Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2427896, 12 pages
https://doi.org/10.1155/2021/2427896

Research Article

Sharing Pandemic Vaccination Certificates through Blockchain: Case Study and Performance Evaluation

José L. Hernández-Ramos, Georgios Karopoulos, Dimitris Geneiatakis, Tania Martin, Georgios Kambourakis, and Igor Nai Fovino

European Commission, Joint Research Centre, Ispra 21027, Italy

Correspondence should be addressed to José L. Hernández-Ramos; jose-luis.hernandez-ramos@ec.europa.eu

Received 3 June 2021; Accepted 2 August 2021; Published 26 August 2021

Academic Editor: Wenjuan Li

During 2021, different worldwide initiatives have been established for the development of digital vaccination certificates to alleviate the restrictions associated with the COVID-19 pandemic to vaccinated individuals. Although diverse technologies can be considered for the deployment of such certificates, the use of blockchain has been suggested as a promising approach due to its decentralization and transparency features. However, the proposed solutions often lack realistic experimental evaluation that could help to determine possible practical challenges for the deployment of a blockchain platform for this purpose. To fill this gap, this work introduces a scalable, blockchain-based platform for the secure sharing of COVID-19 or other disease vaccination certificates. As an indicative use case, we emulate a large-scale deployment by considering the countries of the European Union. The platform is evaluated through extensive experiments measuring computing resource usage, network response time, and bandwidth. Based on the results, the proposed scheme shows satisfactory performance across all major evaluation criteria, suggesting that it can set the pace for real implementations. Vis-à-vis the related work, the proposed platform is novel, especially through the prism of a large-scale, full-fledged implementation and its assessment.

1. Introduction

The World Health Organization (WHO) declared COVID-19 a pandemic on March 11th, 2020. This disease is caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) which was initially detected at the end of 2019 in the city of Wuhan, China [1]. Since then, the disease has spread unhindered worldwide. Besides the obvious health consequences, the socioeconomic impact is already notable in many countries globally. Indeed, the drastic—and sometimes controversial—measures to curb the spread, including social distancing and curfew, have already changed our daily behavior. Furthermore, recent economic analysis [2] predicts that many countries will not recover their economic levels of 2019 until 2022. These forecasts may vary based on the evolution of the pandemic during 2021.

To defend against the COVID-19 pandemic, several initiatives and actions have been hitherto undertaken, including rapid diagnosis and isolation of infected people, as well as the creation of digital contact tracing frameworks [3, 4]. However, the second COVID-19 wave during the fall of 2020 and the successive outbreaks during 2021 showed that these measures are insufficient, especially when they are abruptly relaxed. Therefore, the sheer objective has been the development of effective and safe vaccines to be rolled out globally. Indeed, numerous efforts were initiated during 2020 involving medical institutions, pharmaceutical companies, and research centers worldwide to get a vaccine at unprecedented speed. At the end of May 2021 [5], there were 101 and 184 vaccines in clinical and preclinical development, respectively.

While the realisation of vaccines represents currently the main objective to terminate the pandemic, their manufacturing, distribution, and deployment are also associated with important challenges. First, logistics, storage, and transport requirements, say, regarding the temperature of

preservation, impose strong pressure on the supply chain to ensure global access to vaccines in a timely manner [6, 7]. Therefore, data transparency is the key to foster a secure monitoring of the epidemiological and vaccination situation in a certain region. Second, the vaccination process is being prioritised for certain population groups according to different aspects, such as age, health condition, and profession. Furthermore, the rate of vaccinations varies depending on the country [8]. Hence, immune and vulnerable people will live together during a certain period of time. Such a situation could be prolonged in case the virus that causes COVID-19 becomes endemic [9]. In this context, the use of digital vaccination certificates could help alleviate the burden on health systems, as vaccinated people would not need to perform viral tests, which are currently required to, say, travel to different countries. Unlike the current paper version of vaccination certificates, namely, the International Certificate of Vaccination or Prophylaxis (ICVP), these digital documents would allow a far more scalable solution along with a faster and more secure verification process [10].

Blockchain technology has been already identified as a promising approach to combat the pandemic in distinct scenarios, such as early detection of outbreaks, medical supply chain, or donation tracking [11, 12]. In the same mindset, the creation of a blockchain platform to share information about the pandemic would increase transparency, interoperability, and accountability, so that potential discrepancies among data from different sources, say, medical centers or governments, could be avoided. This would foster a more trustworthy reporting and monitoring of the pandemic evolution considering diverse territories and countries. Furthermore, such a platform would increase citizens' trust in the vaccination process, as the information related to vaccines could be publicly available [13].

The work at hand analyses the key requirements to build a scalable platform for sharing vaccination data and the advantages of blockchain for the realisation of such a platform. We focus on the scenario of vaccination certificates that can be generated after a citizen is vaccinated and how blockchain could aid in maintaining such information towards enabling a secure and privacy-aware verification process. Furthermore, unlike existing approaches that do not offer experimental results or consider small-scale deployment scenarios [14–17], we provide a comprehensive performance evaluation of the proposed platform by considering the vaccination of the EU population and 27 blockchain nodes, representing each member state (MS) in the EU. We meticulously assess our platform under different realistic network conditions, including latency and bandwidth, in an emulated infrastructure. To our knowledge, this is the first work to offer an estimation of the performance requirements associated with a blockchain-based platform for vaccination data in a large scale. Furthermore, we discuss practical aspects and security considerations for a large-scale deployment of the intended platform, along with potential regulatory implications of vaccination certificates.

The structure of this paper is as follows: the next section describes other works using blockchain technology for COVID-19-related certificates. Section 3 elaborates on the needs for sharing COVID-19 information, as well as the advantages provided by blockchain for this purpose. Furthermore, Section 4 provides insights into the definition of digital vaccination certificates. The proposed blockchain platform for the registration and validation of digital vaccination certificates is described in Section 5. The results derived from the platform's evaluation are described in Section 6. Finally, Section 7 concludes our work with an outlook of potential future research directions.

2. Related Work

Since the beginning of the COVID-19 pandemic, different initiatives have been proposed for the implementation of COVID-19 certificates, so that individuals granted with such credentials could be exempt from physical restrictions to carry out certain activities in their daily life [18]. Indeed, based on our analysis of existing literature, three different types of COVID-19-related certificates can be identified: (a) *vaccination certificates*, referring to whether a person has received the vaccine or not; (b) *diagnostic test certificates*, demonstrating that a person has undergone a test; and (c) *immunity certificates* or *immunity passports*, implying that a person has developed antibodies after being infected. As shown in Table 1, some proposals support more than one type of certificates, while only a few of them provide an actual implementation, although in a small scale.

