A Blockchain-Based COVID-19 Protection Framework

Basundhara Chakrabarty and Harish Krishnamoorthy

Abstract Diseases like COVID-19, SARS-CoV2 and Ebola have led to loss of lives, economic breakdown and mass hysteria. Governments and healthcare workers are on an incessant strive to isolate and curb the community spread of the virus. Several countries have employed mobile-based applications for tracing contacts, distributing COVID protection guidelines, helping people self-diagnose and forming infection patterns and control groups. These existing strategies, however, do not provide end-to-end privacy in the collection and handling of critical patient data. Moreover, they are vulnerable to linkage attacks. In this paper, we introduce a privacy-preserving COVID-19 protection strategy resting on a decentralized, blockchain-based framework, that aids in contact tracing and social distancing. Our simulation validates that our proposed system maintains the confidentiality of the user.

Keywords COVID-19 · Pandemic control · Contact tracing · Surveillance · Blockchain technology · Ethereum

1 Introduction

On December 31st 2019, The Wuhan Municipal Health Commission, China, reported a cluster of pneumonia cases in Hubei Province [1]. The causative agent was soon identified as novel coronavirus (COVID-19). It belonged to a large family of virus that gave rise to symptoms varying from mild flu to severe respiratory distress [2].

The number of COVID cases burgeoned through 2020, and as of today, COVID-19 has affected more than 11 million people in the world and has caused more than 4 lakh deaths [3]. With no promise of a vaccine in the near few months, countries struggle to diagnose the afflicted and identify people who have been exposed to

B. Chakrabarty (✉) · H. Krishnamoorthy
Cisco Systems Inc, Bangalore, India
e-mail: baschakr@cisco.com

H. Krishnamoorthy
e-mail: hkrishn5@cisco.com

R. J. Kannan et al. (eds.), *International Virtual Conference on Industry 4.0*,
Lecture Notes in Electrical Engineering 355,
https://doi.org/10.1007/978-981-16-1244-2_9

the virus to prevent community spread. A multitude of existing pandemic handling schemes resort to mobile-based contact tracing and mass surveillance applications, like the ones used in Australia, China, Israel, South Korea and Singapore. However, these applications have suffered criticism due to serious privacy threats. Parallelly, nationwide lockdowns have halted economies and given rise to unemployment and recession [4]. The world needs a strategy that improves COVID protection systems, while allowing businesses and corporates to carry out their activity in a sustained manner.

Blockchain is among the most promising technologies of the twenty-first century and has caused a major paradigm shift in the healthcare sector [5]. The paper applies blockchain to COVID protection and delineates three major features of our approach: the contact tracing subsystem, blockchain network and COVID status checking scheme. The contact tracing scheme allows stakeholders to identify people who have come in proximity with individuals diagnosed with COVID-19, to test and isolate them, and treat them when applicable, preserving user privacy while doing so. The COVID status checking scheme allows citizens to stay protected while they carry out their daily activities in a controlled manner. The blockchain network forms the skeleton of the proposed system, stores patient records on a distributed ledger and coordinates access management. Experimental simulation shows the framework to be highly efficient in preserving privacy.

2 Related Work

Several countries have come up with ingenious contact tracing and surveillance methods in the wake of COVID-19. The World Health Organization adopted contact tracing to contain the Ebola outbreak in Africa. WHO defined it as the ‘identification and follow-up of people who may have come into contact with a person infected with Ebola virus’ [6]. It enforced rules for conducting systematic contact tracing for frontline epidemiologists, surveillance officials, healthcare specialists and other volunteers. No mobile applications were used during the Ebola outbreak.

Danquah introduced an application-based contact tracing system to track Ebola cases in Sierra Leone [7] and demonstrated how it improved on data storage and accuracy over paper-based systems.

Several organizations have, thence, engaged in developing contact tracing applications for pandemic control. With the rise of COVID-19, countries have adopted mobile technologies to conduct business in the safest manner possible. The Indian Government conceived the Aarogya Setu app for the same purpose [8]. Aarogya Setu utilizes the smartphone’s Bluetooth and GPS features to determine the user’s infection risk and perform contact tracing. It generates a randomized device identifier (DiD), maps it with the mobile number of a registering user and stores an encrypted version on it. This method gives the government authority access to the user’s epidemiological and GPS information, which poses serious security concerns.

