The University of Texas at Austin
Center for Identity

Self-Sovereign Identity and User Control for Privacy-Preserving Contact Tracing

Wenting Song
Razieh Nokhbeh Zaeem
David Liau
Kai Chih Chang
Michael R. Lamison
Manah M. Khalil
K. Suzanne Barber

UTCID Report #22-02

February 2022

Self-Sovereign Identity and User Control for Privacy-Preserving Contact Tracing

Wenting Song
Razieh Nokhbeh Zaeem
David Liau
Kai Chih Chang
The University of Texas at Austin
Austin, Texas, USA
{wentingsong,nokhbeh,davidliau,kaichih1013}@utexas.edu

Michael R. Lamison
Manah M. Khalil
Verizon
Dallas, Texas, USA
{michael.lamison,manah.khalil}@verizon.com

K. Suzanne Barber
The University of Texas at Austin
Austin, Texas, USA
sbarber@identity.utexas.edu

ABSTRACT

Contact tracing apps use mobile devices to keep track of and promptly identify those who come in contact with an individual who tests positive for COVID-19. However, privacy is a major obstacle to the wide-spread use of such apps since users are concerned about sharing their contact and diagnosis data. This research overcomes multiple challenges facing contact tracing apps: (1) As researchers have pointed out, there is a need to balance contact tracing effectiveness with the amount of user identity and diagnosis information shared. (2) No matter what information the user chooses to share, the app should safeguard the privacy of user information. (3) On the other hand, some essential test result information must be shared for the contact tracing app to work. While contact tracing apps have done a good job maintaining contact information on the user's device, most such apps publish positive COVID-19 test results to a central server which have some risks for compromise. We address these challenges by (1) giving the user the right to choose how much information to share about their diagnosis and their identity, (2) building our novel contact tracing app on top of Self-Sovereign Identity (SSI) to assure privacy preserving user authentication with verifiable credentials, and (3) decentralizing the storage of COVID-19 test results. We, in collaboration with Verizon, have implemented our Privacy-preserving Contact Tracing (PpCT) app, leveraging SSI advances based on the blockchain for their 5G network.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; Privacy-preserving protocols; • **Human-centered computing → Ubiquitous and mobile devices**; • **Applied computing → Health informatics**.

KEYWORDS

contact tracing, privacy, self-sovereign identity, application development, blockchain

WI-IAT '21, December 14–17, 2021, ESSENDON, VIC, Australia

ACM ISBN 978-1-4503-9115-3/21/12…$15.00
https://doi.org/10.1145/3486622.3493914

ACM Reference Format:
Wenting Song, Razieh Nokhbeh Zaeem, David Liau, Kai Chih Chang, Michael R. Lamison, Manah M. Khalil, and K. Suzanne Barber. 2021. Self-Sovereign Identity and User Control for Privacy-Preserving Contact Tracing. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI-IAT '21), December 14–17, 2021, ESSENDON, VIC, Australia.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3486622.3493914

1 INTRODUCTION

The unprecedented COVID-19 pandemic has wreaked havoc on literally every aspect of life. As of November 4th, 2021, the coronavirus has infected over two hundred forty eight million and killed over five million twenty one thousand people globally[1]. To curb the spread of this virus (named SARS-CoV-2), many governments have enforced stay-at-home orders and social distancing measures. These measures, however, drastically disrupt financial and social activities. The economic impact of COVID-19 is still unfolding, very much like its social impacts. In March 2020, the U.S. National Bureau of Economic Research estimated a year-on-year contraction in U.S. real GDP of 11% as of the fourth financial quarter of 2020 [8].

As societies seek to reopen after the stay-at-home orders eventually lift, effective contact-tracing of infected individuals is paramount. Contact-tracing involves identifying those who have come in close contact with an infected individual during the time he/she is potentially infectious with COVID-19, and notifying contacted individuals to take further actions such as getting tested, monitoring for symptoms, and self-quarantining. Mathematical models have demonstrated how "highly effective contact-tracing and case isolation is enough to control a new outbreak of COVID-19 within 3 months." [18].

A mobile app that automatically detects close contact with other individuals in real-time, keeps track of the contact lists, and proactively notifies contacts is shown to be considerably more effective than traditional reactive contact-tracing [17]. A major concern with such mobile apps, however, is the potential privacy breach of user sensitive information. At a minimum, these apps need to record contacts of individuals and positive COVID-19 test results, but some solutions go as far as collecting exact [23] or approximate [26] geographical locations. Even with the minimal contact information, many have raised privacy concerns [11, 27] with respect to the government access to the data [7], potential for snooping, and lack of privacy from contacts [13].

