Information Processing and Management 58 (2021) 102572

Contents lists available at ScienceDirect

Information Processing and Management

journal homepage: www.elsevier.com/locate/ipm

A blockchain empowered and privacy preserving digital contact tracing platform

Eranga Bandara [a,*], Xueping Liang [b], Peter Foytik [a], Sachin Shetty [a], Crissie Hall [c], Daniel Bowden [c], Nalin Ranasinghe [d], Kasun De Zoysa [d]

[a] Old Dominion University, Norfolk, VA, USA
[b] University of North Carolina at Greensboro, Greensboro, NC, USA
[c] Sentara Healthcare, Norfolk, VA, USA
[d] University of Colombo School of Computing, Sri Lanka

ARTICLE INFO

Keywords:
Blockchain
Self-sovereign identity
Smart contact
Cloud computing
COVID-19

ABSTRACT

The spread of the COVID-19 virus continues to increase fatality rates and exhaust the capacity of healthcare providers. Efforts to prevent transmission of the virus among humans remains a high priority. The current efforts to quarantine involve social distancing, monitoring and tracking the infected patients. However, the spread of the virus is too rapid to be contained only by manual and inefficient human contact tracing activities. To address this challenge, we have developed Connect, a blockchain empowered digital contact tracing platform that can leverage information on positive cases and notify people in their immediate proximity which would thereby reduce the rate at which the infection could spread. This would particularly be effective if sufficient people use the platform and benefit from the targeted recommendations. The recommendations would be made in a privacy-preserving fashion and contain the spread of the virus without the need for an extended period of potential lockdown.

Connect is an identity wallet platform which will keep user digital identities and user activity trace data on a blockchain platform using Self-Sovereign Identity(SSI) proofs. User activities include the places he/she has travelled, the country of origin he/she came from, travel and dispatch updates from the airport etc. With these activity trace records, Connect platform can easily identify suspected patients who may be infected with the COVID-19 virus and take precautions before spreading it. By storing digital identities and activity trace records on blockchain-based SSI platform, Connect addresses the common issues in centralized cloud-based storage platforms (e.g. lack of data immutability, lack of traceability).

1. Introduction

Due to the widespread pandemic of COVID-19, nations around the world are investing tremendous time and effort to control the COVID-19 outbreak. Currently, as of the beginning of May 2020, there are over 4.2 million cases worldwide, with the majority found in the US for a total of 1.2 million confirmed cases. According to the World Health Organization (WHO), there has been evidence of transmission found from symptomatic, pre-symptomatic and asymptomatic people infected with COVID-19, making the situation even more severe and challenging (World Health Organization, 0000). To effectively reduce the spread, it is highly recommended

* Corresponding author.
E-mail addresses: cmedawer@odu.edu (E. Bandara), x_liang@uncg.edu (X. Liang), PFoytik@odu.edu (P. Foytik), sshetty@odu.edu (S. Shetty), cehallre@sentara.com (C. Hall), dsbowden@sentara.com (D. Bowden), dnr@ucsc.cmb.ac.lk (N. Ranasinghe), kasun@ucsc.cmb.ac.lk (K. De Zoysa).

https://doi.org/10.1016/j.ipm.2021.102572
Received 15 May 2020; Received in revised form 12 February 2021; Accepted 1 March 2021
Available online 12 March 2021
0306-4573/

that people practise social distancing so that possible contact with potential cases of COVID-19 is reduced. Another practice is to limit travelling both internationally and domestically.

To help people around the world stay updated regarding the status of the COVID-19 spread, it is vital that user activities are updated and tracked (Ferretti et al., 2020). People nearby should be notified about potential cases of exposure. This is especially beneficial for cases in a given region so that people can engage in outdoor activities in the region where there are no cases and reduce the possibility of contact. However, the privacy of both the potential patient and the people they could come in contact should be preserved during the process as best as possible (Abeler, Bäcker, Buermeyer, & Zillessen, 2020). Thus, there is a need for an automated digital contact tracing platform that can post information about cases in a geographical region instantaneously without exposing sensitive identity from individuals.

The main problem faced in the quarantine process is identifying and tracking activities of COVID-19 positive people who were not in the quarantine process (Wu & McGoogan, 2020). The likelihood of spread of infection is higher if a COVID-19 does not self-quarantine. There have been several cases reported in different countries, such as, Australia, Italy, Sri Lanka, where overseas travellers who were infected by COVID-19 checked into a hospital and resulted in widespread of the virus through healthcare workers (Australia-Covid19, 0000; Italy-Covid19, 0000). In all these scenarios, patients checked into a hospital to treat a non-COVID-19 related problem. The infected person may not have known that the travel had put him at a higher risk or may not have understood the timeframe that the COVID-19 virus was spreading in different areas. The lack of awareness immediately put the hospital and its staff at risk and forced them to self-quarantine for two weeks.

Some issues that can be shown from the above-mentioned scenarios are the difficulty to trace the history of user activities and the lack of guaranteed privacy. If a system existed that provided a means to trace the user activities (e.g where the user has been in the past few days, from which country the user came from etc.) and guarantee that privacy of information is retained, medical staff and other authorities could identify the suspected patients before they get affected. In the scenario mentioned above, the availability of the user activity trace would be beneficial to the medical staff to determine if the patient travelled had already visited a hot spot.

Blockchain is a distributed ledger which stores a chronological sequence of transactions in a tamper-evident manner (Androulaki et al., 2018; McConaghy et al., 2016; Nakamoto, 2008), and provides a decentralized trust system without the need for a trusted third party. Multiple parties can utilize the blockchain network and each party is guaranteed to have the same order or change of the data. The order of the data is determined by the underlying consensus algorithm of the blockchain which ensures any change to the system is applied to all participating nodes. Novel blockchains come with a component of Smart contract which is the programming API of the blockchain (Buterin et al., 2014; Eykholt, Meredith, & Denman, 2017). Smart contact is the database abstraction layer for the blockchain (Bandara, NG, De Zoysa, & Ranasinghe, 2019).

Self-Sovereign Identity (SSI) is a decentralized identity mechanism which can be implemented on top of blockchain (Mühle, Grüner, Gayvoronskaya, & Meinel, 2018). With SSI the data owner owns and controls their identity and associated data without the intervening administrative authorities. The identity owner having sole ownership of their digital and analogue identities, and control over how their personal data is shared and used. Systems like this ensure owners of data that their data is not lost during attacks on centralized large data storage or spoofed/manipulated by anyone. SSI proofs offer the ability to mathematically prove data in range or aggregation without disclosing actual values. For example, mathematical proof could be that a data holder is over 21 without revealing their actual age. Having abilities of proof such as this can encourage the sharing of critical data without the worry of revealing more information than necessary. This adds a layer of security and flexibility allowing the identity holder to only reveal the necessary data for any given transaction or interaction. With mathematical proofs of data, the cost of third party data verification and the time to process data is reduced. The digital data is proved once, and all parties that access this data can have a higher degree of trust. This will increase the throughput and access to valuable data in times where officials need to know important information in a timely manner.

The SSI cryptographic identity and proofs are stored in a decentralized blockchain, any party can use that proof to verify the identity or data proof of the individual. The process of acquiring data is done in a peer to peer fashion. If an officer wants to know if an individual has been in contact with suspected hot spots, they query the individual for proof of data. The individual can share just the information necessary to prove their tracked whereabouts. This is an important difference to current systems which attempt to grab complete travel history along with personal information. The cryptographic information that is stored on the blockchain is visible to all parties that participate, but the content of the proof is owned by the individual. Just viewing a proof on the blockchain alone is not valuable but viewing the proof with data is. This concept is how data cannot be obtained by malicious attackers. If an attacker were to steal all the proofs on the blockchain (which would be easy to do) the attackers could not utilize that information unless they were to attack each individual separately to get access to their data. If an attacker tries to spoof another use and refer to their proof on the blockchain they will not be able to alter the data in any way as the data will not match the cryptographic proof. A peer to peer information exchange is needed to acquire the data and then the blockchain distributed ledger is used to verify the integrity of the data.

Some challenges exist with an SSI system and this paper will work towards the improving or solving of these problems. From the data owner perspective, there will be a culture change. Individuals will need to be responsible for managing and protecting their own data. From a system-wide standpoint, this will offer better security, where an attacker will have to attempt to change or get access to each individual rather than one location for a large amount of data. To aid the data owner, newer designed user interfaces (UI) will ease the process of transactions and proofs on the blockchain-based system. These UI will utilize common operations that users are familiar with in other software applications. Good UI will also need to include ways to facilitate backups of the data. With users managing their own data it should be clear that if a user were to lose their device holding the data, there is not a company that can restore it for them. This personal responsibility is the cost of the added value that is brought to a SSI system. Practical

wallet systems will be the solution to easing this cost and Connect will be a solution that provides means to make these actions easier and clear.

In this paper, we propose a blockchain and self-sovereign identity-based wallet and user activity tracing platform, Connect, for tracing the confirmed COVID-19 cases and all the potential contacts of each case. The main goal of this platform is to facilitate user activity tracing by using a self-sovereign identity based mobile wallet (Mühle et al., 2018). This mobile wallet can be installed by any person who might be at risk of contacting COVID-19, or any virus. All the users' digital identities(which identified as decentralized identity (Baars, 2016) DID) and activity trace(such as the country he/she came from when he dispatched from to the airport, where the places he/she has travelled etc.) can be easily traced and proven in the blockchain as self-sovereign proof. The user's digital identity is embedded into a QR code in the mobile application. The admin authorities can scan the QR code and fetch all the activity traces which are related to this user from the blockchain. For that, we provide another mobile application "Trace" for admin authorities. This platform can be easily used to address the above-mentioned user activity tracings issues and reduce the risk of spreading the COVID-19 virus through the community.

