applied sciences

MDPI

Article

SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations

Yazeed Alabdulkarim [1,*,†], Abdulmajeed Alameer [2,†], Mohammed Almukaynizi [1] and Abdulaziz Almaslukh [1]

[1] Information Systems Department, King Saud University, Riyadh 11362, Saudi Arabia; malmukaynizi@KSU.EDU.SA (M.A.); aalmaslukh@ksu.edu.sa (A.A.)
[2] Computer Science Department, King Saud University, Riyadh 11362, Saudi Arabia; abalameer@ksu.edu.sa
* Correspondence: yalabdulkarim@ksu.edu.sa
† These authors contributed equally to this work.

Abstract: The COVID-19 pandemic has caused many countries around the globe to put strict policies and measures in place in an attempt to control the rapid spread of the virus. These measures have affected economic activities and have impacted a broad range of businesses, such as international traveling, restaurants, and shopping malls. As COVID-19 vaccination efforts progress, countries are starting to relax international travel constraints and permit passengers from certain destinations to cross the border. Moreover, travelers from those destinations are likely required to provide certificates of vaccination results or negative COVID-19 tests before crossing the borders. Implementing these travel guidelines requires sharing information between countries, such as the number of COVID-19 cases and vaccination certificates for travelers. In this paper, we introduce SPIN, a framework leveraging a permissioned blockchain for sharing COVID-19 information between countries. This includes public data, such as the number of vaccinated people, and private data, such as vaccination certificates for individuals. Additionally, we employ cancelable fingerprint templates to authenticate private information about travelers. We analyze the framework from scalability, efficiency, security, and privacy perspectives. To validate our framework, we provide a prototype implementation using the Hyperledger Fabric platform.

Keywords: blockchain; COVID-19; Hyperledger Fabric; immunity passports

Citation: Alabdulkarim, Y.; Alameer, A.; Almukaynizi, M.; Almaslukh, A. SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations. *Appl. Sci.* **2021**, *11*, 8767. https://doi.org/10.3390/app11188767

Academic Editor: Gianluca Lax

Received: 12 August 2021
Accepted: 18 September 2021
Published: 21 September 2021

1. Introduction

The COVID-19 pandemic has caused many countries around the globe to adopt strict policies and measures in an attempt to control the rapid spread of the virus. These policies include enforcing social distancing, schools and universities closure, and travel restrictions [1–4]. Reports show that the pandemic has caused nearly 90% of commercial flights to be grounded, and has made more than 130 countries introduce some forms of travel restrictions, including quarantine, screening, or travel banning to high-risk countries [5]. The United Nations Conference on Trade and Development (UNCTAD) estimates the loss in the international tourism sector to be at least $1.2 trillion [6].

As living with the virus is becoming the norm, countries have started lifting some travel restrictions. For example, many countries require negative polymerase chain reaction (PCR) test results, vaccination certificates, or certificates of having recovered from COVID-19 [7]. Enforcing these travel requirements raises several challenges, such as the ability to verify the authenticity of vaccination and test records. Extensive research has been conducted to tackle the challenges associated with the COVID-19 pandemic. Researchers proposed multiple techniques for sharing health-related records [8–15]. Most of the proposed techniques utilize blockchain technology to provide mechanisms for sharing health-related information without relying on a central authority [8–11]. The majority of existing approaches rely on cryptography techniques to publish encrypted personal health

records in the public blockchain; to preserve privacy, much of these data do not need to be in the blockchain. Unlike previously proposed techniques, our approach provides a secure and privacy-preserving mechanism for sharing both public data and private data of individuals. COVID-19 data feeds with personal data being anonymized, such as records of new COVID-19 tests, cases, and vaccinations provided, may be shared publicly with other countries [16–18]. Such data feeds would help in estimating the contemporary risk level associated with each participating country. In addition, personal private data, such as test and vaccine certificates of individuals traveling to specific countries, may only be shared with the travel destination countries to preserve privacy, i.e., without being pushed to the blockchain. This motivates our work in developing a framework for sharing both public and private health-related information between countries.

In this paper, we introduce SPIN [19] (a framework for Sharing Pandemic Information across Nations). SPIN is a blockchain-based framework that allows countries to quickly verify COVID-19 vaccination and test results at their ports of entry. Countries are represented as peers in the blockchain network. A country may select a local authority to act as a peer in the decentralized network (e.g., a ministry of health). In the blockchain network, local entities that administer public health facilities and control ports of entry are represented as clients connecting to their country's peer. Moreover, clients may invoke transactions to read/write public and private data, and peers may share public data by executing transactions to the blockchain network. Public data are transformed and stored in the form of key–value pairs, allowing other peers in the network to read it. Additionally, each peer may send private data to a recipient peer. For sharing private data, such as COVID-19 test results, we utilize cancelable fingerprint templates to authenticate information about individuals. More specifically, the contribution of our paper is as follows:

1. A decentralized framework (SPIN) for sharing COVID-19 vaccination and test certificates as well as public health-related data.
2. A publicly available implementation of our framework.
3. A detailed analysis of the properties associated with the design decisions we chose for the framework in terms of efficiency, scalability, security, and privacy.
4. An illustration of the utility of the framework by presenting simple statistics that can be derived from the data supplied by the framework. Such statistics may help countries to maintain awareness of the aggregate level of risk associated with the relaxation of travel restrictions.

The organization of our paper is as follows. In Section 2, we describe the design details for our framework. In Section 3, we provide an analysis of the properties associated with the framework. In Section 4, a prototype implementation of the framework is described. In Section 5, we show some use case applications that are derived from the data supported by our framework. We give an overview of the research work that is related to our framework in Section 6. A conclusion is provided in Section 7.

2. Design

We utilized the blockchain technology [20–22] to design the SPIN framework that allows one to share COVID-19 information between countries, specifically vaccination and test-taking information. At the heart of SPIN is a permissioned blockchain network of peers, representing participating countries. Peers are the blockchain nodes and accept requests from clients, which represents entities that are involved in issuing vaccine and test certificates, such as hospitals and clinics, and verifying them, such as border security departments. Clients issue transactions, such as generating a vaccine certificate, to their corresponding peers, which execute the transactions on the blockchain network.

The framework facilitates the exchanging of public and private data between peers (see Section 2.2 for details). Public data may include aggregate data, such as the number of vaccinated people and the number of daily cases. Private data include travel requests for individuals containing their COVID-19 test and vaccination certificates.

Moreover, our framework employs a fingerprint mechanism based on template protection [23] to authenticate private information about individuals, such as their COVID-19 vaccination certificates (see Section 2.3 for details). Fingerprint authentication is commonly used to verify people across borders [24] because it has several desired features; for example, it is nontransferability and difficult to spoof. For instance, a person may easily pass her travel documents, or have them stolen by a fraudster pretending to be her. Committing such a crime becomes more difficult with fingerprint and biometric authentication in general.

We explain the main components of SPIN, as shown in Figure 1, in the following subsections. Figure 1 shows four different countries that are represented by their peers. A client is able to communicate with its representative peer in the given country. Each peer may execute a transaction to the blockchain containing public data for other peers to read. Any peer can privately send data to exchange COVID-19 certificates with another peer residing in a different country, while its hashed data are written on the blockchain.

To simplify the discussion and without a loss of generality, we use the term "COVID-19 certificate" to refer to both COVID-19 vaccine and test result certificates. The certificates contain all necessary information, such as the administration date, validity period, and result.

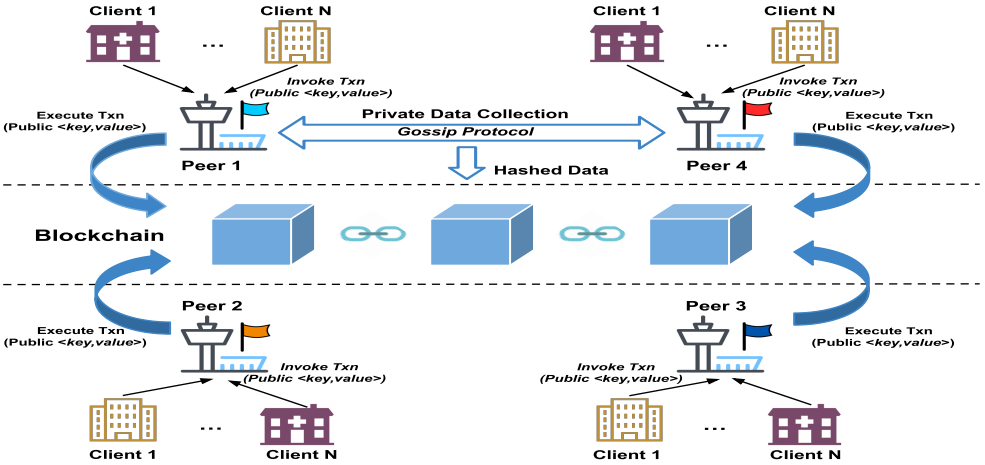

Figure 1. SPIN Framework Overview.