Similarly, China, Singapore South Korea and Australia have urged citizens to install apps for contact tracing and surveillance. However, the concerns of privacy have not been addressed in most of these endeavors. The South Korean surveillance app utilizes GPS data. Furthermore, it requires users to provide their real names and government-issued identity numbers, which infringes on user privacy. Singapore's TraceTogether app operates by exchanging random tokens between nearby phones via Bluetooth, which are then sent to a central server [9]. When an individual is diagnosed with COVID-19, the tokens recorded by the patient's apps are released. Since the government authority maintains a mapping of tokens and associated phone numbers, it can use the released list of tokens to trace the list of exposed users. TraceTogether maintains privacy from other user by using anonymized tokens; however, it provides little privacy for infected citizens. Additionally, the system banks on a central authority (the Singaporean government) and is, hence, less scalable and secure.

Owing to the disadvantages of centralized systems, decentralized COVID protection projects have emerged. Some notable endeavors include COVID watch, PACT and that of Google/Apple [10]. COVID watch is a group of volunteers spread over various continents, comprising security and public health experts [11], and uses Bluetooth Beacon technology for contact tracing. This framework can potentially collect more data than necessary for surveillance and is also susceptible to man-in-the-middle attacks.

Hekmati's work introduces CONTAIN, a privacy-centric mobile contact tracing application that has no dependency on GPS or any other form of location-sensing and reduces the quantity of personally identifiable data logged on a server [12]. The simulation study outlined in the paper emphasizes the efficiency of the system. However, CONTAIN users can choose to reveal their COVID status in an opt-in fashion to the concerned authorities. This stands on the unrealistic assumption that all users shall operate in good faith and shall cooperate and furnish information wherever necessary.

Torky describes a four-tiered blockchain-based COVID containment system [13]. The system adopts the concepts of regex to digitally represent and verify infection patterns under the 'Infection Verifier Subsystem.' A 'blockchain subsystem' acts as a backbone and stores data about confirmed COVID-19 cases in real time, and a peer-to-peer app is used by users to stay abreast of COVID developments. The paper also introduces a mass surveillance subsystem which works in tandem with the infection verifier subsystem, but it provides scarce technical details about the system design and the protocols involved.

3 Blockchain Technology

The groundwork for blockchain technology was laid out by Nakamoto when his whitepaper on bitcoin shook the world of cryptocurrency in 2008 [14].

A blockchain essentially stores a list of transaction records, with each block pointing to the previous block via a hash reference. The block header contains, among other notable fields, the block version, the hash of the parent block, the nonce and a merkle tree root hash [15] of all transactions in the block. The block body contains the transaction list. New blocks are added to the ledger by the block miners after a consensus mechanism, the most common being proof-of-work, which is based on a cryptographic block-racing game [16]. Being a decentralized ledger, blockchains prevent a single point of failure. Furthermore, since each block stores the hash of the previous block, it is computationally infeasible to tamper with blockchains.

4 The Proposed System

In this paper, we propose a blockchain-based framework for protection against COVID that has the following salient features:

- A contact tracing subsystem backed by the Bluetooth beacon technology. The proposed system differs from existing systems in using a decentralized consortium blockchain for storing patient data. Additionally, it uses a highly secure Diffie-Hellman (DH) key exchange algorithm instead of the symmetric algorithms used by existing frameworks.
- A dynamic COVID status record of participating users that need a mandatory daily update, and which can be leveraged by offices, grocery stores, restaurants, etc., to maintain social distancing norms.

The various stakeholders in the system are as follows:

- Medical practitioners, hospitals and testing centers reserve the right to update the blockchain with the COVID status of patients based on their test report. (positive, negative, etc.)
- Research and development centers and government nodes can request to read the epidemiological data in the blockchain for research purposes.
- Shops, restaurants, malls, offices and government personnel maintain read-only access to the blockchain.

4.1 Dapp Registration

Every user, during registration to the Dapp, is assigned a public-private key pair. On registration, the following additional information is collected:

- A collective dataset of the user's epidemiological information ('Info') comprising the age, gender, blood type, pre-existing diseases and the location, encrypted with the user's private key. This ensures that only agencies with the user's public key (e.g., treating medical agencies) can decrypt this information.

