ".help" for more information.
> const { Credentials } = require('uport-credentials')
undefined
> Credentials.createIdentity()
{
  did: 'did:ethr:0x6cc3b48d3ac4d4bf04f8d52e69e9e0e8cc2c4de2',
  privateKey: '038d70d97f451cf33111fc36c319a575304c2f42a139b34aa17615f010efbfd8'
}
>
```

Figure 8. Obtaining SmartHealthCard dApp identity

Access to SmartHealthCard dApp

To access the app, the identification data is sought, and the sharing of the required information is approved by a uPort client, which acts for the Ethereum identity. This is known as a selective disclosure request. After the provided data has satisfied the SmartHealthCard server-side business logic, the holder will be regarded as authorised to use the validated certificates that he or she has agreed to share.

The SmartHealthCard server-side login service, which employs uPort for verification, consists of the following components:

- The production of a disclosure request message in the form of a JWT, which will be ingested by the mobile app and shown as a QR code;
- To return selective disclosure responses, which is named a callback server.

Generating and issuing COVID-19 certificates

An authorised healthcare practitioner should complete the generation and issuance of COVID-19 certificates. Holders will be able to construct their digital identities and offer actual values to the SmartHealthCard dApp by attesting facts about them. Furthermore, they may have a frictionless “evidence of being a person” validation across the decentralised web. In providing a certificate to a holder, the SmartHealthCard dApp will cryptographically sign a claim for that holder, so attesting to the veracity of a piece of information about the holder. Anybody with access to the DID of the SmartHealthCard application may then verify that a given identification certificate came from the SmartHealthCard dApp. For example, during onboarding, the SmartHealthCard dApp asks for and confirms a holder’s complete name, country, phone number or physical ID number, after which the user can acquire a COVID-19 outcome certificate.

Issuing a certificate at a high level entails, on behalf of the SmartHealthCard application, cryptographically signing user data; and holders can get their COVID-19 certificate as a JWT by scanning an issuing a QR code or receiving a push message.

http://doi.org/10.18080/jtde.v11n3.764

Requesting COVID-19 certificates

The uPort Credentials process is used to request COVID-19 certificates from the SmartHealthCard dApp. An authorised service provider should complete this activity. Requesting COVID-19 certificates follows the exact steps as submitting a disclosure request. Requesting a verification entails, at a high level, on behalf of the SmartHealthCard dApp, cryptographically signing a request to expose the holder's information and send a JWT request to the holder using a verification QR code or a push notification.

COVID-19 certificate request encryption and decryption

The uPort process employs the ERC 1098 encryption mechanism (Alabi, 2018) that employs an ephemeral transmitting key and box method tweet-nacl (Ecrypt, 2019) approach. It enables the Verifier to decrypt the message without first resolving the holder's public key.

The Holder should use this encryption technique:

1) Make the signed JWT payload as usual;
2) JWT is padded to the nearest multiple of 64 bytes using \os;
3) Using nacl.box.keyPair(), make an ephemeral keypair;
4) Using nacl.randomBytes(nacl.box.nonceLength), generate a random nonce of 24 bytes;
5) Use nacl.box(ephemeralKeyPair.secretKey, recipient publicKey, nonce, message) to encrypt the resultant JWT;

In a JSON payload, combine the base64 encoded versions of the ciphertext values, ephemPublicKey and nonce as well as the version of x25519-xsalsa20-poly1305; the Verifier needs to recognise the Holder's secretKey and needs to apply the following technique to decrypt the request:

1) Verify if the version field contains the string x25519-xsalsa20-poly1305 to proceed;
2) Decode the base64 encoded ciphertext attributes, ephemPublicKey and nonce;
3) use nacl.box.open(receiverEncryptionPrivateKey, ephemPublicKey, nonce, ciphertext) to decrypt the message;
4) Remove any trailing \os in the payload;
5) Decode JWT in the usual way.