Similar kind of user identity and activity tracing platform can be implemented with centralized cloud service as well. Cloud storage comes with inherent security and privacy issues, centralized control, immutability, and data provenance. Due to these reasons, data fraud and attacks are easier and more likely. Unauthorized third parties such as hackers, or employees of the cloud service company, may access the data and alter them. Whenever a large amount of data is stored in a central location it creates a greater incentive to attackers. To overcome these issues, we have used a blockchain-based SSI approach to build the Connect platform. In Connect, all user personal data is stored in users' physical mobile devices based on SSI architecture. Only the cryptographic identity proofs and artefacts will be stored in blockchain storage. In this way, the Connect platform addressed the above-mentioned issues with a cloud storage approach by providing Data Privacy, Confidentiality, Integrity, Authentication, Authorization security features.

We have done a performance evaluation of underlying blockchain storage in Connect platform. The evaluation shows the scalability and transaction throughput features in Connect platform. Following are our main contributions from Connect.

1. Blockchain empowered digital contact tracing platform has been introduced to address the challenges in the COVID-19 outbreak control.
2. Android/IOS based mobile identity wallet has been introduced to capture/verify the user identity proofs and activity trace record proofs.
3. A mechanism to store user identity data and activity trace record data on blockchain platforms by using self-sovereign identity proofs has been introduced.
4. The self-sovereign identity proof-based identity and activity trace storage architecture is presented to address the common issues in cloud-based data storage (e.g lack of data privacy, lack of data immutability, lack of traceability, lack of data provenance Liang et al., 2017; Yu et al., 2016).
5. A mechanism to build machine learning models(e.g isolation forest (Liu, Ting, & Zhou, 2008) unsupervised machine learning algorithm based anomaly detection model) with the activity trace data in the blockchain has been introduced.

1.1. Paper outline

The rest of the paper is organized as follows. Section 2 discusses the architecture of the Connect platform. Section 3 introduces the functionality of the Connect platform. Section 4 presents the performance evaluation, Section 5 presents a survey of related work. Section 6 concludes the Connect platform with suggestions for future work.

2. Connect platform architecture

2.1. Overview

Connect is a blockchain, self-sovereign identity-based user identity, and activity tracking platform. It can be used to track the activity of COVID-19 suspected patients during a quarantine process. For this paper, we are using COVID-19 patient activity tracking to illustrate the process of the Connect platform. Connect is application agnostic and well-suited for diverse applications such as user identity wallets, Know Your Customer(KYC) platforms, transport/delivery tracking platforms, user authentication/authorization platforms, etc. The Connect platform is built using a layered architecture shown in Fig. 1 containing four main layers.

1. Distributed ledger — Where all user cryptographic artefacts for identity (DIDs) and proofs of activity are stored.
2. DID communication layer — Where peer to peer data exchange between user identity wallets happens within the DID communication layer.
3. Credential layer — Where different entities in the platform(users, admins) create and exchange credentials for verification via credential layer.
4. Activity trace layer — Where user activity trace recording and verification happens.

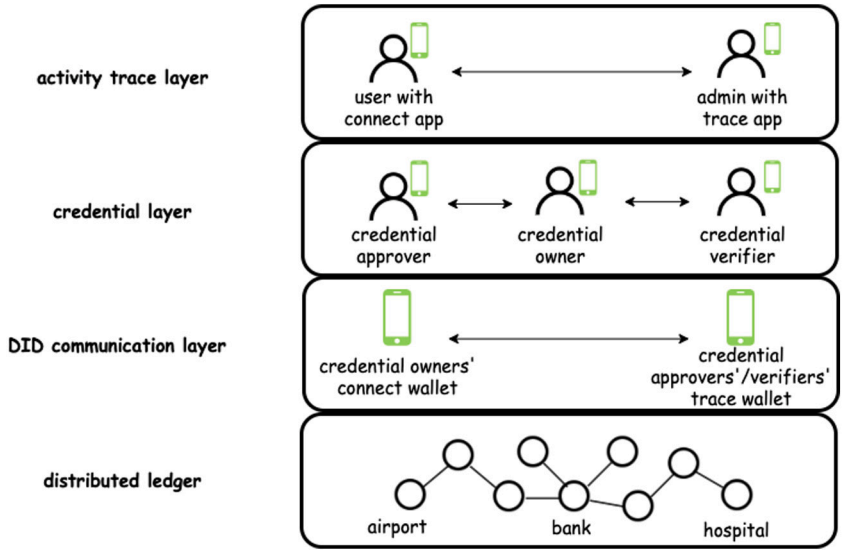


Fig. 1. Connect platform layered architecture. Distributed ledger used to store DIDs. Peer to peer data exchange between user identity wallets happens in DID communication layer. Credential create, verification happens in Credential layer. User activity trace recording and verification happens in the activity trace layer.

2.2. Distributed ledger

Distributed ledger is the blockchain-based peer to peer storage system used in the Connect platform. The blockchain can be deployed among multiple organizations such as government organizations, hospitals, airport/port customer offices, banks, identity authorities etc. Each organization in the network can run its own blockchain node connected as a ring cluster, Fig. 2. It stores all user digital identity proofs (which are identified as DID or decentralized identity proof Baars, 2016) and user activity trace record proofs on Connect platform. The user identity proofs and activity trace records stored in one node will be synced with all other nodes by using the underlying blockchain consensus algorithm. The format of the DID proof stored in the blockchain is shown in Fig. 2. The credential owners in the platform create DID proofs in the blockchain ledger. The issuers approve it and update the status of the DID proof. The verifiers use the DID proofs to verify the user identity.

DID and a self-sovereign approach puts identity proofs on a distributed ledger but the owner of the identity holds the key to the proof. This is contrasted to current systems where central authorities manage and hold the identity information in a form where they can verify the contents. The W3C is currently working on specifications of common data models, formats, and operations (Reed et al., 2019). When impersonation occurs in the current system, an attacker needs to obtain several pieces of information to prove that they are the owner of the identity. In a DID and self-sovereign approach, impersonation can occur in fewer steps where the attacker only needs to obtain the owners private key associated with their DID's. This threat is counteracted by the difficulty of an impersonator obtaining the necessary information to impersonate. Centralized systems that store the necessary information to impersonate someone offers a higher incentive to attackers versus the decentralized nature of individuals holding their own private keys. For example, the payout and cost to obtain thousands of identification information from a central location would be worth more to an attacker than it would be to attack thousands of individual devices.

In this paper, Mystiko blockchain (Bandara et al., 2018) is used, which is a highly scalable blockchain targeted for big data as the distributed ledger of Connect platform. Mystiko utilizes functional programming (Hughes, 1989) and actor (Hewitt, 2010) based "Aplos" smart contract platform to facilitate blockchain functions (Bandara et al., 2019) that are implemented with Aplos smart contracts. Identity smart contracts are used to handle the user identities and Trace smart contracts are used to handle the user activity trace records. Apache Kafka is used as the consensus platform of the Mystiko blockchain, where both the consensus algorithms and the peer to peer communication between Connect platforms' blockchain peers are handled with Apache Kafka. All transactions published by the clients will be stored and ordered in a Kafka message broker. Each blockchain peer takes the ordered transactions from a Kafka message broker and executes them with the smart contracts. For each peer in the blockchain network, there is a separate Kafka topic.

2.3. DID communication layer

The DID communication layer is used to exchange the actual credential information(such as user image, id numbers, etc.) between the credential approvers/versifiers(admins) mobile wallet and the credential owners(users) mobile wallets. Peer to peer data exchange between user identity wallets happens in this layer. When a user's identity needs to be verified/approved, admin request proof of identity from the holder, the holder consents and shares data along with cryptographic proof stored on the blockchain. The

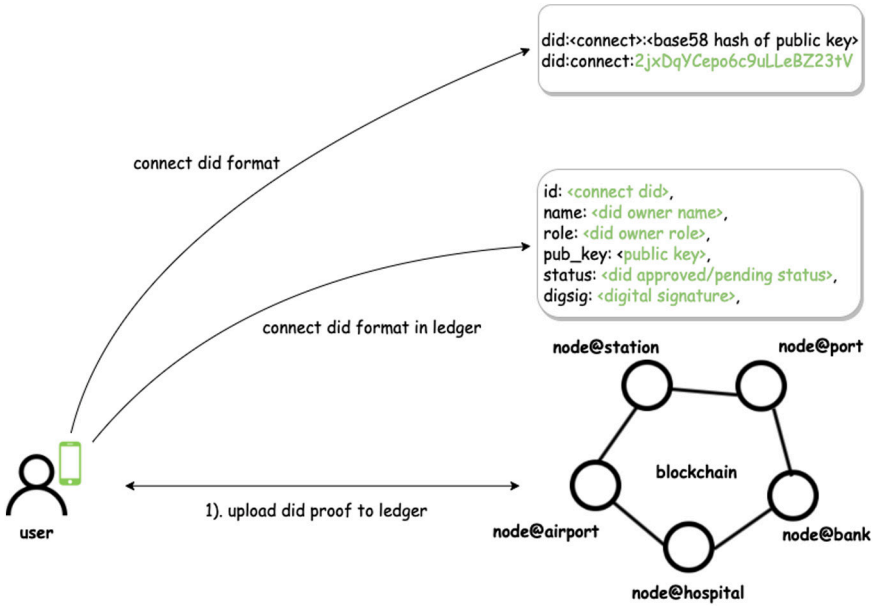


Fig. 2. Each organization in the network can run their own blockchain node connected as a ring cluster. It stores all user digital identity proofs which are identified as DID or decentralized identity proof and user activity trace record proofs on Connect platform.