Table 1 COVID states and their meaning

COVID state	Meaning
Positive	User shows active strain of COVID-19 in his blood
Negative	User has never been diagnosed with COVID1-9/in contact with a diagnosed patient
Has_to_be_quarantined	User has been in contact with a COVID-19 positive patient and been advised to self-quarantine
Quarantined	User has begun self-quarantine
Off_quarantine	User has served the quarantine period and has not been diagnosed with COVID-19
Recovered	User has been diagnosed with COVID-19 and has recovered

- The COVID-19 status of the patient (status) can take either of the values described in Table 1.

4.2 The Contact Tracing Subsystem

Let us assume that Alice and Bob have registered themselves to the Dapp and have received the public keys (A and B) and private keys (a and b), respectively. When they come in proximity, Alice sends her public key to Bob and requests his public key. When Bob accepts and sends over the same, the two users use the Diffie-Helman (DH) algorithm to create a shared secret key. This shared secret is known only to Alice and Bob. Being an asymmetric key exchange algorithm, DH is more secure than the symmetric key exchange used by Bluetooth beacon-based COVID systems (Fig. 1).

Both Alice and Bob then periodically send beacons using Bluetooth. These beacons are pseudorandom numbers encrypted by the DH-shared secret key generated in the previous step. The beacons are encrypted by the user's private key and are stored locally by the receiver.

When Bob is diagnosed with COVID, the certifying medical practitioner interacts with the consortium blockchain to update his COVID status as 'positive,' and at the same time, it downloads the encrypted beacons from his Dapp and updates the list on the consortium blockchain.

All users are required to perform a 'status check' on their Dapps every 24 h. This 'status check' basically interacts with the consortium blockchain, obtains the list of encrypted beacons (from the patients marked COVID positive in that city) and attempts to decrypt the same using the repository of public keys which it has collected. When Alice performs the same, she shall be able to decrypt Bob's beacons (as she has Bob's private key). She is, thus, advised to take the necessary steps to quarantine herself for 21 days. Her COVID status is automatically changed from positive to 'has_to_be_quarantined' and the 'status check' is marked complete. Since

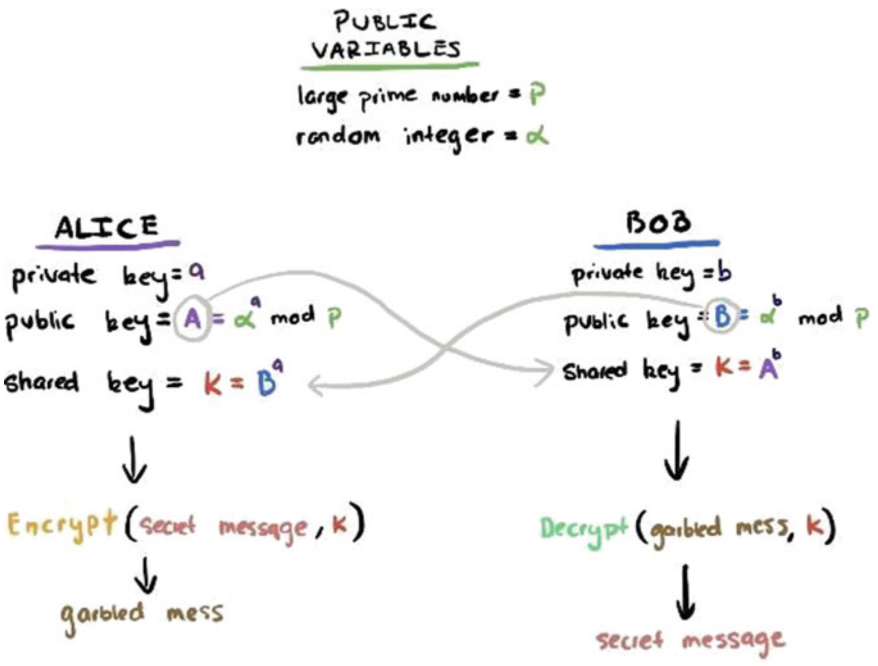


Fig. 1 Diffie-Helman key exchange

the beacons used are anonymized, the identity of the COVID infected patients is not revealed.