In the case of vaccination certificates, the authors of [19] focus on privacy aspects and propose a hashing algorithm that enables users to store the information on the blockchain anonymously using an ID that is created from their iris. In this case, the vaccination certificate data and a hash of the user ID are stored on the blockchain. This could imply a potential issue since it would demand a very high storage requirements of the blockchain nodes. This could be exacerbated in the case of populous or multiple countries using the same blockchain.

Furthermore, other works address several kinds of certificates. In particular, both vaccination and immunity certificates are considered by [15], which is based on Verifiable Credentials (VC) [22] as digital IDs, the decentralised data storage platform *Solid* [23], and a consortium Ethereum-based blockchain [24]. In a similar direction, [16] uses Ethereum smart contracts, Self-Sovereign Identity (SSI), and InterPlanetary File System (IPFS) to store medical tests and travel history in a decentralised manner. In addition, [14] addresses all the different types of certificates by integrating the use of VCs in a blockchain implementation called *uPort* [25], which provides SSI aspects on top of the Ethereum platform.

The authors of [20] introduce the concept of digital health passports, which is similar to the diagnostic test results required for travelers in certain cases. It is based on a private blockchain using the proof-of-authority consensus mechanism, where the test results are registered and stored.

For immunity certificates, the work of [17] presents SecureABC, a privacy-oriented protocol based on public key cryptography. This proposal does not use blockchain, and the certificates can be either paper- or app-based. As a

Table 1: Related work on COVID-19 certificates.

Scheme	Vaccination	Diagnostic test	Immunity	Blockchain	Benchmarks
[19]	✓			✓	—
[15]	✓		✓	✓	Small scale
[16]	✓		✓	✓	Small scale
[14]	✓	✓	✓	✓	Small scale
[20]		✓		✓	—
[17]			✓		Small scale
[21]			✓	✓	—
[10]		✓	✓		—

consequence, if the paper certificate or the mobile device is lost, so are the respective certificates. In [21], the concept of COVID-19 immunity certificates is based on a government-run blockchain, in which the information related to testing facilities and hospitals is also included. Furthermore, [10] proposed the use of VCs and Decentralized Identifiers (DID) [26] to link individuals' identity with their certificates. However, further details about implementation/-deployment aspects are not given.

In spite of recent efforts, only a few of these works present technical details or proof-of-concept implementation including evaluation results. For instance, they rather provide simple short high-level descriptions of the proposed solutions, or unconvincing benchmarks, limited to a small number of simultaneous requests, thus being far from real-world deployment scenarios. In contrast, our work tackles this problem through a comprehensive evaluation of a benchmark that includes 27 blockchain nodes (one node for each EU country) by considering different aspects, such as computing resource usage, network response time, and bandwidth. As highlighted by [12], even if the potential of blockchain to combat the COVID-19 pandemic has been reported by several works, there is a lack of studies related to latency and scalability aspects, which are key aspects for the deployment of this technology. Furthermore, our work concentrates on vaccination certificates, influenced by the views of WHO on immunity passports: "...there is not enough evidence about the effectiveness of antibody-mediated immunity to guarantee the accuracy of an 'immunity passport'." Another aspect driving us to this direction is that vaccination certificates will incite people to get vaccinated, while immunity certificates could motivate individuals get infected for possessing the necessary antibodies.

3. Managing COVID-19 Information through Blockchain

The global deployment of COVID-19 vaccines sets out unprecedented challenges to be addressed in the period ahead, including an efficient supply chain and effective monitoring of vaccination coverage in a certain region. Indeed, in the case of two-shot vaccines, more than 15 billion vaccines would be required to be distributed and deployed worldwide. Furthermore, the distribution of additional shots could be required depending on the immunity period provided by a certain vaccine or in case the virus that causes COVID-19 becomes endemic [9]. In this context, the WHO established the *COVAX* program together with *Gavi* and the Coalition for Epidemic Preparedness Innovations to facilitate equitable access and distribution of future vaccines, while those people most at risk are prioritized. COVAX is part of the global ACT Accelerator initiative that is designed to enhance the resources for COVID-19 tests, treatments, and vaccines.

At the European level, the commission published in Oct. 2020 a document on COVID-19 vaccination strategies and vaccine deployment for the 27 MS [27]. This document established the need to define a common strategy for the vaccination process, promoting coordination and collaboration among EU countries. One of the main goals of this strategy is to increase the acceptance of COVID-19 vaccines. Actually, recent studies reveal that a significant part of the population would not be willing to be vaccinated against the COVID-19 disease [13]. To address this issue, there is a need for an effective, consistent, and transparent communication of information related to COVID-19 vaccines and the vaccination process itself. As described in [27], the sharing of pandemic-related information among MS would cater for a better monitoring of the different vaccines under development, including data on possible side effects, which would be made readily available to the relevant authorities. Furthermore, this information could include data on the transport and distribution of vaccines to enable real-time monitoring and improve the supply chain process by considering the specific needs of each vaccine.

Moreover, vaccination campaigns have been carried out by considering different aspects (e.g., age or medical condition) established by organisations such as the WHO's Strategic Advisory Group of Experts on Immunization to prioritize the vaccination for certain groups of people. Therefore, currently a large part of the population is still vulnerable to the COVID-19. This situation is especially exacerbated in developing countries [8]. Furthermore, depending on the immunity period of each vaccine, the immunity of a certain person could come to an end at a certain point in time. Beyond the information on vaccines, the easy sharing of these vaccination data would improve the monitoring of the epidemiological situation of a territory and the vaccination coverage among different population groups. In fact, monitoring these aspects can make the vaccination strategy more flexible to be adapted in a certain region or country [27].

For the realisation of this COVID-19 data sharing platform, blockchain technology has been postulated in different related scenarios, including contact tracing and outbreaks, where information sharing is essential [28]. Blockchain is based on a distributed ledger that is shared by a set of entities. The ledger contains a list of immutable transactions that are validated by the participating entities through a consensus mechanism. Furthermore, a blockchain can be permissionless (any entity can participate) or permissioned (participation is limited to a set of entities). The development of a blockchain-based platform offers a high degree of transparency and accountability, fostering a trustworthy environment for the sharing of COVID-19 data.