Connect mobile app fetches the identity information stored in local storage to send to the admins Trace mobile wallet. The admin can do further verification/approvals based on this information.

The peer to peer communications can be implemented with TCP/WebSocket based communication service or firebase (Khawas & Shah, 2018) push notifications service. In Connect platform firebase push notification service is used to implement the peer to peer communication between mobile wallets.

2.4. Credential layer

There are two main types of entities(users) in the Connect platform, credential owners, admins(credential issuers and verifiers). Connect provides a self-sovereign identity based mobile wallet application for each type of user. Credential owners use "Connect mobile wallet" and admins use "Trace mobile wallet". Credential owners register their DID proofs on blockchain and enrol in the Connect platform with the Connect mobile application. Admins(credential issuers/verifiers) verify credentials(DID proofs) via Trace mobile wallet. All credential cryptographic information is stored on the blockchains distributed ledger. When performing DID register and credential verification, credential owners and verifiers interact with the underlying blockchain ledger to put and fetch credentials. The credential exchange process happens in the Credential layer, where credential owners and admins exchange the credentials for verification. It implements all credentialing functions such as credential create, approval, and verification.

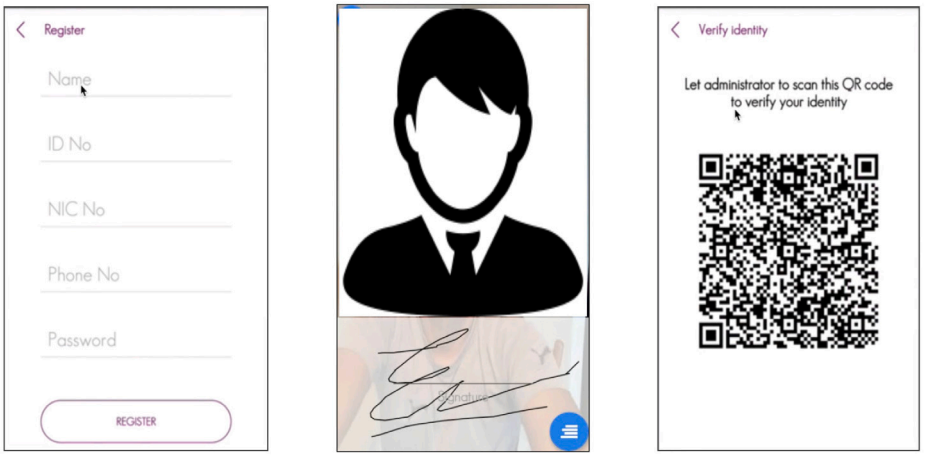
2.5. Activity trace layer

All user activity traces(such as the country he/she came from when he dispatched from to the airport, where the places he/she has travelled etc.) in the Connect platform are stored in the blockchain ledger based on an SSI approach. When a user decides to go to a specific place(e.g airport, bank, hospital) the admin officers there can verify the identity of the user and create an activity trace record for the user on the blockchain. This identity verification and activity trace data creation process is done via Trace mobile wallet application given to the admin officers. Admins also can fetch user activity trace records which are stored in the blockchain when consent is given, verify them, and view through the Trace mobile application. Trace mobile app comes with a QR code scan-based identity and activity trace data verification process. All activity trace data is handled with functions(activity trace data creation, activity trace data verification) implemented in the Activity trace layer.

3. Connect platform functionality

3.1. Use case

Consider a scenario where a blockchain network is deployed at the Airport, Hospital network, Government Bank and Identity office. The admin officers at each organization installed the Trace mobile app. A user who comes from overseas installed the Connect



(a) Add identity information (b) Capture photo and signature (c) Connect identity in QR code

Fig. 3. Connect mobile wallet application. It will embed users' digital identity on QR code.

mobile wallet and registered on it before entering the airport. As shown in Fig. 3, when registering it first captures basic user information with ID number/Passport number. After that, it asks users to capture their photo and put a signature on top of the photo. This information can be used as additional proof which administrators can use to approve/verify the user identity. The captured information will be saved in secure storage in a mobile application and the proof of this information will be uploaded to the blockchain as a self-sovereign identity proof(DID proof). When uploading credentials, the app will generate a public/private key pair which corresponds with the user/mobile wallet. The private key will be saved on the Keystore on the mobile application. The public key and base58 (Fisher & Sanchez, 2016; Nakamoto, 2008) hash of the public key will be uploaded to the blockchain along with other DID proof information. The base58 hash of the public key will be used as the digital identity(DID) of the user on the Connect platform. Fig. 2 shows the format of the DID proof on the Connect platform. This DID will be embedded to QR code in the mobile app, which the user can show to admin officers (e.g admin at the hospitals, custom officer at the airport, banks officers) for verification, Fig. 3. The registration flow described in Fig. 4.

When the user comes to the airport he/she needs to show the QR code identity which is embedded in the mobile app to the admin officer(e.g customer officer) at the airport to have their digital identity issued, Fig. 3. The officer will scan the QR code via Trace application and fetch the user identity proofs which are saved in the blockchain. After that, it requests for consent to specific data and connects to users through the "Connect mobile wallet" application. This process is achieved via push notification(DID communication layer) to fetch the actual user identity information(e.g Id numbers, photo, signature) to the Trace mobile app, Fig. 5. Then the admin could check the information against the passport/id card of the user. If the data is correct according to the passport/id card, the admin approves the identity of the user. When approving, it updates the status of users' digital identity in the blockchain, Fig. 6. This is the first-time vetting process which needs to be done to approve the user identity saved in the blockchain is authentic and verified by a trusted source. Once identity is approved by an authorized administration user can use his/her identity wallet in any other place to prove his/her identity (ex in a bank, hospital etc.). When approving the identity, it will use the Identity smart contact. After identity approved blockchain will create an activity trace record (along with user digital identity/DID, date/time and location) by using Trace smart contract. This activity trace record specifies the user is dispatched from the airport. Once the activity trace record is created in the blockchain node at the airport, it will be available to other blockchain nodes at hospitals and banks.

For example, assume the user goes to a bank a few days after he/she enters the country. User needs to show his/her identity wallet QR code to prove identity at the bank. Then the admin at the bank scans the QR code, fetches the identity proof of the blockchain and verifies the user. At the end of this process, blockchain will save another activity trace record which mentions that the user came to the bank with date/time and location. In this way, the Connect platform traces all the user activities as self-sovereign identity proofs (or proof of location). Now assume the user goes to the hospital for some various treatment. The user shows the identity wallet with QR code, then an officer at the hospital scans it and fetches the user identity proof with all user activity record proofs from the blockchain. The activity trace contains an activity that mentions the user came from a foreign country and dispatched from the airport on a specific date, Fig. 5. With this information, it can be easily identified if a person could be suspected of COVID-19. Further precautions can be taken before spreading the virus to more people.

With this information, Connect platform can support and trace activities of potential COVID-19 infections (symptomatic individual), people who have been in contact with COVID-19 infections, people who are a risk of getting infected with COVID-19(e.g people who have come from foreign countries, people who have visited an area/place where COVID19 infected person visited). By recording an activity trace of users, Connect platform can support in identifying spread from three main transmission

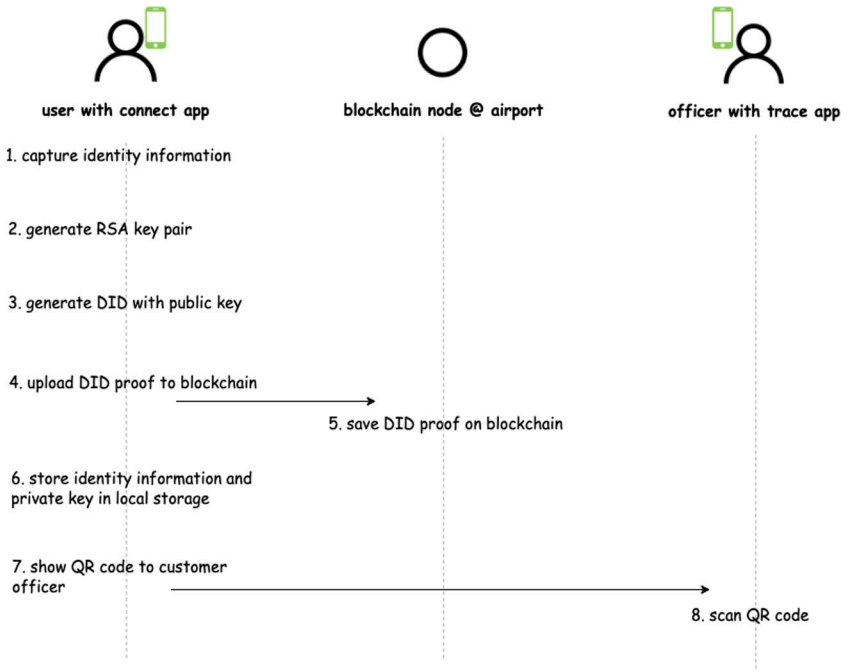
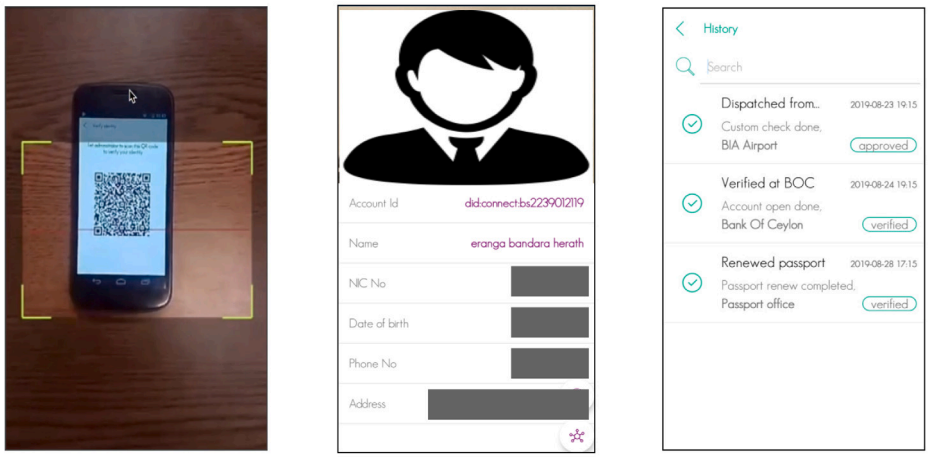


Fig. 4. User capture credentials and register on the Connect platform when coming to the airport. Blockchain will store a proof of user credentials.