4.3 The Blockchain Network

The consortium blockchain stores transactions only on users that have either of the following COVID states: 'positive,' 'has_to_be_quarantined,' 'quarantined,' 'off_quarantine' and 'recovered.' Only medical agencies, testing centers and government agencies certified with a miner ID (ID_p) can add transactions to the blockchain. Table 2 illustrates the fields contained in each transaction in the proposed blockchain.

The epidemiological information of each afflicted/quarantined user is stored in an encrypted format. Government/Research authorities that aim to perform epidemiological surveys are required to request the public key of the transaction creator with a justification, in order to decrypt the data and obtain the content. This ensures that agencies access epidemiological data only when they absolutely need to do so.

Each set of transactions is bundled into a block. The mined blocks are verified by other nodes, spanning healthcare agencies and government bodies, and a consensus is reached via proof-of-work. Since the block verification system is decentralized and involves various stakeholders, linkage attacks are infeasible.

Table 2 Block contents

Field	Value/description
ID	Unique identifier of the patient
H(P)	Cryptographic hash of the user's public key
info	Info = E_p(age, gender, blood type, disease history, location information) where E denotes encryption with key 'p,' the private key of the user
state	The individual's COVID-19 infection state
org_public_key	Public key of the organization who made the last update to the patient's record
updated	A yes/no value indicating whether the beacon decryption check has been performed
allow	If 'yes,' then the user is COVID negative or recovered, and if 'no,' then the user is contagious and is not allowed in shops, offices, etc
public_keys	List of public keys that the user has collected over past 14 days

4.4 Role of COVID State in Maintaining Social Distancing

The COVID state of an individual can help people practice social distancing norms. Offices, shopping stores, malls, restaurants, grocery stores, etc., may reserve the right to deny any individual whose COVID state is 'Positive,' 'Quarantined' or 'Has_to_be_quarantined' from entering their premises. Moreover, they may reserve the right to deny access to any individual who has not performed his COVID

'status check' for the day, or whose status check 'updated' parameter reflects as 'no.'.

An example would be the case of Alice, who wants to go to her office. The office can verify Alice's COVID state following these simple steps:

- The office generates a nonce and transmits it to Alice with a request for her COVID state
- Alice calculates the following:

$$Y = E_{\mathrm{a}}\,(\text{nonce}) \tag{1}$$

where a is Alice's private key, and E is an encryption function.

- Alice transmits 'Y' and her public key 'A' to her office authorities
- Her office decrypts 'Y' with the public key and verifies whether it obtains the 'nonce' value
- The office then queries the consortium COVID-19 blockchain for an entry against H(A)
- If the office observes that Alice's entry shows 'updated = Yes' and 'state = negative/off_quarantine/recovered,' it allows her in. In other words, if Alice's entry shows 'allow = yes,' she is allowed in. In all other cases, Alice is denied access.