[1] https://coronavirus.jhu.edu/map.html

A number of simultaneous attempts are being made to produce privacy-preserving contact tracing apps. Most of these apps rely on the Bluetooth Low Energy (BLE) [4] signals to collect the contact list. Each device constantly broadcasts hashed identifiers over BLE. When a user's device comes in contact with another, the app collects the hashed identifier of the other user, and keeps this contact information exclusively on the user's device. When a user tests positive for COVID-19, he/she voluntarily publishes their diagnosis and his/her identifier to a centralized server (typically government server) which in turn propagates the diagnosis to the other users. The other users match the hashed identifier of the infected user against their contact lists to determine if they have been in contact with the infected individual. The matching usually happens on the user's device. Researchers have proposed a range of privacy-preserving components into this high-level solution, including a public server to collect and propagate positive COVID-19 diagnosis (in lieu of a trusted third-party server) [12], a decentralized peer-to-peer system that eliminates the server altogether [10, 31], or a zero-knowledge proof approach [20]. Amid these solutions, some researchers have aimed to replace the server with blockchain technology to enable privacy-preserving contact-tracing [7, 30].

Yet, prominent privacy researchers have argued that [14] "digital contact tracing may protect privacy, but [without proper balance between privacy and contact tracing effusiveness] it is unlikely to stop the pandemic". While some researchers feel confident that privacy and contact tracing can go together [2], others view such apps as major risk to privacy [27]. To address this concern, we offer our **first contribution**: we give users the right to choose how much information to share with others with no sharing to a centralized public authority. Users can share as much or as little identity and diagnosis data they wish. We are not aware of any other contact tracing app that gives users such wide range of options about what to share without decreasing contact tracing efficacy.

No matter how much the user decides to share, user information should be safeguarded. To provide the ultimate protection of user privacy, we make our **second contribution**. We utilize Self Sovereign Identity (SSI) built on top of blockchain, and available to 5G network users through our industrial partner in this research. Blockchain was first introduced with Bitcoin [22], a crypto-currency (i.e., electronic cash) technology that allows online transactions to take place without going through a trusted financial third party. Digital signatures and a peer-to-peer network form the backbone of the blockchain technology. The two parties of the transaction communicate through digital signatures (i.e., public and private keys). The peer-to-peer network timestamps transactions by hashing them into a chain of blocks, forming a record of transactions. This ledger (also known as blockchain) cannot be altered without the consensus of the network majority. **Self-sovereign identity (SSI)** is the concept of individuals or organizations having sole ownership of their digital and analog identities. Blockchain exhibits several properties that make it a suitable candidate for self-sovereign identity applications [16], including but not limited to distributed consensus, immutability and irreversibility of ledger state, distributed data control, accountability and transparency. Because of its support for self-sovereign identity, blockchain platforms have already been exploited to develop self-sovereign identity applications, such as uPort [21], Jolocom [15], Sovrin [25] and Blockcerts[28]. These applications are deployed at the top (application) layer where a blockchain platform resides underneath. Our industrial partner (Verizon) has a similar implementation of SSI on top of the Hyperledger blockchain.

While our use of SSI strengthens the privacy protection of user private information, there is an essential part of COVID-19 positive test results that must be available to other PpCT users for the app to function. Individuals who came in contact with a user who has tested positive for COVID-19 must be notified. Even this limited notification is under the user's control in our app. To the best of our knowledge, however, the publication of positive test results to a central server seems almost ubiquitous in contact tracing apps. Such central server is a single point of failure and may be compromised to flood the PpCT users with deliberately fabricated COVID-19 positive results or other formulations of inaccurate results. To resolve this issue, we take advantage of the blockchain network (in particular Hyperledger Fabric) as a distributed repository of positive test results, disassociated from user identities. As our **third contribution**, blockchain replaces the central repository of COVID-19 positive test results (hashed identifiers) and adds decentralization, immutability, transparency, and security. Note that the *public* Fabric ledger is used only for the part of test results that must be shared.

We have implemented our PpCT for Android devices in collaboration with Verizon. We are currently testing PpCT with college students at the University of Texas. It is also noteworthy that our Privacy-preserving Contact Tracing app is transferable for tracing any other infectious disease.

2 PRELIMINARY

2.1. Privacy Concerns in Traditional Contact Tracing Apps

There are lots of important issues waiting to be addressed for a traditional contact tracing app. Among these are privacy and security concerns of users' information: Contact tracing apps involve the storage of users' contact data, associated with users' interaction history log for a pre-set duration (usually set as two weeks). The collection of this information imposes possible threats to user privacy as the log data may disclose users' private information such as identities, locations, trajectories, and lifestyle-related information. A contact tracing app aggravates the privacy problem even further because it may disclose users' health and diagnosis information. Such threats to privacy would discourage people from participating in contact tracing through apps.

2.2. Our Design for Privacy Preserving Contact Tracing

To ensure the maximum possible privacy of users, and at the same time assure the proper functioning of the contact tracing app, we make the following attempts in our privacy-preserving contact tracing application:

(1) We make contact tracing happen strictly through Bluetooth Low Energy (BLE) beaconing. User location information is never recorded or stored.
(2) BLE Identifiers change every fifteen minutes, which reduces the risk of privacy exposure during the process of broadcasting identifiers and collecting contacts.
(3) The participation in each functionality of the app requires users' explicit consent. Users decide to opt into registration,

contact collection, self-reporting, and notification. In line with this privacy preserving design decision, we allow users to self-report instead of having third party COVID testing labs report on their behalf.