Thus far, the use of blockchain to fight against the COVID-19 pandemic has been proposed for several use cases, including the distribution and delivery of vaccines, recording of patients' data, preventing fake news, registration of testing and reporting, and the distribution of medicines and healthcare equipment [11, 28–31]. While a blockchain platform for sharing pandemic data could help in distinct scenarios, we focus on the registration and verification process of the data associated with a vaccinated citizen. The envisioned platform will enable a trusted ecosystem to track the deployment of vaccines in a certain region and consider priority groups. That is, blockchain inherently supports decentralisation and data replication (data from all countries are replicated to all other countries), deterring issuance of fraudulent vaccination certificates as well. For this purpose, we examine the concept of digital vaccination certificates that could be demonstrated by citizens to carry out certain activities without the need of diagnostic tests. The following sections describe the design and architecture of a blockchain platform for digital vaccination certificates, as well as a thorough evaluation where each MS is represented by a blockchain node.

4. Digital Vaccination Certificates

Digital vaccination certificates can be viewed as a digital version of the ICVP certificates created by WHO that show a person's vaccines and the date they were received. For the representation of such a certificate, there is a need to identify which specific information should be included, so that they can be used across the world. Such certificates should be interoperable globally, as well as supported by identity management techniques to unequivocally link the vaccination of citizens with their identity; in this way, the resulting certificate will be verifiable, scalable, and privacy-preserving.

The European Commission proposed a Digital Green Certificate in March 2021 [32] to facilitate safe and free movement inside the EU during the COVID-19 pandemic. Furthermore, the eHealth Network, which provides a platform of EU MSs' competent authorities dealing with eHealth, has recently described a set of guidelines on verifiable vaccination certificates, including trust and interoperability aspects. Precisely, [33] identifies a minimum dataset with the essential pieces of information to be embedded in the certificate, including person identification (e.g., citizen ID), vaccination information (e.g., vaccine manufacturer), and certificate metadata, such as issuer and validity period.

Other worldwide initiatives have been established for the development of digital vaccination certificates. In particular, the WHO Smart Vaccination Certificate Working Group [34] is intended to define standard specifications for digital vaccination certificates based on an architecture linking national and crossborder digital systems. Furthermore, the IATA Travel Pass Initiative [35] provides a mobile app to be used by travelers to store and manage their verified certifications for COVID-19 tests or vaccines. Another relevant effort is represented by the *Certify.health* initiative [36], which concentrates on the development of a privacy-by-design COVID-19 status certificate that will be extended into vaccination certificates.

For the representation of digital vaccination certificates, several formats could be considered. For example, [33] mentions QR codes and Verifiable Credentials (VC), which have been also considered by recent research proposals, as described in Section 2. The use of VC (together with DIDs) is intended to realize the vision of Self-Sovereign Identity (SSI), which has emerged as a decentralised alternative to traditional centralised identity management (IdM) systems. A VC represents a digital version of a paper certificate in which a certain entity (issuer) asserts certain information (claims) about a subject in a way that can be verified by other entities (verifiers). A VC is usually employed together with a DID, which is an identifier under the control of a DID subject that indicates a DID method and a specific identifier of such method. DIDs are registered in a Verifiable Data Registry (VDR), such as blockchain, and are intended to foster a decentralised authentication process.

It should be noted that the use of VCs in the context of the COVID-19 crisis has been fostered by the COVID-19 Credentials Initiative [37], which groups around 100 organisations to support efforts of using VCs to mitigate the spread of the virus.

While it is not the focus of our work, Figure 1 shows an example of VC that includes certain claims based on ongoing discussions about the use of VCs for vaccination certificates. In our example, we have considered that the validity of the certificate is associated with the period during which this vaccination is effective, taking into account that two shots are required. In particular, the *context* establishes a common language for referring to the attributes and values contained in the VC. Also, for our example shown in the figure, the URI https://covid-19-vaccination-certificate.org/v1 indicates that the communication is about vaccination certificates. Furthermore, the *id* and *type* fields are used to identify the VC and indicate its type. Moreover, the *issuer* represents the entity that issued the VC and it makes reference to the medical center, which provided the vaccine. In this case, it is described through a DID that could be included in the blockchain, so that verifiers can use this information to validate the VC. This field can also indicate the type and name of the issuer, as well as its URL for more information. Besides, the *issuanceDate* and *expirationDate* indicate the validity of the certificate that is associated with the immunity period provided by the vaccine. Also, the *CredentialSubject* represents the entity on which the claims are made, i.e., the