(a) Scan user identity (b) View user identity (c) View activity trace

Fig. 5. Trace mobile application. It can view users' identity information and activity trace.

methods of COVID-19 virus, Symptomatic transmission(direct transmission from a symptomatic individual), Pre-symptomatic transmission(direct transmission from an individual that occurs before the source individual experiences noticeable symptoms), Asymptomatic transmission(direct transmission from individuals who never experience noticeable symptoms).

3.2. Contact tracing

The users in the Connect platform can be notified via the peer to peer notification system. These notifications can be used to notify the users who are at risk of getting infected with COVID-19 virus. For example, assume a user who has registered in the Connect platform is diagnosed as a COVID-19 infected person. The medical officer at the hospital can report the patient to the Connect platform via Trace mobile application. Additionally, the Connect mobile wallet provides a feature to self-report the diagnosis of the users. This diagnosis information will be uploaded and stored in the blockchain. Once COVID-19 case is reported, the Connect platform can identify all places where the patient has visited(during the last 14 days) by using the activity trace data in

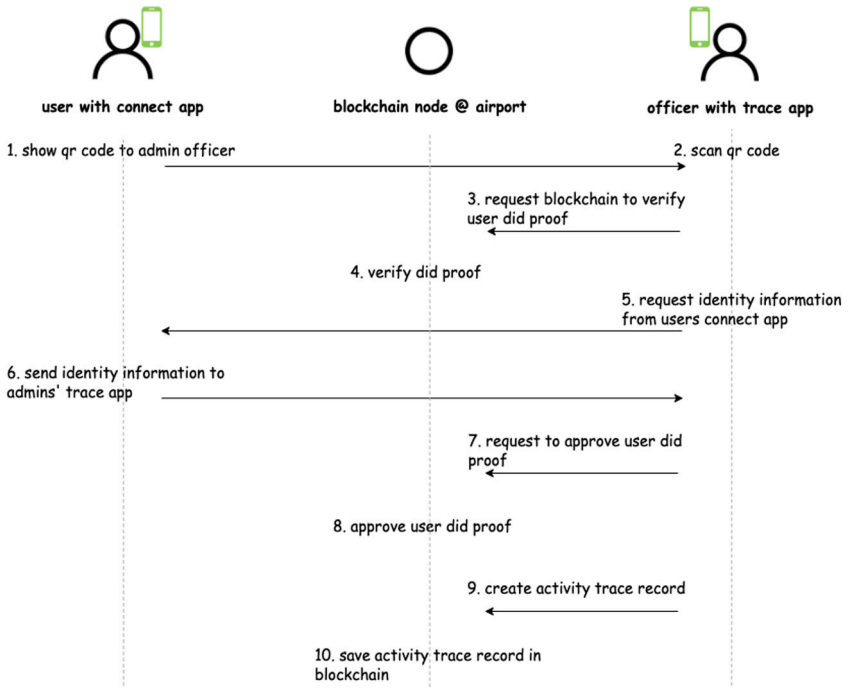


Fig. 6. Custom officer at airport scans QR code identity of the user and fetches the credentials from blockchain. Then the officer verifies and approves the credential.

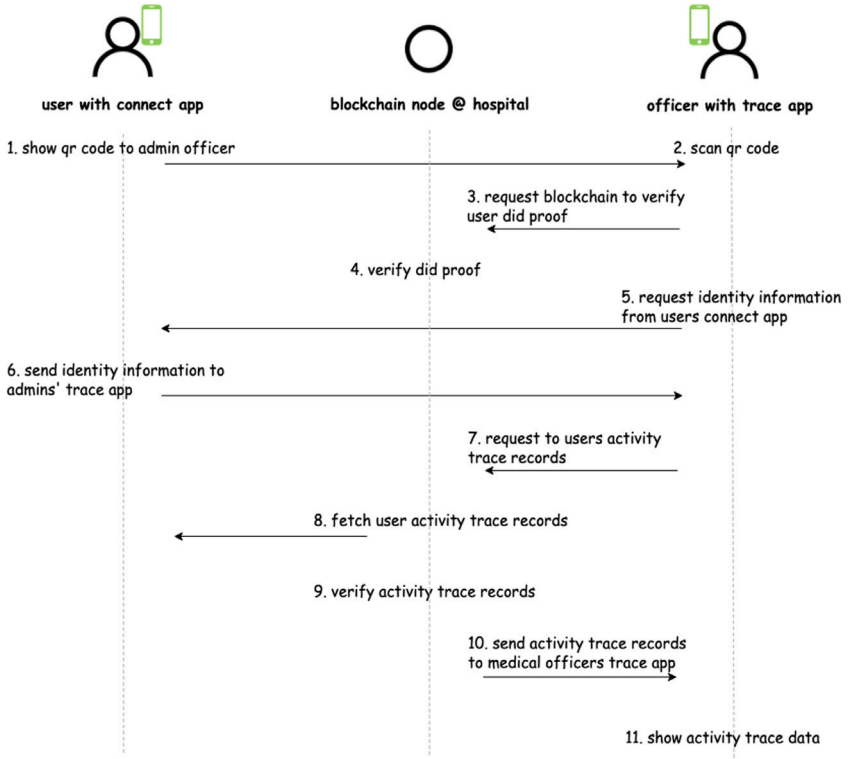


Fig. 7. Medical officer at hospital scan QR code identity of the user and fetch the activity trace record history of the user from blockchain.

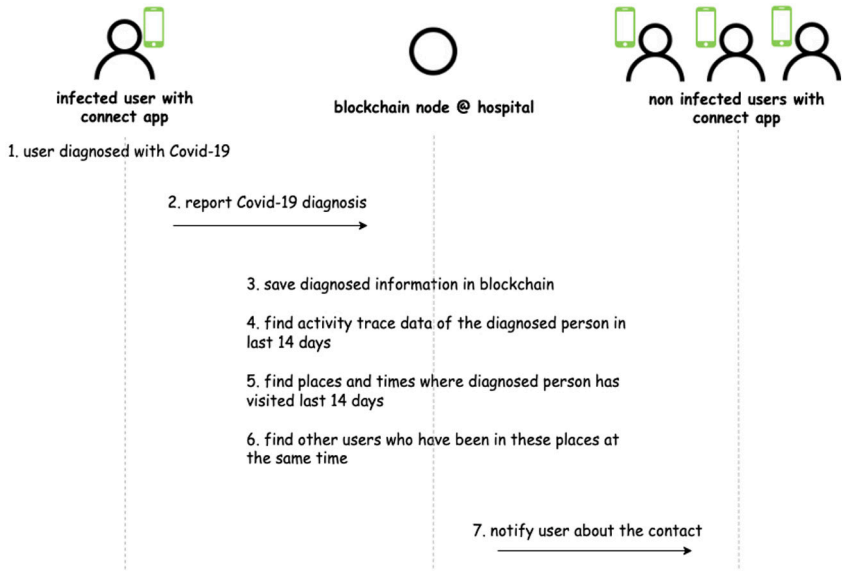
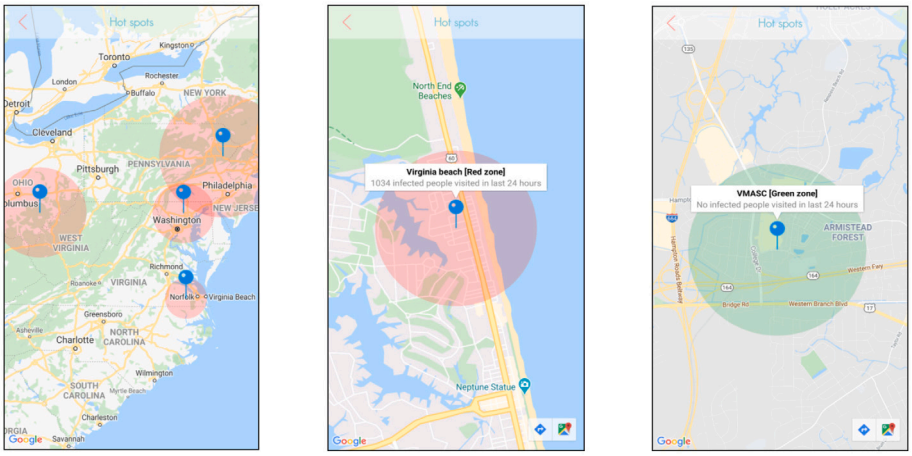


Fig. 8. COVID-19 contact tracing. Once user identified as COVID-19 infected person, Connect platform finds the other users who has contacted with that person and notify to them.