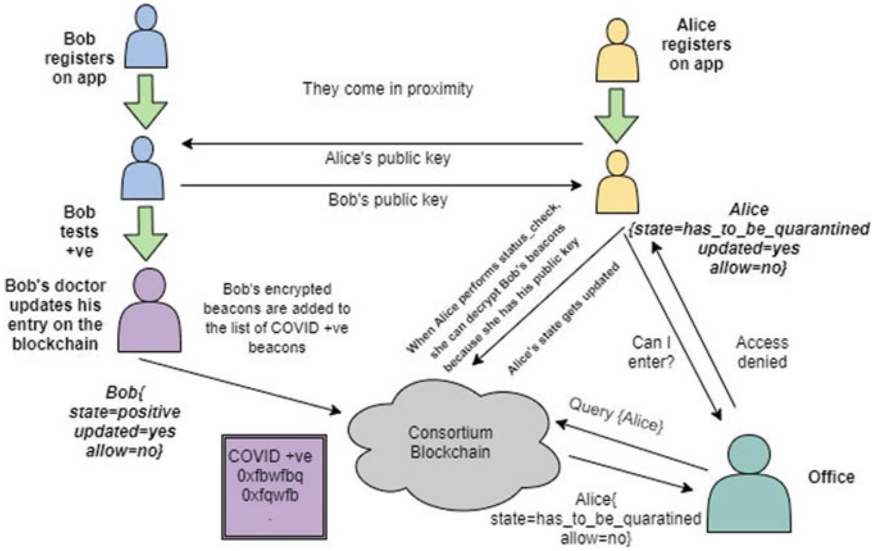

Bob registers on app
Alice registers on app
They come in proximity
Alice's public key
Bob's public key
Bob tests +ve
Bob's doctor updates his entry on the blockchain
Bob's encrypted beacons are added to the list of COVID +ve beacons
When Alice performs status_check, she can decrypt Bob's beacons because she has his public key
Alice's state gets updated
Alice {state=has_to_be_quarantined updated=yes allow=no}
Can I enter?
Access denied
Bob{ state=positive updated=yes allow=no}
COVID +ve 0xfbwfbq 0xfqwfb -
Consortium Blockchain
Query {Alice}
Office
Alice{ state=has_to_be_quaratined allow=no}

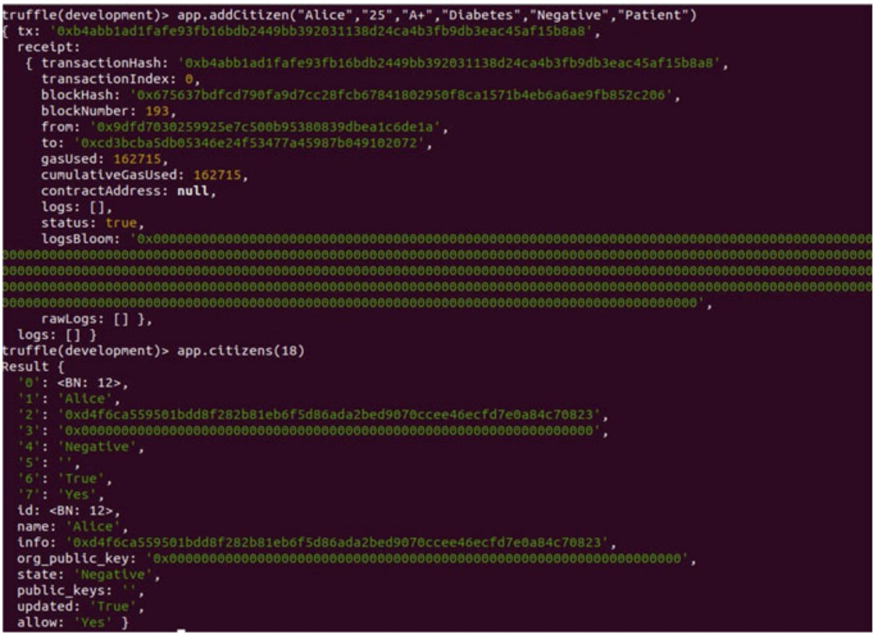
Fig. 2 Schematic representation of the contact tracing and status checking scheme

This implementation allows people to engage in their economic or business activities in a sustained manner, while offering an extra layer of protection against the pandemic in their day-to-day lives. The implementation also facilitates user privacy because an individual can obtain only the COVID state of another individual from the blockchain by using the ID/public key, and for any further information, one must reach out to the miner authority with a proper justification (Fig. 2).

The system provides sufficient incentive to businesses, offices, shopping centers, delivery agencies for using and updating the Dapp because in using the same, they are allowed to carry out their normal operations in a safe manner.

5 Simulation

Ethereum solidity 0.5.16 has been used with Ganache on Ubuntu 18.04 LTS to simulate the smart contract and observe the block structure as maintained and modified by the proposed framework. Truffle framework 5.1.33 is used to interact with the Ganache blockchain testbed. A modular approach has been followed in solidity, with separate functions coded for user registration, status check and for updating the COVID states. Figure 3 shows the usage of the addCitizen() module to implement user registration. The function addCitizen() contains access control checks to verify the role of the invoking user and throws an error if anybody but a ‘Patient/Citizen’ invokes it. In the smart contract, a total of 30 identities are created, including a doctor, a testing agency and a government official. The entire epidemiological information