(4) Anonymization. The basic idea is to remove identification information from all interactions between users, and of course between the user and application. One way to make users anonymous is to replace their identifiable information with pseudonyms or suppressing users' identities.
(5) The user selects the extent to which they wish to share their identity through self-reports and/or add identity verification from an organization who knows them. Users may have third party organizations attest their identities.
(6) All user authentication information is secured with SSI and saved in their wallet on the device. User private key for SSI is generated on the device and never leaves it.
(7) Persons in a user's contact list (i.e., those who came in contact) are notified that the user's test results have been verified if the user is willing to provide their positive test report, but report contents are never shared outside the PpCT app.
(8) Contact information never leaves user devices and contact matching takes place locally on their devices.

3 SELF-SOVEREIGN IDENTITY (SSI)

Self-sovereign identity, is the concept of individuals or organizations having sole ownership of their digital and analog identities. SSI adds a layer of security and flexibility allowing the identity holder to only reveal the necessary data for any given transaction or interaction. Allen proposed his ten guiding principles of SSI [3], which are summarized in Table. 1.

3.1 Background: Flow of Typical SSI

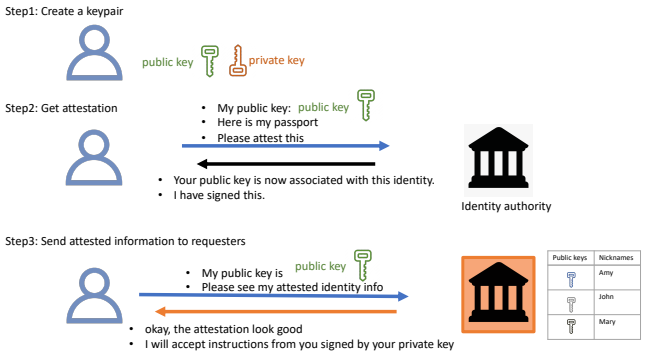


Figure 1: High-level workflow of self-sovereign identity [5].

Hyperledger Indy combined with Aries is an example of practical implementation of the SSI concept. While Indy itself is a form of SSI implementation already, Aries provides the flexibility and additional functionality in practical software development across platforms.

Figure 1 displays the high-level workflow of SSI. In addition, a typical Indy SSI example adds the concept of derived credentials in addition to root credentials as follows: At the beginning, an individual user has root credentials like one's names or driver's licence that are issued and documented by trusted government agencies. An entity like a local bank or a university can create SSI for the user to use in future applications by creating a derived credential with the root credentials. For example, a university can create a diploma (derived credential) with one's name (root credential) and the information is stored in its database. In this case, the university offers and the user accepts the diploma. By accepting this offer, the user utilizes root credentials to create a derived credential. Once the university gets that information as a whole, it fills in all the other information it had for the diploma and sends the completed SSI back to the user. The user now stores this completed SSI in their wallet on their device and use it in the future without a typical authentication process that has to involve the university. This process would greatly increase user controllability of the identity because the technology enables an authentication process that minimizes the involvement of administrative authorities.

4 HIGH-LEVEL USE CASE OF PPCT

In this section, we explain the high-level use case of our PpCT app. Inspired by SSI, we provide four distinct levels of authentication. Users may choose any level to authenticate themselves without exposing the identity document used outside the secure SSI wallet. We select one sample level of assurance from these four levels and explain our PpCT functions in more details.

4.1 Four Privacy Layers of SSI

Four privacy layers of SSI allow users to share as much as they desire about their identities:

- Level 0: No sharing
- Level 1: identity defined by public/private key pairs
- Level 2: identity known to trusted third parties/organizations
- Level 3: individual Personal Identifiable Information sharing

Table 2 elaborates on these four levels of assurance.

For the sake of brevity, we do not extensively explain all the four layers. Rather, we select layer two and cover its implementation.

4.2 Overarching Flow

We display the swim-lane diagram of the entire PpCT at level two of authentication in Figure 2. The overarching flow of the swim-lane diagram can be divided into six parts: Registration, Contact Collection Setting, Contact Collection, Contact Notification Setting, COVID Test Reporting, and Contact Notification.

Procedure I: Registration.
John and Mary, two users of PpCT, both have PpCT installed on their phones. In the registration phase, they each provide identity information in accordance with Section 3.1 to have their identities attested and verified. Similar to a typical SSI application, their identity information and their private keys are stored in their SSI wallets, solely on their devices. The figure includes methods provided by the SSI API that PpCT calls in white boxes. First, the PpCT app sends Request Identity Credential to the identity provider. The identity provider follows up by Creating Identity Credential Offer and sending back to the user to accept. Once the user accepts this offer, the identity provider generates the verified Identity Credential, sends it back to the user for future use and also stores the Identity

