Efficient Contact Tracing for pandemics using blockchain


Published in: Informatics in Medicine Unlocked

Document Version: Publisher's PDF, also known as Version of record

Queen's University Belfast - Research Portal: Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2021 the authors. Published by Elsevier Ltd. This is an open access article published under a Creative Commons Attribution-NonCommercial-NoDerivs License (https://creativecommons.org/licenses/by-nc-nd/4.0/), which permits distribution and reproduction for non-commercial purposes, provided the author and source are cited.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen’s institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person’s rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Efficient Contact Tracing for pandemics using blockchain

Nida Bari\textsuperscript{a}, Usman Qamar\textsuperscript{a, b}, Ayesha Khalid\textsuperscript{b}

\textsuperscript{a} Knowledge & Data Science Research Centre, Computer & Software Engineering Department, College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan
\textsuperscript{b} The Centre for Secure Information Technologies (CSIT), ECIT Institute, Queen’s University of Belfast, Belfast, BT7 1NN, UK

ARTICLE INFO

Keywords:
Contact tracing
COVID-19
Interplanetary file system
Blockchain
Distributed system
And pandemic

ABSTRACT

Blockchain technologies have been benefiting many industries by being decentralized, secure and confidential. They offer great potential in pandemic impacted scenarios as well. Contact tracing helps to mitigate the transmission of disease by alerting people who may have been exposed so they can act on time to protect themselves. Contact tracing systems face many challenges related to issues of medical privacy, data security and transparency. Multiple researches show concern that contact tracing discourages people to seek medication because of the fear of loss of data, subsequent stigma, discrimination, or abuse. In this paper, we discuss how contact tracing can be improved using blockchain technology and could be able to solve these issues. The aim of our proposed system would be to reduce the impact of pandemic, to implement this merger of the blockchains and the Contact tracing app and to ensure user privacy and avoid data misuse by incorporating a symmetric key cryptographic mechanism. To tackle the scalability related issues of Blockchain this framework uses IPFS, a distributed file storage system also known as Interplanetary File System. This blockchain based solution system will enhance contact tracing by making it more stable, secure, performant, highly usable and above all effective in the fight against any pandemic.

1. Introduction

This Coronavirus 2019 (COVID-19) is rapidly spreading infectious disease caused by novel severe acute respiratory syndrome coronavirus SARS-COV-2 \cite{1}. Throughout the globe, millions of people were sent to quarantine and lockdown to mitigate the wide spread of this disease. WHO reported 27,486,960 confirmed cases and this deadly disease took 894,983 precious lives across worldwide, as of September 9, 2020 \cite{2}. There are different vaccine available for COVID-19 in different regions of world but being vaccinated does not guarantee a person for avoiding COVID-19 for lifetime \cite{3}. It definitely build immunity against COVID-19. For decreasing the rate of COVID-19 transmission various countries have implemented non-pharmaceutical interventions (NPIs) by reducing the contact rate in general public \cite{4}. Strict measures were adopted by shutting down crowded areas and avoided gathering in large groups such as schools, airlines, workplaces etc. Maintaining social distancing of 6 feet was advised to be strictly followed all around the world. Strict measures have successfully reduced the number of new cases in cities that implemented NPIs timely. In the absence of vaccine, NPIs have been a great success in the H1NI influenza pandemic (1918–1919) \cite{5}, the last pandemic that matched up to COVID-19 scale. Along with the serious threat to human lives, infectious diseases also bring huge economic losses. This pandemic COVID-19 has caused biggest setback to US economy. Statistically, GDP collapsed at 32.9% annualized rate known as the deepest decline since records begin back in 1947 \cite{6}. To cope up with the damage various countries are developing balanced strategies. Contact Tracing had worked significantly to control infectious diseases for decades and shows impeccable capacity in controlling COVID-19. With no vaccine \cite{3}, the strategies of easing up lockdown and social distancing restrictions of most countries focused more on tracking approach. This approach will help in bringing normality into the society as well as saving lives and in the long run rescuing economy.

