frontiers | Frontiers in Blockchain

TYPE Methods
PUBLISHED 13 March 2023
DOI 10.3389/fbloc.2023.1075083

OPEN ACCESS

EDITED BY
Tin-Chih Toly Chen,
National Yang Ming Chiao Tung University, Taiwan

REVIEWED BY
Alex Butean,
Lucian Blaga University of Sibiu, Romania
Yu Cheng Wang,
Chaoyang University of Technology, Taiwan

*CORRESPONDENCE
Merlin George,
sendtomerlin@gmail.com

SPECIALTY SECTION
This article was submitted to Blockchain in Industry, a section of the journal Frontiers in Blockchain

RECEIVED 20 October 2022
ACCEPTED 24 February 2023
PUBLISHED 13 March 2023

CITATION
George M and Chacko AM (2023), Health Passport: A blockchain-based PHR-integrated self-sovereign identity system. *Front. Blockchain* 6:1075083. doi: 10.3389/fbloc.2023.1075083

Health Passport: A blockchain-based PHR-integrated self-sovereign identity system

Merlin George* and Anu Mary Chacko

Department of Computer Science and Engineering, National Institute of Technology, Kozhikode, Kerala, India

During the COVID-19 pandemic, it was necessary to validate a person's health status along with their identity to permit travel. This was facilitated *via* paper-based certificates and centralized digital apps. Even after COVID-19, it is anticipated that such health status verifications will be required for travel and other purposes. As a result, there needs to be an additional credential, a "Health Passport," that establishes whether a person satisfies the health requirements for various purposes. Digital credentials so prepared should be trustable, unforgeable, and verifiable. The Health Passport should be designed to protect the end-users' privacy and give people control over the data they use to confirm their credentials. This article explores the requirements for a generalized Health Passport system and uses agent-oriented modeling (AOM) to design a blockchain-based self-sovereign identity (SSI) system integrated with the Personal Health Record (PHR) to address this requirement. The article demonstrates the feasibility of the solution by implementing a proof of concept on Hyperledger Indy and Aries, integrated with the PHR – MediTrans. Credential issuance and verification time were calculated, and it was observed that the time overhead was minimal. This solution allows users to verify their credentials with the verifier without revealing any significant personal information. Our solution can be integrated into any PHR solution as the SSI solution is added as a plugin to the PHR accessible *via* a mobile/web app.

KEYWORDS

blockchain technology, decentralization, self-sovereign identity (SSI), verifiable credentials (VCs), zero-knowledge proof (ZKP)

1 Introduction

During the last 2 years, organizations across the world had to accelerate the digitalization of the healthcare sector owing to the COVID-19 pandemic. The need for Personal Health Records (PHRs) was felt more as patients relied more on teleconsultations. The PHR, if used, can provide easy access to one's health records, vaccine records, and test results. During COVID-19 and post-COVID-19, the results which confirm a person's immunization, testing, or recovery status determined their access to different places. It looks like this requirement of knowing a person's health status to determine their entry is going to stay even post-COVID-19. Thus, along with a passport that proves a person's identity, there needs to be another credential, a "Health Passport," which determines whether a person meets the governmental health conditions to allow entry/exit.

Numerous centrally maintained credential systems have emerged worldwide for COVID-19 vaccination record maintenance (Wang and Ping., 2022), and most of them provide downloadable vaccine certificates that can be saved or printed out. Various apps

have been developed during COVID-19, which enable users to access records such as test results and vaccination certificates (Song et al., 2022). Although these options are handy, establishing their legitimacy can take time and effort. These certificates can be easily forged and misused, disclosing personal choices and violating an individual's privacy. The storage of digital health information in a centralized database may pose ethical, security, and privacy concerns. The apps that use QR code scanning to verify a vaccination certificate share the user identity and diagnosis information with the verifiers, thereby not safeguarding the privacy of user information. These solutions were tailor-made for COVID-19 times and did not consider the general health credential requirement. COVID-19 has taught us that in the times ahead, validating health may be necessary; thus, an individual needs to have a "credential" to prove their health status. This credential should satisfy the verification requirement while protecting the user's privacy as far as possible.

Health credentials should contain enough identity and context information to make them a powerful unit of highly portable, valuable, and self-contained data. It is desirable that during the verification of these credentials, the verifier should be able to verify whether requirements are met without revealing additional data. Thus, health credential that ensures trustworthiness, user-centricity, and data security is the need of the hour.

A decentralized architecture is needed by hospitals and governments to bring in trustworthy validation of credentials (Bahar et al., 2020). The architecture should allow hospitals and organizations to issue digital health credentials to patients/users that could be shared with and verified by appropriate authorities. A distributed ledger, with strict governance practices and verification of signatures, can assure the participants that the process is trustworthy. This can be done using blockchain technology, whose immutability and decentralized nature are suitable for applications and environments where the integrity of identity and content is vital for recording transactions. Users should be able to manage their credentials through an encrypted digital wallet on their smartphone and control what they share, with whom, and for what purpose.

The literature discusses this approach to digital identity that gives individuals control over their digital identities as self-sovereignty (Bahar et al., 2020). Self-sovereign identity (SSI) is a new approach to identity management based on decentralization, distributed ledger technology, and cryptography. SSI entrusts individuals with the ownership and complete control of their identity without the intervention of administrative or centralized authorities. When blockchain is used as the fundamental technology behind SSI, it replaces the silo-creating client-server approach of centralized and federated identity systems with a peer-to-peer model for managing identities and credentials. Users are identified using a globally unique decentralized identifier (DID). Each DID has associated cryptographic elements that help authenticate users and issue and verify credentials. The use of DID, with its cryptographic elements and blockchain backbone, helps create a "trust triangle" between the user, issuer, and verifier without violating the user's privacy (Das and Kersey, 2020). In this case, there is no need for third parties in the process, and the user will have "sovereignty" over their "personal data."

In order to share credentials with peers in a secure and privacy-preserving manner, W3C verifiable credential (VC) (W3C, 2022) standard can be used. It helps standardize the document and format definitions, making them machine-readable and communicable.

This work contributes toward a blockchain-based SSI system, Health Passport, using DIDs and verifiable credentials that allow secure creation, sharing, verification, and revocation of generic health credentials.

The organization of this article is as follows. Section 2 describes the related work. In Section 3, the novelty of the proposed method and research contributions are mentioned. Section 4 describes the proposed system design, architecture, and functions. The prototype implementation, experimentation, and test results are discussed in Sections 5, 6. Detailed discussion and analysis of the proposed system are given in Section 7. Section 8 concludes the article and discusses future directions for research.

2 Related work

Many SSI-based verifiable credentials (VCs) were implemented during the pandemic for COVID-19 vaccination certificates (Karopoulos et al., 2021). This section briefly overviews these existing works, their features, and the problems faced by these systems, which led to the development of the proposed system.

The work by Hicks et al. (2020) presented SecureABC, a privacy-oriented protocol for immunity certificates based on public key cryptography. This proposal does not use the blockchain or any centralized repository, and the certificates can be either paper- or app-based. A proof-of-concept implementation of the basic operation of the proposed system is provided. Here, the method chosen for the digital certificate affects the system's scalability.

Eisenstadt et al. (2020) developed an application for vaccination and immunity certificates based on VCs as digital IDs, a decentralized data storage platform, Solid, and an Ethereum-based consortium blockchain. In this work, the hash of the VC is stored on the Consortium blockchain to facilitate verification. The performance evaluation shows scalability issues, as the certificate's issuance or verification could take more than 15 s in the best-case scenario for 100 concurrent requests (Karopoulos et al., 2021).

Hasan et al. (2020) proposed a blockchain-based solution for COVID-19 digital medical passports and immunity certificates using SSI, re-encryption proxies, and decentralized storage, i.e., InterPlanetary File systems (IPFSs). The solution features smart contracts for the Ethereum blockchain. The patient's smart contract stores the hash of the vaccination and immunity records and also the travel history to perform contact tracing. The certificate holder can decide to store sensitive information on the IPFS on an encrypted form and register the hash on the blockchain for verification purposes. No performance evaluation was carried out for this work. Since the system works on smart contracts on the Ethereum network, transactions have costs, even if they are negligible, necessitating the availability of financial resources from those involved.