2.1. Blockchain

A blockchain is a distributed, decentralized database that groups and processes transactions into a sequence of cryptographically linked blocks. Blockchain has many desired features, such as immutability, decentralization, and transparency, that make it suitable for sharing information between countries. A consensus protocol is implemented for agreement and to append a block of transactions to the blockchain network. A blockchain network may be public, private, or permissioned. A public network, such as Bitcoin [20], is open and allows anyone to join the network and propose transactions. In contrast, a private network permits a predefined set of entities to join the network and propose transactions. A permissioned network sits in the middle between private and public networks, offering a mechanism to permit entities to the network. For our framework, we use a permissioned blockchain network because it has several desirable characteristics that suit our use case. First, participants are identified, which is required to authenticate the shared information. Second, it allows for more scalable consensus protocols, compared to public blockchain networks, which are vulnerable to attacks and have a lower throughput and scalability characteristics [25,26]. We use Hyperledger Fabric [27,28] to serve as the underlying permissioned blockchain network because it supports the sending of private data (see Section 2.2 for details). It is possible to select other blockchain platforms with similar features or implement them to fulfill the SPIN functional requirements. Hyperledger Fabric is an open-source permissioned blockchain platform. It is highly modular and configurable for various use case applications. We describe four main components of Hyperledger

Fabric: membership service provider (MSP), clients, peers, and orderers (see Figure 2). The MSP component is responsible for establishing and verifying the cryptographic identities of entities in the permissioned blockchain network using a public key infrastructure (PKI) [29,30]. Clients represent end-users and submit transaction invocations to peers. Peers execute and commit transactions. They maintain a copy of the blockchain and a private database recording the current state of the blockchain modeled as a key–value store. Orderers form the ordering service that implements the consensus protocol and provides communication and delivery guarantees. The life cycle of transactions in Hyperledger Fabric follows an execute–order–validate model. First, peers execute, check, and approve transactions. Second, the ordering service orders transactions using the implemented consensus protocol. Last, before committing the transactions, peers validate them with their defined endorsement policies. An endorsement policy specifies the set of peers that must execute and approve a transaction to be considered valid.

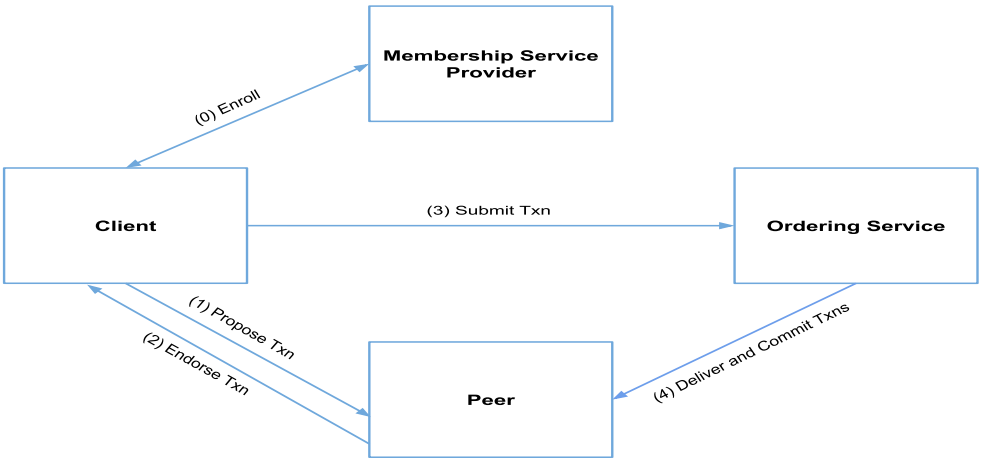

Figure 2. Main components of Hyperledger Fabric.

Each country is represented as a peer in our blockchain network and has an MSP to enroll and authenticate members of the blockchain network and their transactions. Entities that are involved in issuing and verifying COVID-19 certificates are represented as clients. Those clients issue transactions that are executed by their peers on the network. Blockchain transactions read and write data items for sharing COVID-19 information between countries. These data items are represented as key–value pairs key = K, value = V and classified into private and public data, as detailed in Section 2.2.

For our implementation, we employ Raft [31] as a consensus protocol for the blockchain network. Raft uses a leader–follower model to replicate transactions. A leader node is elected to process transactions and replicate them to other nodes. It offers several advantages, such as immediate finality and a fast block time. Raft is crash-fault-tolerant and continues to operate as long as the majority of nodes are running. Raft is not Byzantine-fault-tolerant and does not protect against malicious leaders, which is acceptable for our framework because it operates on a permissioned blockchain network. The identity of all members is verified and known, which prevents them from acting maliciously. Moreover, write transactions must be approved by their owning peers to be processed in the blockchain network. For instance, a transaction writing key–value pairs belonging to Saudi Arabia, such as the number of vaccinated people or a vaccination record, must be approved by the peer of Saudi Arabia using PKI. This design protects against malicious peers that may issue false transactions about other countries. To implement this design, we utilize the endorsement policy in Hyperledger Fabric [32] (see Section 4 for details).

2.2. Public and Private Data

The SPIN framework facilitates the sharing of public and private data between peers. Public data, such as records of new COVID-19 tests, cases, and vaccinations provided, are

written to the blockchain after personal data are removed. Such data are written as key–value pairs and is accessible by all peers to read it. Key templates for publicly shared data are agreed upon and may be generated in various ways, such as concatenating the country code with the type of data. For instance, the key–value pairs representing the number of vaccinated people in Saudi Arabia may be constructed as {key = SA-VAC-COUNT, value = 10,123,456}.

In contrast, private data are sent to a specific peer, and its hash is written on the blockchain, as evidence of the transaction. These data are stored in a private database state of the peers who are authorized to view it. We utilized the private data collection feature and gossip protocol of Hyperledger Fabric [33] to exchange COVID-19 certificates for travelers between countries. When an individual plans to travel, her data are sent privately to her destination countries. Individuals' private data are represented as key–value pairs. A key template for a traveler's private data is agreed upon and may be generated in various ways, such as concatenating the country code with the individual's passport number. The corresponding value contains the individual's COVID-19 certificate C and a transformed fingerprint template $T(fp)$, as described in Section 2.3.

2.3. Fingerprint Authentication

The SPIN framework employs fingerprint authentication to verify individuals holding COVID-19 certificates. Using fingerprint templates is an effective technique for authentication due to fingerprint uniqueness, as even identical twins have two different fingerprints. In addition, compared to other biometric-based techniques, the hardware used to scan fingerprints is relatively cheap and mostly available in the border security for most countries [24]. When individuals visit other countries, they are authenticated using their passport (ID) along with their fingerprint template fp to prevent fraudsters from impersonating others.

To preserve the privacy of individuals' fingerprints and meet all the requirements described in the ISO/IEC 24745 biometric data protection standards [34], our framework uses cancelable biometrics to protect fingerprint templates, as described in [23]. The technique works by transforming the original fingerprint template in a way that it becomes practically infeasible to obtain the original template from the transformed one. If the transformed fingerprint template is compromised, a new template can be reissued and used subsequently. Note that the transformed data here are fingerprint templates and not the actual fingerprint images. Fingerprint templates represent unique features that have been extracted from actual fingerprints, which can be used for identification and authentication. Cancelable biometrics are shown to be effective in matching biometric information while preserving the privacy of the stored biometric templates [23].