Screen Interfaces

Screen interfaces of the issuing and verification process done by the issuer and verifier through the SmartHealthCard dApp, which supports the self-sovereign uPort Credential Mobile Wallet app on user's smartphone, are shown in this section (Figures 9–14). Subsequently, the COVID-19 credential verification process by the healthcare provider/issuer at the hospital is shown in

http://doi.org/10.18080/jtde.v11n3.764

Figures 15–18. Figure 19 shows the COVID-19 credential verification process by the service provider/verifier at the airport when the result is invalid (expired) due to exceeding the valid time (which is only four minutes).

Figure 9. Homepage

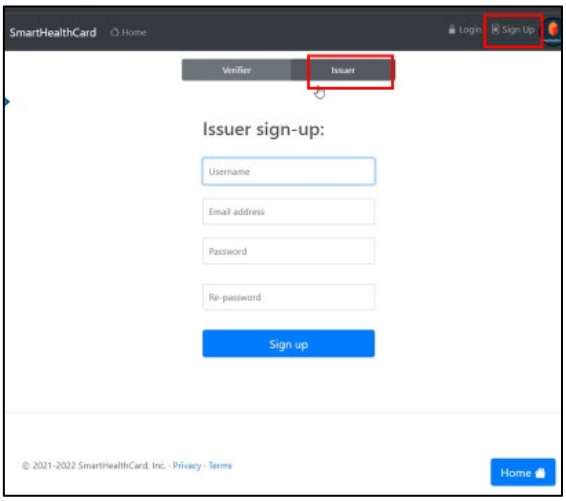

Figure 10. Issuer and verifier sign-up page

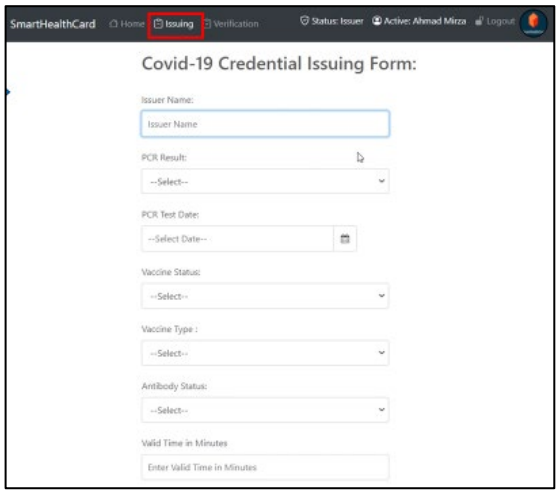

Figure 11. Credential creation

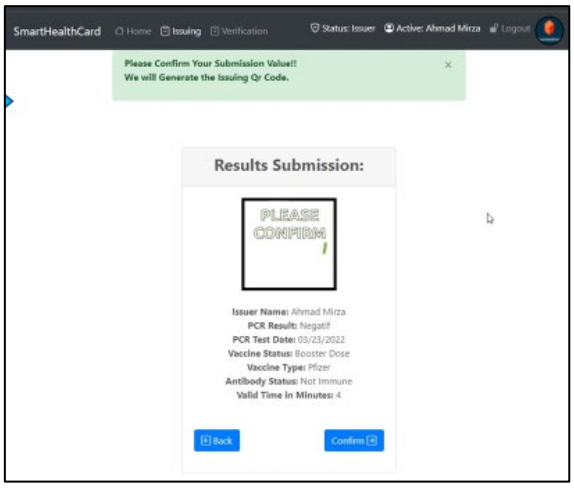

Figure 12. Credential confirmation

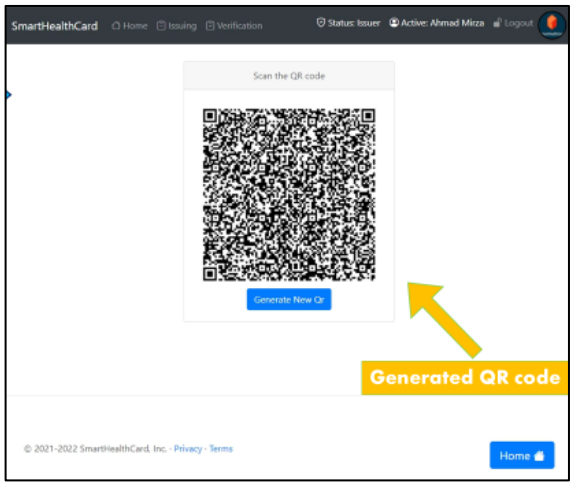

Figure 13. User scans the issuing QR code

http://doi.org/10.18080/jtde.v11n3.764

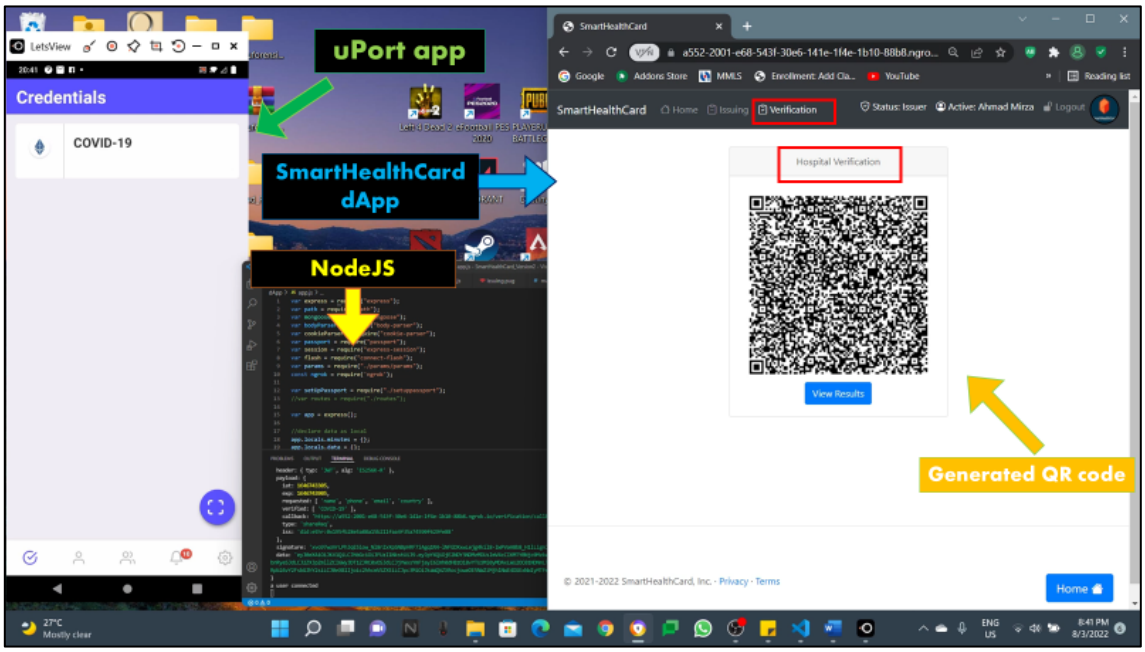

Figure 14. Credential is stored in uPort mobile wallet

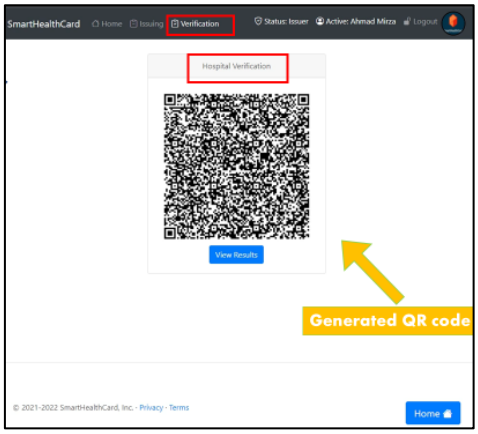

Figure 15. Hospital verification QR code page generated by the issuer

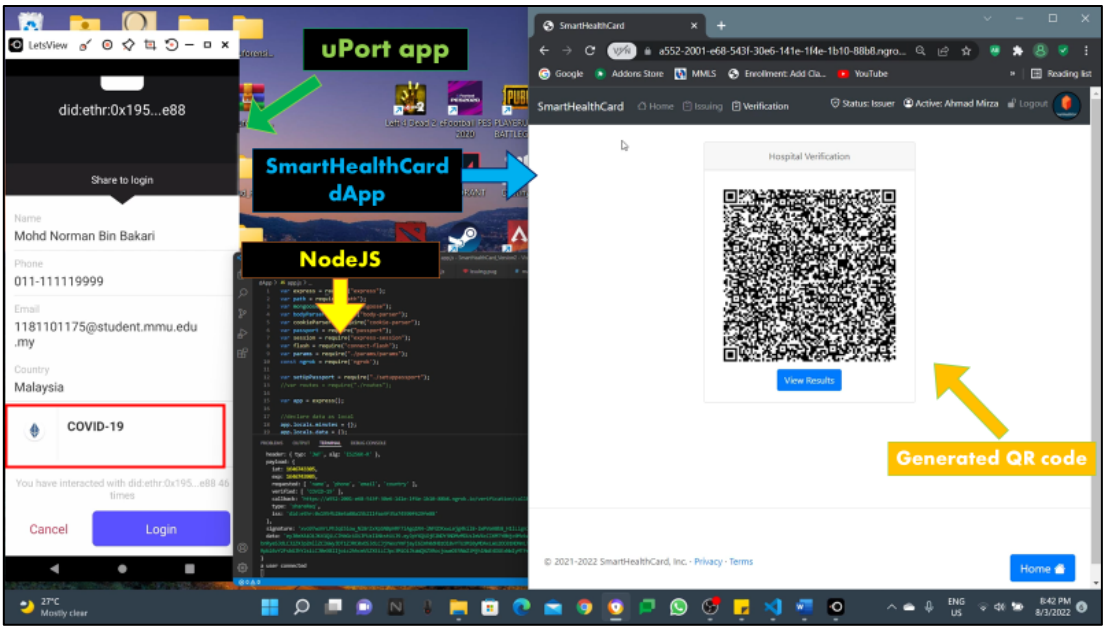

Figure 16. User scans the hospital verification QR code