NovidChain (Abid et al., 2022) addresses COVID-19 test/vaccine certificates by integrating the use of VCs in a blockchain implementation called uPort (Naik and Jenkins, 2020), which provides SSI aspects on top of the Ethereum platform. The certificate holder's personal data and test results are stored encrypted on the IPFS, and only the IPFS hash is kept on a

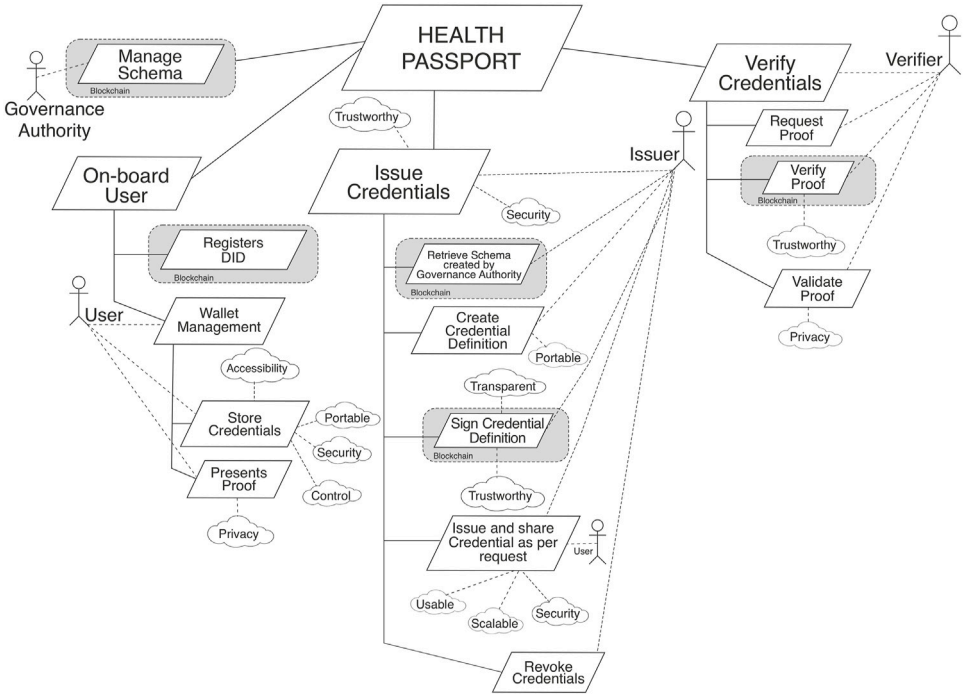

FIGURE 1
Health Passport- agent-oriented modeling (AOM) diagram.

TABLE 1 Problems of the existing systems.

Work	Technology used	COVID-19 specific	Drawbacks
Hicks et al. (2020)	Public Key Cryptography	YES	No performance evaluation was carried out for this work. The method chosen for digital certificate revocation can affect the system's scalability
Eisenstadt et al. (2020)	Blockchain (Ethereum)	YES	Scalability issue, certificate issuance, or verification takes more than 15s
Hasan et al. (2020)	Blockchain (Ethereum)	YES	No performance evaluation was carried out for this work. Since this system works on smart contracts on the Ethereum network, transactions have costs
Abid et al. (2022)	Blockchain (Ethereum)	YES	The cost of certificate issuance is high
Hernández-Ramos et al. (2021)	Blockchain (Hyperledger Fabric)	YES	Focused only on verifying the COVID-19 vaccination certificate
Harrell et al. (2022)	Blockchain (Hyperledger Indy)	NO	No performance evaluation was carried out for this work. Data are manually entered, which may contain errors affecting credential creation
Barros et al. (2022)	Blockchain (Hyperledger Indy)	YES	No performance evaluation was carried out for this work. Focused only on verifying the COVID-19 vaccination certificate

private-permissioned Ethereum blockchain. In terms of identity protection, SSI is used while end-users are free to decide which information they want to share with the trusted parties they choose. The performance evaluation of NovidChain reveals that the rate of issuing certificates, which is its most expensive operation, has an upper bound of ≈ 34 certificates/sec.

The abovementioned three works (Eisenstadt et al., 2020; Hasan et al., 2020; Abid et al., 2022) use Ethereum as their framework. Solutions that use the main public Ethereum network will have challenges with the cost involved for each transaction. The solutions that use Ethereum (not necessarily the main public Ethereum network) for digital identities, such as uPort, face the challenge of transaction speed.

Hernández-Ramos et al. (2021) proposed a blockchain-based platform based on Hyperledger Fabric for vaccination certificates. This work leverages VCs together with decentralized identifiers (DIDs) as credentials, allowing end-users to control their identities. The certificate is stored encrypted on the IPFS, and only its hash is registered on the blockchain. This system focuses only on verifying the COVID-19 vaccination certificate.

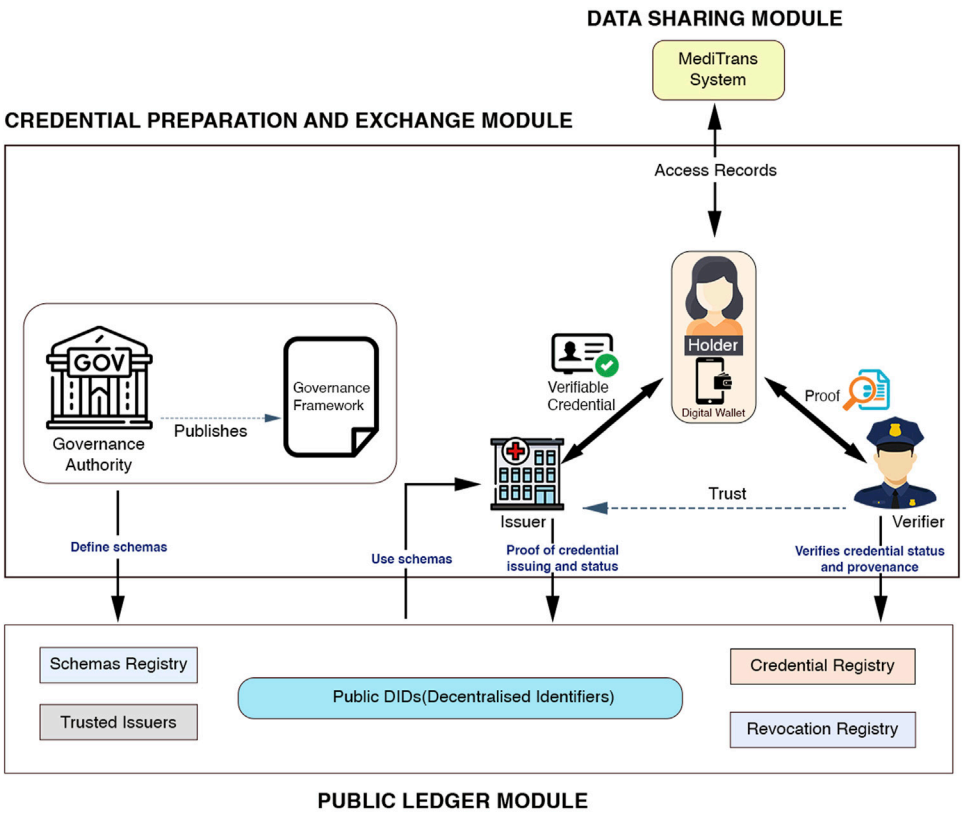

FIGURE 2
Proposed system design.

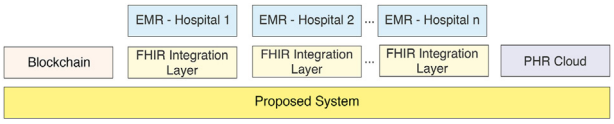

FIGURE 3
Modified MediTrans system.