Our proposed approach will combine the best of both contact tracing and blockchain technology and overcome any challenges that is faced by existing contact tracing solutions. Details discussion on contact tracing and blockchain technology will be found later in this paper. Researchers are trying to expand different domains with benefits of blockchain technology. Authors in Ref. \cite{40} overlapped blockchain, a decentralized mechanism with IoT and overcome multiple challenges...
related to centralization that was creating applicability limits in large number of IoT devices. For the protection of integrity of data while communicating with drones and the control system, a distributed blockchain technology is used along with cloud services [41]. Authors have successfully solved the scalability issues as well as securing the data collected by drones. A smart city is known for achieving better quality of life by using IoT technologies. Authors in Ref. [42] designed a smart district model, the most vital step in building sustainable smart city using the combination of new technologies such as IoT and Blockchain.

5G technology has changed the game for augmented reality, IoT application and self-driving vehicles because of its reliable and fast communication. To enhance the security and privacy, Authors [43] have combined 5G services and blockchain, these two promising future technologies would overcome the current challenges faced in deployment and upliftment of 5G. Researchers in Ref. [44] have conducted a survey in analyzing the hidden opportunities that blockchain acquire in uplifting the 5G services. Smart healthcare, smart city, smart transport, smart grid and UAVs are some of the fruitful outcomes of these two future technologies. Authors in Ref. [37] proposed a user authentication scheme using blockchain-enabled fog nodes to handle the limitations of IoT devices. Fog units resolve the scalability issues of the system by performing heavy computational authentication related tasks.

Breaking the traditional centralized schemes, blockchain have merged as an effective decentralized storage with perks of security management. Authors in Ref. [45] benefited from this and modeled vehicle blockchain data. Their work also highlight the potential of blockchain technology for future vehicle networking. Security has been the concern for every crucial application because of the enormous amount of malicious attackers. Authors in Ref. [46] guarantee the safety of mobile services by proposing a decentralized authentication mechanism for IoV. They used the benefits offered by consensus algorithm of the blockchain technology. There’s been rapid increase of the energy consumption monitored while updating ledgers with potential issues for vehicles. Authors [47] resolved this issue by an effective blockchain-enabled Internet of Vehicles model distributed clustering.

2. Related work

A Most recent releases of contact tracing solution are NHS COVID-19 App [26], TraceTogether from Singapore [27], Google/Apple joint contact tracing project [28], and China Health code system [29]. These new launches are premature at the moment and results have also not been published except the German “corona warn app” [39], so it’s hard to tell the success rate. Every scheme is facing some challenges that need to be addressed.

Health Code System uses QR code associated with each user for relational cross-match. This centralized approach does not preserve privacy and user identity. As for power usage, this approach scans only at the time of passing checkpoints that reduces the consumption of battery and data [29]. The network coverage can be easily stretched due to its central hierarchy.

Contact tracing developed by Google Apple protects user identity and thus this approach becomes privacy preserving. But still, due to the use of central server for searching of contacts and notification, privacy can come under attack and intruder can access user credentials from the server [28].

In TraceTogether, BLE (Bluetooth low energy) is used to find and locate potential virus carriers. A drawback of this scheme is that it requires the user device to be on active mode all the time, hence it consume a huge amount of device power. Bluetooth contact tracing solutions are not secure, thus have a risk of data misuse that creates huge panic among general public. This being a centralized service, thus inherit all the related drawbacks making privacy a major concern [27].

Similar to all the other technique NHS COVID-19 App is also struggling with user privacy, concern of misuse of user information. This app also uses BLE that eventually leads to the battery drainage of user device. Long term impact of this technology over health care is still questionable. Lacking infrastructure, limited interoperability and underinvestment are some of the underlying challenges of NHS that needs to be addressed [30].

Authors in Ref. [34] proposed a blockchain based solution for digital health passports that will eventually provide immunity certificates. They focused on reducing the response time, providing immutable logs, decentralized solution and re-encryption proxies. This approach addresses many challenges and developed a solution that provide accurate and timely response to reduce the impact of this contagious disease COVID-19.

In [12], the authors provide guidance on how to control COVID-19 by developing contact tracing capacity. All the investigation and suggestion conducted in this study related to COVID-19 is carried according to the consideration of WHO. This document provides details of steps in undertaking contact tracing such as identifying contacts, informing contacts, managing contacts and analysis. This study highlighted Go Data software application and other tools for recording the symptoms submitted by contacts, as well as proximity applications that indicate potential clusters of COVID-19.