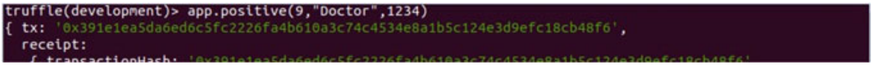
```
truffle(development)> app.addCitizen("Alice","25","A+","Diabetes","Negative","Patient")
{ tx: '0xb4abb1ad1fafe93fb16bdb2449bb392031138d24ca4b3fb9db3eac45af15b8a8',
  receipt:
   { transactionHash: '0xb4abb1ad1fafe93fb16bdb2449bb392031138d24ca4b3fb9db3eac45af15b8a8',
     transactionIndex: 0,
     blockHash: '0x675637bdfcd790fa9d7cc28fcb67841802950f8ca1571b4eb6a6ae9fb852c206',
     blockNumber: 193,
     from: '0x9dfd7030259925e7c500b95380839dbea1c6de1a',
     to: '0xcd3bcba5db05346e24f53477a45987b049102072',
     gasUsed: 162715,
     cumulativeGasUsed: 162715,
     contractAddress: null,
     logs: [],
     status: true,
     logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000',
     rawLogs: [] },
  logs: [] }
truffle(development)> app.citizens(18)
Result {
  '0': <BN: 12>,
  '1': 'Alice',
  '2': '0xd4f6ca559501bdd8f282b81eb6f5d86ada2bed9070ccee46ecfd7e0a84c70823',
  '3': '0x0000000000000000000000000000000000000000000000000000000000000000',
  '4': 'Negative',
  '5': '',
  '6': 'True',
  '7': 'Yes',
  id: <BN: 12>,
  name: 'Alice',
  info: '0xd4f6ca559501bdd8f282b81eb6f5d86ada2bed9070ccee46ecfd7e0a84c70823',
  org_public_key: '0x0000000000000000000000000000000000000000000000000000000000000000',
  state: 'Negative',
  public_keys: '',
  updated: 'True',
  allow: 'Yes' }
```

Fig. 3 User registration

of the user stored in an encrypted format. Please note that a separate variable is created to store the plaintext 'name' only for understanding purposes on this paper. In the actual framework, the 'name' shall also be encrypted within 'info.'

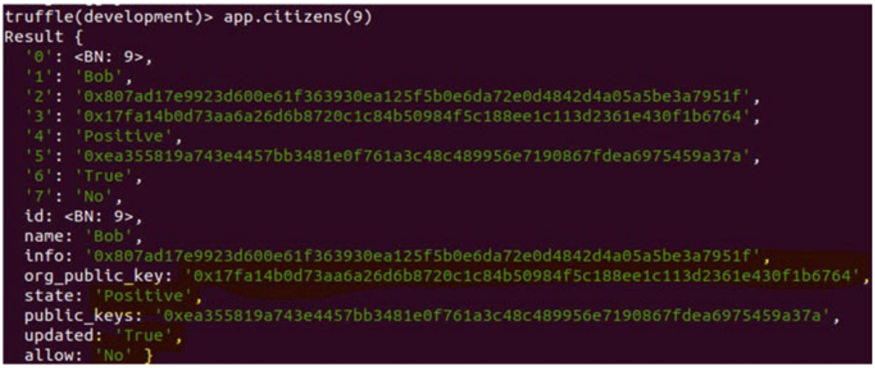
Similarly, Bob registers himself to the blockchain. When he tests positive, his doctor invokes the positive() function to update his COVID state to 'positive.' This triggers the status_check() function, which sets the 'allow' value to 'no.' Figure 4 shows the status update, and Fig. 5 shows the block state after the update. Note that the doctor's public key is now stored in 'org_public_key.'

Alice has maintained the list of public keys obtained from users in the last 14 days, including Bob's key. When she does her daily status update, the citizen_update() function is triggered (Fig. 6), and her status is updated on the blockchain, to 'state=has_to_be_quarantined' and 'allow=no.' Hereafter, both Alice and Bob are not allowed in offices, shops, etc., (Fig. 7).