http://doi.org/10.18080/jtde.v11n3.764

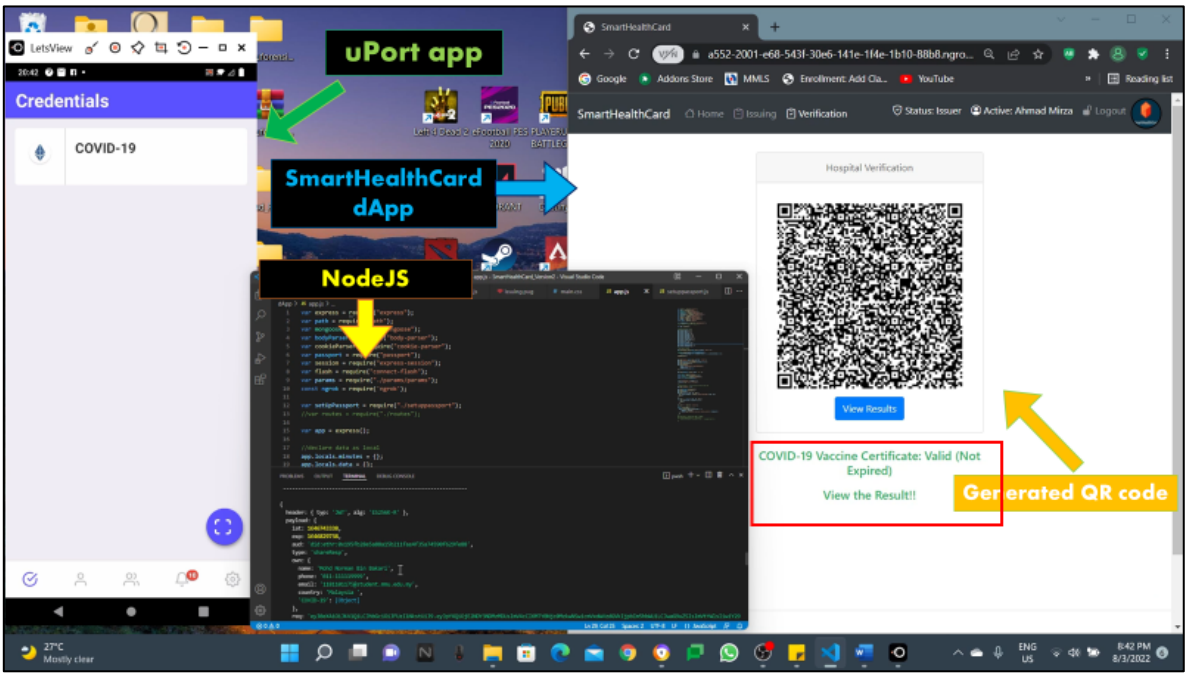

Figure 17. The credential is verified and valid

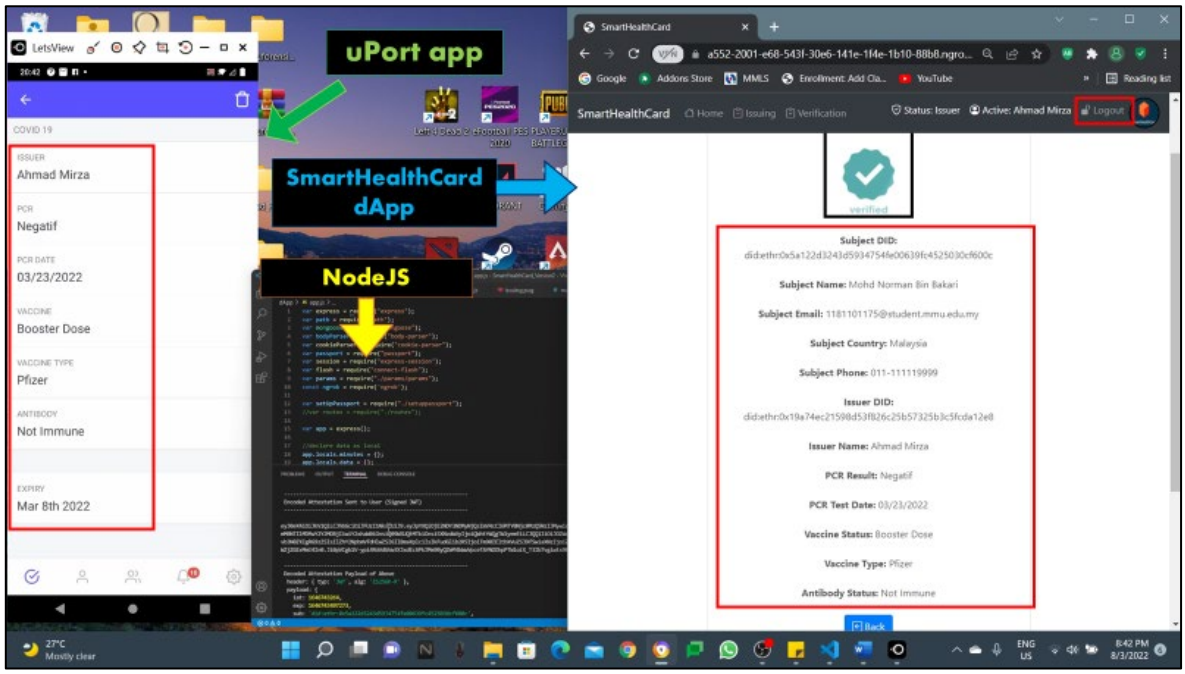

Figure 18. Issuer views the verified credential

Conclusion

When the COVID-19 pandemic illness spread at an unprecedented rate throughout the world in 2021, both major and small economic sectors experienced the effects of government-imposed limitations and regulations, such as social distancing and movement control orders. The tourism industry was one of the most affected economic sectors. As vaccines become more widely available, each government has been working to develop a system that can generate a digital vaccine certificate and PCR lab test result to verify that a person is fully vaccinated or

http://doi.org/10.18080/jtde.v11n3.764

has a negative PCR test result, in order to allow them to enter business premises, travel, cross state borders, and a variety of other activities. Each country will be able to reclaim its business activities, which have been harmed for several years. However, the use of centralised systems in the development of the digital COVID-19 pass system results in a number of issues and limitations, including the system's high sensitivity to failures, slow and inefficient information exchange, and vulnerability in data security and privacy protection for users.