A blockchain solution for identity management, MediLinker (Harrell et al., 2022), proposed by Khurshid A. et al., has been designed to allow patient autonomy and interoperability between clinics using a custom-built web and mobile application. They have used Hyperledger Indy and Hyperledger Aries to develop an operational identity management system for patients to track current medications and doses for sharing with healthcare providers. Patients must show a legitimate physical identity card to the receptionist at a participating clinic before they begin using MediLinker (for example, preferably a government-issued ID, such as a passport, driver's license, or residence ID). In this application, the data are manually entered, which may contain errors causing issues with the credentials created.

Barros et al. (2022) proposed a system architecture that allows the issuing and verifying of VCs based on SSI for proof of vaccination. The proposed design was based on Hyperledger Indy and Hyperledger Aries. This implementation produces a VC with vaccination information through selective disclosure and zero-knowledge proof (ZKP). No performance evaluation was done for this system and it is in the preprint stage. The article does not clarify how the initial data are accepted into the system, and implementation is specific to vaccination.

The problems faced by the existing systems are shown in Table 1.

The idea of the VCs created for COVID-19 vaccination certificates will continue to be relevant in a post-COVID-19 world. This will play an important role throughout the health sector and can have wide-ranging adoption in segments such as communicable disease control, routine immunization, and personal health records (Jain, 2022). There must be a system meant not only for COVID-19 vaccine certificate data but also for all medical records in a user's PHR that need verification for various needs.

3 Novelty and research contributions

Unlike previous works (Hicks et al., 2020; Eisenstadt et al., 2020; Hasan et al., 2020; Abid et al., 2022; Hernández-Ramos et al., 2021; Barros et al., 2022), our work is not limited to COVID-19 certificate verification, and it can be used for general health records too.

During credential issuance, the issuer needs the medical record from the user in a trustworthy manner. For this purpose, we propose a novel solution of integrating the Health Passport with a trustable PHR. This has two benefits:–1. The medical record sent directly

```
{
   "$schema": "http://json-schema.org/draft-07/schema#",
    "description": "Vaccination schema using JSON interchange format",
    "properties": {

    "name": {
    “type": "string"
    },
    "age": {
    “type": "string”
    },
    "VaccineName": {
    “type": "string”
    },
    "VaccineType": {
    “type": "string”
    },
    "NoOfDose": {
    “type": "string”
    },
    "location": {
    “type": "string”
    },
"required": [
    "VaccineName ",
    "VaccineType ",
    "NoofDose",
    "location",
  ]
"additionalProperties": false
}
```

FIGURE 4
Example of a verifiable credential schema.

from the PHR will have a trust guarantee. 2. The patient can select the appropriate record and forward it with no need for the manual entry of details. When the data are retrieved from a trustworthy PHR, the issuer can validate the medical record easily and use the same to create the VC. As the data for credential issuance are automatically populated from the PHR information, the risk of human error is minimal.

In this work, we explored the requirements for and designed a generalized verifiable credential management system, a Health Passport for healthcare, which can be used with any PHR system for converting medical records to credentials. The proposed methodology is a novel app-based system integrated with the PHR that uses cryptography and blockchain technology to manage credentials.

The research contribution of this article can be summarized as follows:

- Design and implementation of a PHR-integrated credential management system, Health Passport, with three major functions:
  1. Credential issuance function that creates credentials based on any record from the user's PHR.
  2. Credential revocation function that allows the issuer to revoke the user's credentials under special circumstances.
  3. Credential verification function, which allows individuals to share credentials for verification purposes. The verification process supports selective disclosure and ZKP that permits users to share credentials with chosen trusted parties without compromising privacy.
- Validation of the framework by building a proof of concept built on Hyperledger Indy (Indy, 2019) and Hyperledger Aries (Aries, 2022) integrated with a PHR.

4 Design of the proposed system

An agent-oriented modeling (AOM) design approach by Udokwu (2022) is used for modeling the Health Passport as an SSI-based credential verification framework for handling all aspects of the application from user onboarding, issuing of credentials, verification of credentials, management of credential schema, and revocation of credentials. The system shown in Figure 1 consists of agents interacting with each other to share credentials and perform specific tasks or functions to achieve common goals. The developed model highlights the different agents and their tasks and also the role of blockchain technology in the proposed system to achieve the functionality proposed.

The different agents in the proposed "Health Passport" system are as follows:

1. Governance authority: The governance authority is the entity that creates and administers a governance framework (trust framework). The framework defined by the governance authority provides business, legal, and technical rules/guidelines to issue credentials.

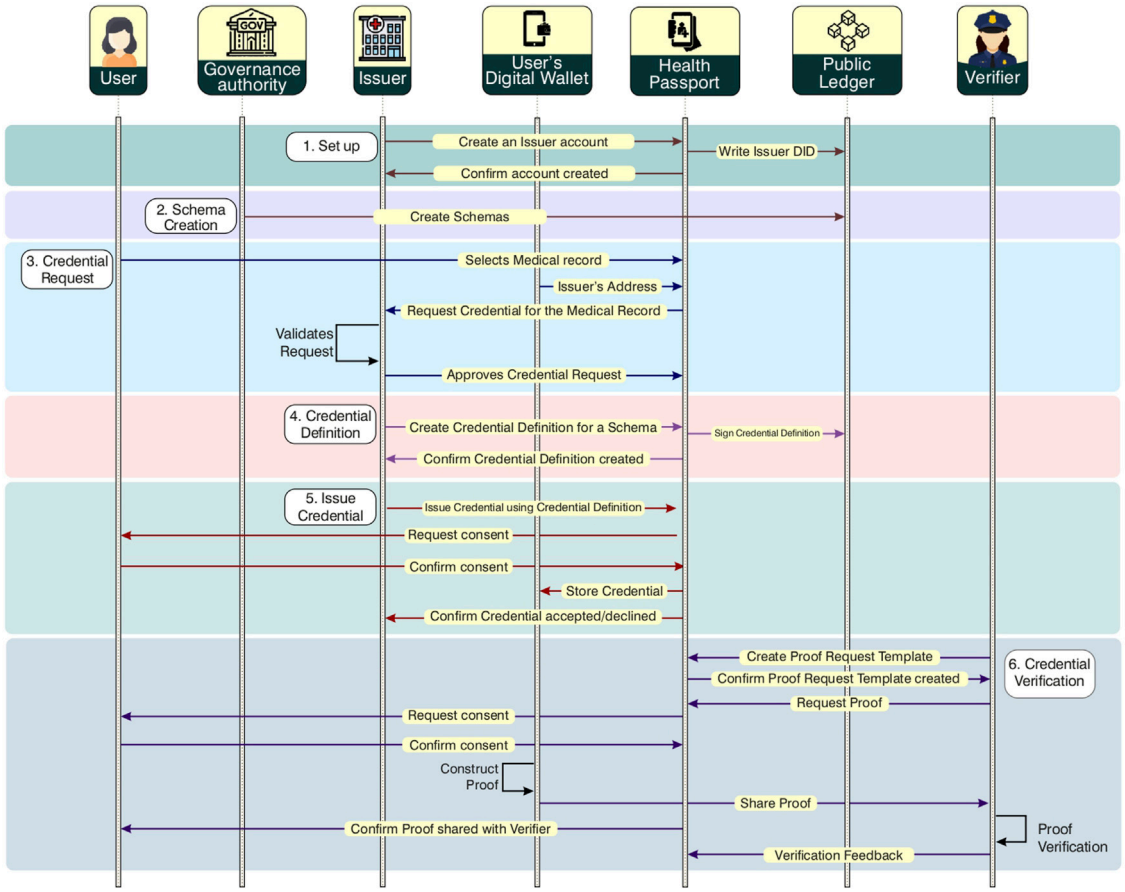

FIGURE 5
Sequence diagram for the Health Passport system.

They are responsible for creating semantic structures describing the list of attributes that a credential can contain (schemas). This will be added to the public ledger module, and the issuers retrieve the schema while preparing credentials, and the verifier checks the schema before verification.