Fingerprint authentication involves two stages, the enrollment stage and the authentication stage. In the enrollment stage, the fingerprint template fp is captured from an individual, and the system then transforms it before storing it in the local database. Details of the transformation process are described in [23]. When an individual decides to travel, the individual's transformed fingerprint template $T(fp)$ along with the key that is used for the transformation are sent to the traveler's destination country per the individual's request. The authentication stage takes place when individuals arrive at their destination country. At the border control of the destination country, the record that matches the individual's passport ID is retrieved from the local database, and the individual's transformed fingerprint templates $T(fp)$ are matched against the ones that the country received. This puts an additional factor of authentication on top of authenticating individuals only by their passport IDs, which helps in preventing individuals' impersonation.

2.4. Issuance of COVID-19 Certificates and Public Information

Entities that issue COVID-19 certificates and public information, such as hospitals and clinics, are represented as clients in SPIN. A client signs and issues a transaction to its corresponding peer, representing its country. A transaction manipulates data that are

represented as key–value pairs. For instance, the key "SA-VAC-COUNT" refers to the count of vaccinated people in Saudi Arabia, and the key "SA-PASS-P012345" refers to the COVID-19 certificate for an individual with passport number P012345 in Saudi Arabia.

The corresponding peer checks the transaction, which includes verifying the client's signature and ensuring that it is authorized to perform the proposed transaction. If these checks pass, the corresponding peer signs the transaction, executes it, and broadcasts it to all peers. Each peer in the network verifies the signature of the issuing peer, appends the block of the transaction to its blockchain replica, and updates its database state.

Transactions containing public data, such as the number of vaccinated people, are executed, as described above. Transactions that contain private data, namely private transactions, are sent to their target peers (see Section 2.2 for details). Private transactions are utilized to send travelers' COVID-19 certificates between countries, as follows. First, a traveler communicates with a local client to issue a travel request, sending her COVID-19 certificate C and fingerprint template fp to a set of countries (destination peers). The communication mechanism between individuals and local clients is out of scope and left to be implemented by each country, as desired. For instance, health authorities may provide a mobile application for individuals to book COVID-19 vaccine/test and issue travel requests. Next, the client issues and signs a transaction, containing the COVID-19 certificate along with the individual's cancelable fingerprint template $T(fp)$, to its corresponding peer (source peer). The client may capture the individual's fingerprint in various ways. One way to do so is by capturing the fingerprint physically when an individual takes the vaccine or test, then stores its cancelable template. Alternatively, the National Information System, containing residents' fingerprints, may provide a mechanism, such as an API call, allowing clients to permit sending the cancelable fingerprint template without capturing it [35,36].

The source peer verifies the transaction, as described with public transactions, signs it, and sends it to the destination peers only. Additionally, the source peer executes the transaction publicly containing a hash of the private data collection to be written on the blockchain, as evidence for the transaction. In this design, the source peer sends the private data immediately to the destination peers, based on travelers' requests. If a traveler cancels her trip for any reason, the private data are still accessible by destination peers. One solution to mitigate this issue is to allow clients to schedule the execution of the transactions, based on travelers' requests, rather than executing it immediately. This solution allows travels to terminate the scheduled transaction, in case their trips are canceled for any reason.

2.5. Verification of COVID-19 Certificates

When an individual reaches her travel destination, a client, such as a border control, generates the key corresponding to her, using passport information. The client issues a read transaction for the key to its corresponding peer. The corresponding peer checks the transaction, which includes verifying the client's signature and ensuring that it is authorized to perform the proposed transaction. The peer retrieves the value, containing certificate C and transformed fingerprint $T(fp)$, for the key from its private database state and sends it to the client for verification purposes. The client verifies the certificate C and matches the transformed fingerprint $T(fp)$ with the individual's fingerprint captured at border control. Figure 3 depicts the process of issuing and verifying the travelers' COVID-19 certificate.

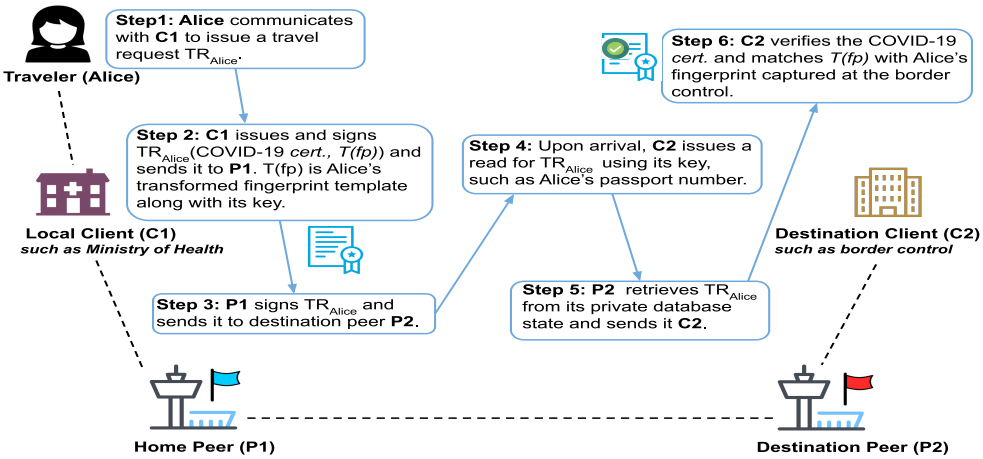

Figure 3. Issuing and Verifying COVID-19 Certificates.

3. Framework Analysis

In this section, we analyze the main properties of the SPIN framework presented in Section 2 from various aspects including efficiency, scalability, security, and privacy. We detail each aspect and its considerations in the following subsections.

3.1. Efficiency

Our proposed framework may be configured to employ widely embraced practices such as fingerprint authentication, which has indeed been in place in many ports of entry around the world as a primary measure. Utilizing such practices makes the adoption of SPIN framework processes seamless and rapid with minimal mitigation to the existing traveling procedures. Thus, it makes the implementation of the framework efficient; consequently, the overall cost can be significantly reduced. The framework design divides communication of the main actors into local (within the country) and global (between the countries). To make the framework flexible, the interaction between individuals and local clients to issue vaccination certificates and travel requests is left to be decided on a country-by-country basis (see suggestion provided in Section 2.4). Clients, such as border control and vaccination centers, issue transactions through their corresponding peers. This contributes to the disciplined governance and transparency of exchanging information between members of the network. Moreover, peers have full control to admit their clients and assign them read and write privileges.

3.2. Scalability

The scalability of SPIN depends on the scalability of its blockchain network implemented using Hyperledger Fabric. Several papers have evaluated the scalability and overall performance of Hyperledger Fabric [37–39]. Studies show that the endorsement policy and the number of endorsing peers are major factors that impact the scalability of Hyperledger Fabric. Increasing the number of endorsing peers causes additional overhead, as it requires obtaining the approval of more peers. For our framework, the number of endorsing peers is always one, and it is the peer corresponding to the country issuing the transaction. Another factor that impacts the scalability of a blockchain network is its consensus protocol. Our framework employs Raft as its consensus protocol, which provides a fast block time and is able to scale for various workloads.

3.3. Security and Privacy

Authentication: Peers and clients are authenticated using a public key infrastructure (PKI). The MSP component of Hyperledger Fabric handles authenticating members and verifying their identities. Moreover, for travel request transactions, SPIN verifies the identity of individuals by employing fingerprint authentication, explained in Section 2.3.

This fingerprint authentication provides a highly secured mechanism by nature due to the fingerprint uniqueness of every single individual.

Availability: Decentralized databases derived from blockchain technology are protected against the single point of failure. Therefore, any transaction can be executed between the main actors at all times, as a failure in such applications can be costly and burdensome. To enhance availability, a country may be physically represented by multiple peer nodes in the network. The blockchain consensus protocol impacts its availability characteristics. For our implementation, we employ the Raft protocol to reach a consensus, which is crash-fault-tolerant and continues to operate as long as the majority of nodes are running.

Integrity: Blockchain technology features a temper-proof and immutable ledger that ensures the integrity of transactions. Moreover, when issuing transactions, either public or private, clients and their corresponding peers sign them. These digital signatures verify the identity of issuing clients and their corresponding peers and ensure that transactions have not been altered.

Attribution and nonrepudiation: In order to issue transactions, clients and their corresponding peers must sign transactions with their private keys. Moreover, the hash of the private data is written to the blockchain, as evidence for the transaction. These mechanisms prove the issuance of transactions by peers and their clients, enabling attribution and accountability to verify transactions if needed.