(a) Hot spots (b) Red zone (c) Green zone

Fig. 9. View hot spot information. Hot spot critical level decided based on the infected people count visited to the place. These location data traced with the activity trace records of the COVID-19 diagnosed people in Connect platform. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

the blockchain. The activity trace data contains the times and places the diagnosed person has visited. Based on these activity trace information, it can identify the other users who have been in these places at the same time with COVID-19 infected person without revealing personal information. Then Connect platform can send a notification to these users mentioning there is a risk of contact with COVID-19 since they have been in a place where COVID-19 infected person visited, Fig. 8. With the notification function, the user can be aware of the risks in time and take some actions accordingly.

Based on the activity trace data of the COVID-19 diagnosed people, Connect platform can identify COVID-19 hot spots. These hot spots information will be shown in a Map view (Fig. 9(a)) on Connect mobile wallet application. The users can search specific location in the map and see the critical level of that place, red zone (Fig. 9(b)) or green zone (Fig. 9(c)). Hot spot critical level is decided based on the infected people count visited that place recently. These location data traced with the activity trace records of the COVID-19 diagnosed people in the Connect platform.

3.3. Additional trace features

The Connect platform can be used to track the COVID-19 patient status, behaviour and all the locations travelled. For example, if a user is identified as a COVID-19 patient there is a function in the users' mobile application to track the status of the user and the locations. Then the app will track all the location records he/she is visiting behind the scene via google location API (Doshi, Jain, & Shakwala, 2014) and upload to the blockchain as trace records. This feature in Connect platform can further identify the people who had close contact with the infected individual and take the necessary precautions. When a patient is discharged from the hospital(due to tested negative after a while or having mild symptoms) Connect platform can record a trace record about that event. The discharged patients also can be further monitored for two or three weeks by enabling user location tracking of the Connect app while still maintaining privacy. Also, this platform can be used to communicate with patients such as updates to the patients about medicine, precautions he/she needs to take, quarantine dates etc.

3.4. Identity verification

The identity verification of issued material on Connect uses the QR code embedded in a users' mobile application. The QR code in the mobile application contains the users' digital identity(DID) as well as a digitally signed random number by using users private key(users private key stored in secure storage in the Connect mobile application). Trace app will scan the QR code content(user identity and the digital signature of the random number) and submit it to the blockchain to verify the identity of the user. The smart contract in the blockchain will verify the identity status and digital signature of the message using the public key of the user(public keys of the users are saved in the blockchain). If the identity is verified, the status will be sent back to Trace mobile application. Trace mobile application will send a push notification to the User's mobile wallet application(DID communication layer), fetch the actual identity information(id numbers, image, signature etc.) and show them on the mobile screen. The actual identity information saved on users' mobile wallet(not in blockchain, blockchain keeps only the proof of the identity as a self-sovereign identity). If desired the administrator can do further verification of the user by requesting to see the actual identity information in addition to the proof(image, signature etc.) (Hammudoglu et al., 2017; Othman & Callahan, 2018).

3.5. Activity trace verification

When creating trace records, the blockchain node will sign the trace record with its private key and save it on the blockchain. For example, when creating a trace record of the user dispatch event from the airport, the blockchain node at the airport signs that trace records with its private key. All the digital signatures are stored with the trace records in the blockchain. When Trace mobile app requests to fetch the trace records of a user, the Trace smart contract will get the trace records of the user and verify their digital signatures first. Then it will return all valid activity trace records of the user to the Chose mobile application. Finally, Trace app will show this information on the mobile screen.

3.6. Data privacy and security

The Connect platform guarantees Privacy, Confidentiality, Integrity, Authentication, Authorization security features. To guarantee privacy, only the users' identity proof will be stored on the blockchain. Actual identity data such as id/passport numbers, image, and signature is stored on a users' physical mobile phones secure storage(the DID generation and credential storage process shown in Fig. 4). When this information is needed by officials for verification, it can fetch directly via user's mobile application using push notifications(credential fetching process shown in Figs. 6 and 7). By using the SSI based approach, Connect platform addresses the common issues in centralized cloud-based storage platforms (e.g. lack of data privacy, lack of data immutability, lack of traceability).

All the peer to peer messages transferred between mobile wallet applications are end-to-end encrypted. When initiating the peer to peer communication, the peers exchange an AES encryption key using RSA encryption keys (Jonsson & Kaliski, 2003). For example, when sending credential information from the user's Connect mobile application to trace mobile wallet application, the Connect app generates an AES key and exchange it with the trace app. When exchanging the AES key, Connect app encrypts the key with trace app owners' RSA public key. Then trace app takes the encrypted key, decrypts it with the private key, and obtains the AES key. After the key exchange happens, all communications will be encrypted with the exchanged key. Further to guarantee the integrity of the messages, RSA cryptography-based digital signature mechanism (Jonsson & Kaliski, 2003) is used. All data in the Connect platform are digitally signed by a corresponding party. We have used JWT based authentication/authorization services to handle the authentication/authorization of the Connect platform. The users' authentication information(username/password fields) of Connect platform is stored in JWT auth service (Jones, 2011). On login, the user sends an authentication request to the auth service, then it verifies the credentials and returns the JWT auth token to the user. This auth token contains user permission, token validity time, digital signature etc. All subsequent requests need to add the JWT token into the HTTP request header to do the authentication and authorization. The token verification is handled by the gateway service in Connect platform, as is shown in Fig. 10.

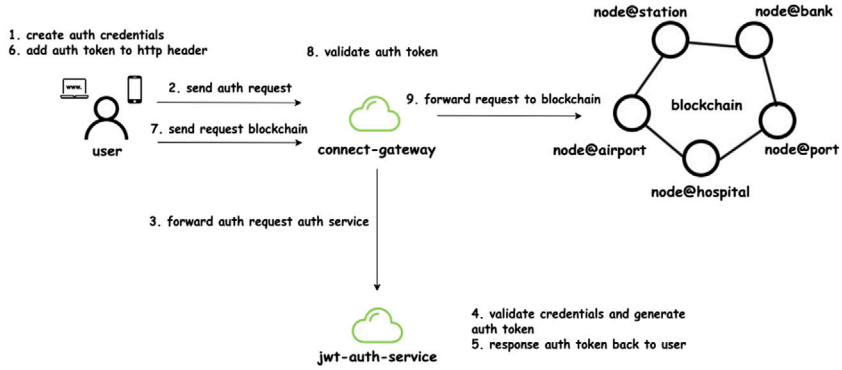


Fig. 10. JSON Web Token(JWT) based auth service in Connect platform. Auth tokens will be issued by auth service. Token validation happens at gateway service.

4. System evaluation

Before we dive into the details of the performance evaluation of the Connect platform, we will discuss the security capabilities in the following. Firstly, Connect can provide a self-sovereign identity based mobile wallet application for each type of users, including the credential owners and admins. All credential cryptographic information is recorded on the blockchain ledger. When uploading credentials, the application will generate a public/private key pair which corresponds with the user/mobile wallet. The private key will be saved on the Keystore on the mobile platform. Users have the option to subscribe to the notification service while preserving their user privacy. User access records are anonymized among the blockchain nodes. The service provider cannot access the data of user activities. Anonymity is implemented by two practical design features. For one hand, each user's identity will not be related to activity data records since the self-sovereign identity is adopted. For the other hand, the unlinkability between each user's activity records is also achieved, especially for the data related to the tracking status of the user and the locations.

Secondly, the Connect platform provides real-time tracking for all user activities via the Trace mobile wallet application. We use activity record as a data unit and all the traces of a particular user registered in this platform are automatically audited and recorded by the blockchain nodes. In this way, evidence for all user track events can be monitored. For each of the activity track record, we transform the track data and upload the record to the blockchain network. By doing so, we create an unalterable fingerprint of user activities, with the functions of the secure and permanent record keeping as well as a tamper-proof timestamping. Any event related to the personal record will be collected by the blockchain, and once the data record is published, no one can rewrite or alter the records without being detected. By utilizing the blockchain network, the need for trust is reduced or even removed. There is no need to rely on the trustworthiness of the owner of the remote computers involved in the blockchain network, thus removing the necessity for a trusted third party. Even the service provider is not trusted for keeping the user activity data record. With the decentralized architecture, data records are to be confirmed and validated by the consistent checking and validation among computing nodes.

Overall, the Connect platform guarantees privacy, confidentiality, integrity, authentication, and authorization. To guarantee privacy, only the users' identity proof will be stored on the blockchain. Actual identity data such as id/passport numbers, image, and signature is stored on the users' physical mobile phones secure storage. Besides, the decentralized architecture ensures the integrity of data records and each data record has a copy on multiple distributed nodes in the blockchain network, thereby resisting against DDoS attacks. Meanwhile, there is no single point failure since no single node in the network keeps all the data records.

A performance evaluation of Connect was completed and is discussed. We deployed Connect platform with multi peer Mystiko blockchain cluster in AWS 2xlarge instances(16 GB RAM and 8 CPUs). The mystiko blockchain is supported with 4 Kafka nodes, 3 Zookeeper nodes and utilizes Apache Cassandra (Gormley & Tong, 2015; Lakshman & Malik, 2010; Strapdata, 2018) as the state database. The smart contracts on the Mystiko blockchain implemented with Scala functional programming (Odersky et al., 2004; The Scala Programming Language, 0000) and Akka actor (Akka, 0000; Gupta, 2012) based Aplos (Bandara et al., 2019) smart contract platform. The evaluation results are presented below, with a varying number of blockchain peers (1 to 5 peers) used in different evaluations.