2. Issuer: The issuer prepares the credentials according to the schema from the governance framework. The prepared credential is signed and converted to a VC and given to the holder.
3. Holder/user: The holder/user requests the credential from the issuer when they need the same. The user receives the credentials from the issuer, maintains them in their wallet, and presents the VC whenever required.
4. Verifier: A verifier receives and verifies credentials presented by the holder.

The relationship between issuers, holders, and verifiers is often referred to as the trust triangle because it is fundamentally how human trust relationships are conveyed over a digital network. In our use case of VC generation for health, to ensure the chain of trust, issuers must be trusted. Hence, we propose that DIDs issued to health agencies must be endorsed by the government or an international body. The government then makes available a list of trusted DIDs, contributing to a global chain of trust.

The fundamental assumption of this work is that all the agents are verified and found trustworthy. The system contains three main modules: i) the public ledger module, ii) the data-sharing module, and iii) the credential preparation and exchange module, as shown in Figure 2. The functioning of each module is described as follows.

4.1 Public ledger module

When the user boards the platform, they can choose a human-memorable name for their identity and the platform converts the name to a unique identity called DID. The public ledger module is responsible for creating this decentralized identity, providing users with a unique key, DID. The metadata associated with the key is known as DID descriptor objects (DDOs). The combination of DDO and DID is referred to as the DID record. The user's identity, as a DID record on the distributed ledger, is secured cryptographically by an identity owner's private key. A public key corresponding to the key pair is generated in the DDO with a key description. A DDO also contains a set of service endpoints to initiate trusted interactions with the identity owner. A DID method specification is associated with each DID, which defines how a DID is registered, updated, resolved, and revoked on this network. DIDs issued to healthcare

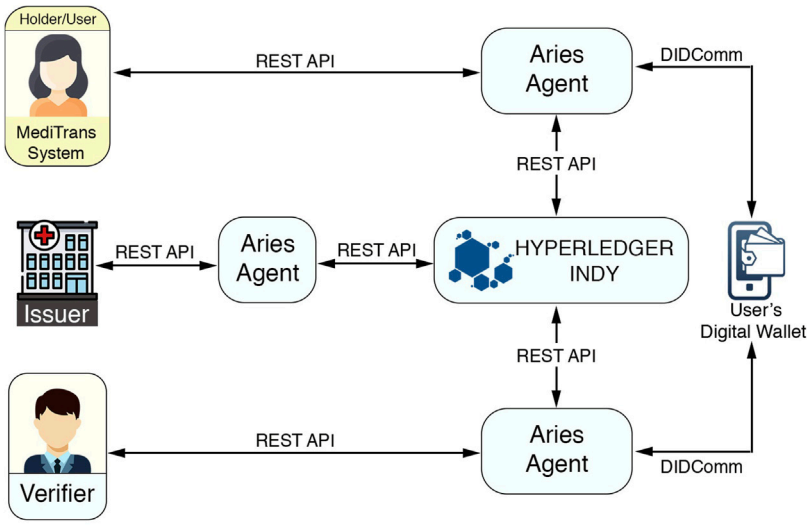

FIGURE 6
Health Passport prototype.

institutions must be endorsed by the government or an international body to ensure the chain of trust. The government then makes a list of trusted DIDs, contributing to a global chain of trust.

This module also stores the credential schema, the base semantic structure of a credential describing the list of attributes. A governance authority is responsible for defining and updating credential schemas in this ledger per changing guidelines. The governance authority prepares a schema per the requirement/regulation, signs it with their DID, and submits it in the public ledger. The issuer who creates the credentials refers to this schema and submits a credential definition as evidence to the ledger.

Since the ledger is public, it should not expose any personal information directly on the ledger. To achieve the privacy of the public ledger, the items stored in the ledger are i) DIDs, ii) public keys, iii) service end-points, and iv) proofs (Hashed or ZKP artifacts that help credential holders to prove the validity of the credentials).

4.2 Data-sharing module

This module is responsible for data sharing between the user and the hospital. In our design, it is coordinated by MediTrans. MediTrans is a cloud-based PHR that focuses on secure data access and sharing between users and different hospital systems using an integration layer (FHIR) and can fetch records from the hospital EMR system. Users/patients can access their records from the hospital and store them in the MediTrans cloud for later use.

4.2.1 MediTrans system

MediTrans is a cloud-based PHR that focuses on secure data access and sharing between users and different stakeholders in the healthcare industry. As explained in the introduction section, this system aims to address the challenges of the portability of hospital records. With MediTrans, users (say, patients) can make consultations in two different hospitals, and both visit and health records of both hospitals are available on the MediTrans platform, provided the hospitals are already boarded on the platform. The platform's main advantage is not only the accessibility of health records but also that data can be shared with others and revoked when needed. This helps the patient selectively share their record with a new doctor when a consultation is made and revoke access to the doctor. Even though the digital identity ecosystem can take care of verifiable credential issuance and verification, MediTrans, when it comes to the ecosystem, can serve as the data provider for credential issuance and revocation.

For SSI implementation, MediTrans was modified to enable the option for users to take the record available on the platform to be issued as a verified credential. For this, the MediTrans app was given the added functionalities of an SSI client (Figure 3).

The data from hospitals to the PHR are fetched over the FHIR integration layer, which is authenticated and brought to the platform. The data fetched from the hospital server in a standard format will be currently delivered through the HL7 FHIR standard. The FHIR layer is a plugin created to fetch data from hospital EMR systems as data elements called resources. The web application part of the system can communicate with all the hospital systems through the FHIR layer, where data are exchanged as resources. Users can log in to the application and get medical records. Hence, it is easy for users to have access to the records irrespective of the device they use. The patient uses the HTTPS protocol to establish an encrypted and integrity-protected link for securing all transfers between the patient and the FHIR server.

4.3 Credential preparation and exchange module

This module is responsible for exchanging VCs. The three significant functions of the credential exchange module are explained as follows.

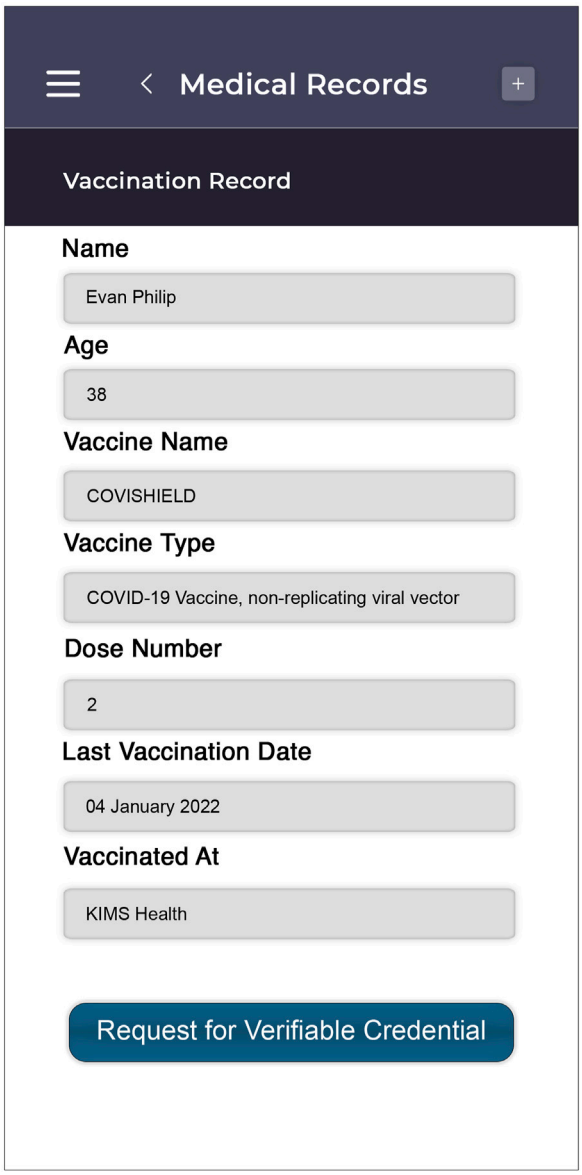

FIGURE 7
User requesting for VC from his medical records.