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://covid-19-vaccination-certificate.org/v1"
    ],
    "id":"https://covid-19-vaccination-certificate.org/
            credentials/JohnDoe",
    "type": [
        "VerifiableCredential",
        "VaccinationCertificate"
    ],
    "issuer": {
        "id":"did:web:vc.brussels.vaccination.centre",
        "location": {
            "type":" MedicalCenter",
            "name":" BrusselsVaccinationCentre",
            "url":" https://brussels-vaccination-centre.org/"
        }
    },
    "issuanceDate":" 2020-01-31T14:30:23",
    "expirationDate":" 2020-07-31T14:30:23",
    "name":" VaccinationCertificate",
    "description":" Electronicdocumentcertifyingthatthesubject
                        fulfilledtheCOVID-19vaccinationprocedure.",
    "credentialSubject": {
        "id":" did: key: subject_key_value",
        "type":" VaccinationCertificateSubject",
        "givenName":" John",
        "familyName":" Doe",
        "birthDate":" 1979-05-28",
        "image":"  image_value",
    },
   "injection":{
        "id":"    injection_id  ",
        "type":" VaccinationCertificateInjection",
        "name":"    vaccine_name    ",
        "issuanceDate":" 2020-01-10T11:15:46",
    },
     "proof": {
        "type":" Ed25519Signature2018",
        "created":" 2020-01-31T14:30:23",
        "jws":"    JSON_Web_signature_value  ",
        "proofPurpose":" assertionMethod",
        "verificationMethod":" did:web:vc.brussels.vaccination.
                                centre #  additional_id_value"
  }
}
```

Figure 1: Example of a potential vaccination certificate based on VCs [22].

individual getting vaccinated, that includes the personal data about the user. In addition, the claim *injection* is used to describe which specific injection is being provided, including the vaccine and vaccination date. This information could be used to track the vaccines and injections being provided and may help with the management of the supply chain. Finally, the field *proof* makes reference to the cryptographic technique (typically a digital signature) that is used by the issuer to make the VC tamper-resistant.

While the design of an interoperable approach for the definition of digital vaccination certificates is still under discussion, in our approach, only a hash digest of such a credential will be stored in the blockchain platform. In this way, the proposed platform will be agnostic both of the vaccination certificate presentation format and of the data format being considered. The details of such a platform are described in the subsequent section.

5. Vaccination Certificate Scenario

For the development of the proposed blockchain platform, we consider the architecture in Figure 2. Naturally, the

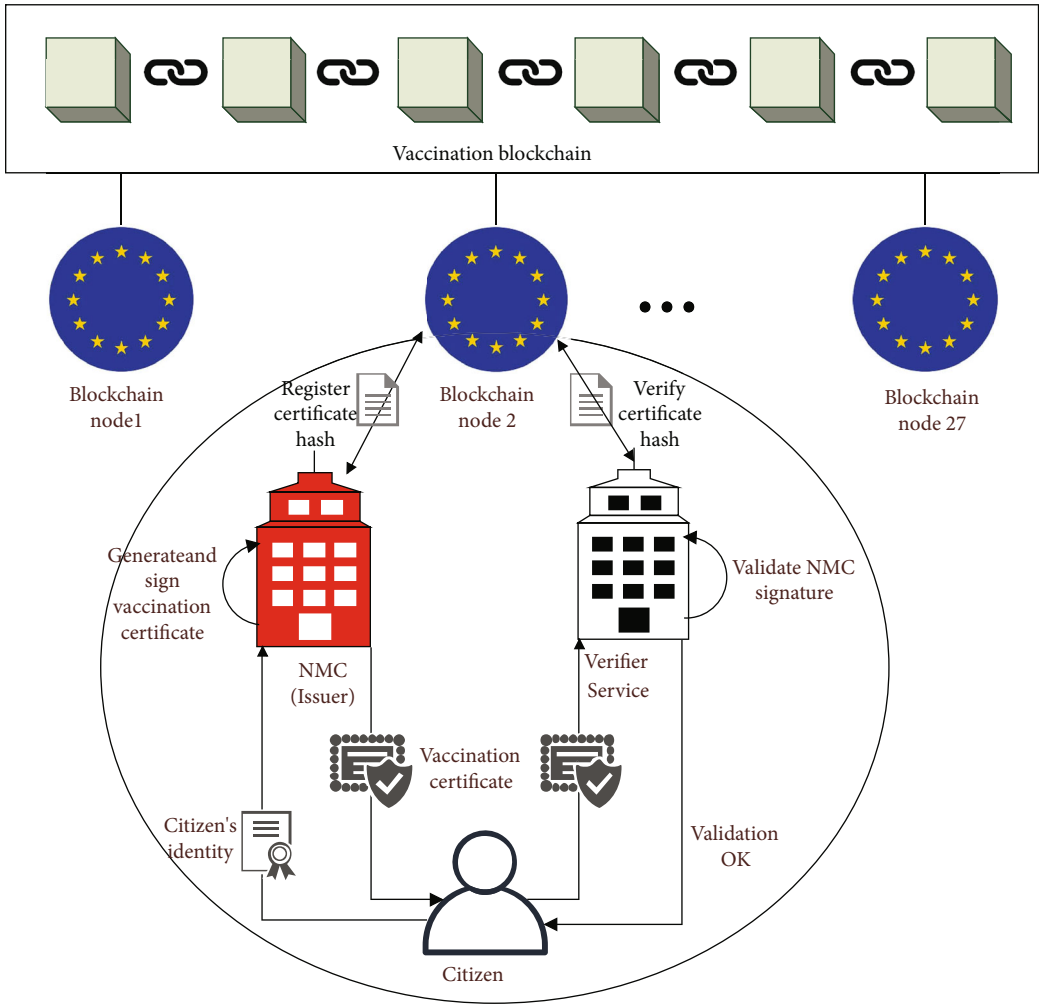

Figure 2: Overview of the proposed blockchain-based vaccination certificate platform.

depicted architecture does not reflect the reality of any decision made at the EU level, but it solely serves as a proof of concept for evaluation purposes. The architecture includes the vaccination permissioned blockchain where blockchain nodes in each MS are the only authorised entities to store vaccination information.

Each of the 27 MSs can designate a blockchain client node (which can be represented by a national health authority, say, the Ministry of Health) to interact with the blockchain. This entity is also responsible for designating a set of national medical centers (NMC) to generate vaccination certificates associated with already vaccinated people. These certificates will be validated by *verification centers*, which represent any organisation, public or private (e.g., airport or public administration building), that needs to verify the vaccination status of an individual.

The blockchain is used to store all relevant information about the vaccination process, including the registration of NMC. The registration of these entities can be performed by the national health authorities, which represent the blockchain nodes of their MS, by using smart contracts. Furthermore, the blockchain will simply contain a hash digest of the vaccination certificate per citizen that will be generated during the registration process and used later to facilitate the process of verifying the vaccination status of them. It is noteworthy that the registration and verification processes analysed below are only illustrative examples of how our scheme can be used to manage vaccination certificates, while these processes are considered for evaluation purposes in the next section.

During the *registration* process, citizens go to an NMC, where they present a valid identity document, to get vaccinated. For this purpose, the citizen may use a VC through a digital wallet app on their smartphone (as proposed by [10]) or other more traditional approaches based on X.509 certificates. A physician performs the vaccination, and the corresponding certificate is generated. As described in Section 4, this certificate may contain information about the vaccine itself, as well as data about the specific dose to facilitate the management of the supply chain. Furthermore, the citizen's identity shown at the beginning of the process can be embedded in the credential. Assuming a two-shot vaccine, this credential may demonstrate that the citizen received the first shot, so it can be used in the process of administering the second one, or that they are immune as they already received both shots. The NMC, or the physician