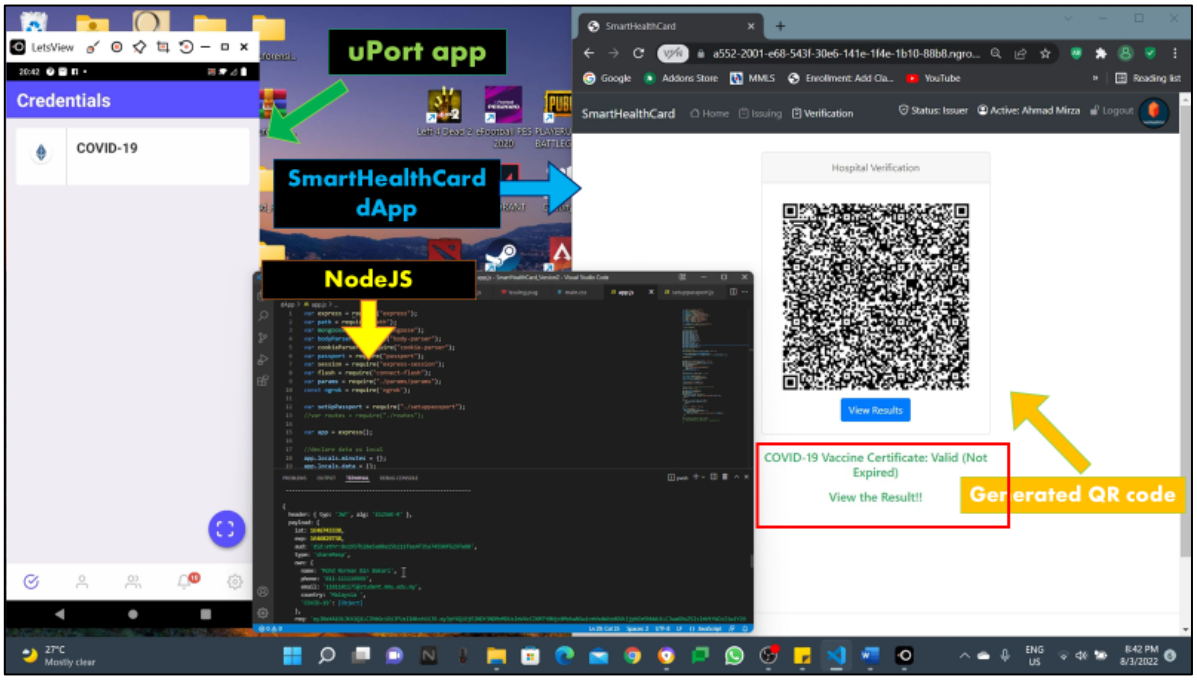

Figure 19. The credential is verified by the verifier and invalid (expired)

As a result, the goal of this research is to offer a new digital COVID-19 pass that uses the "SmartHealthCard" blockchain-based system solution. SmartHealthCard is a decentralised application (dApp) that replaces the old, centralised approach by encrypting and hashing user data and safely storing it in a distributed database. Privacy preservation, GDPR compliance, self-sovereignty, KYC compliance, and data integrity are additional characteristics of SmartHealthCard. This initiative has the potential to benefit the user, healthcare professional, service provider, and the government. The suggested platform enables quick validation of tamper-proof COVID-19 tests/vaccinations, aiding in COVID-19 transmission control while respecting the user's right to privacy.