Authorization and confidentiality: SPIN employs a permissioned blockchain network. Peers represent countries, and they admit their clients, such as a hospital or border control, into the network. Furthermore, peers may assign read and write privileges to their clients. Public data are accessible to all peers of the network, while private data are only sent to the destination peers to access it.

Anonymity: It is preserved and indeed a prominent feature in all the procedures including individuals' fingerprints. Cancelable biometrics, described in Section 2.3, is utilized to protect the original fingerprint of individuals without compromising any security aspects explained previously. Thus, the stored fingerprint templates cannot be linked to any individual. Thus, all the exchange of public and private data between the peers or between the peers and the local entities cannot be tracked back to the individuals.

The right to delay the transaction: SPIN supports that any individual can schedule the execution of her transaction, so her information will not be sent to the destination peer until the scheduled time. This helps to increase the privacy of the individual as her information is stored only in the origin peer, while the destination peer does not have access to the individual's information until the scheduled time has passed.

4. Prototype Implementation

We used Hyperledger Fabric [28] to implement a prototype of SPIN [19], as a permissioned blockchain network. We represented each country as an organization with one peer that maintains a blockchain of transactions, and a database state maintains the current values of ledger states. Multiple peers per country can be created for availability and durability purposes. The peer corresponding to the country issuing a write transaction acts as the endorsing peer that must approve the transaction for it to be considered valid. Each organization has a Membership Service Provider (MSP), which handles identity and authentication issues using PKI. We used Hyperledger Fabric's cryptogen utility tool to generate the public and private keys for all entities in the network. For the purpose of our prototype, we created five organizations with a total of five peers and five clients, i.e., one peer and one client per organization. Additionally, we created a cluster of five orderer instances, colocated with their peers, for the ordering service of Hyperledger Fabric. The ordering service implements Raft as the consensus protocol for the blockchain network.

We deployed one channel to facilitate communication among organizations, their peers, and their clients. We implemented two smart contracts for each organization, one for public data and the other for private data. A smart contract is a program that consists of

transactions that define the business logic. Invoking a smart contract executes transactions and records them in the blockchain.

The smart contract for public data consists of set and get transactions, allowing peers belonging to the same organization to write/modify and retrieve key–value pairs. Other peers are only authorized to get key–value pairs and not to set them. This enables peers and clients belonging to the same organization to write public data (key–value pairs) for the organization. In contrast, other peers, belonging to different organizations, may read the public data without the ability to write/modify it.

The smart contract for private data consists of set and get transactions as well. It maintains the private data collection belonging to an organization. It may be read by only peers and clients belonging to the same organization. It allows other peers to execute a set transaction sending private data to that organization and the hash of the data to the blockchain network. This enables one to send COVID-19 certificate and fingerprint templates belonging to a traveler to her destination country, as described in Section 2.2, which will only be accessible to that country.

For evaluation, we show screenshots of the execution of SPIN functionalities. The performance and scalability of the underlying blockchain framework (Hyperledger Fabric) have been extensively evaluated in previous work [37–39], showing superior results. This is attributed to several design decisions, including the fact that Hyperledger Fabric operates in a permissioned blockchain network allowing it to opt for more scalable consensus protocols and avoid protocols with limited performance characteristics, such as proof of work [40,41]. Therefore, we show the execution steps with screenshots from our prototype implementation using a CloudLab testbed [42].

First, we show an execution of the smart contract for sharing public data of Org1, namely, "public_record." Its client executes "SetRecord" transaction via Peer0 of Org1 to share the number of vaccinated people formatted as key–value pairs {key = SA-VAC-COUNT, value = 123,456}, as seen in Figure 4. Next, we show a client belonging to another organization, Org2, which executes a "GetRecord" transaction via Peer0 of Org2 to retrieve the value of key= "SA-VAC-COUNT", as seen in Figure 5. Alternatively, the client of Org2 may retrieve all public key–value pairs of Org1 by invoking "GetAll", as seen in Figure 6. Notice that the client of Org2 is not permitted to invoke a "SetRecord" transaction for the smart contract belonging to Org1 (see Figure 7). Only clients belonging to the same organization are permitted to publish public data. Fine-grained access control may be set to allow a subset of clients to publish specific data items [43,44].

```
root@node0:/mydata/fabric/fabric-samples/5host-deployment# docker exec cli peer chai
ncode invoke -o orderer.example.com:7050 --tls true --cafile /opt/gopath/src/github.
com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/orderer
.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C mychannel -n public_record
 --peerAddresses peer0.org1.example.com:9051 --tlsRootCertFiles /opt/gopath/src/gith
ub.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.example.com/peers/peer0
.org1.example.com/tls/ca.crt -c '{"Args":["SetRecord","SA-VAC-COUNT","123456"]}'
2021-05-18 14:09:22.921 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chainc
ode invoke successful. result: status:200
```

Figure 4. Peer0 of Org1 executes the transaction "SetRecord", sharing the number of vaccinated people as key–value pairs {key=SA-VAC-COUNT, value = 123,456}.

```
root@node1:~# docker exec cli peer chaincode invoke -o orderer.example.com:7050 --tl
s true --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrg
anizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com
-cert.pem -C mychannel -n public_record --peerAddresses peer0.org2.example.com:9051
--tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrg
anizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt -c '{"Args":["Ge
tRecord","SA-VAC-COUNT"]}'
2021-05-18 14:10:54.328 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chainc
ode invoke successful. result: status:200 payload:"{\"key\":\"SA-VAC-COUNT\",\"value
\":\"123456\"}"
```

Figure 5. Peer0 of Org2 executes the transaction "GetRecord" to retrieve a public record shared by Org1 with key = SA-VAC-COUNT.

```
root@node1:~# docker exec cli peer chaincode invoke -o orderer.example.com:7050 --tl
s true --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrg
anizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com
-cert.pem -C mychannel -n public_record --peerAddresses peer0.org2.example.com:9051
--tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrg
anizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt -c '{"Args":["Ge
tAll"]}'
2021-05-18 14:11:45.857 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chainc
ode invoke successful. result: status:200 payload:"[{\"Key\":\"SA-COVID-COUNT\",\"Re
c\":{\"key\":\"SA-COVID-COUNT\",\"value\":\"654321\"}},{\"Key\":\"SA-VAC-COUNT\",\"R
ec\":{\"key\":\"SA-VAC-COUNT\",\"value\":\"123456\"}}]"
```

Figure 6. Peer0 of Org2 executes the transaction "GetAll" to retrieve all public key–value pairs shared by Org1.

```
root@node1:~# docker exec cli peer chaincode invoke -o orderer.example.com:7050 --tl
s true --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrg
anizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com
-cert.pem -C mychannel -n public_record --peerAddresses peer0.org2.example.com:9051
--tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOrg
anizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt -c '{"Args":["Se
tRecord","SA-VAC-COUNT","0"]}'
Error: endorsement failure during invoke. response: status:500 message:"Unauthorized
 Org2MSP"
```

Figure 7. Peer0 of Org2 is not authorized to call "SetRecord" in the public_record smart contract belonging to Org1.