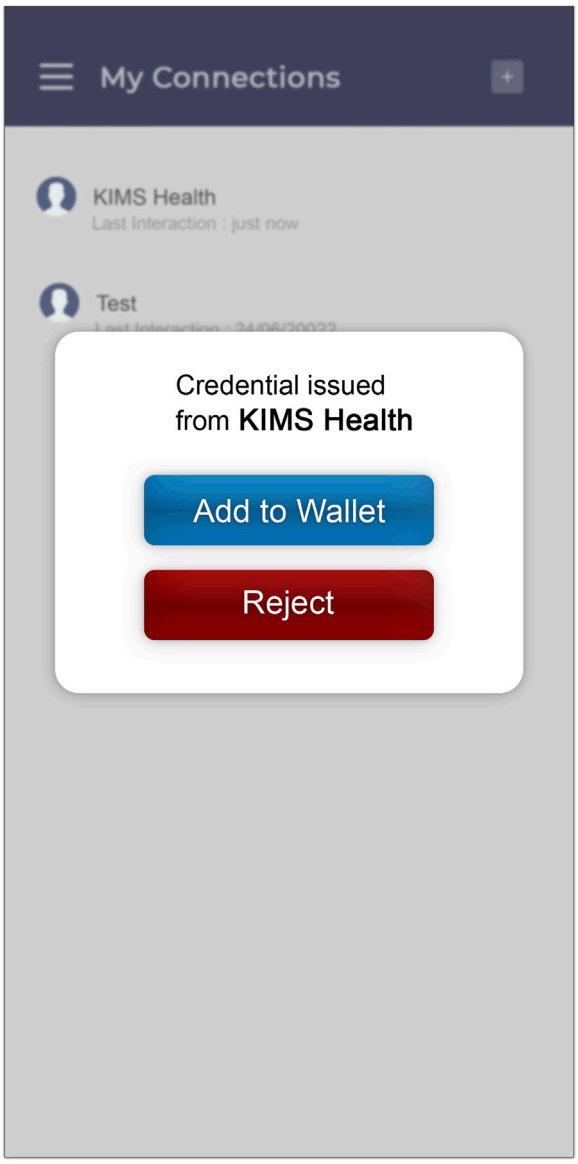

FIGURE 8
Requesting confirmation to save the received VC to the wallet.

4.3.1 Credential issuance

The step-by-step procedure to issue a credential is given as follows:

- Step 1: When a user needs a health record to be converted to a credential, the user selects the record in MediTrans and sends a credential request message to the issuer.
- Step 2: After receiving the request, the issuer will refer to the latest schema of the requested credential in the public ledger. An example of a vaccination credential schema is shown in Figure 4
- Step 3: The issuer will create a credential definition based on a schema, issuer DID, and other metadata that are needed for verifying a credential during the verification process.
- Step 4: The credential definition is signed using the issuer's DID and the issuer's public key and submitted to the ledger. The issuer verifies the relevant details, including expiry/revocation details.
- Step 5: The issuer then prepares the VC using the signed credential definition, his DID, and the private key. All personal information is held off-chain and only sent between the issuer and the user using encrypted peer-to-peer connections. The unique identifier saved in the blockchain is cryptographically connected to this off-chain data storage.
- Step 6: The user receives the credential from the issuer. The credential issued contains the requested attributes by the user and the revocation status of the credential. The credential is given to the user and is added to the user's digital wallet for verification.

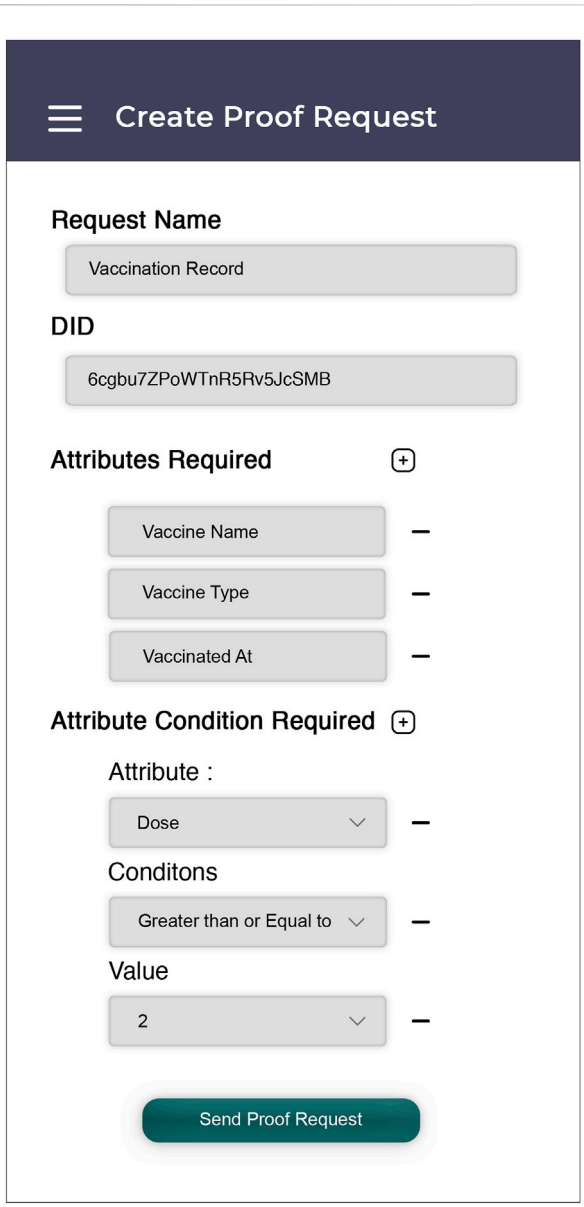

FIGURE 9
Verifier creating proof request to the user.

FIGURE 10
Proof request on the verifier's mobile device will be displayed as a QR code, and the user scans the QR code as consent to share the proof.

The issuer must provide a VC in a way that allows the holder to communicate the information to a verifier in a privacy-preserving manner for implementing ZKP. This means that the holder will be able to prove the reliability of the issuer's signature even without revealing the values that were signed. The two requirements for VCs used in ZKP systems are as follows:

- The VC created must contain the credential definition as metadata that may be used by all parties to carry out different cryptographic operations in zero knowledge.
- The VC must provide proof to prove the information contained in the VC during presentation. Any information not intended to be shared by the presenter must not be revealed during the zero-knowledge presentation.

4.3.2 Credential revocation

The Health Passport needs the user's credentials to be revoked by the issuer under certain circumstances. Credentials can be revoked for the reasons as follows:

- Change of policy: If there is any change in government policies, this will revoke the credential as a condition of deployment policy in health and social care. When this happens, credentials issued with the old policy will be revoked.
- Schema update: If the government adds an extra attribute for verification, then the version of the schema issued by the governing authority will get updated. All the previous version's credentials will be revoked when the version is updated.