1. Transaction throughput
2. Transaction scalability
3. Transaction execution rate
4. Search performance
5. Block generate time

4.1. Transaction throughput

This experiment recorded the number of DID proof create transactions and DID proof query transactions that were executed in each peer in the Connect platform. When creating a DID, an invoke transaction will be executed in the underlying blockchain.

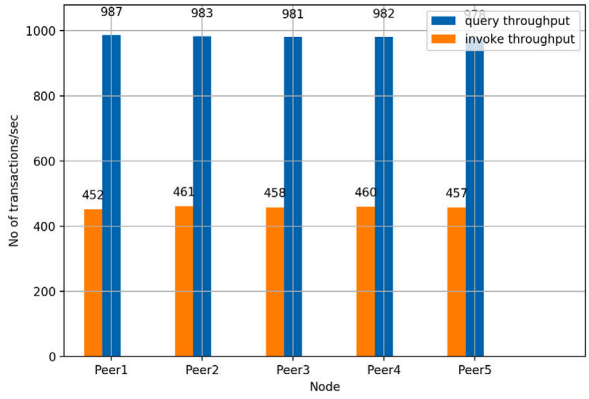


Fig. 11. Invoke and query transaction throughput of Connect platform.

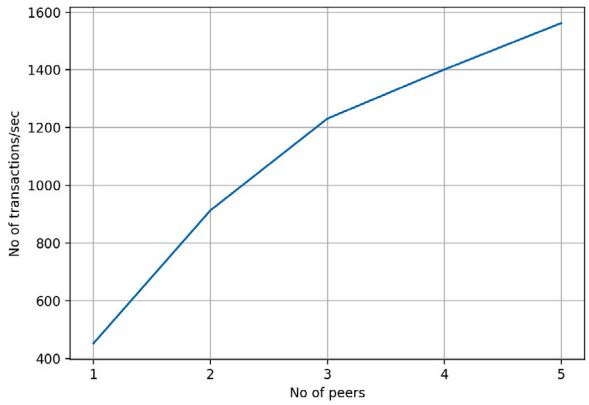


Fig. 12. Transaction scalability of Connect platform.

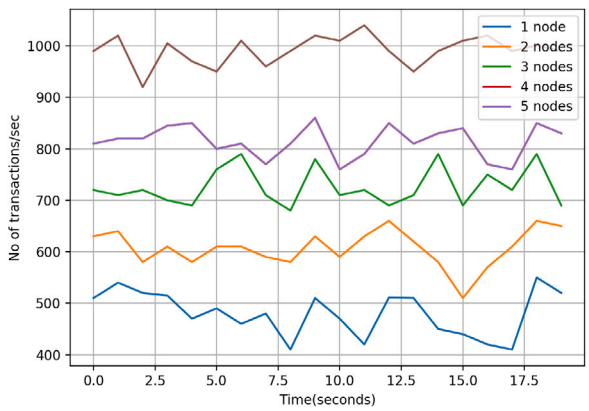


Fig. 13. Transaction execution rate with no blockchain peers in the Connect platform.

Invoke transaction creates a record in the ledger and updates the status of the shared ledger in the blockchain. Query transaction searches the status of the underlying blockchain ledger. They neither create transactions in the ledger nor update the ledger status. We flooded concurrent transactions for each peer and recorded the number of completed results. As shown in Fig. 11 we have obtained consistent throughput in each peer on the Connect platform. Since queries are not updating the ledger status, it has high throughput(2 times) compared to invoke transactions.

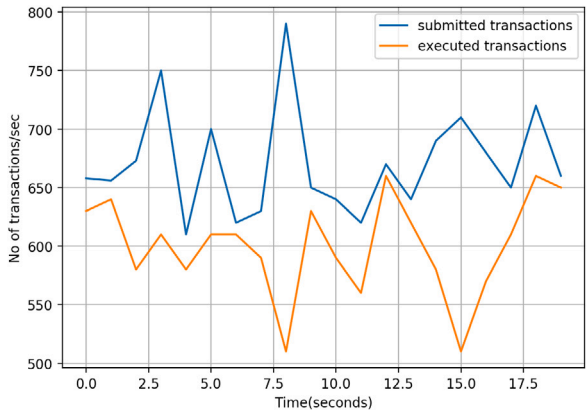


Fig. 14. Transaction execution rate and transaction submission rate in a one blockchain peer of the Connect platform.

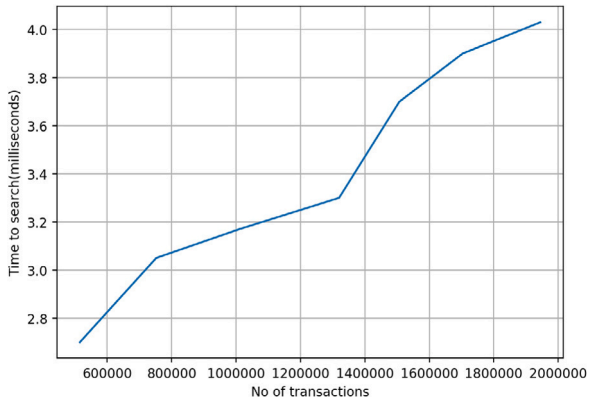


Fig. 15. Search performance of Connect platform.

4.2. Transaction scalability

For this evaluation, we recorded the number of transactions that can be executed (per second) against the number of peers in the network. We flooded concurrent transactions in each peer and recorded the number of executed transactions. Fig. 12 shows transaction scalability results. When adding a node to the cluster, it nearly linearly increases the transaction throughput. Which means the transaction latency will be decreased when adding blockchain peers to the cluster. As peers are added there is a diminishing return where the performance benefit will degrade if too many peers are added.

4.3. Transaction execution rate

Next, we evaluate the transaction execution rate in the Connect platform. We tested the number of submitted transactions and executed transactions in different blockchain peers recording the time. Fig. 13 shows how transaction execution rate varies when having a different number of blockchain peers in the Connect platform. When the number of peers increases, the rate of executed transactions is increased relatively. Fig. 14 shows the number of executed transactions and submitted transactions in a single blockchain peer. There is a back pressure operation (Destounis, Paschos, & Koutsopoulos, 2016) between the rates of submitted transactions and executed transactions. We have used a reactive streaming (Akka Streams Documentation, 0000; Davis, 2019) based approach with Apache Kafka to handle these backpressure operations in the Connect platform.

4.4. Search performance

Connect provides the ability to search identity information and activity trace information via underlying Mystiko blockchains' Lucene Index-based search API. For this evaluation, we issued concurrent search queries into Connect and computed the search time. As shown in Fig. 15, to search 2 million records, Connect took 4 ms.

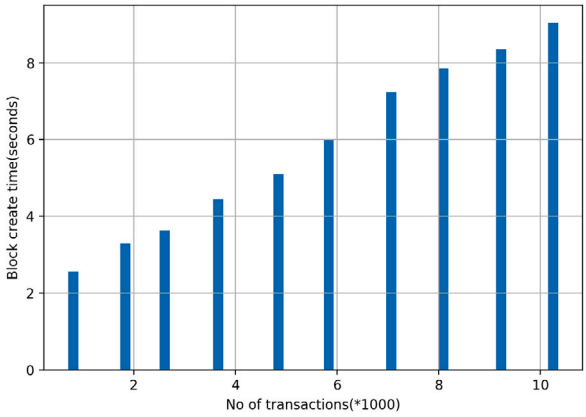


Fig. 16. Block create time of Connect platform.

4.5. Block generate time

Finally, we have evaluated the time taken to create blocks in the underlying blockchain storage of the Connect platform. The statistics recorded against the no of transactions in a block. Block generate time depends on (a). data replication time (b). Merkel proof/block hash generate time (c). transaction validation time. When the transaction count increases in the block, these factors will be increased. Due to this reason, when the transaction count increases, block generation time also increases correspondingly. As shown in Fig. 16 to increase a block when having 10k transaction, it takes 8 s.

5. Related work

Research has been conducted to find new technologies that mitigate virus outbreaks like COVID-19 (Allam & Jones, 2020; Cho, Ippolito, & Yu, 2020; TraceTogether, 0000) and integrate self-sovereign identity concepts with blockchain technology (Liu, Sun, & Schuckers, 2019; Sharma & Lim, 2019). In this section, we outline the main features and architecture of these research projects.

TraceTogether (TraceTogether, 0000) is a mobile application-based platform to detect potential COVID-19 virus carriers in Singapore by exchanging short distance Bluetooth signals with other users of the app. It gives officials a database to track potential COVID-19 carriers diagnosed with COVID-19, the respiratory illness caused by the coronavirus. Users allow Singapore's health ministry to access their app data to identify people who had close contact with the infected individual. The app alerts those who come in contact with someone who has tested positive or is at high risk for carrying the coronavirus.

Google/Apple Contact Trace (Google and Apple, 2020) Google and Apple recently announced a joint initiative to build a contact tracing feature and capability within their mobile smartphone operating systems to help contain the COVID-19 spread. They will be launching a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing applications. Their system uses Bluetooth, a standard way for most mobile devices to communicate with each other within short proximity's. Apple and Google stressed that their system preserves users' privacy by utilizing cryptographic methods in order to preserve privacy. Consent is required and location data is not collected. The technology also will not notify users who they came into contact with, or where that happened.