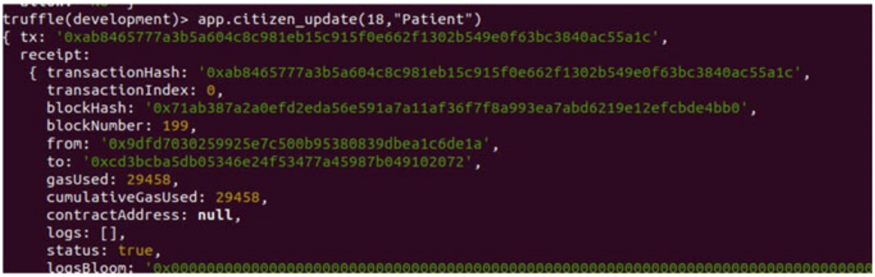
```
truffle(development)> app.positive(9,"Doctor",1234)
{ tx: '0x391e1ea5da6ed6c5fc2226fa4b610a3c74c4534e8a1b5c124e3d9efc18cb48f6',
  receipt:
   { transactionHash: '0x391e1ea5da6ed6c5fc2226fa4b610a3c74c4534e8a1b5c124e3d9efc18cb48f6'
```

Fig. 4 Doctor updates Bob as COVID 'positive'



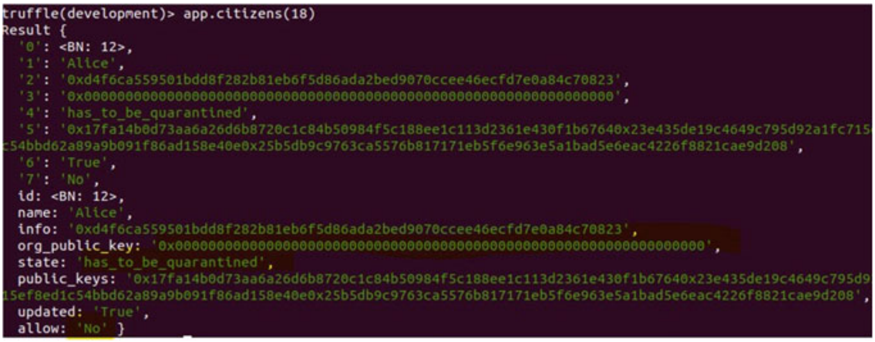
```
truffle(development)> app.citizens(9)
Result {
  '0': <BN: 9>,
  '1': 'Bob',
  '2': '0x807ad17e9923d600e61f363930ea125f5b0e6da72e0d4842d4a05a5be3a7951f',
  '3': '0x17fa14b0d73aa6a26d6b8720c1c84b50984f5c188ee1c113d2361e430f1b6764',
  '4': 'Positive',
  '5': '0xea355819a743e4457bb3481e0f761a3c48c489956e7190867fdea6975459a37a',
  '6': 'True',
  '7': 'No',
  id: <BN: 9>,
  name: 'Bob',
  info: '0x807ad17e9923d600e61f363930ea125f5b0e6da72e0d4842d4a05a5be3a7951f',
  org_public_key: '0x17fa14b0d73aa6a26d6b8720c1c84b50984f5c188ee1c113d2361e430f1b6764',
  state: 'Positive',
  public_keys: '0xea355819a743e4457bb3481e0f761a3c48c489956e7190867fdea6975459a37a',
  updated: 'True',
  allow: 'No' }
```

Fig. 5 Block structure (Bob) after testing positive



```
truffle(development)> app.citizen_update(18,"Patient")
{ tx: '0xab8465777a3b5a604c8c981eb15c915f0e662f1302b549e0f63bc3840ac55a1c',
  receipt:
   { transactionHash: '0xab8465777a3b5a604c8c981eb15c915f0e662f1302b549e0f63bc3840ac55a1c',
     transactionIndex: 0,
     blockHash: '0x71ab387a2a0efd2eda56e591a7a11af36f7f8a993ea7abd6219e12efcbde4bb0',
     blockNumber: 199,
     from: '0x9dfd7030259925e7c500b95380839dbea1c6de1a',
     to: '0xcd3bcba5db05346e24f53477a45987b049102072',
     gasUsed: 29458,
     cumulativeGasUsed: 29458,
     contractAddress: null,
     logs: [],
     status: true,
     logsBloom: '0x0000000000000000000000000000000000000000000000000000000000000000000000000000
```