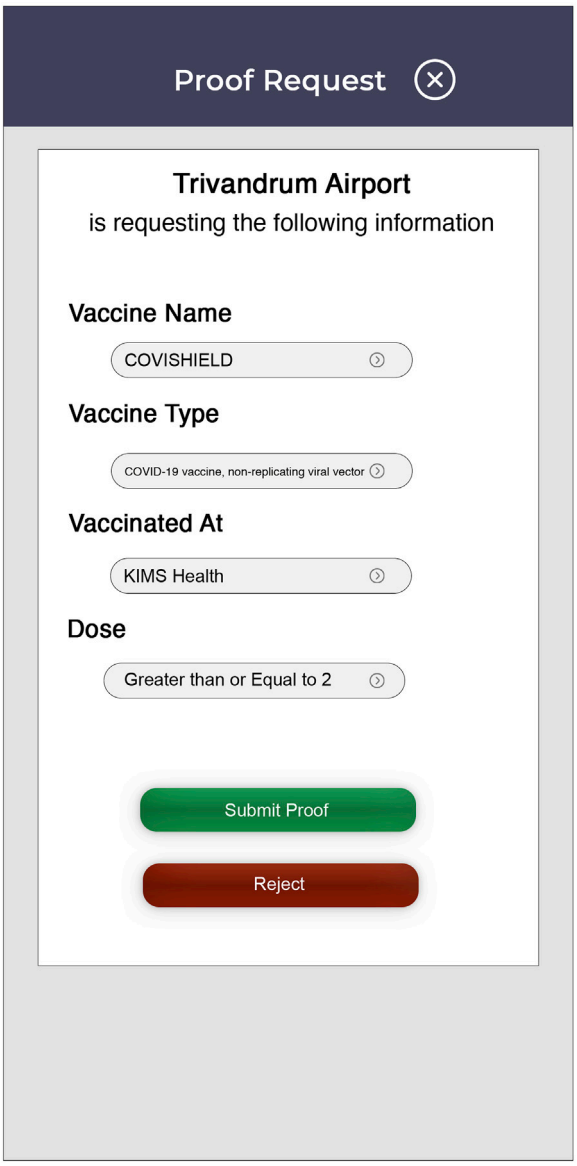

FIGURE 11
In the user's mobile, details will be filled in which are stored in the user's wallet as credentials.

FIGURE 12
User provides second-level authentication for submitting the proof.

- Validity expiration: If the credential loses its active status, it can be revoked anytime by the issuer. This status check will also be carried out on the verifier's side while checking the conditions.

Hence, our Health Passport must have a scheme to provide a revocation mechanism for an issued certificate. Here, the revocations of the VC can be accepted only when it is made by their trusted issuers. The following steps are followed in the process of revocation of a credential:

- Step 1: Issuers publish a revocation list containing the list of revoked credentials. Issuers maintain a revocation registry in the public ledger to publish this list as and when needed.
- Step 2: The issuer signs the revocation list and labels for authenticity.
- Step 3: This list is validated before any verification of the presented credentials happens. Thus, if the user presents revoked credential, then the credential is identified as revoked, and further processing is prevented. Hence, the issuer need not be contacted again, and the user is in control of the credential.

4.3.3 Credential verification

The verifier should ensure that the credential is valid and satisfies all the requirements for verification. The following steps are carried out in the verification process:

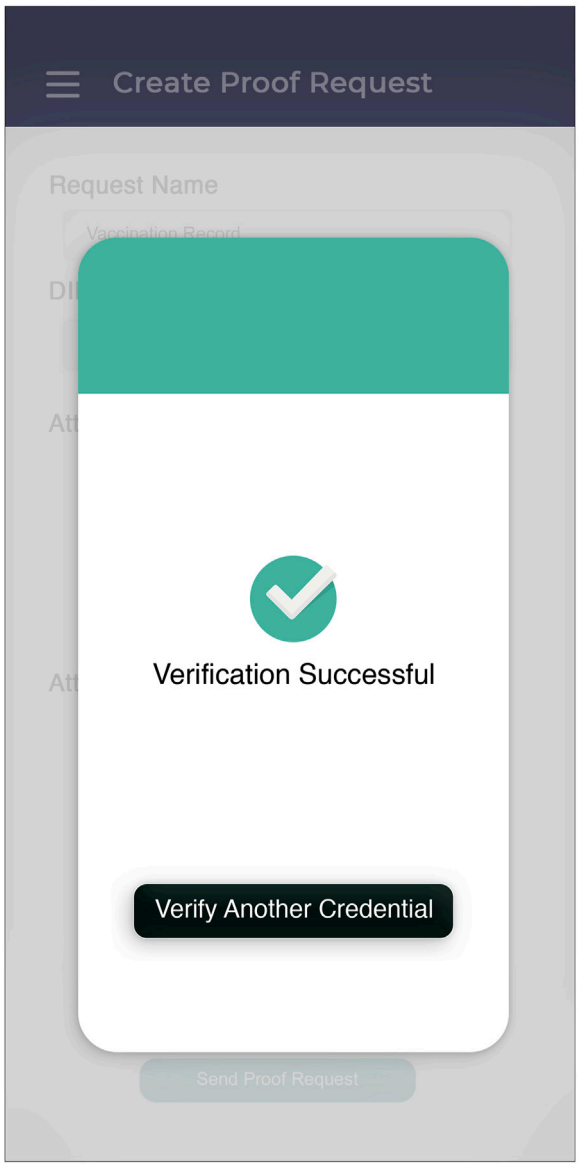

FIGURE 13
Successful verification without seeing any details of the user.

- Step 1: The verifier creates a proof request that tells about the attributes the verifier needs to check from the user.
- Step 2: The user accepts this request and gives consent to share the proof of the information requested by the verifier.
- Step 3: The information of VCs requested by the verifier is transformed into a proof presentation. All VCs in the proof presentation must reference the credential definition used to generate the proof. The users can, thus, prove that they possess a certain attribute or fulfill certain conditions without disclosing details *via* ZKP.
- Step 4: The verifier utilizes the issuer's DID, which is present in the proof, to read the public key and other cryptographic information from the blockchain.
- Step 5: The verifier then checks the validity of the proofs and the integrity of the digital credential using the issuer's public key.

Figure 5 shows the sequence diagram that gives an overview of the entire VC flow and the working of the Health Passport system.

5 Prototype implementation

This article demonstrates the feasibility of the solution by implementing a proof of concept built on Hyperledger Indy (Indy, 2019) and Hyperledger Aries (Aries, 2022), which have been integrated with a PHR – MediTrans. The proposed solution is app-based and uses cryptography and blockchain technology to create a VC. VCs can be generated from any information in the PHR by the user.

The Hyperledger Indy (Indy, 2019) platform has an inbuilt function for handling identity management features that focus on SSI. Hyperledger Aries is used as a middleware (API) to connect Hyperledger Indy with the front end. Hyperledger Aries (Aries, 2022) implements a RESTful programming interface to handle different workflows and interactions that help to create, transmit, and store verifiable digital credentials. MediTrans is used as a PHR agent to coordinate the whole process.

For the proof-of-concept implementation, this work utilized Hyperledger Aries Framework JavaScript (AFJ) (AFJ, 2022) and Aries React NatIve Mobile Agent (ARNIMA) Flutter SDK (Jadhav, 2021) for building SSI agents and DIDComm services. The verifier uses the mobile app to specify proofs and send this request to users, while the issuer uses the website to issue VCs. We consider all the users who will be credential holders as users of the MediTrans application. When a user boards the MediTrans system, upon specifying a secret seed (such as a password), the user will enroll in the SSI system by calling the API of the Aries agent, which will create the DID and store it in Hyperledger Indy. A wallet for each user profile is created to store the VCs received from the issuer. Here, the wallet is in the mobile app of the user.

VCs are tamper-proof JSON files. These credentials are stored in the users' ID wallets, and their authenticity is verifiable on the blockchain. VCs are based on the W3C standard created to bring trust to identity and access management. These VCs are exchanged *via* Aries agents with the help of a peer-to-peer credential protocol, DIDComm, as shown in Figure 6.

Let us consider the use case of a user that uses COVID-19 vaccination status for international travel. The user's health records from various hospital systems are available in the MediTrans application. The user can get their vaccination record from MediTrans and request for issuance of a credential, as shown in Figure 7. A request will be sent to the hospital (issuer) for the issuance of the VC using the hospital's unique DID. Once the VC is prepared, the user clicks on "Add to Wallet" as shown in Figure 8 to add the credential to the user's wallet from which they can access using any agents whenever required (including this mobile app).

The verifier at the verification site can use a mobile-based app for verification purposes. The verifier creates a proof request template to describe the conditions that verify credentials for the particular instance, for example, for travel, as shown in Figure 9. This proof request on the verifier's mobile device will be displayed as a QR code, as shown in Figure 10, for the user to give consent to share the information requested by the verifier.

TABLE 2 Details of tools used in the experimentation.