WeTrace (De Carli et al., 2020) is a fully privacy-preserving approach and application built on top of BTE(Bluetooth Low Energy). This solution meets major GDPR (General Data Protection Regulation) requirements, which are in force in certain European countries. WeTrace fulfils key requirements on privacy-preserving for arbitrary mobile devices, communicating via BTE and used by their owners in a once-used, once-associated manner. The application of low-range BTE communications determines a highly suitable coincidence between the COVID-19 "social distancing" requirements and the communications technology.

COVID Credentials Initiative(CCI) (CCI, 0000) is a collaboration of more than 60 organizations working to deploy self-sovereign identity(SSI) based verifiable credential solutions to help stop the spread of COVID-19. The goal of CCI is to provide cryptography referred to as "immunity passport", which is a digital certificate that lets individuals prove (and request proof from others) that they have recovered after testing negative, have tested positive for antibodies, or have received a vaccination once one is available. The digital certificates could be issued by verified authorities such as health care institutions, but held and controlled by the user and shared in a peer-to-peer manner. The CCI group includes members and collaborators of Evernym, ID2020, uPort, Dutch research organization TNO, Microsoft, ConsenSys Health and consultants Luxoft.

Hyperledger Indy (indy, 0000) is a public/permissioned distributed ledger(blockchain) designed and built as a standard means of achieving decentralized self sovereign identity. Indy permits registered members to manage (write) their self-sovereign identity, and makes public the content of the blockchain that contains cryptographic material that users can use to prove their identities. The ledger is maintained by nodes, which run Plenum Byzantine Fault-Tolerant Protocol, i.e. (a consensus protocol based on Redundant Byzantine Fault Tolerant Aublin, Mokhtar, & Quéma, 2013) to agree on the order of transactions in the ledger. Pairwise

Pseudonymous Identifiers and Decentralized Public Key Infrastructure (using asymmetric key cryptography) guarantee full privacy, prevent identity correlation and ensure that Connections between the members of the system (nodes and clients) are established in a secure, encrypted manner. Indy uses DIDs as the primary keys on Indy ledger, enable long-term digital identities requiring no centralized registry services.

Sovrin (Tobin & Reed, 2016) is an open-source decentralized identity network built on permissioned Distributed Ledger Technology built on the Hyperledger Indy platform. Sovrin is public, but only trusted institutions, called stewards – which could be banks, universities, governments, etc can run nodes that take part in consensus protocols: thus, the ledger is permissioned. The non-profit Sovrin Foundation ensures the proper governance of the stewards and their respect for a legal agreement called the Sovrin Trust Framework. Sovrin enables a user to generate as many identifiers as needed to keep contextual separation of identities for privacy purposes; each identifier is unlinkable and controlled by a different asymmetric key pair. Sovrin identifiers themselves are managed by the user or an appointed guardian service and follow the Decentralized Identifier (DID). A DID is standardized data structure containing the user identifier, cryptographic public key and other meta-data necessary to transact with that identifier.

Portable Trust (Hammudoglu et al., 2017) is a biometric-based authentication and blockchain storage for self-sovereign identity systems. A biometric-based authentication prototype is developed that is permissionless, autonomous, and open-source. This allows the user to securely store personal information that can only be accessed after successful biometric authentication. It integrates a permissionless blockchain with identity and key attestation used on mobile phones. The focus with this project is to implement self-sovereignty while storing and using secrets and biometric material held by the user. In this way the user maintains full control ensuring privacy enhancements.

Horcrux (Othman & Callahan, 2018) protocol is a method for securing biometric information, registration, and access. The protocol is generalized for two or more biometric shares that can be stored across mobile devices and personal storage providers with redundancy for added availability and safety. The biometric data owner is able to authorize others to get access to the data without permission from a third party. The owner can assert the identity transaction claim or authorize a verified and trusted third party to do so. The trust is diffused in its self sovereign environment and is not controlled by any single or grouped organizations. Blockchain is used to enable this environment by creating multiple department nodes which are official trusted entities like organizations and governments. As a result, department nodes mutually form distributed consensus and record data in different places providing more resistance to mistakes by keeping redundant copies.

uPort (uPort, 0000) allows the identity owners to control their personal identity and corresponding keys and data. Owners can authorize others to access to data, enable digital services such as signing documents, interact with smart contracts as well as applications with the blockchain, and encrypt data. The uPort enterprise can create identities for new customers and employees, establish a Know-Your-Customer (KYC) process, build secure access-controlled environments with less friction, hold little sensitive information to reduce liability, maintain the network of vendors, and establish an environment where identities have specific roles and nothing to do with actors.

Jolocom (Jolocom, 2019) is an open-source protocol that is general in nature to facilitate identity records for a person and non-person entities. The protocol is designed to operate on public blockchain infrastructures such as Ethereum. Digital identifier (DID) information is stored on the blockchain and all personal information is stored off-chain in control of the user in a self sovereign way. The protocol currently exists as a working prototype on the Ethereum test network.

EtherTwin (Putz, Dietz, Empl, & Pernul, 2021) work proposes blockchain-based Digital Twin (DT) information sharing platform. Digital Twin has widespread with industrial 4.0 and digitization of industrial processes. The confidentiality and access control are the major issues raised in information management and sharing in Industry 4.0 with DTs. To tackle these challenges EtherTwin proposes blockchain-based decentralized DT data-sharing model with the owner-centric approach. EtherTwin handles the sharing of Digital Twins data among multiple lifecycle parties without trust while ensuring confidentiality, integrity and availability. The prototype of the proposed EtherTwin platform is implemented on Ethereum as a blockchain-based DApp.

B-FERL (Oham, Michelin, Jurdak, Kanhere, & Jha, 2021) is a Blockchain-based Framework for sEcuring smaRt vehicLes. It utilizes a permissioned blockchain to allow only trusted entities to manage the record of vehicles in the blockchain network. B-FERL defines a two-tier blockchain-based architecture that introduces an initialization operation used to create and record vehicles for authentication purposes. A challenge–response mechanism where the integrity of a vehicle's internal network is queried when it connects to an RSU is used to ensure its security. The approach used by this solution meets the integrity requirement for securing smart vehicles and the availability requirement for securing vehicular networks. Ultimately, B-FERL achieves various critical automotive functions such as vehicular forensics, secure vehicular communication and trust management.

Amanuensis (Hardin & Kotz, 2021) is an information provenance platform for mHealth device-based Health-Data Systems. mHealth devices continuously monitor patient data and give healthcare providers a more holistic view of a patient's health. Because of the constant connection and exchange of information, confidentiality, access control, and data provenance are major issues raised in the mHealth data. To address these issues Amanuensis proposes a trusted and secure data sharing ecosystem for mHealth devices by leveraging Blockchain and Trusted Execution Environment (TEE). In Amanuensis, data access and computation take place inside of TEEs preserving data confidentiality, and provides a verifiable attestation that can be stored on the blockchain in support of information provenance. A blockchain is used to record and enforce data access policies guaranteeing information provenance for mHealth data and removes the need to trust a single entity with gate-keeping the health data. The prototype of the Amanuensis system is developed on VeChain Thor blockchain platform utilizing Intel SGX trusted execution hardware.

A summary of the comparison of these platforms with our Connect platform is presented in Table 1. It compares six different properties including the Architecture(Centralized/Decentralized), blockchain infrastructure used, Supported credential types(e.g biometric), SSI support, Activity trace support, and the Privacy level. Based on the comparison in Table 1 we have observed that

Table 1
Self-sovereign identity and activity trace tracking platform comparison.

Platform	Architecture	Running blockchain	Credential type	SSI support	Activity trace support	Privacy level
Connect	Decentralized	Mystiko	Any	Yes	Yes	High
TraceTogether (TraceTogether, 0000)	Centralized	N/A	Any	No	Yes	Low
Google/Apple Contact Trace (Google and Apple, 2020)	Centralized	N/A	N/A	No	Yes	Mid
WeTrace (De Carli et al., 2020)	Centralized	N/A	N/A	No	Yes	High
CCI (CCI, 0000)	Decentralized	Sovrin	Medical	Yes	No	High
Hyperledger Indy (indy, 0000)	Decentralized	Indy	Any	Yes	N/A	High
Sovrin (Tobin & Reed, 2016)	Decentralized	Indy	Any	Yes	N/A	High
Portable trust (Hammudoglu et al., 2017)	Decentralized	N/A	Biometric	Yes	Yes	Mid
Horcrux (Othman & Callahan, 2018)	Decentralized	N/A	Biometric	Yes	No	Mid
uPort (uPort, 0000)	Decentralized	Ethereum	Biometric	Yes	No	Mid
Jolocom (Jolocom, 2019)	Decentralized	Ethereum	Any	Yes	No	High
EtherTwin (Putz et al., 2021)	Decentralized	Ethereum	N/A	No	N/A	High
B-FERL (Oham et al., 2021)	Decentralized	N/A	N/A	No	N/A	Mid
Amanuensis (Hardin & Kotz, 2021)	Decentralized	VeChain Thor	Medical	No	N/A	Mid

none of the existing platforms support privacy-preserving contact tracing which is built into our Connect platform as a contribution. The self-sovereign identity approach used by the Connect platform does not expose user personal data and activity trace data to any third parties. In Connect all data resides on users personal mobile wallet application which guarantees a high level of privacy. Only identity proofs are stored in the distributed blockchain storage. Unlike Connect, the existing contact tracing platforms use centralized storage to store all the user personal data and activity trace data. Users do not have control of their own data once published into centralized storage. This approach is highly vulnerable to various types of attacks and privacy breaches. Connect uses a blockchain-based decentralized approach to facilitate the contract tracing functions among different participating entities and but none of the existing contact tracing platforms support a decentralized approach similar to Connect. The listed platforms are governed by trusted centralized entities which are vulnerable to privacy attacks. When compared with existing self-sovereign identity platforms, Connect guarantees all privacy measures and identity types that are supported. With these observations, we claim that Connect is a privacy-preserving contract tracing platform to support Covid-19 outbreak control.