Second, we show an execution of the smart contract for sharing the private data of Org1, namely, "private_record." The client of Org2 executed a "SetRecord" transaction via Peer0 of Org2, sending a private data collection to Peer0 of Org1 only (see Figure 8). The arguments of the transaction are sent as transient data to prevent one from storing them in the transaction record inside the blockchain. These data represent a travel request for an individual containing necessary information, such as passport details, vaccination certificates, and cancelable fingerprint templates, which may be sent as a JSON object. The key for the private data collection is the passport number of the individual. This private data collection is sent to Org1 to retrieve (see Figure 9). Clients of other organizations, such as Org2, are not able to retrieve the private data collection, even if its key is known and they may retrieve its hash only (see Figure 10).

```
root@node1:~# export KEYVALUE=$(echo -n "{\"key\":\"SA_Passport_P1\",\"value\":\"Per
sonalRecordJSON\"}" | base64 | tr -d \\n)
root@node1:~# docker exec cli peer chaincode invoke -o orderer.example.com:7050 --tl
s true --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrg
anizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com
-cert.pem -C mychannel -n private_record --peerAddresses peer0.org2.example.com:9051
 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOr
ganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt --peerAddresses
 peer0.org1.example.com:9051 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledg
er/fabric/peer/crypto/peerOrganizations/org1.example.com/peers/peer0.org1.example.co
m/tls/ca.crt -c '{"Args":["SetRecord"]}' --transient "{\"keyvalue\":\"$KEYVALUE\"}"
2021-05-18 17:12:29.668 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chainc
ode invoke successful. result: status:200 payload:"PersonalRecordJSON"
```

Figure 8. Peer0 of Org2 executes the transaction "SetRecord" to send a private data collection to Org1 with the key=SA_Passport_P1.

```
root@node0:/mydata/fabric/fabric-samples/5host-deployment# docker exec cli peer chai
ncode invoke -o orderer.example.com:7050 --tls true --cafile /opt/gopath/src/github.
com/hyperledger/fabric/peer/crypto/ordererOrganizations/example.com/orderers/orderer
.example.com/msp/tlscacerts/tlsca.example.com-cert.pem -C mychannel -n private_recor
d --peerAddresses peer0.org1.example.com:9051 --tlsRootCertFiles /opt/gopath/src/git
hub.com/hyperledger/fabric/peer/crypto/peerOrganizations/org1.example.com/peers/peer
0.org1.example.com/tls/ca.crt -c '{"Args":["GetRecord","SA_Passport_P1"]}'
2021-05-18 17:14:27.018 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chainc
ode invoke successful. result: status:200 payload:"PersonalRecordJSON"
```

Figure 9. Peer0 of Org1 executes the transaction "GetRecord" to retrieve the private data collection sent by Org2 with the key=SA_Passport_P1.

```
root@node1:~# docker exec cli peer chaincode invoke -o orderer.example.com:7050 --tl
s true --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/ordererOrg
anizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com
-cert.pem -C mychannel -n private_record --peerAddresses peer0.org2.example.com:9051
 --tlsRootCertFiles /opt/gopath/src/github.com/hyperledger/fabric/peer/crypto/peerOr
ganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt -c '{"Args":["G
etRecord","SA_Passport_P1"]}'
Error: endorsement failure during invoke. response: status:500 message:"Failed to ge
t asset: SA_Passport_P1 with error: GET_STATE failed: transaction ID: 341f607cc7f9c5
2da8a46d0bfbaacc9de7c87897e98ff72affccf6fff268bec6: private data matching public has
h version is not available. Public hash version = {BlockNum: 14, TxNum: 0}, Private
data version = <nil>"
```

Figure 10. Peer0 of Org2 is not able to retrieve private data collections sent to Org1.

5. Applications

The World Health Organization (WHO) encourages national agencies to share up-to-date statistics related to the progression of the COVID-19 pandemic [45]. This includes the number of new cases, recovered cases, deaths, and health service capacity and performance.

The SPIN framework functions as a facilitator to the timely sharing of such data. This feature enables a wide range of applications that can potentially be useful for risk mitigation. Using data from our framework, countries may maintain an awareness of the aggregate level of risk associated with the relaxation of travel restrictions. For example, estimating the number of infected and/or susceptible travelers who entered a country may help to predict whether the current health service capacity can accommodate the potential risk from imported cases [15,46]. In this section, we show that some simple statistics can be derived from the data (public and private) that are supplied by our framework and have significant utility for risk mitigation.

Number of susceptible individuals: Assuming people who have taken the vaccine or have recovered from COVID-19 are completely immune to the disease, the number of susceptible individuals in a given tourism site (a country, city, or place) may be computed by counting the total number of people who have not taken the vaccine nor recovered from COVID-19 at that site. We use the notion $|\cdot|$ for the cardinality of a set. The fraction of susceptible individuals in a given tourism site s may be computed from the total number of visitors to s as follows:

$$\frac{|S_s|}{|A_s|}$$

where S_s is the set of susceptible individuals in the tourism site s, and A_s is the set of all the individuals in s.

Probability of being susceptible: A traveler i may be partially immune to the disease, i.e., either by being recovered from an infection or by taking a vaccine with some known effectiveness. COVID-19 vaccine efficacy may be known from the national health authorities or from the related literature [47–49]. Let $p_{im}(i)$ be the probability that a traveler i is immune to COVID-19 [50]. We say that each traveler i is associated with a probability of being susceptible, $p_{su}(i)$:

$$p_{su}(i) = 1 - p_{im}(i)$$

With no prior knowledge about i's COVID-19 vaccination records or knowledge about recovery from a previous COVID-19, $p_{su}(i)$ will always be assumed to be 1.

Probability of being infected: Let c_i be the country of departure for traveler i. With no prior knowledge about i's COVID-19 vaccination records or recovery from a previous COVID-19 infection, i.e., $p_{su}(i) = 1$, the probability that i is infected, denoted as $p_{in}(i)$, may be approximated from the set of COVID-19 active cases in i's country of departure, denoted as I_c, and the set of population of c_i, denoted as C_c, as follows:

$$p_{in}(i) = \frac{|I_c|}{|C_c|}$$

However, traveler i may be partially immune to COVID-19, i.e., having been vaccinated or recovered from an infection. In this case, the probability that i is infected given that she has been vaccinated or recovered from an infection $p'(i)$ may be approximated from $p_{su}(i)$ and $p_{in}(i)$ as follows:

$$p'(i) = p_{su}(i) * p_{in}(i)$$

Expected number of infected tourists: Given a set of travelers $T = \{1, \ldots, n\}$ entering a country from a port of entry x, each traveler i is associated with a probability of being infected $p'(i)$. The expected number of infected tourists at a port of entry x can be computed as follows:

$$\sum_{i=1}^{n} p'(i)$$

Similarly, the set T may be any set of travelers sharing certain properties, e.g., a set of travelers entering a tourism site, a set of travelers holding a certain type of visa, or a set

of travelers having a higher priority to enter the country. We show in this section that the aggregate level of risk may be informed from the data supplied by our framework. Such information raises awareness about the disease and guides risk mitigation plans. Decisions related to applying control measures, such as social distancing and partial business closure, may also be informed from the presented statistics.

6. Related Work

A wide range of papers have been published intending to address the challenges associated with the COVID-19 pandemic. In the next three subsections, we present an overview of the recent related work to our paper. In Section 6.1, we provide an overview of recent techniques aiming to restrain the COVID-19 pandemic. In Section 6.2, we discuss related work targeting Health Information Exchange (HIE) challenges, and in Section 6.3 we present research related to generic Privacy-Preserving Information Sharing Techniques.

6.1. Restraining COVID-19

A wide range of papers have been published aiming to address the challenges related to COVID-19, mainly for diagnosing COVID-19 [51–54], collecting public web data [55], contact tracing [56–58], social distancing [59,60], vaccine delivery [61–63], and immunity passports [8–15]. Kalla et al. [64] discussed the different use cases for blockchain technology to fight against COVID-19. Among the discussed use cases, our framework is closely related to those developing immunity passports. Several immunity passport papers [8–10] use self-sovereign identity (SSID) and verifiable credentials techniques to allow individuals to have full control over their private data, which is a desirable feature. However, these solutions require offering a mechanism, such as a mobile app, to allow individuals to practice this control, which may not be feasible for people across the globe.

A closely related work to our approach [11] proposed using blockchain to share vaccination records for individuals. The authors of this work proposed using the users' iris template along with users' date of birth and gender to uniquely identify and authenticate individuals. To preserve the privacy of individuals' biometric information, the authors proposed using locality-sensitive hashing (LSH) to hash the iris templates before being written to the public ledger. Unlike our approach, which utilizes private messages, this approach relies on publishing health record information of individuals publicly in the blockchain, which makes these records accessible to anyone who acquires the user's iris template along with her date of birth and gender. This could potentially lead to the irreversible exposure of the users' private health records.

In another work [13], the authors introduced a secure antibody certificate system (SecureABC) that uses a standard public-key signature scheme to ensure the binding and authenticity of certificates. A limitation of this work is that it relies on individual's photo and name for verification, which might not be sufficient. To tackle this issue, we proposed using biometric information such as fingerprints to uniquely identify individuals.