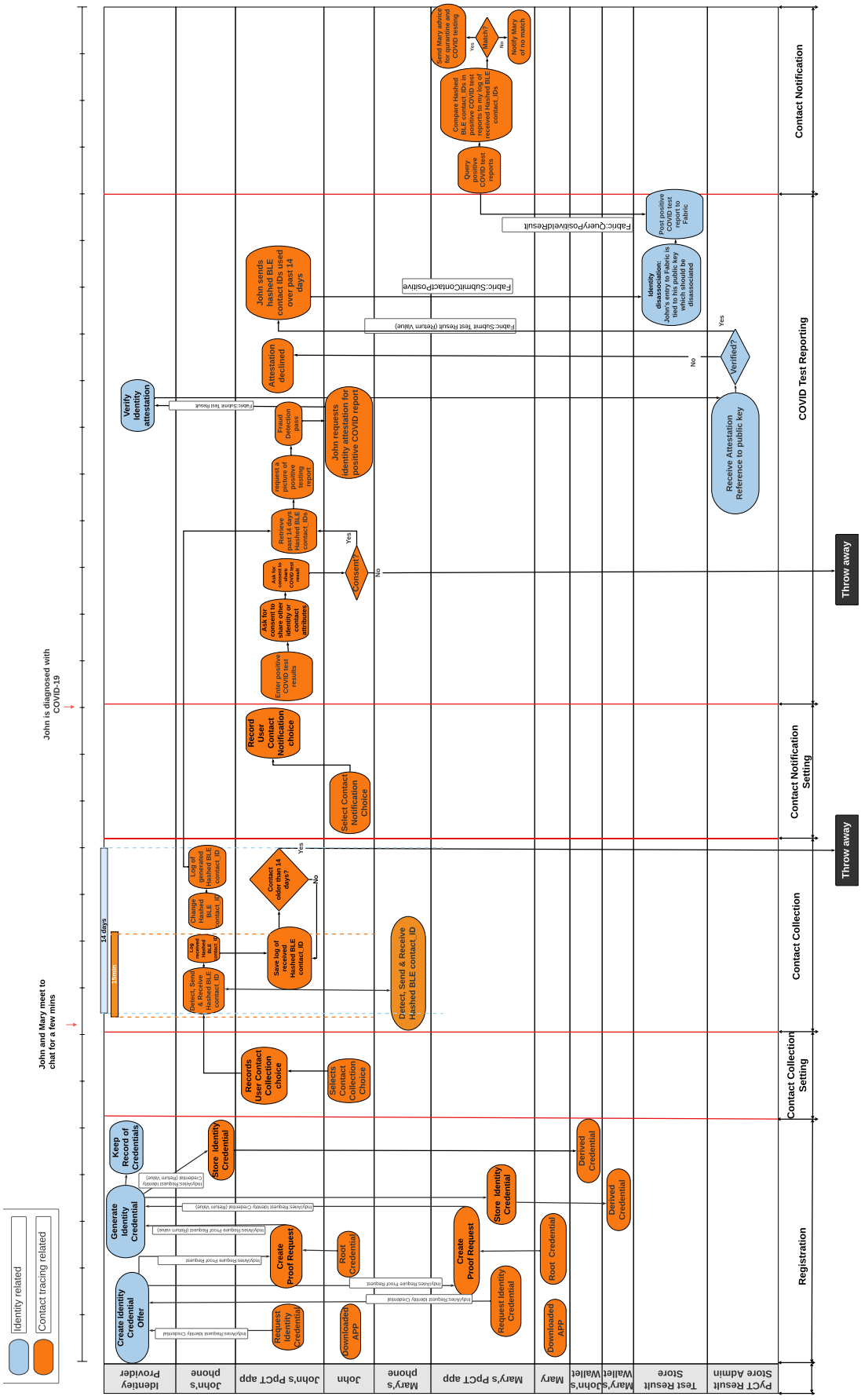


Figure 2: Swim-lane diagram of the entire PpCT.

Security	Controllability	Portability
Keep identity information secure.	Users must take control of their own data, e.g who can see or access.	Users can utilize their identities wherever they want, without being tied to any provider.
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

Table 1: Ten guiding principles of self-sovereign identity (SSI), categorized into three sections [16, 29].

	Technology	Purpose	Examples	Thoughts
Level 0	Zero Knowledge Proof Scene	Achieve proof of asset or identification without exchange of the identity itself	Zero-Knowledge Password Proof (ZKPP) (standardized as part of IEEE IEEE 1363.2)	Needs sophisticated design depending on the application scenario
Level 1	General Blockchain Technology without Know Your Customer (KYC)	A virtual identity which is not related to a limit of real world identity is established within some systems	Hyperledger Fabric enabled blockchain, Ethereum	Usually requires additional resource to maintain the system
Level 2	Private Blockchains, Hyperledger Indy	Achieve self-sovereign identity in this level of Trust	College Certificate, Loan Application, Work Pre-screening	Self-sovereign Identity can be achieved but privacy preserving needs further discussion
Level 3	Traditional authentication or authorization			