on its behalf, digitally signs the certificate to guarantee its validity and sends this credential to the citizen, say, through a smartphone app, so that they can maintain the control of how the certificate is used. It should be noted that the process of sending the vaccination certificate is done through a secure channel by using well-known approaches, such as Transport Layer Security (TLS). Furthermore, the certificate could be encrypted before being stored in the user's smartphone to protect the credentials while at rest. Moreover, a hash digest (e.g., by using SHA-256) of the certificate is generated and stored on the blockchain. The NMC sends this hash to the MS's blockchain node that is responsible for registering it on the EU vaccination blockchain. Additionally, an encrypted version can be stored in the InterPlanetary File System (IPFS) [38] or another repository, so that the vaccination certificate can be recovered by the citizen in case of losing their smartphone. Again, such processes are carried out by using renowned approaches, such as TLS to protect the data in transit.

After citizens have received a certificate, they can use it to access certain places that require proof of citizens' vaccination status, such as an airport or public administration building. During the *verification* process, citizens present their certificate to a verifier service. This service creates a hash digest of the provided certificate that is verified against the hash stored in the blockchain. For this process, the verifier service contacts the country's blockchain node that is in control of performing the verification on the EU vaccination blockchain. Like in the issuance procedure, this process is performed through well-known security mechanisms, such as TLS. Furthermore, the verifier service validates the signature created by the NMC to confirm that the credential was generated by an approved entity. Additionally, it checks the validity of the citizen's identity to ensure that they are indeed the person associated with the credential presented.

Alternatively, citizens are empowered to show a subset of their identity attributes by using zero-knowledge proofs (ZKPs) to access certain places that only require confirmation of a person's vaccination status but do not need personal data. For example, in the case of VCs, the holder of a certain credential is enabled to combine several VCs from different issuers and selectively disclose specific claims composing a certain VC. However, this aspect is outside the scope of this work. Indeed, as described in the next section, the evaluation of our platform is focused on the performance requirements from the perspective of the blockchain implementation to register and verify vaccination certificates. Nevertheless, it should be noted that the proposed blockchain platform is intended to serve as a decentralized approach to manage vaccination information and to be integrated with SSI approaches, such as VCs, for the sake of providing privacy-preserving features. Furthermore, as already mentioned, only a hash of the vaccination certificate is stored on the blockchain, and an encrypted version of such certificate is stored on an off-chain repository (IPFS), so that users' sensitive data is never disclosed to external entities. Therefore, citizens are enabled with the ownership of their data to manage their vaccination certificates. The integration of the proposed platform with SSI approaches, such as VCs and DIDs, will enable a more advanced privacy-preserving approach for the issuance and verification processes through the integration of ZKPs in the whole ecosystem.

Table 2: Network evaluation of registering and verifying vaccination certificates using blockchain.

Step	TPS	Response time (msec)	Peer bandwidth (kB)	Ordering bandwidth (kB)
Register	1	84	395	636
	2	81	419	825
	4	78	457	2019
	8	87	516	3644
	16	109	588	4938
	28	133	700	6019
Verify	1	91	394	701
	2	87	415	1123
	4	83	447	1788
	8	94	495	2153
	16	117	553	5069
	28	153	639	8122
	50	168	671	5919
	100	189	804	12109

6. Evaluation

6.1. Testbed. To evaluate our proposal, we rely on the Experimental Platform for Internet Contingencies (EPIC) [39]. EPIC is an emulation testbed based on the Deter software [40, 41] for studying the security and stability of distributed systems. The use of emulation-based testbeds in cybersecurity is well established [42–44] and ensures repeatability and measurement accuracy. Furthermore, this approach was chosen for the sake of overcoming the major difficulties that arise while trying to simulate the behaviour of ICT components under stress, attacks, or failures. The infrastructure of EPIC comprises 356 experimental nodes, 8 switches, and a few special equipment, such as programmable logical controllers.

Overall, the setup relies on the deployment of Hyperledger Fabric on an emulated network in EPIC and implements the proposed architecture shown in Figure 2. It is assumed that the European health authorities, which are considered trusted, provide the "ordering" services, while each MS is a "peer" node in the Hyperledger Fabric terminology. This emulated 1 Gbps blockchain network comprises 27 nodes corresponding to the current EU MS with a network latency of 3 msec.

The ordering services comprise the following: ZooKeeper (3 instances), Kafka (4 instances), and orderer (3 instances). Their main purpose is to sort the messages/requests exchanged among the participants. Each instance of a given service runs on a different machine for supporting failover of the ordering services. This setup ensures ordering service availability if at maximum one instance of each service is in the fail status. The peer nodes are managed by the MSs for endorsing the transactions proposed by the clients. They also receive the ordered blocks of transactions