Hasan et al. [8] provided a blockchain solution to issue and publish COVID-19 vaccine and test certificates using Ethereum smart contracts. These smart contracts execute actions, such as adding a test center, issuing a test result, and updating patient information. Data stored on the blockchain are mainly notifications about the execution of smart contracts. Private information is stored off-chain using the InterPlanetary File System (IPFS) with proxy re-encryption schemes. Moreover, it relies on SSID to allow individuals to have full control over their private information. Our proposed framework differs in various ways. First, it employs a permissioned blockchain, while Ethereum is a public blockchain that is more vulnerable to attacks and has lower throughput and scalability compared to permissioned blockchain [25]. Second, their proposed solution consists of several components that are a blockchain, SSID, and IPFS, which may not be easily adaptable across the globe. Third, our framework employs cancelable fingerprint templates to authenticate individuals. Their solution stores individuals' biometric information with their unique Ethereum address (EA) on-chain, but details are not provided. Fourth, our

solution is more flexible as it allows peers to send any kind of public data in the form of key–value pairs, while their solution is limited to events about executed smart contracts.

Eisenstadt et al. [9] developed a mobile app to facilitate issuing and verifying COVID-19 test and vaccine certificates. Their solution is limited to sharing private data, which are test and vaccine certificates, and does not support sharing public data. It utilizes Verifiable Credentials to issue digital certificates and allow individuals to store their private documents on their phones or their preferred cloud providers. They used a permissioned blockchain to store public keys and the hashes of the documents for verification purposes. A limitation of their proposed solution is that it requires individuals to hold smartphones to present a QR code for their certificates. Without a smartphone, their solution allows for simple document checking which is not sufficient for verifying the test and vaccine certificates. Furthermore, it is not clear how their solution addresses the case of fraudulent individuals who may hold the mobile app and pretend to be someone else.

Butler et al. [15] proposed randomized health certificates that are based on differential privacy to protect against immunity-based discrimination. It allows for collecting aggregate transmission risk statistics. This solution is suitable for use cases that do not require knowing the identity of individuals.

In another work [14], the authors proposed building an end-to-end protocol for sharing COVID-19 test results and verification. Unlike other proposed techniques, this approach does not rely on any distributed ledger to share result information. It uses individuals' smartphones to download and hold the encrypted certificates that were issued to them by public health providers. One of the drawbacks of this work as stated by its authors is its limited capability to only verify a testing or immunization result and not support any arbitrary credential verification. In addition, the proposed protocol relies on using smartphones for verification, which could be challenging for elderly individuals and individuals with limited income.

In [12], the authors proposed a framework to support digital health passports in an effort to alleviate the traveling problem during the COVID-19 pandemic using a private blockchain. The framework consists of three main components: (1) local healthcare facilities that issue digital health passports for the travelers; (2) health service authorities (at the country level) that have full access rights on the blockchain, including registered issued digital health passports; (3) blockchain members (such as airline companies, airport security, and border control authorities) that have only read rights on the blockchain, mainly to check if a person is the holder of a valid digital health passport. In addition, the framework uses smartphones to preserve the individual's privacy. The proposed framework suffers from the limitations of privacy issues, including the leakage of the history of traveler exams in addition to the fact that any blockchain member can possibly obtain an individual's information, which is not of concern to the given blockchain member.

The authors of another work [65] suggested a blockchain solution to manage the performance of self tests for COVID-19 and the sharing of the results. Encrypted versions of the test results are stored in the blockchain. The paper lacks major details. For instance, there are no details about the implementation of the suggested software that executes the self tests. There is also no discussion about how the credibility of test results would be ensured, and how authorities would decrypt the test results and verify them.

Bansal et al. [66] proposed an abstract design using blockchain to handle the challenges of digital immunity certificates and contact tracing, without providing important design details or the concrete implementation of their solution.

In [55], the authors proposed a blockchain-based tracking system for sharing COVID-19 information from different sources. The proposed system mitigates the spread of falsified or modified data by utilizing Ethereum smart contracts to track the reported data from trusted resources. Unlike our approach, this system is suitable for sharing only public data such as the number of new and recovered cases, but is not suitable for exchanging private data such as vaccination and test certificates.

Shazad et al. [67] conducted a systematic literature review to identify the challenges associated with building reliable COVID-19 software. The authors then proposed using blockchain to gather and negotiate the COVID-19 systems requirements. The proposed approach is effective at improving the operational process of COVID-19 software requirement engineering. However, such an approach does not target our problem, which is sharing public and private data regarding COVID-19.

6.2. Health Information Exchange

Health information exchange (HIE) solutions have been studied extensively in the literature [68]. It allows healthcare practitioners to access and share patients' information. It defines standards and architectures to provide secure and efficient access of data within national boundaries. HIE systems are either centralized, such as cloud-based solutions [69,70], or decentralized, such as blockchain-based solutions [71–74]. A major difference between most HIE solutions and SPIN is that the latter focuses on sharing health information across nations, which imposes additional challenges to authenticating and verifying information about individuals. We highlight the similarities and differences between SPIN and some related HIE blockchain-based solutions as follows. BlocHIE [72] maintains two loosely coupled blockchains: one for medical records and the other for personal health data. In contrast to SPIN, individuals directly interact with the blockchain network for various tasks, such as signing medical records and submitting personal health data. This design is not feasible for an across-nation solution, as individuals may not be able to access the blockchain network. Similar to BlocHIE, SPIN stores private data off-chain and records their hashes on the blockchain network as evidence of the transaction. However, it is not clear how the private off-chain data are shared across hospitals in BlocHIE. Another paper reports on M-Blocks [73], which uses a private blockchain to store and manage patients' data. The paper lacks details about how hospitals will share data across private blockchain networks. Other authors have proposed ssHealth [74], a healthcare system utilizing blockchain and edge computing technologies to share information. It consists of entities that generate and process health data, such as health service providers, medical Internet of Things (IoT) devices, and internal edge nodes. Patient information is stored in the blockchain network to be accessed by other entities, such as insurance companies, pharmacies, and government health agencies. In contrast to ssHealth, SPIN stores the hash of private data on the blockchain network and not the actual data.

6.3. Generic Blockchain and Privacy-Preserving Information Sharing Techniques

Sharing information in the blockchain is not limited to healthcare data. Researchers also proposed techniques for sharing Industrial IoT (IIoT) transactions [75]. The authors of [75] proposed a technique (Fair-Pack) that allows for time-efficient information sharing between IIoT devices. Although Fair-Pack is not targeting HIE, the proposed approach can be used to reduce the average response time in permissioned blockchain networks.

Another approach [76] provides a mechanism for multi-keyword search over encrypted data on the blockchain. Such a technique is not applicable to our approach, since our approach stores only the hash of the private data on the blockchain network and not the actual data. As mentioned earlier, in our approach, the actual data are sent directly to the travel destination country without being pushed to the blockchain.

7. Conclusions

In this paper, we introduce SPIN, a framework using a permissioned blockchain to share information, which is effective in combating COVID-19 spread across the globe. The SPIN framework enables the sharing of public data through a permissioned ledger, which is visible to all peers, and private data through private data collections, which are only visible to peers who are authorized to view them. We leveraged cancelable fingerprint templates to authenticate private information about travelers. The scalability, efficiency, security, and privacy of our introduced framework was analyzed. A prototype of SPIN

was implemented using Hyperledger Fabric, and the full source code is publicly available to ensure the reproducibility of this work. To further illustrate the utility of our framework, the paper presents a series of simple statistics that can be computed from the public and private data that are supplied by the framework. Such statistics may guide, in real-world scenarios, decisions related to applying control measures, such as social distancing and partial business closure. Deploying the SPIN framework could effectively facilitate efforts to fasten the alleviation of travel restrictions while limiting the spread of COVID-19 in particular and pandemics in general.

Author Contributions: Conceptualization, Y.A., A.A. (Abdulmajeed Alameer) and M.A.; Formal analysis, M.A. and A.A. (Abdulaziz Almaslukh); Methodology, A.A. (Abdulmajeed Alameer); Software, Y.A. and A.A. (Abdulmajeed Alameer); Supervision, Y.A.; Writing—original draft, Y.A., A.A. (Abdulmajeed Alameer), M.A. and A.A. (Abdulaziz Almaslukh); Writing—review & editing, Y.A., A.A. (Abdulmajeed Alameer), M.A. and A.A. (Abdulaziz Almaslukh). All authors have read and agreed to the published version of the manuscript.