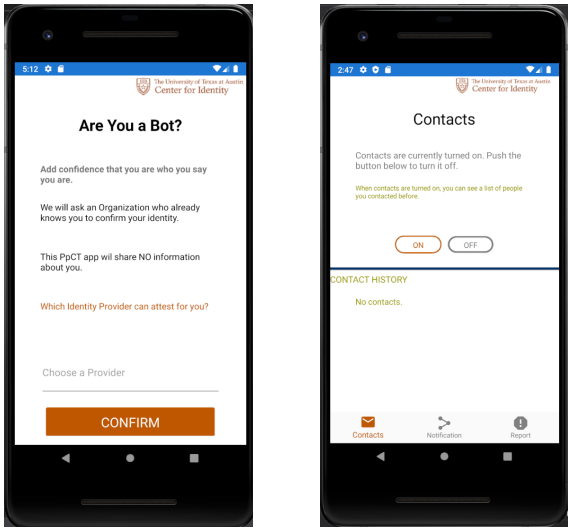
Table 2: Four Privacy Layers of self-sovereign identity (SSI).

Credential at the provider side. John's PpCT app (also Mary's) receives Unique Identity Credential and store keys in the wallet.

Figure 3a shows the screenshot of PpCT that implements registration. Users are allowed to pick an identity provider in the page and then press the confirm button to submit their choices. If a user choose an identity provider, the user's identity is verified at level 1. If the user further has a third party organization attest their identities through single sign on (SSO), they will be verified at level 2. If the user provides the full identity, they are verified at level 3.

Procedure II: Contact Collection Setting.
In PpCT, the user's explicit consent is asked every step of the way. Users can decide whether or not to give the PpCT app permission to broadcast BLE signals (Contact Collection Setting of the swim lane) on the PpCT Contacts page. Only when contacts are turned on, they could see the list of people they have been in contact before, and at the same time, they themselves will show up in other users' contacts correspondingly.

Procedure III: Contact Collection.
When John and Mary meet to chat for a few minutes, their smartphones exchange hashed (anonymous) identifiers over Bluetooth to register that they have been in contact. To avoid the possibility of associating an identifier with a device, these identifiers change every 15 minutes and remain resident on user phones. Each contact



(a) Identity provider page to ask users for identity attestations. **(b) Contacts tab with switch turned on.**

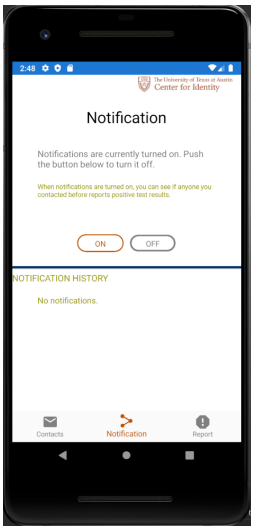
Figure 3: Identity provider page and Contacts tab.

is saved for a preset number of days for which the viral disease is believed to be infectious—in the case of COVID-19 for 14 days. Figure 3b is the screenshot of the Contacts page. The past contacts

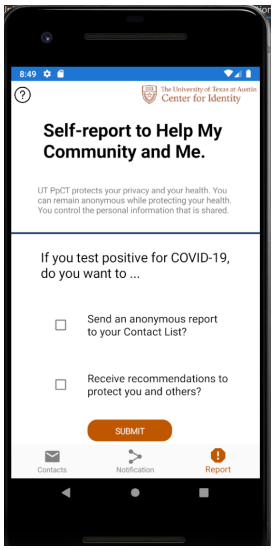
will show in the contact history with hashed IDs and timestamps.

Procedure IV: Contact Notification Setting.
Again, the user's consent is requested in the settings of contact notification. We show a screenshot of this page in Figure. 4a.

Procedure V: COVID Test Reporting.
When John is diagnosed with COVID-19, he voluntarily enters his positive COVID-19 test results into the PpCT app. Then, PpCT asks for his informed consent on the PpCT app Report tab. (Figure 4b).



(a) Notification tab with switch turned on.



(b) Report tab.

Figure 4: Notification tab and Report tab.

With John's approval, the app will lead him to the other page of the Report Tab (Figure 5) to select the information to attest—the test result from the test agency and the personal information to share (Name, Contact duration or Contact time). For example, if John selects to share contact duration and contact time (only month), anonymous and time-stamped notifications stating the following will be sent out to users on his contact log list, including Mary: "You came into contact with a COVID-19 positive individual in June, which lasted for one hour."

Note the nuances of test reporting in Figure 2. Once a user grants permission, the hashed BLE IDs from his past 14 days are retrieved from his device. If the user is still considered contagious according to the timing of test results, his future hashed BLE IDs will also be periodically retrieved. PpCT then asks for a picture of positive test results, if the user is willing to share one. Then, John may decide to have his identity attested with the identity provider, without actually sharing his identity. Depending on his chosen level of assurance (Section 4.1), his report to the distributed PpCT Result Store is attested and automatically verified by the PpCT Result Store Admin. Then John's hashed BLE IDs are saved to Hyperledger Fabric's ledger—publicly available to other PpCT users.