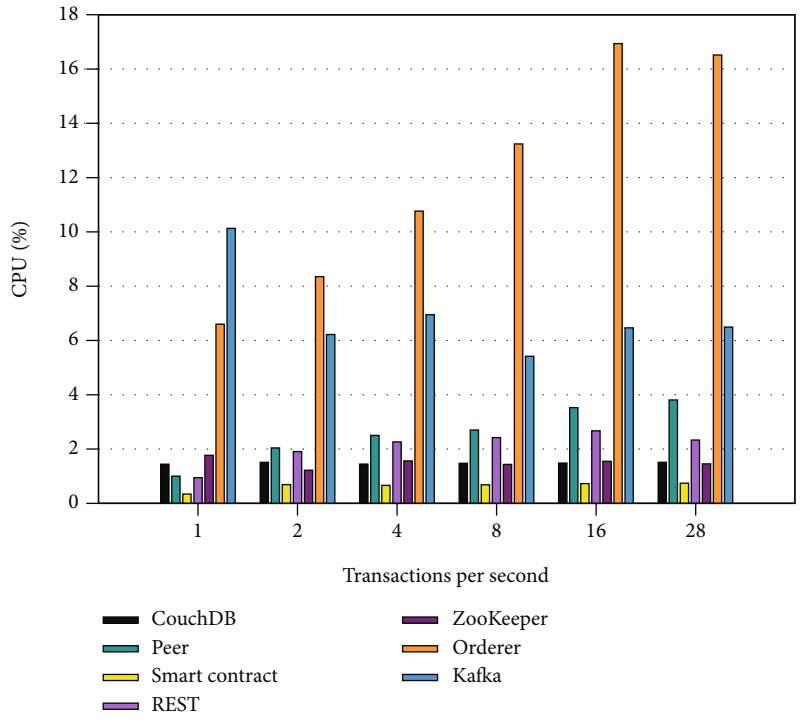

Figure 3: Dockerised services' CPU utilisation considering different TPS for registering new vaccination certificates in a blockchain system.

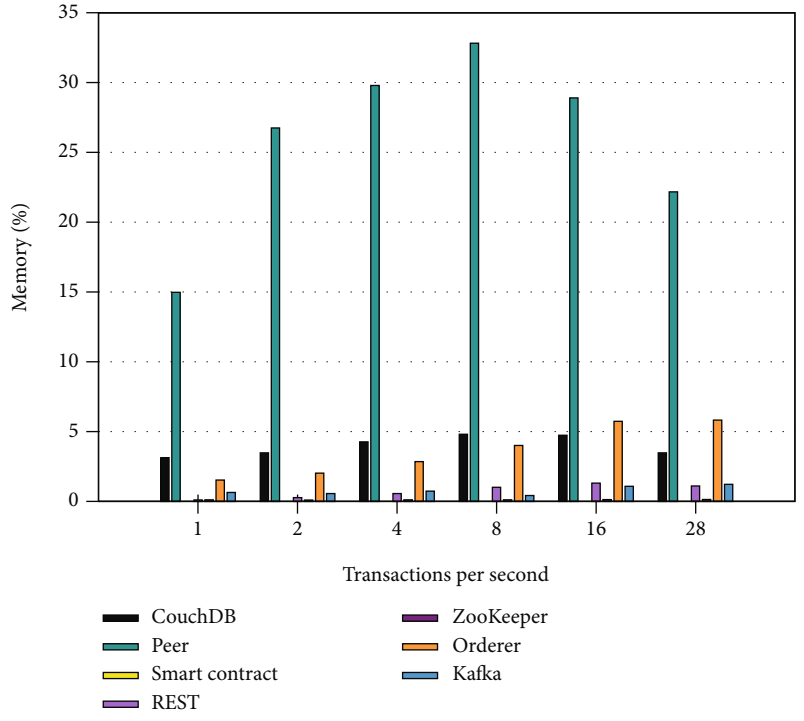

Figure 4: Dockerised services' memory utilisation considering different TPS for registering new vaccination certificates in a blockchain system.

from the ordering service to maintain their local copy of the ledger. The following services of a MS node are hosted on a single machine:

(1) *CouchDB*: a database that maintains the valid transactions of the blockchain and allows content-based JSON queries

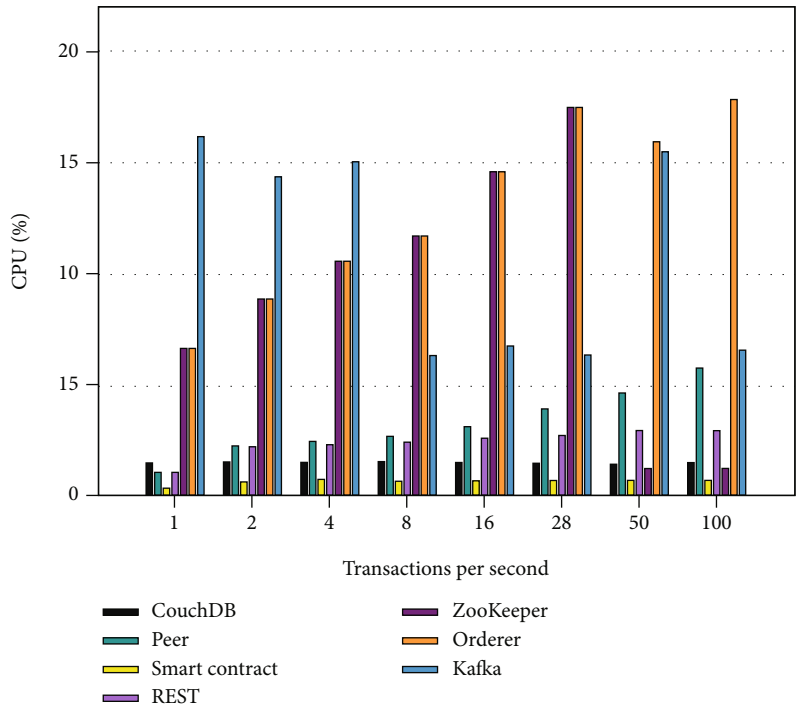

Figure 5: Dockerised services' CPU utilisation considering different TPS for verifying vaccination certificates in a blockchain system.

(2) *Peer*: a core service in the Hyperledger Fabric architecture storing the ledger and validating the transactions

(3) *Certificate authority*: this provides digital certificates to the participants of the MS node

(4) *Smart contract*: this implements basic functionalities such as user access control and message conformity

(5) *Application interface*: this interacts with the blockchain. It is implemented as a representational state transfer (REST) service and accomplishes all the interactions on behalf of the national health centers for committing a transaction in the blockchain network

As each MS acts independently, we deploy a single disjunctive ("OR") policy among the participants, meaning that a transaction originating from a MS is only validated by the originating MS. What the system checks is whether the submitted transaction bears a valid digital signature from the MS blockchain node. This also means that any transaction stemming from a MS on behalf of another MS will be rejected by the blockchain.

All ordering and peer services are configured and executed using the corresponding Docker images with the standard deployment options. Moreover, all the underlying network communications among the participants (clients, peers, and the ordering service) are securely protected by Transport Layer Security (TLS). The certificates and private keys for both TLS and the blockchain services are generated during the blockchain network initialisation procedure, according to the Hyperledger Fabric specifications.

6.2. Results. We evaluate the adequacy of deploying our proposal in a real, large-scale architecture, concentrating on two fundamental provisioned services, namely, vaccination registration and verification. The focus is on user experience in terms of request round-trip time, i.e., the time required for receiving a response after submitting a request, and the utilisation of system resources, i.e., CPU, memory, and network bandwidth.

For the registration process, we consider the maximum number of transactions required to get all European citizens vaccinated in one year. According to Eurostat, the EU-27 population is ≈447.5 M inhabitants [45]. Thus, assuming that a vaccine requires two doses, that is, two blockchain transactions, a total of 28 transactions per second (TPS) will be required in the worst case. Table 2 summarises the average latency perceived when registering or verifying a vaccination certificate in the blockchain, as well as the bandwidth consumed by both the peer and the ordering nodes. As observed, the response time for registration ranges between 83 and 133 msec. Moreover, at the peer side, the bandwidth utilisation increases from 500 to 700 kB. Overall, both these numbers can be characterised as absolutely tolerable. On the other hand, the bandwidth consumed by the ordering service demonstrates a significant augmentation among the different TPS values, reaching ≈6000 kB in the most demanding case.

CPU and memory utilisation for registering new vaccination certificates under different traffic conditions per service are illustrated in Figures 3 and 4. Particularly, considering the worst case, CPU and memory utilisation for the peer services remain under 4 and 35%, respectively, while the ordering services' utilisation is under 17 and 7%. In any case, these requirements for both services are

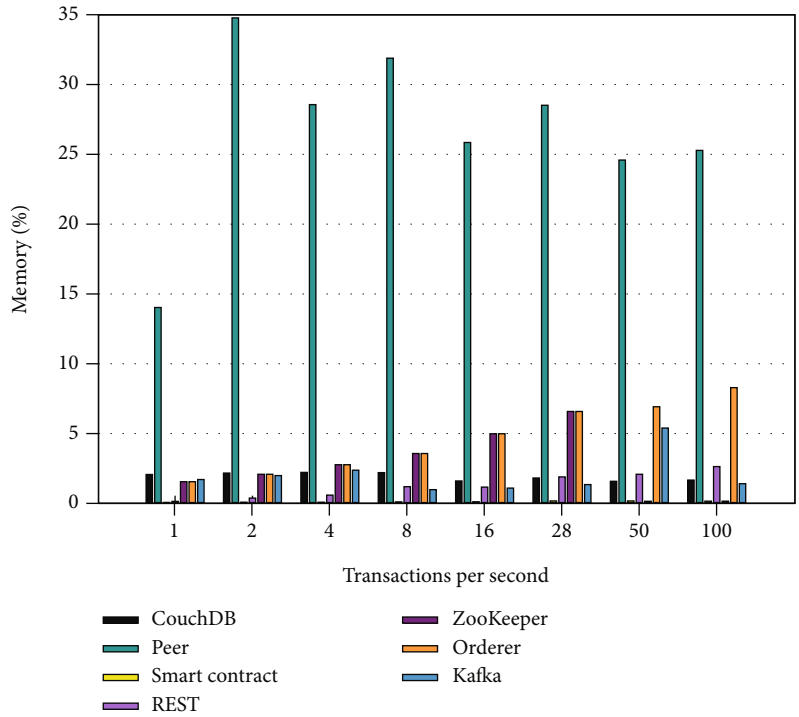

Figure 6: Dockerised services' memory utilisation considering different TPS for verifying vaccination certificates in a blockchain system.

manageable. It is also perceived that, when TPS increase from 8 to 16 and above, memory utilisation for the peer services starts to decrease. This can be explained by the fact that, along with TPS, the response time augments, having transactions submitted to the system at a lower rate. Interestingly and also on the positive side, CPU utilisation for the smart contract remains almost constant under different TPS, consuming less than 1% of the available CPU cycles. Overall, the registration process is more demanding in terms of CPU on the orderer and secondly on the Kafka services, while in terms of memory on the peer service.

Regarding vaccination certificate verification, we used data from Eurostat to calculate realistic requirements in terms of TPS. Specifically, we calculated the total number of air, marine, rail, and bus passengers for 2018, which is the latest year with data for all these categories. As verification transaction requests are forwarded to the national node of each MS, we consider the worst case, that is, the MS with the highest combined number of passengers in one year (3.2 billion); this gives us ≈100 TPS. Regarding the search operation, the worst case scenario is again followed; that is, the correct record is the last one. Similar to vaccination registration, the response time increases proportionally to the number of TPS, demonstrating a similar pattern. Overall, with reference to Table 2, the response time and bandwidth utilisation at a MS blockchain node fluctuate between 91 and 189 msec and 394 and 804 kB, respectively. However, for ordering, the utilised network bandwidth reaches up to 12,109 kB.