6. Conclusions and future work

With Connect we have proposed blockchain and self-sovereign identity-based user identity and activity tracings platform. The blockchain can be deployed among various organizations such as airports, banks, and hospitals. The user identity proofs and activity trace data proofs are stored and shared between different organizations by using the blockchain and specific data is shared peer to peer. This information can be used to trace the activities of suspected patients of COVID-19 virus. Connect will support the effort to stop the spread of viruses like COVID-19 by giving users a way to prove location and travel as well as provide valuable information on if they might be at risk.

In the Connect platform, all personal data is stored in the users' physical mobile devices based on SSI architecture. Only identity proofs will be stored in the distributed blockchain storage. With this approach the Connect platform addresses security and privacy issues on cloud centralized storage(e.g lack of data privacy, lack of traceability, centralized control, lack of data provenance etc.) providing Data Privacy, Confidentiality, Integrity, Authentication, and Authorization security features.

We have proven the scalability and transaction throughput features of the Connect platform with empirical evaluations. The 1.0 version of the Connect platform as described in this paper is currently running as a prototype.

CRediT authorship contribution statement

Eranga Bandara: Methodology, Software, Writing - original draft. **Xueping Liang:** Investigation, Writing - review & editing, Supervision. **Peter Foytik:** Validation, Writing - review & editing. **Sachin Shetty:** Supervision, Investigation, Writing - review & editing. **Crissie Hall:** Supervision, Investigation, Review & editing. **Daniel Bowden:** Supervision, Investigation, Review & editing. **Nalin Ranasinghe:** Supervision, Investigation. **Kasun De Zoysa:** Supervision, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was funded by the Department of Energy (DOE) Office of Fossil Energy (FE), United States (Federal Grant #DE-FE0031744).

References

Abeler, J., Bäcker, M., Buermeyer, U., & Zillessen, H. (2020). Covid-19 contact tracing and data protection can go together. *JMIR mHealth and uHealth*, *8*(4), Article e19359.

Akka, Akka Documentation. URL https://doc.akka.io/docs/akka/2.5/actors.html.

Akka Streams Documentation, URL https://doc.akka.io/docs/akka/2.5/stream/.

Allam, Z., & Jones, D. S. (2020). On the coronavirus (covid-19) outbreak and the smart city network: Universal data sharing standards coupled with artificial intelligence (ai) to benefit urban health monitoring and management. In *Healthcare, Vol. 8* (p. 46). Multidisciplinary Digital Publishing Institute.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (p. 30). ACM.

Aublin, P.-L., Mokhtar, S. B., & Quéma, V. (2013). Rbft: Redundant byzantine fault tolerance. In *2013 IEEE 33rd international conference on distributed computing systems* (pp. 297–306). IEEE.

Australia-Covid19, Australia-Covid19. URL https://www.wsws.org/en/articles/2020/04/29/heal-a29.html.

Baars, D. (2016). *Towards self-sovereign identity using blockchain technology*. (Master's thesis), University of Twente.

Bandara, E., NG, W. K., DE Zoysa, K., Fernando, N., Tharaka, S., Maurakirinathan, P., et al. (2018). Mystiko—Blockchain meets big data. In *2018 IEEE international conference on big data (big data)* (pp. 3024–3032). IEEE.

Bandara, E., NG, W. K., De Zoysa, K., & Ranasinghe, N. (2019). Aplos: Smart contracts made smart. In *BlockSys'2019*.

Buterin, V., et al. (2014). *A next-generation smart contract and decentralized application platform*: *White paper*.

CCI, CCI. URL https://www.covidcreds.com/.

Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. arXiv preprint arXiv:2003.11511.

Davis, A. L. (2019). Akka streams. In *Reactive streams in Java* (pp. 57–70). Springer.

De Carli, A., Franco, M., Gassmann, A., Killer, C., Rodrigues, B., Scheid, E., et al. (2020). Wetrace–a privacy-preserving mobile covid-19 tracing approach and application. arXiv preprint arXiv:2004.08812.

Destounis, A., Paschos, G. S., & Koutsopoulos, I. (2016). Streaming big data meets backpressure in distributed network computation. In *IEEE INFOCOM 2016-the 35th annual IEEE international conference on computer communications* (pp. 1–9). IEEE.

Doshi, P., Jain, P., & Shakwala, A. (2014). Location based services and integration of google maps in android. *International Journal of Engineering and Computer Science*, *3*(03).

Eykholt, E., Meredith, L. G., & Denman, J. (2017). Rchain architecture documentation.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., et al. (2020). Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing. *Science*.

Fisher, J., & Sanchez, M. H. (2016). *Authentication and verification of digital data utilizing blockchain technology*. Google Patents, US Patent App. 15/083, 238.

Google and Apple (2020). Privacy-preserving contact tracing. https://www.apple.com/covid19/contacttracing, [Online].

Gormley, C., & Tong, Z. (2015). *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*. " O'Reilly Media, Inc.".

Gupta, M. (2012). *Akka essentials*. Packt Publishing Ltd.

Hammudoglu, J., Sparreboom, J., Rauhamaa, J., Faber, J., Guerchi, L., Samiotis, I., et al. (2017). Portable trust: biometric-based authentication and blockchain storage for self-sovereign identity systems. arXiv preprint arXiv:1706.03744.

Hardin, T., & Kotz, D. (2021). Amanuensis: Information provenance for health-data systems. *Information Processing & Management*, *58*(2), Article 102460.

Hewitt, C. (2010). Actor model of computation: scalable robust information systems. arXiv preprint arXiv:1008.1459.

Hughes, J. (1989). Why functional programming matters. *The Computer Journal*, *32*(2), 98–107.

indy, indy. URL https://github.com/hyperledger/indy-sdk.

Italy-Covid19, Italy-Covid19. URL https://www.medscape.com/viewarticle/926777.

Jolocom (2019). *Jolocom, A decentralized, open source solution for digital identity and access management*: *White paper*, Jolocom, URL https://github.com/jolocom/jolocom-lib/wiki/Jolocom-Whitepaper.

Jones, M. B. (2011). The emerging json-based identity protocol suite. In *W3C workshop on identity in the browser* (pp. 1–3).

Jonsson, J., & Kaliski, B. (2003). *Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1*. RFC 3447, February.

Khawas, C., & Shah, P. (2018). Application of firebase in android app development-a study. *International Journal of Computer Applications*, *179*(46), 49–53.

Lakshman, A., & Malik, P. (2010). Cassandra: a decentralized structured storage system. *Operating Systems Review*, *44*(2), 35–40.

Liang, X., Shetty, S., Zhao, J., Bowden, D., Li, D., & Liu, J. (2017). Towards decentralized accountability and self-sovereignty in healthcare systems. In *International conference on information and communications security* (pp. 387–398). Springer.

Liu, Y., Sun, G., & Schuckers, S. (2019). Enabling secure and privacy preserving identity management via smart contract. In *2019 IEEE conference on communications and network security (CNS)* (pp. 1–8). IEEE.

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *2008 eighth IEEE international conference on data mining* (pp. 413–422). IEEE.

McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., et al. (2016). *BigchainDB: a scalable blockchain database*: *White paper*, BigChainDB.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Odersky, M., Altherr, P., Cremet, V., Emir, B., Maneth, S., Micheloud, S., et al. (2004). *An overview of the Scala programming language*: *Tech. rep.*.

Oham, C., Michelin, R. A., Jurdak, R., Kanhere, S. S., & Jha, S. (2021). B-ferl: Blockchain based framework for securing smart vehicles. *Information Processing & Management*, *58*(1), Article 102426.

Othman, A., & Callahan, J. (2018). The horcrux protocol: a method for decentralized biometric-based self-sovereign identity. In *2018 international joint conference on neural networks (IJCNN)* (pp. 1–7). IEEE.

Putz, B., Dietz, M., Empl, P., & Pernul, G. (2021). Ethertwin: Blockchain-based secure digital twin information management. *Information Processing & Management*, *58*(1), Article 102425.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2019). Decentralized identifiers (dids) v1.0 - core data model and syntaxes. W3C First Public Working Draft, URL https://www.w3.org/TR/did-core/.

Sharma, M., & Lim, J. (2019). A survey of methods guaranteeing user privacy based on blockchain in internet-of-things. In *Proceedings of the 2019 2nd international conference on data science and information technology* (pp. 147–153).

Strapdata (2018). *strapdata/elassandra*. GitHub, URL https://github.com/strapdata/elassandra.

The Scala Programming Language, URL https://www.scala-lang.org/.

Tobin, A., & Reed, D. (2016). The inevitable rise of self-sovereign identity. *The Sovrin Foundation*, *29*.

TraceTogether, TraceTogether. URL https://www.tracetogether.gov.sg/.

uPort, uPort. URL https://github.com/uport-project/specs.

World Health Organization, Coronavirus disease 2019 (COVID-19) Situation Report. URL https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200402-sitrep-73-covid-19.pdf?sfvrsn=5ae25bc7_2.

Wu, Z., & McGoogan, J. M. (2020). Characteristics of and important lessons from the coronavirus disease 2019 (covid-19) outbreak in China: summary of a report of 72 314 cases from the chinese center for disease control and prevention. *Jama*.

Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., et al. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 767–778.