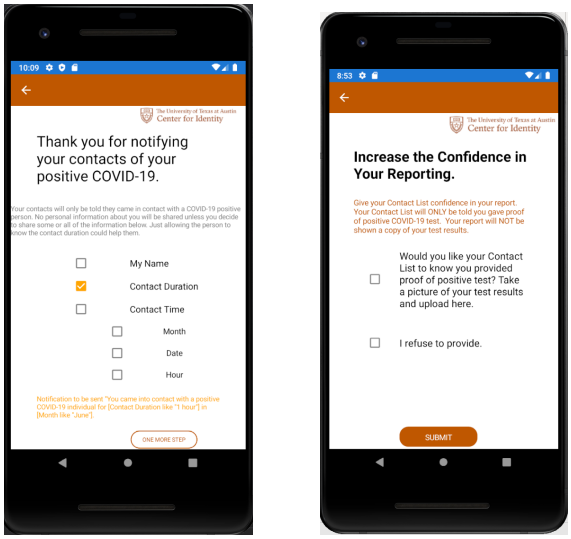


Figure 5: Subsequent pages in Report tab.

Procedure VI: Contact Notification.
Mary's PpCT app periodically queries positive COVID test reports, and compares Hashed BLE contact IDs in positive COVID test reports to her log of received Hashed BLE contact IDs. If there is a match, the app will send Mary advice for self-quarantine and COVID testing, if she has turned on the notifications. Figure 4a shows the screenshot of the notification tab. Past notifications will show under the notification history.

5 THE TECHNOLOGICAL STACK

In this section, we cover various technologies we use for the development of the PpCT mobile app. Fig 6. gives a top level description of how different technologies interact with one another. Although Google/Apple have released a contact tracing library [1] that utilizes the same technology as this work, the Google/Apple API is available to health authorities only. As a result, we build our own tracking libraries from scratch.

5.1 Bluetooth Low Energy

We leverage Bluetooth Low Energy (BLE), a short-range radio communication standard that uses less transmission power than normal Bluetooth to minimize its impact on battery consumption. The technology utilized the same ISM band of 2.4GHz as many of the wireless communication protocols sit in, while giving 40 physical channel with separation of 2 Mhz. Of the 40 physical channels, 3 are dedicated for BLE advertisement and 37 are for data. In our application, we do not establish bi-directional data link with the BLE protocol but rather advertise one-sided the device identifier generated in our app periodically. It is worth noting that the contact tracing functionality provided by the Google/Apple's Exposure Notification system also utilize this technology to achieve the goal. A typical detection of contact would looks like the following: John's phone is periodically advertising its own device identifier. Mary's phone would be scanning for such identifiers with a certain power measurement and records the time of receiving. We consider contact

duration and tune for contact distance so that PpCT can evaluate different risk levels of contact with the information provided (e.g., 15 minute contact within 6 feet distance). After a pre-set period of time, John's phone will generate a new identifier for it to be detected. Note that even though Mary's phone received the first and second identifier from John's phone, the system is designed so that it cannot determine whether these two identifiers are from the same phone. This feature was enabled by the Media Access Control (MAC) address randomisation introduced in the BLE standard. In order to lower the risk of being tracked by other devices, the MAC address and the device identifier shall be changed at the same time. Another feature of BLE protocols is that it can be configured to be extra power saving than many other communication protocols. Therefore, even if our PpCT app requires users to turn on Bluetooth the entire time, their batteries still last long.

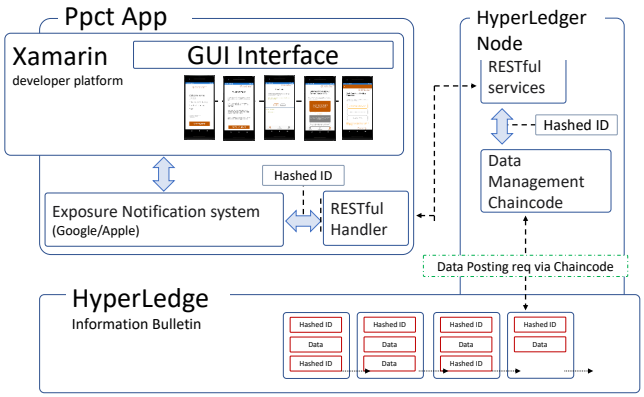


Figure 6: The Technology Stack of PpCT App.

5.2 App Development

We use Xamarin for the implementation of the mobile app. Signal Protocol is applied for cryptography and Amazon Web Services (AWS) for deployment. To allow our PpCT app to run in the background even if the app exits or the phone restarts, we use WorkManager which is also a battery-friendly API like BLE. To perform responsive UI design, we use ViewModel, DataBinding, and LiveData so that our PpCT app can adapt to different sizes of screen and these APIs also make it easier to manage UI when data in the background has changed.

5.3 Implementation of Self-Sovereign Identity

We choose the HyperLedger Indy combined with Aries as the tool to implement the SSI identity management system. The app starts with establishing derived credentials that are being used in the app from root credentials. Root credentials are usually credentials that are strongly trusted by the app designer. For instance, since we have a strong understanding of how the Single Signed On (SSO) system works at our organization, the membership of the the organization can be considered a valid root credential to create a derived credential that will be used in future authentication processes. The advantage of this method is that once derived, the SSI is fully controllable by the user. Only the identity owner has the ability to initiate an authentication or authorization process.