Figures 5 and 6 depict CPU and memory utilisation for vaccination certificate verification per blockchain service. As observed, CPU utilisation for both the peer and REST services increases proportionally to TPS, while it is relatively stable for couchDB and smart contract. The orderer service initially increases and then stabilises, while the Kafka service fluctuates between 6 and 16%. However, in all cases, the CPU load remains under 18%.

As expected and similar to registration, memory usage for the peer service ranges between ≈14% and 35%, demonstrating that it is memory intensive. For the rest of the services, memory requirements are low, that is, under 8%. In summary, the verification process is more demanding in terms of CPU on the ordering services, while in terms of memory on the peer service.

7. Conclusions

The work at hand sheds light on the timely and intriguing issue of managing digital vaccination certificates on a large scale. After arguing that under the prism of COVID-19 and future epidemics, this need is rather a sine qua non, we specifically attempt to answer two key questions: how such an endeavour can be realistically organised with a focus on reducing complexity, and if so, would it be smooth-running under pragmatic conditions or even stress in terms of performance? For the first matter, we scrutinised on an envisaged wide-scale deployment capable of covering the needs of EU-27 and elaborated on a practical vaccination certificate scenario. For the second, we relied on the EPIC platform.

Specifically, based on the performance results obtained, including scalability aspects and challenges for the deployment of such platform, it is demonstrated that, for both registration and verification operations, the system achieves

satisfactory results even under stress. This strongly suggests that even a network decreased by one order of magnitude (100 Mbps) would be more than enough. Regarding CPU requirements, the ordering nodes need to be more powerful than MS ones, while the peer nodes necessitate more memory. Also, it is shown that, at least in a similar setup as our testbed, 100 TPS is the boundary, considering that above this limit, the system is saturated, producing errors and experiencing inconsistencies. This indicates that in most populated European countries, the MS node specifications should be carefully devised to support such a large number of TPS or even greater, if necessary.

Future work will concentrate more on the security, privacy, and ethical aspects associated with the registration and verification process of digital vaccination certificates. Also, an appealing direction is to investigate if this kind of platform could cater for the needs of the vaccine supply chain, ensuring efficient vaccine warehousing, handling, and stock administration.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

A preliminary version of this paper can be found at [46].

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] World Health Organization (WHO), *Timeline of WHO's Response to COVID-19*, 2020, https://www.who.int/news/item/29-06-2020-covidtimeline.

[2] OECD Economic Outlook, *Interim Report September 2020*, OECD, 2020.

[3] T. Martin, G. Karopoulos, J. L. Hernández-Ramos, G. Kambourakis, and I. N. Fovino, "Demystifying COVID-19 digital contact tracing: a survey on frameworks and mobile apps," *Wireless Communications and Mobile Computing*, vol. 2020, 29 pages, 2020.

[4] V. Kouliaridis, G. Kambourakis, E. Chatzoglou, G. Dimitrios, and H. Wang, "Dissecting contact tracing apps in the android platform," *PLoS ONE*, vol. 16, no. 5, p. e0251867, 2021.

[5] World Health Organization, "Draft landscape and tracker of COVID-19 candidate vaccines," WHO, 2021, https://www.who.int/publications/m/item/draft-landscape-of-covid-19-candidate-vaccines.

[6] DHL, *DHL White Paper-Delivering Pandemic Resilience-How to Secure Stable Supply Chains for Vaccines and Medical Goods during the COVID-19 Crisis and Future Health Emergencies*, 2020, https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-delivering-pandemic-resilience-2020.pdf.

[7] O. J. Wouters, K. C. Shadlen, M. Salcher-Konrad et al., "Challenges in ensuring global access to COVID-19 vaccines: production, affordability, allocation, and deployment," *The Lancet*, vol. 397, no. 10278, pp. 1023–1034, 2021.

[8] *Tracking COVID-19 Vaccinations Worldwide*https://edition.cnn.com/interactive/2021/health/global-covid-vaccinations/.

[9] N. Phillips, "The coronavirus is here to stay — here's what that means," *Nature*, vol. 590, no. 7846, pp. 382–384, 2021.

[10] D. Gruener, *Immunity Certificates: If We Must Have Them, We Must Do It Right*, 2020.

[11] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, "The role of blockchain to fight against COVID-19," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 85–96, 2020.

[12] A. A. Abd-alrazaq, M. Alajlani, D. Alhuwail et al., "Blockchain technologies to mitigate COVID-19 challenges: a scoping review," *Computer Methods and Programs in Biomedicine Update*, vol. 1, 2020.

[13] J. V. Lazarus, S. C. Ratzan, A. Palayew et al., "A global survey of potential acceptance of a COVID-19 vaccine," *Nature Medicine*, vol. 27, no. 2, 2021.