Sl. no.	Tools	Description
1	Hyperledger Indy (Aries, 2022)	It is a permissioned blockchain used for identity management and the Indy ledger provided by AWS as a service is used in setting up blockchain networks locally
2	Hyperledger Aries Js (Aries, 2022)	Aries Cloud Agent Python library (Agent, 2022) is used for issuing, storing, and verifying the credentials in a non-mobile environment
3	REST APIs	Representational state APIs are used for exchanging the credentials between two end-points of Aries agents

Once the user scans the QR code, Figure 11 shows how the digital wallet shows the proof request to the user. The user will need to present values for the fields "Vaccine name,' "Vaccine type," and "Vaccinated at," which are stored in the user's wallet as credentials. A compulsory check to the request is given for the number of doses that is greater than or equal to 2. The wallet will create the presentation and exchange it on the user's behalf. After submitting the proof, the app leverages second-level authentication, as shown in Figure 12, which is the authentication present in the device. On successful authentication, the proof is submitted and reaches the proof requester agent using the Aries agent DID communication protocol.

The immigration officer will now be able to see the verification status as shown in Figure 13, which is successful in this case, and the person is permitted to travel. If any assertion attribute is wrong, the verification fails and the person will not be given permission.

6 Experimentation and test results

The following are the details of the experimental setup to perform tests and analyze the prototype performance.

The Hyperledger Indy and Hyperledger Aries setups were realized using three nodes in the AWS cloud instance. The EC2 instance type used was a T2 medium with a processor speed of 3.3 GHz and Ubuntu 20.04 as the operating system.

The mobile app was tested on One Plus 7T. The test device runs with a Snapdragon 855 Plus processor with 128 GB storage and 8 GB RAM. Details of tools used in the experimentation are given in Table 2.

The main functions in any SSI system to analyze are credential issuance and verification. We have analyzed by varying the number of credentials and calculated the average time for both functions. The test results of the analysis conducted are shown in Table 3. The results show that credential issuance takes more time than verification with the increase in the sample of the number of credentials.

7 Discussion and analysis

This paper demonstrates the technical feasibility of the SSI blockchain-based Health Passport integrated with the PHR. The proof of concept used Hyperledger Indy and Hyperledger Aries to manage the identity management and the PHR MediTrans for coordination among the user, issuer, and verifier. This section analyzes the performance of the proof of concept built in Hyperledger Indy and Hyperledger Aries.

7.1 Privacy and security analysis

The proposed solution satisfies all the privacy and security requirements mentioned as follows.

7.1.1 Trustability of the verification process

The proposed system provides multi-layer security. As discussed in George and Chacko (2022), medical records in MediTrans stored in the PHR cloud are protected using multilevel authentication and verification by smart contracts and encryption using Ciphertext-Policy Attribute-Based Encryption (CPABE). The data in the PHR are trustworthy as they can be validated using the blockchain backbone. The credential, thus, received is directly transferred for the issuance of the VC by the issuer. This allows the issuer to be assured about the trustworthiness of the record used for issuing the VC.

7.1.2 Unforgeability of verifiable credentials

The Health Passport uses blockchain security to deliver forgery-proof credentials. These credentials are tamper-proof JSON files that an issuer issues with a cryptographic key or signature. This will be stored in the users' ID wallets, and their authenticity is verifiable on the blockchain using cryptographic methods. Since they are cryptographically signed, they cannot be forged to replace an original. This leaves no room for fraudulent activity, making it easier for the verifier to verify credentials.

When the device is lost or misused, the person who gets the mobile cannot ever impersonate the user in any existing relationships or new relationships based on anything he gains from the stolen device. The application is secured with a username and password, and also only upon specifying a secret seed, a user can enroll in the SSI system. The credentials stored in the wallet by the identity owner will be secure. Wallet files are stored in the MediTrans PHR cloud, making them easy to recover if lost. Users can continue to use the app on whichever device he/she likes. Users can continue using their existing credentials in relationships with the same trust as before. Users can also request and receive new credentials that are just as secure as the old ones.

7.1.3 Compliance with varying government guidelines

During the COVID-19 pandemic, it was observed that the guidelines for CVs kept changing. So, the flexibility to adapt to varying guidelines was an essential requirement in the development of the Health Passport. The changes can be incorporated with the help of schemas defined by the governance authority on the public ledger module. It is not possible to update an existing schema. So, if the schema needs to be evolved, a new schema with a recent version

TABLE 3 Average time duration for issuing and verifying credentials.

Sl. no.	No. of credentials	Average time per credential issuance (sec)	Average time per credential verification (sec)
1	10	2.10	2.14
2	50	2.32	2.45
3	100	3.05	2.51
4	500	4.1	3.13
5	1,000	5.61	3.14
6	1,500	7.12	3.22
7	2,000	8.23	3.51

TABLE 4 Comparison of the performance of the Health Passport with the state of the art.

Work	Privacy	Scalability	Interoperability	PHR integrated
Hicks et al. (2020)	YES	NO	NO	NO
Eisenstadt et al. (2020)	YES	NO	NO	NO
Hasan et al. (2020)	YES	NO	NO	NO
Abid et al. (2022)	YES	YES	NO	NO
Hernández-Ramos et al. (2021)	YES	YES	NO	NO
Harrell et al. (2022)	YES	Not Known	YES	NO
Barros et al. (2022)	YES	Not Known	YES	NO
Health Passport	YES	YES	YES	YES

or name needs to be created. The issuer will then refer to the latest schema version with the new guidelines for preparing credentials.

7.1.4 Verification without breaching user privacy

The evolving use of technology has taught many lessons regarding the privacy of individuals being misused. Hence, in the Health Passport, verification is carried out without revealing personal information and provides the verifier with all the features without decreasing the level of trust. The privacy and freedom for the selective disclosure of the information are enabled by the SSI ecosystem built on Hyperledger Indy, a distributed ledger built for decentralized ID with transferable, private, and secure credentials. Thus, if there are multiple conditions for verification, the user details are not known to the verifier, but the verifier is assured that the conditions are met as per the credential provided by the user. Thus, verification is carried out in a ZKP manner with minimal information exposure, thereby protecting the user's privacy. At the same time, the verifier verifies with confidence. This will enable compliance with GDPR and other international data protection laws.

7.2 Efficiency and scalability

The prototype's performance is evaluated in terms of time duration for issuing and verifying the credentials using the experimental setup described previously. The average time duration for issuing and verifying credentials is shown in Table 3, and it is observed that the time overhead is minimal. For 100 VC requests, our solution takes only 3.05 s for credential issuance and 2.51 s for credential verification, which shows that the proposed solution is efficient and scalable for the secure sharing of health credentials.

7.3 Interoperability

The Health Passport uses Hyperledger Aries for peer-to-peer interaction and facilitates an interoperable interaction between different blockchains and other distributed ledger technologies (DLTs) to share VC metadata. The use of DIDs, DDOs, VCs, and agents can achieve interoperability of decentralized identity across DLTs. Since the DIDs are open standard, any agent that supports the DID method can resolve VCs issued on this system, regardless of the network the verifying agent may use. Thus, the Indy DID method enables smooth network-to-network interaction, enabling credentials to work globally.

7.4 PHR integration

The integrated PHR–EHR approach in the proposed system can provide the patient with more convenience in selecting their record for credential requests. Medical records, such as images, can also be considered when the issuer verifies the image and prepares a VC

which is trustworthy and accepted by the verifier. The VC is a JSON file and does not contain the medical image that is part of the PHR. The schema defined by the governance authority based on the needs of the verifier will provide the details the VC needs to contain; hence, this is extensible.

7.5 Comparison with existing systems

Section 2 described the related work in this area. One of the issues with most of the articles on blockchain built to combat the COVID-19 pandemic is that there is no study about latency and scalability as reported by Abd-alrazaq et al. (2020).