5.4 Public Ledger as Information Bulletin

Even though a main important design concept of our PpCT app is privacy, the hashed BLE IDs voluntarily shared by PpCT users have to be accessible to other users for the app to function properly. In our design, we emphasize the need for designing an entity for storing the proper amount of information for exposure notification. In our case, this entity should not store information that can be directly linked to the identity of app users but should still enable users to know if they have been exposed to COVID-19. We choose to implement the entity utilizing the HyperLedger technology, which enables us to build a decentralized ledger with extra power of smart contracts to perform crucial privacy preserving operations in a decentralized way which can be modified after deployment.

HyperLedger is one of the blockchain projects that has gained popularity over the past few years since launching in 2015. Within the maturing ecosystem of HyperLedger, HyperLedger Indy is chosen for identity management and credential distributing. Indy project is a ledger project that specialized in identity management by providing digital identities rooted on blockchain. Once a credential is issued with Indy, users have full control over that credential comparing to other common digital identities. For development flexibility, we also adopt Hyperledger Aries for cross system identity support. Last but not the least, a distributed ledger supported by Hyperledger Fabric is also adopted for the purpose of securely storing the information needed within the design scope. Since distributed ledger empowered by Hyperledger Fabric also supports smart contracts, more high level functionalities can be developed.

We want to emphasize that our app can operate the notification functionality without storing information that relates to the real world identity of the user, but information that may be traced back to the user can still be processed with the app user's consent to support higher level functionalities such as the calculation of trust scores. Note that even in the scenario that the user is posting data with derived credentials, the user is the one initiating the authentication process. Once the credential is used for establishing some level of trust, the information will not be stored at any entity. In this case, a one-time posting key is generated for the user to post the data he/she would like to share. By design, the user's privacy is more protected compared to transitional peer-to-peer systems.

We reiterate that even though the blockchain ledger that replaces the central server of COVID-19 positive test results is public, what is saved is hashed anonymous identifiers that would not be possible to map back to identify devices. Blockchain protects PpCT from a single point of failure and adds decentralization and immutability.

6 RELATED WORK

While there are many different concrete implementations of contact-tracing apps, such as BlueTrace [9], Exposure Notifications API [6], TraceTogether [19], etc., none are based on blockchain. In this section, we review the work most close to ours on leveraging blockchain for contact-tracing. To the best of our knowledge, there are three manuscripts that cover blockchain-based contact-tracing

with the goal of preserving user privacy: BeepTrace [30], Pronto-C2 [7] and P^2B-Trace [24]. BeepTrace [30] utilizes blockchain to propose architectural design of a privacy-preserving contact-tracing app, and further numerically analyzes network storage and computing capacity requirements. P^2B-Trace [24] proposed a blockchain-based contact tracing initiative and a zero-knowledge scheme to verify proximity claims as well as protect privacy. In comparison with our work, both BeepTrace and P^2B-Trace are abstract open initiatives without concrete prototype implementation. Pronto-C2 [7] presents a decentralized BLE-based peer-to-peer contact-tracing system, which can optionally be implemented with blockchain. Pronto-C2 seeks to protect users against mass surveillance by governments and authorities through decentralization. Likewise, Pronto-C2 is a high-level design proposal lacking a concrete implementation or prototype with blockchain. Furthermore, using self-sovereign identity (SSI) is the contribution of our work and we have not been able to find any contact tracing apps based on SSI.

7 CONCLUSION

We presented the prototype of our privacy-preserving contact-tracing (PpCT) mobile app, which leverages Self-Sovereign Identity (SSI) on top of blockchain (Hyperledger Indy/Aries). We put the control of identity and diagnosis information back in the hands of users by enabling them to choose how much to share and keeping their identity/diagnosis information in their SSI wallets except for a part of diagnosis data that is absolutely necessary to be shared for the app to function. Even for this shared public information, we eliminate the use of a central server by employing peer to peer networks (Hyperledger Fabric). Users voluntarily report positive diagnosis results, following the same rationale to make the users the sole owners of their diagnosis data. We covered technical details of the implementation of PpCT in collaboration with Verizon. Our PpCT app is now fully developed and is in the beta testing phase by college students. We plan to deploy PpCT to actual customers of Verizon after beta testing. Our PpCT can help stop the spread of COVID-19, while simultaneously protect users' personal information privacy by giving users the right to choose how much to share.

ACKNOWLEDGMENTS

The University of Texas Center for Identity wishes to thank Verizon for its collaboration, leadership, and sponsorship in this transformative research. This research is funded in part by Verizon, Inc.