[14] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "Novidchain: blockchain-based privacy-preserving platform for COVID-19 test/-vaccine certificates," *Software: Practice and Experience*, 2021.

[15] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third, and J. Domingue, "COVID-19 antibody test/vaccination certification: there's an app for That," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148–155, 2020.

[16] H. R. Hasan, K. Salah, R. Jayaraman et al., "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020.

[17] C. Hicks, D. Butler, C. Maple, and J. Crowcroft, "SecureABC: secure antibody certificates for COVID-19," 2020.

[18] L. Alexandra, "COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges," *The Lancet*, vol. 395, no. 10237, pp. 1595–1598, 2020.

[19] S. Chaudhari, M. Clear, and H. Tewari, "*Framework for a DLT based COVID-19 passport*," in *Intelligent Computing. Lecture Notes in Networks and Systems*, K. Arai, Ed., vol. 285, Springer, Cham, 2021.

[20] C. M. Angelopoulos, A. Damianou, and V. Katos, "DHP framework: digital health passports using blockchain-use case on international tourism during the COVID-19 pandemic," 2020, http://arxiv.org/abs/2005.08922.

[21] A. Bansal, C. Garg, and R. P. Padappayil, "Optimizing the implementation of COVID-19 imunity certificates using blockchain," *Journal of Medical Systems*, vol. 44, no. 9, p. 140, 2020.

[22] World Wide Web Consortium (W3C), "Verifiable credentials data model 1.0," 2019, https://www.w3.org/TR/vc-data-model/.

[23] A. V. Sambra, E. Mansour, S. Hawke et al., "Solid: a platform for decentralized social applications based on linked data," *MIT CSAIL & Qatar Computing Research Institute, Tech. Rep.*, 2016.

[24] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, 2014.

[25] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, "Uport: a platform for self-sovereign identity," 2017, https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.

[26] World Wide Web Consortium (W3C), "Decentralized identifiers (dids) v1.0- core architecture, data model, and representations," 2021, https://www.w3.org/TR/did-core/.

[27] European Commission, "Communication from the Commission to the European Parliament and the Council-preparedness for COVID-19 vaccination strategies and vaccine deployment," 2020, https://ec.europa.eu/health/sites/health/files/vaccination/docs/2020_strategies_deployment_en.pdf.

[28] D. Marbouh, T. Abbasi, F. Maasmi et al., "Blockchain for COVID-19: review, opportunities and a trusted tracking system," 2020, https://www.techrxiv.org/articles/preprint/Blockchain_for_COVID-19_Review_Opportunites_and_a_Trusted_Tracking_System/12609344.

[29] A. Musamih, R. Jayaraman, K. Salah, H. Hasan, I. Yaqoob, and Y. Al-Hammadi, "Blockchain-based solution for distribution and delivery of COVID-19 vaccines," IEEE Access, 2021.

[30] M. Chang and D. Park, "How can blockchain help people in the event of pandemics such as the COVID-19?," *Journal of Medical Systems*, vol. 44, no. 5, p. 102, 2020.

[31] D. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey," *TechRxiv Preprint*, vol. 4, 2020.

[32] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)," 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130.

[33] EHealth Network, "Guidelines on verifiable vaccination certificates - basic interoperability elements release 2," 2021, https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf.

[34] *Smart Vaccination Certificate Working Group*https://www.who.int/groups/smart-vaccination-certificate-working-group.

[35] *IATA Travel Pass Initiative*https://www.iata.org/en/programs/passenger/travel-pass/.

[36] *Certify.health*https://eithealth.eu/project/certify-health/.

[37] *COVID-19 Credentials Initiative*https://www.covidcreds.org/.

[38] J. Benet, *IPFS - Content Addressed, Versioned, P2P File System*, CoRR, 2014, http://arxiv.org/abs/1407.3561.

[39] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: a testbed for scientifically rigorous cyber-physical security experimentation," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 319–330, 2013.

[40] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab, "The DETER Project: advancing the science of cyber security experimentation and test," in *In 2010 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 1–7, 2010.

[41] T. Benzel, "The science of cyber security experimentation: the DETER Project," in *In 27th Annual Computer Security Applications Conference*, 2011.

[42] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "Scada cyber security testbed development," in *In 2006 38th north American power symposium*, pp. 483–488, 2006.

[43] T. C. Eskridge, M. M. Carvalho, E. Stoner, T. Toggweiler, and A. Granados, "Vine: a cyber emulation environment for MTD experimentation," in *In Proceedings of the Second ACM Workshop on Moving Target Defense, MTD 15*, pp. 43–47, New York, NY, USA, 2015.

[44] K. E. Stewart, J. W. Humphries, and T. R. Andel, "Developing a virtualization platform for courses in networking, systems administration and cyber security education," in *in Proceedings of the 2009 Spring Simulation Multiconference, ser*, SpringSim '09. San Diego, CA, USA: Society for Computer Simulation International, 2009.

[45] Eurostat, "Population and population change statistics 2021," 2021, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Population_and_population_change_statistics.

[46] J. L. Hernández-Ramos, G. Karopoulos, D. Geneiatakis, T. Martin, G. Kambourakis, and I. N. Fovino, "Sharing pandemic vaccination certificates through blockchain: case study and performance evaluation," 2021, http://arxiv.org/abs/2101.04575.