Among the related works, many have not performed an explicit performance evaluation. The systems proposed by Hicks et al. (2020); Eisenstadt et al. (2020); Hasan et al. (2020); and Abid et al. (2022) will have scalability issues when compared to our system due to the underlying choice of blockchain and revocation techniques. Abid et al. (2022) presented the implementation details of their proposal. The performance evaluation reveals that the rate of issuing certificates is its most expensive operation and has a maximum limit of approximately 34 certificates/sec. In Eisenstadt et al. (2020), the certificate's issuance or verification could take more than 15 s in the best-case scenario for 100 concurrent requests. Our approach promises better scalability as it requires only 3.05 s for credential issuance and 2.51 s for credential verification for 100 VC requests.

The systems proposed by Eisenstadt et al. (2020); Hasan et al. (2020); and Abid et al. (2022) use Ethereum, which has recurring financial implications and issues with transaction speed.

MediLinker, proposed by Harrell et al. (2022), is the closest to the proposed work. This app considers six types of patient records to be shared as credentials. This app has multiple points of human intervention where the user has to enter their medical record, which is validated by the receptionist of the medical firm to start with credential creation. In our work, the user selects the appropriate record from the trustworthy PHR and forwards it to the issuer, and no data need to be manually entered on the user's or issuer's side.

Our work stands apart in the option of PHR integration and flexibility of using any medical document as the credential. In order to have credentials created, the schema for credentials should be defined in the public ledger, and once it is done, any health document can be converted to a credential. Since the data comes through a trustable PHR, credential issuance is easier as it has a trust guarantee.

Although our solution is demonstrated as an extension of MediTrans, it can be extended to any PHR solution as the SSI solution is added as a plugin to the PHR or existing EHR that can be accessed *via* a mobile/web app. A comparison of existing works with the Health Passport is shown in Table 4.

8 Conclusion and future directions

This paper presents the design of an SSI blockchain-based Health Passport integrated with the PHR that helps in health credential management. The solution is flexible so that it can be integrated with any PHR such that any health record can be converted to a credential as required. The governance authority has to define the corresponding schema in the public ledger. The user selectively discloses the information required to build the VC from the PHR and is assured privacy as verification can be carried out with minimal disclosure of private information to the verifier. The blockchain backbone helps in assuring trustworthiness and unforgeability of credentials. Thus, adding a Health Passport to the PHR helps in giving the user a one-stop location to deal with all their health-related requirements. In this work, we have demonstrated the feasibility of the Health Passport by building and analyzing the proof of concept. As a future work, we are exploring the option of building the Health Passport as a decentralized application on top of the OntoChain Framework (Papaioannou and Stamoulis, 2022).

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material. Further inquiries can be directed to the corresponding author.

Author contributions

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abd-alrazaq, A. A., Alajlani, M., Alhuwail, D., Erbad, A., Giannicchi, A., Shah, Z., et al. (2020). Blockchain technologies to mitigate Covid-19 challenges: A scoping review. *Comput. Methods Programs Biomed. Update* 1, 100001. doi:10.1016/j.cmpbup.2020.100001

Abid, A., Cheikhrouhou, S., Kallel, S., and Jmaiel, M. (2022). Novidchain: Blockchain-based privacy-preserving platform for Covid-19 test/vaccine certificates. *Softw. Pract. Exp.* 52, 841. doi:10.1002/spe.2983

AFJ (2022). Aries framework javascript (built using typescript). Available at: https://github.com/hyperledger/aries-framework-javascript (Accessed January 30, 2022).

Agent (2022). hyperledger/aries-cloudagent-python. Available at: https://github.com/hyperledger/aries-cloudagent-python/tree/main/docs/GettingStartedAriesDev (Accessed November 24, 2022).

Aries (2022). Hyperledger aries. Available at: https://www.hyperledger.org/use/aries (Accessed November 24, 2022).

Bahar, H., Senhaji, H. A., and Dimitrios, M. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access* 8, 90478–90494. doi:10.1109/ACCESS.2020.2994090

Barros, M., Schardong, F., and Custódio, R. F. (2022). *Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass*. arXiv. doi:10.48550/ARXIV.2202.09207

Das, S., and Kersey, J. (2020). *Jumpstart the global travel industry using self-sovereign identity for COVID-19 immunity credentials*. Available at: https://www.tcs.com/content/dam/tcs/pdf/perspectives/covid-19/self-sovereign-identity-implementation-travel-industry.pdf (Accessed January 31, 2022).

Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A., and Domingue, J. (2020). Covid-19 antibody test/vaccination certification: There's an app for that. *IEEE Open J. Eng. Med. Biol.* 1, 148–155. doi:10.1109/OJEMB.2020.2999214

George, M., and Chacko, A. M. (2022). MediTrans—patient-centric interoperability through blockchain. *Int. J. Netw. Manag.* 32, e2187. doi:10.1002/nem.2187

Harrell, D., BaUsman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J., et al. (2022). Technical design and development of a self-sovereign identity management platform for patient-centric health care using blockchain technology. *Blockchain Healthc. Today* 5, 196. doi:10.30953/bhty.v5.196

Hasan, H. R., Salah, K., Jayaraman, R., Arshad, J., Yaqoob, I., Omar, M., et al. (2020). Blockchain-based solution for Covid-19 digital medical passports and immunity certificates. *IEEE Access* 8, 222093–222108. doi:10.1109/ACCESS.2020.3043350

Hernández-Ramos, J. L., Karopoulos, G., Geneiatakis, D., Martin, T., Kambourakis, G., and Fovino, I. N. (2021). Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation. *Wirel. Commun. Mob. Comput.* 2021, 1–12. doi:10.1155/2021/2427896

Hicks, C., Butler, D., Maple, C., and Crowcroft, J. (2020). *SecureABC: Secure antibody certificates for covid-19*. vol. abs/2005.11833.

Indy (2019). Hyperledger indy. Available at: https://www.hyperledger.org/use/hyperledger-indy (Accessed November 24, 2022).

Jadhav, A. (2021). Arnima flutter sdk for aries agent. Available at: https://github.com/ayanworks/ARNIMA-flutter-sdk (Accessed January 31, 2022).

Jain, N. (2022). *Unlocking the value of verifiable credentials in the health sector*. Available at: https://www.affinidi.com/post/unlocking-the-value-of-verifiable-credentials-in-the-health-sector (Accessed January 10, 2023).

Karopoulos, G., Hernandez-Ramos, J. L., Kouliaridis, V., and Kambourakis, G. (2021). A survey on digital certificates approaches for the COVID-19 pandemic. *IEEE Access* 9, 138003–138025. doi:10.1109/ACCESS.2021.3117781

Naik, N., and Jenkins, P. (2020). "Uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in 2020 IEEE International Symposium on Systems Engineering (ISSE) (Vienna, Austria: IEEE), 1–7. doi:10.1109/ISSE49799.2020.9272223

Papaioannou, T., and Stamoulis, G. D. (2022). *A business model for multi-tiered decentralized software frameworks: The case of ontochain*. Available at: http://2022.gecon-conference.org/images/pdfs/9167.pdf (Accessed December 22, 2022).

Song, W., Nokhbeh Zaeem, R., Liau, D., Chang, K. C., Lamison, M. R., Khalil, M. M., et al. (2022). "Self-sovereign identity and user control for privacy-preserving contact tracing," in WI-IAT '21: IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (New York, NY, USA: Association for Computing Machinery), 438–445. doi:10.1145/3486622.3493914

Udokwu, C. J. (2022). *A modelling approach for building blockchain applications that enables trustable inter-organizational collaborations*. Lappeenranta-Lahti University of Technology LUT. Available at: https://lutpub.lut.fi/handle/10024/164663 (Accessed December 20, 2022).

Wang, B., and Ping, Y. (2022). A comparative analysis of Covid-19 vaccination certificates in 12 countries/regions around the world: Rationalising health policies for international travel and domestic social activities during the pandemic. *Health Policy* 126, 755–762. doi:10.1016/j.healthpol.2022.05.016

W3C (2022). *Verifiable credentials data model v1.1*. Available at: https://www.w3.org/TR/vc-data-model/f (Accessed April 24, 2022).