Funding: This research project was supported by a grant from the "Research Center of College of Computer and Information Sciences", Deanship of Scientific Research, King Saud University.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chinazzi, M.; Davis, J.T.; Ajelli, M.; Gioannini, C.; Litvinova, M.; Merler, S.; y Piontti, A.P.; Mu, K.; Rossi, L.; Sun, K.; et al. The Effect of Travel Restrictions on the Spread of the 2019 Novel Coronavirus (COVID-19) Outbreak. *Science* **2020**, *368*, 395–400.
2. Linka, K.; Peirlinck, M.; Sahli Costabal, F.; Kuhl, E. Outbreak Dynamics of COVID-19 in Europe and The Effect of Travel Restrictions. *Comput. Methods Biomech. Biomed. Eng.* **2020**, *23*, 710–717.
3. Chen, L.H.; Freedman, D.O.; Visser, L.G. COVID-19 Immunity Passport to Ease Travel Restrictions? *J. Travel Med.* **2020**, *27*, taaa085.
4. Oum, T.H.; Wang, K. Socially Optimal Lockdown and Travel Restrictions for Fighting Communicable Virus Including COVID-19. *Transp. Policy* **2020**, *96*, 94–100.
5. Devi, S. Travel Restrictions Hampering COVID-19 Response. *Lancet* **2020**, *395*, 1331–1332, doi:10.1016/s0140-6736(20)30967-3.
6. Narayanan Gopalakrishnan, B.; Peters, R.; Vanzetti, D. *COVID-19 and Tourism: Assessing the Economic Consequences*; United Nations Conference on Trade and Development: Geneva, Switzerland, 2020.
7. COVID-19 Travel Regulations Map (Powered by Timatic). Available online: https://www.iatatravelcentre.com/world.php (accessed on 19 May 2021).
8. Hasan, H.R.; Salah, K.; Jayaraman, R.; Arshad, J.; Yaqoob, I.; Omar, M.; Ellahham, S. Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates. *IEEE Access* **2020**, *8*, 222093–222108 .
9. Eisenstadt, M.; Ramachandran, M.; Chowdhury, N.; Third, A.; Domingue, J. COVID-19 Antibody Test/Vaccination Certification: There's an App for That. *IEEE Open J. Eng. Med. Biol.* **2020**, *1*, 148–155.
10. Hernández-Ramos, J.L.; Karopoulos, G.; Geneiatakis, D.; Martin, T.; Kambourakis, G.; Fovino, I.N. Sharing Pandemic Vaccination Certificates Through Blockchain: Case study and Performance Evaluation. *arXiv* **2021**, arXiv:2101.04575.
11. Chaudhari, S.; Clear, M.; Tewari, H. Framework for a DLT Based COVID-19 Passport. *arXiv* **2021**, arXiv:cs.CR/2008.01120. .
12. Angelopoulos, C.M.; Damianou, A.; Katos, V. DHP Framework: Digital Health Passports Using Blockchain. *arXiv* **2020**, arXiv:2005.08922.
13. Hicks, C.; Butler, D.; Maple, C.; Crowcroft, J. SecureABC: Secure AntiBody Certificates for COVID-19. *arXiv* **2020**, arXiv:cs.CR/2005.11833. .
14. Singh, A.; Raskar, R. Verifiable Proof of Health using Public Key Cryptography. *arXiv* **2020**, arXiv:2012.02885.
15. Butler, D.; Hicks, C.; Bell, J.; Maple, C.; Crowcroft, J. Differentially Private Health Tokens for Estimating COVID-19 Risk. *arXiv* **2020**, arXiv:2006.14329.
16. Señor, I.C.; Fernández-Alemán, J.L.; Toval, A. Are personal health records safe? A review of free web-accessible personal health record privacy policies. *J. Med. Internet Res.* **2012**, *14*, e114.
17. Vandenberg, O.; Martiny, D.; Rochas, O.; van Belkum, A.; Kozlakidis, Z. Considerations for diagnostic COVID-19 tests. *Nat. Rev. Microbiol.* **2021**, *19*, 171–183.
18. Rocher, L.; Hendrickx, J.M.; De Montjoye, Y.A. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat. Commun.* **2019**, *10*, 1–9.
19. Available online: https://github.com/yaz1/COVID-19-Data-Sharing-Framework (accessed on 19 May 2021).
20. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Technical Report; Manubot: San Francisco, CA, USA, 2019.
21. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375.
22. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187.

23. Shahzad, M.; Wang, S.; Deng, G.; Yang, W. Alignment-Free Cancelable Fingerprint Templates with Dual Protection. *Pattern Recognit.* **2021**, *111*, 107735, https://doi.org/10.1016/j.patcog.2020.107735.
24. Bischoff, P. Biometric Data Collection by Country: What's Collected, How Is It Used? Available online: https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/ (accessed on 19 May 2021).
25. Wüst, K.; Gervais, A. Do You Need a Blockchain? In Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; IEEE: New York, NY, USA, 2018; pp. 45–54.
26. Longo, R.; Podda, A.S.; Saia, R. Analysis of a Consensus Protocol for Extending Consistent Subchains on the Bitcoin Blockchain. *Computation* **2020**, *8*, 67.
27. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
28. Hyperledger Fabric—Hyperledger. Available online: https://www.hyperledger.org/use/fabric (accessed on 17 May 2021).
29. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654.
30. Hellman, M. An Overview of Public Key Cryptography. *IEEE Commun. Soc. Mag.* **1978**, *16*, 24–32.
31. Ongaro, D.; Ousterhout, J. In Search of an Understandable Consensus Algorithm. In Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference, Philadelphia, PA, USA, 19–20 June 2014; USENIX ATC'14; USENIX Association: Berkeley, CA, USA, 2014; pp. 305–320.
32. Endorsement Policies—Hyperledger Fabric Docs Master Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/endorsement-policies.html (accessed on 19 May 2021)
33. Private Data—Hyperledger Fabric Docs Master Documentation Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html (accessed on 19 May 2021).
34. ISO. ISO/IEC 24745:2011: Biometric Information Protection. In *Standard*; International Organization for Standardization: Geneva, Switzerland, 2011.
35. Lazarick, R.; Cambier, J.L. Biometrics in the Government Sector. In *Handbook of Biometrics*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 461–478.
36. Acharya, L.; Kasprzycki, T. *Biometrics and Government*; Library of Parliament: Ottawa, ON, Canada, 2010.
37. Wang, C.; Chu, X. Performance Characterization and Bottleneck Analysis of Hyperledger Fabric. *arXiv* **2020**, arXiv:2008.05946.
38. Dreyer, J.; Fischer, M.; Tönjes, R. Performance Analysis of Hyperledger Fabric 2.0 Blockchain Platform. In Proceedings of the Workshop on Cloud Continuum Services for Smart IoT Systems, Virtual Event, Japan, 16 November 2020; pp. 32–38.
39. Guggenberger, T.; Sedlmeir, J.; Fridgen, G.; Luckow, A. An In-Depth Investigation of Performance Characteristics of Hyperledger Fabric. *arXiv* **2021**, arXiv:2102.07731.
40. Cachin, C.; Vukolić, M. Blockchain Consensus Protocols in the Wild. *arXiv* **2017**, arXiv:1707.01873.
41. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1432–1465.
42. Duplyakin, D.; Ricci, R.; Maricq, A.; Wong, G.; Duerig, J.; Eide, E.; Stoller, L.; Hibler, M.; Johnson, D.; Webb, K.; et al. The Design and Operation of CloudLab. In Proceedings of the USENIX Annual Technical Conference (ATC), Renton, WA, USA, 10–12 July 2019; pp. 1–14.
43. Access Control Lists (ACL)—Hyperledger Fabric Docs Master Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/access_control.html (accessed on 17 May 2021).
44. Writing Your First Chaincode—Hyperledger Fabric Docs Master Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/chaincode4ade.html (accessed on 17 May 2021).
45. Organization, W.H. *Considerations for Implementing a Risk-Based Approach to International Travel in the Context of COVID-19: Interim Guidance*; Technical Report; World Health Organization: Geneva, Switzerland, 2020.
46. Alrasheed, H.; Althnian, A.; Kurdi, H.; Al-Mgren, H.; Alharbi, S. COVID-19 Spread in Saudi Arabia: Modeling, Simulation and Analysis. *Int. J. Environ. Res. Public Health* **2020**, *17*, 7744.
47. COVID-19 Vaccine Efficacy Summary. Available online: http://www.healthdata.org/covid/covid-19-vaccine-efficacy-summary (accessed on 19 May 2021).
48. Knoll, M.D.; Wonodi, C. Oxford–AstraZeneca COVID-19 Vaccine Efficacy. *Lancet* **2021**, *397*, 72–74.
49. Voysey, M.; Clemens, S.A.C.; Madhi, S.A.; Weckx, L.Y.; Folegatti, P.M.; Aley, P.K.; Angus, B.; Baillie, V.L.; Barnabas, S.L.; Bhorat, Q.E.; et al. Safety and Efficacy of the ChAdOx1 nCoV-19 Vaccine (AZD1222) Against SARS-CoV-2: An Interim Analysis of Four Randomised Controlled Trials in Brazil, South Africa, and the UK. *Lancet* **2021**, *397*, 99–111.
50. Randolph, H.E.; Barreiro, L.B. Herd immunity: Understanding COVID-19. *Immunity* **2020**, *52*, 737–741.
51. Udugama, B.; Kadhiresan, P.; Kozlowski, H.N.; Malekjahani, A.; Osborne, M.; Li, V.Y.; Chen, H.; Mubareka, S.; Gubbay, J.B.; Chan, W.C. Diagnosing COVID-19: The Disease and Tools for Detection. *ACS Nano* **2020**, *14*, 3822–3835.
52. Maghdid, H.S.; Asaad, A.T.; Ghafoor, K.Z.; Sadiq, A.S.; Mirjalili, S.; Khan, M.K. Diagnosing COVID-19 Pneumonia from X-Ray and CT Images Using Deep Learning and Transfer Learning Algorithms. In *Multimodal Image Exploitation and Learning 2021*; Agaian, S.S., Asari, V.K., DelMarco, S.P., Jassim, S.A., Eds.; International Society for Optics and Photonics, SPIE: Bellingham, WA, USA, 2021; Volume 11734, pp. 99–110, doi:10.1117/12.2588672.