Fig. 6 Alice performs her daily status update



```
truffle(development)> app.citizens(18)
Result {
  '0': <BN: 12>,
  '1': 'Alice',
  '2': '0xd4f6ca559501bdd8f282b81eb6f5d86ada2bed9070ccee46ecfd7e0a84c70823',
  '3': '0x0000000000000000000000000000000000000000000000000000000000000000',
  '4': 'has_to_be_quarantined',
  '5': '0x17fa14b0d73aa6a26d6b8720c1c84b50984f5c188ee1c113d2361e430f1b67640x23e435de19c4649c795d92a1fc715
c54bbd62a89a9b091f86ad158e40e0x25b5db9c9763ca5576b817171eb5f6e963e5a1bad5e6eac4226f8821cae9d208',
  '6': 'True',
  '7': 'No',
  id: <BN: 12>,
  name: 'Alice',
  info: '0xd4f6ca559501bdd8f282b81eb6f5d86ada2bed9070ccee46ecfd7e0a84c70823',
  org_public_key: '0x0000000000000000000000000000000000000000000000000000000000000000',
  state: 'has_to_be_quarantined',
  public_keys: '0x17fa14b0d73aa6a26d6b8720c1c84b50984f5c188ee1c113d2361e430f1b67640x23e435de19c4649c795d9
15ef8ed1c54bbd62a89a9b091f86ad158e40e0x25b5db9c9763ca5576b817171eb5f6e963e5a1bad5e6eac4226f8821cae9d208',
  updated: 'True',
  allow: 'No' }
```

Fig. 7 Alice's block structure after being found to have been in contact with Bob

6 Conclusion and Future Work

The staggering increase of COVID-19 cases has caused a major healthcare crisis, and a blockchain-based approach goes a long way in solving it. The proposed framework and accompanying simulations show that user's personal or epidemiological information is never dispelled to any stakeholder without justified reason. Additionally, the blockchain backbone maintains the reliability and immutability of user data. Our work can be extrapolated by designing a more layered access control mechanism roping in bed/ambulance availability checks to bridge the gap between the user, hospital and the government. Moreover, a JavaScript interface can be designed to ease the user interaction, and payment mechanisms via cryptocurrencies can be incorporated.

References

1. WHO COVID Timeline. https://www.who.int/news-room/detail/27-04-2020-who-timeline---covid-19
2. Zheng Y, Ma Y, Zhang J et al (2020) COVID-19 and the cardiovascular system. Nat Rev Cardiol 17:259–260
3. WHO Situation Report-158. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200626-covid-19-sitrep-158.pdf?sfvrsn=1d1aae8a_2
4. Fernandes N (2020) Economic effects of coronavirus outbreak (COVID-19) on the World Economy (March 22, 2020). Available at SSRN: https://ssrn.com/abstract=3557504
5. Gordon C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J 16:224–230
6. Olu O, Kargbo B, Kamara S et al (2015) Epidemiology of Ebola virus disease transmission among health care workers in Sierra Leone, May to December 2014: a retrospective descriptive study. BMC Infect Dis 15:416. https://doi.org/10.1186/s12879-015-1166-7
7. Danquah et al (2019) Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study. BMC Infect Dis 19:810. https://doi.org/10.1186/s12879-019-4354-z
8. Aarogya Setu. https://www.mygov.in/aarogya-setu-app/
9. Cho I, Yu (2020) Contact tracing mobile apps for COVID-19: privacy considerations and related trade-offs, cryptography and security
10. Newsroom. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
11. COVID Watch. https://covid-watch.org/
12. Hekmati, Ramachandran, Krishnamachari (2020) CONTAIN: privacy-oriented contact tracing protocols for epidemics, cryptography and security
13. Torky H (2020) COVID-19 Blockchain framework: innovative approach, cryptography and security
14. Nakamoto Bitcoin Whitepaper. https://bitcoin.org/bitcoin.pdf
15. Szydlo M. (2004) Merkle tree traversal in log space and time. In: Cachin C, Camenisch JL (eds.) Advances in cryptology—Eurocrypt 2004. Lecture notes in computer science, vol 3027. Springer, Berlin, Heidelberg
16. Wang W, Hoang DT, Xiong Z, Niyato D, Wang P, Hu P, Wen Y (2018) A survey on consensus mechanisms and mining management in blockchain networks. arXiv preprint arXiv:1805.02707, 1–33