In principle, a secure COVID-19 credential would serve as evidence that someone has been vaccinated against COVID-19, recovered from COVID-19 or tested negative in a COVID-19 PCR test. Thus, this facilitates safe, unrestricted travel while also removing a person from most government controls. Lastly, this secure COVID-19 certificate may aid public authorities in limiting access to vital or sensitive institutions, such as airports, schools, hospitals, and other public places.

http://doi.org/10.18080/jtde.v11n3.764

Acknowledgement

A version of this paper was presented at the third International Conference on Computer, Information Technology and Intelligent Computing, CITIC 2023, held in Malaysia, 26–28 July 2023.

References

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2020). How blockchain helps to combat trust crisis in COVID-19 pandemic? *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 764–765. https://doi.org/10.1145/3384419.3430605

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Journal of Software: Practice and Experience*, *54*(4), 841–867. https://doi.org/10.1002/spe.2983

Alabi, T. (2018). Add web3.eth.encrypt and web3.eth.decrypt functions to JSON-RPC. *Ethereum/EIPs #1098*. Retrieved from https://github.com/ethereum/EIPs/pull/1098

auth0. (2013). JSON Web Tokens. Retrieved from https://jwt.io/

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. *Computer Science: Networking and Internet Architecture*, ArXiv. https://doi.org/10.48550/arXiv.1407.3561

Braendgaard, P. (2018). Next Generation uPort Identity App released. Retrieved from https://medium.com/uport/next-generation-uport-identity-app-released-59bbc32a83a0

CovidPass. (2020). Balancing Public Safety & Re-Opening Borders to Travellers. Retrieved from https://www.covid-pass.tech/

Ecrypt. (2019). Public-key authenticated encryption: crypto_*box*. *NaCl: Networking and Cryptography library*. Retrieved from http://nacl.cr.yp.to/box.html

HandyVisas. (2020). CommonPass Health App to Facilitate Travel in 2021. Retrieved from https://www.handyvisas.com/news/commonpass-travel-health-app/

IBM Digital Health Pass. (2021). IBM Watson Health is now Merative. Retrieved from https://www.ibm.com/my-en/products/digital-health-pass/individuals

ICC United Kingdom. (2021). ICC AOKpass — General Overview. Retrieved from https://iccwbo.uk/products/icc-aokpass-general-overview

Infura (2022). "Every Blockchain Journey Begins with a Single Step". Retrieved from https://infura.io/

Naik, N., & Jenkins, P. (2020). uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain. *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 1–7. https://doi.org/10.1109/isse49799.2020.9272223

Pavli, A., & Maltezou, H. C. (2021). COVID-19 Vaccine Passport for Safe Resumption of Travel. *Journal of Travel Medicine*, *28*(4). https://doi.org/10.1093/jtm/taab079

Škare, M., Soriano, D. R., & Porada-Rochoń, M. (2021). Impact of COVID-19 on the Travel and Tourism Industry. *Technological Forecasting and Social Change*, *163*, 120469. https://doi.org/10.1016/j.techfore.2020.120469

Thorstensson, J. (2018). ERC: Lightweight Identity. *Ethereum/EIPs #1056*. Retrieved from https://github.com/ethereum/EIPs/issues/1056

W3C. (2022). Verifiable Credentials Data Model 1.0. Retrieved from https://www.w3.org/TR/vc-data-model/