REFERENCES

[1] [n.d.]. Privacy-Preserving Contact Tracing - Apple and Google. https://covid19.apple.com/contacttracing
[2] Johannes Abeler, Matthias Bäcker, Ulf Buermeyer, and Hannah Zillessen. 2020. COVID-19 contact tracing and data protection can go together. *JMIR mHealth and uHealth* 8, 4 (2020), e19359.
[3] Christopher Allen. 2016. The path to self-sovereign identity. *Life with Alacrity* (2016).
[4] Thamer Altuwaiyan, Mohammad Hadian, and Xiaohui Liang. 2018. EPIC: efficient privacy-preserving contact tracing for infection detection. In *2018 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.
[5] antonylewis2015. [n.d.]. A gentle introduction to self-sovereign identity. https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/ Accessed: Nov 23, 2020.
[6] Apple and Google. [n.d.]. Exposure Notifications Android. https://github.com/google/exposure-notifications-android Accessed: Nov 4, 2021.
[7] Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, and Ivan Visconti. 2020. Towards Defeating Mass Surveillance and SARS-CoV-2: The Pronto-C2 Fully Decentralized Automatic Contact Tracing System. *IACR Cryptol. ePrint Arch.* 2020 (2020), 493.
[8] Scott R Baker, Nicholas Bloom, Steven J Davis, and Stephen J Terry. 2020. *Covid-induced economic uncertainty.* Technical Report. National Bureau of Economic Research.
[9] Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, and Tang Anh Quy. 2020. BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep* (2020).
[10] Samuel Brack, Leonie Reichert, and Björn Scheuermann. 2020. Decentralized Contact Tracing Using a DHT and Blind Signatures. *IACR Cryptol. ePrint Arch.* 2020 (2020), 398.
[11] Vinay Chamola, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. 2020. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* 8 (2020), 90225–90265.
[12] Justin Chan, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, et al. 2020. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv preprint arXiv:2004.03544* (2020).
[13] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. 2020. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511* (2020).
[14] Lorrie Faith Cranor. 2020. Digital contact tracing may protect privacy, but it is unlikely to stop the pandemic. *Commun. ACM* 63, 11 (2020), 22–24.
[15] Ch Fei, J Lohkamp, E Rusu, K Szawan, K Wagner, and N Wittenberg. 2018. Jolocom: Self-sovereign and decentralised identity by design. *White paper* (2018).
[16] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. 2019. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7 (2019), 103059–103079.
[17] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 368, 6491 (2020).
[18] Joel Hellewell, Sam Abbott, Amy Gimma, Nikos I Bosse, Christopher I Jarvis, Timothy W Russell, James D Munday, Adam J Kucharski, W John Edmunds, Fiona Sun, et al. 2020. Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health* (2020).
[19] Zhilian Huang, Huiling Guo, Yee-Mun Lee, Eu Chin Ho, Hou Ang, and Angela Chow. 2020. Performance of digital contact tracing tools for COVID-19 response in Singapore: cross-sectional study. *JMIR mHealth and uHealth* 8, 10 (2020), e23148.
[20] Joseph K Liu, Man Ho Au, Tsz Hon Yuen, Cong Zuo, Jiawei Wang, Amin Sakzad, Xiapu Luo, and Li Li. 2020. Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach. *IACR Cryptol. ePrint Arch.* 2020 (2020), 528.
[21] Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, and Michael Sena. 2017. Uport: A platform for self-sovereign identity. *URL: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf* (2017).
[22] Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system (2008).* Technical Report. Manubot.
[23] Sangchul Park, Gina Jeehyun Choi, and Haksoo Ko. 2020. Information technology–based tracing strategy in response to COVID-19 in South Korea—privacy controversies. *Jama* (2020).
[24] Zhe Peng, Cheng Xu, Haixin Wang, Jinbin Huang, Jianliang Xu, and Xiaowen Chu. 2021. P2B-Trace: Privacy-Preserving Blockchain-based Contact Tracing to Combat Pandemics. In *Proceedings of the 2021 International Conference on Management of Data*. 2389–2393.
[25] Drummond Reed, Jason Law, and Daniel Hardman. 2016. The technical foundations of sovrin. *The Technical Foundations of Sovrin* (2016).
[26] Leonie Reichert, Samuel Brack, and Björn Scheuermann. 2020. Privacy-Preserving Contact Tracing of COVID-19 Patients. *IACR Cryptol. ePrint Arch.* 2020 (2020), 375.
[27] Frantz Rowe. 2020. Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management* 55 (2020), 102178.
[28] Philipp Schmidt. 2016. Blockcerts—An open infrastructure for academic credentials on the blockchain. *MLLearning (24/10/2016)* (2016).
[29] Andrew Tobin and Drummond Reed. 2016. The inevitable rise of self-sovereign identity. *The Sovrin Foundation* 29, 2016 (2016).
[30] Hao Xu, Lei Zhang, Oluwakayode Onireti, Yang Fang, William Bill Buchanan, and Muhammad Ali Imran. 2020. BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond. *arXiv preprint arXiv:2005.10103* (2020).
[31] Tyler M Yasaka, Brandon M Lehrich, and Ronald Sahyouni. 2020. Peer-to-Peer contact tracing: development of a privacy-preserving smartphone app. *JMIR mHealth and uHealth* 8, 4 (2020), e18936.

WWW.IDENTITY.UTEXAS.EDU