53. Chowdhury, M.E.; Rahman, T.; Khandakar, A.; Mazhar, R.; Kadir, M.A.; Mahbub, Z.B.; Islam, K.R.; Khan, M.S.; Iqbal, A.; Al Emadi, N.; et al. Can AI Help in Screening Viral and COVID-19 Pneumonia? *IEEE Access* **2020**, *8*, 132665–132676.
54. He, X.; Yang, X.; Zhang, S.; Zhao, J.; Zhang, Y.; Xing, E.; Xie, P. Sample-Efficient Deep Learning for Covid-19 Diagnosis Based on CT Scans. *MedRxiv* **2020**, https://doi.org/10.1101/2020.04.13.20063941 .
55. Marbouh, D.; Abbasi, T.; Maasmi, F.; Omar, I.A.; Debe, M.S.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. *Arab. J. Sci. Eng.* **2020**, *45*, 1–17.
56. Shubina, V.; Ometov, A.; Lohan, E.S. Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control. In Proceedings of the 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Brno, Czech Republic, 5–7 October 2020; IEEE: New York, NY, USA, 2020, pp. 229–235.
57. Rajasekar, S.J.S. An Enhanced IoT Based Tracing and Tracking Model for COVID-19 Cases. *SN Comput. Sci.* **2021**, *2*, 1–4.
58. Elmesalawy, M.M.; Salama, A.I.; Anany, M. Tracy: Smartphone-based Contact Tracing Solution that Supports Self-investigation to Limit the Spread of COVID-19. In Proceedings of the 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 24–26 October 2020; IEEE: New York, NY, USA, 2020; pp. 623–628.
59. Cao, Y.; Dhekne, A.; Ammar, M. 6Fit-A-Part: A Protocol for Physical Distancing on a Custom Wearable Device. In Proceedings of the 2020 IEEE 28th International Conference on Network Protocols (ICNP), Madrid, Spain, 13–16 October 2020; IEEE: New York, NY, USA, 2020; pp. 1–12.
60. Istomin, T.; Leoni, E.; Molteni, D.; Murphy, A.L.; Picco, G.P.; Griva, M. Janus: Efficient and Accurate Dual-radio Social Contact Detection. *arXiv* **2021**, arXiv:2101.01514.
61. Musamih, A.; Jayaraman, R.; Salah, K.; Hasan, H.; Yaqoob, I.; Al-Hammadi, Y. Blockchain-Based Solution for Distribution and Delivery of COVID-19 Vaccines. *IEEE Access* **2021**, *9*, 71372–71387.
62. Antal, C.D.; Cioara, T.; Antal, M.; Anghel, I. Blockchain Platform for COVID-19 Vaccine Supply Management. *arXiv* **2021**, arXiv:2101.00983.
63. Barakat, S.; Al-Zagheer, H. Blockchain Tracking System of COVID-19 Vaccination. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 5059–5067.
64. Kalla, A.; Hewa, T.; Mishra, R.A.; Ylianttila, M.; Liyanage, M. The Role of Blockchain to Fight Against COVID-19. *IEEE Eng. Manag. Rev.* **2020**, *48*, 85–96, doi:10.1109/EMR.2020.3014052.
65. Capece, G.; Bazzica, P. Vpassport: A Digital Architecture to Support Social Restart During the SARS-CoV-2 Pandemic. *Sustainability* **2021**, *13*, 3945.
66. Bansal, A.; Garg, C.; Padappayil, R.P. Optimizing the Implementation of COVID-19 "Immunity Certificates" Using Blockchain. *J. Med. Syst.* **2020**, *44*, 1–2.
67. Shahzad, B.; Javed, I.; Shaikh, A.; Sulaiman, A.; Abro, A.; Ali Memon, M. Reliable Requirements Engineering Practices for COVID-19 Using Blockchain. *Sustainability* **2021**, *13*, 6748, doi:10.3390/su13126748.
68. Hersh, W.R.; Totten, A.M.; Eden, K.B.; Devine, B.; Gorman, P.; Kassakian, S.Z.; Woods, S.S.; Daeges, M.; Pappas, M.; McDonagh, M.S. Outcomes from Health Information Exchange: Systematic Review and Future Research Needs. *JMIR Med. Inform.* **2015**, *3*, e5215.
69. Wang, X.; Tan, Y. Application of Cloud Computing in the Health Information System. In Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), Taiyuan, China, 22–24 October 2010; IEEE: New York, NY, USA, 2010; Volume 1, pp. V1–179.
70. Zhou, J.; Cao, Z.; Dong, X.; Lin, X. TR-MABE: White-Box Traceable and Revocable Multi-authority Attribute-based Encryption and Its Applications to Multi-level Privacy-preserving e-Healthcare Cloud Computing Systems. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM) Kowloon, Hong Kong, 26 April–1 May 2015; IEEE: New York, NY, USA, 2015; pp. 2398–2406.
71. Chukwu, E.; Garg, L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access* **2020**, *8*, 21196–21214.
72. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlocHIE: A Blockchain-based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (Smartcomp), Taormina, Sicily, Italy, 18–20 June 2018; IEEE: New York, NY, USA, 2018; pp. 49–56.
73. Alamir, O.; Raman, R.; Alhashimi, A.F.; Almoaber, F.A.; Alremeithi, A.H. M-Blocks (Medical Blocks): A Blockchain based Approach for Patient Record Management Using IBM Hyperledger. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019; IEEE: New York, NY, USA, 2019; pp. 24–31.
74. Abdellatif, A.A.; Al-Marridi, A.Z.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Refaey, A. ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems . *IEEE Netw.* **2020**, *34*, 312–319.
75. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-Based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7639–7649, doi:10.1109/TII.2020.3046129.
76. Jiang, S.; Cao, J.; McCann, J.A.; Yang, Y.; Liu, Y.; Wang, X.; Deng, Y. Privacy-Preserving and Efficient Multi-Keyword Search over Encrypted Data on Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 405–410, doi:10.1109/Blockchain.2019.00062.