Authors in Ref. [7] gave insight on the requirements for case isolation and contact tracing. They analyzed significant parameters of COVID-19 spread to estimate the involvement of different transmission routes. Further, they described the limitations of using manual contact tracing, that it is slower and less effective in containing this rapid viral spread. A fast and effective system which cover a large scale is required to control this outbreak. This system also needs to notify contacts of surrounding positive cases immediately and has the capability to control this pandemic if used by enough people.

In [13], the authors focused on evaluating how smartphone contact tracing technology can influence the control and spread of infectious diseases. Astochastic model is introduced that further transformed into deterministic model, while taking in account of quarantine measures and the effects of contact tracing. They evaluated various scenarios while using these models and concluded, that quarantining restrictions can be minimized and new developed cases can be controlled with the usage of highly accurate tracing technologies and can overcome this crisis.

In [14], the authors conducted an investigation against this viral spread. They tried to track down the route of this spread to achieve epidemic control by extensive investigating, classifying, tracking, and managing contacts. Previous activities can suffer drawback due to substitute interviews with the patient. Moreover, they presented multiple methods such as card transaction, medical record facility and more, to reduce the queries regarding patient’s claims.

In [15], the authors proposed that for epidemic control, methods such as isolation of cases and contact tracing can perform wonders to mitigate any pandemic. They used a mathematical model to measure whether these methods can be useful for COVID-19 as well.

Privacy and data security being the major concern can affect contact tracing mechanism. Authors in Ref. [16], discussed best possible ways to protect privacy and user’s data and develop contact tracing technologies accordingly. They conducted risk analysis of various techniques according to users and societies. This study gathered all the advantages of previously developed contact tracing technologies and combined them to form a system for limiting concerned challenges. Precautions, prevention and upcoming strategies are also discussed.

Considering all the challenges in the existing contact tracing solution, we propose a system that combines the contact tracing approach with the Blockchain technology [32]. With this combination all the benefits of blockchain technology leads the contact tracing approach to be more secure, information to be immutable and more efficient.

Vujičić et al. [9], presented the framework of Ethereum, the mechanism of blockchain technology and bitcoin. IT is evolving to its full
swing, many novel technologies like blockchain is providing benefits to the information system. Bitcoin is defined as distributed P2P (peer to peer) network that performs transaction of bitcoin. A detailed concept of mining of blockchain and well-known consensus algorithm PoW was elaborated. A comparison conducted between bitcoin and Ethereum blockchain in this paper and it also described Ethereum’s dependencies. There are a number of challenges posed by this novel technology, the authors highlighted its scalability issue and tried to mitigate this by proposing solutions such as Bitcoin Gold and Bitcoin Cash, Lightning and SegWit.

The authors in Ref. [10], discussed elaborately about all the aspects of smart contact, i.e., it’s architecture, the framework it follows, the upcoming challenges related to it and its vast range of applications. Smart Contract is where all the functionality of the blockchain is defined and programmers can easily manipulate them according to their needs. The main reason for using blockchain is because of the programming mechanism and which data should be stored on which mechanism. The study identified such projects that are used to solve this problem. Blockchain is based on peer to peer mechanism that is an intelligent system and programmers can easily manipulate them according to their needs.

Scalability is a major challenge faced by blockchain and to solve it efficiently various techniques are proposed by authors in Ref. [11]. This study identified such projects that are used to solve this problem. Blockchain is based on peer to peer mechanism that is an intelligent combination of both economical and computational concepts. This paper discussed two ways to store records such as on-chain and off-chain mechanism and which data should be stored on which mechanism. The basic concept and implementation of five different off-chain patterns is presented, along with explanation of which data type that is to be stored using other storage medium. For reducing further inconvenience, any data that requires transactions should be stored on-chain and all the remaining should be stored off-chain.

2.1. Contributions

The major contributions of our work are as follows:

- We propose the design of contract tracing application to fight pandemics that is backed up by the blockchain-enabled contact tracing framework. This combines the best of two worlds since Blockchain technology’s benefits can be a game changer for existing contact tracing schemes. The benefits include Improved Traceability, better Transparency, immutability of records.
- The privacy and the confidentiality of each data record is ensured. Using the Role-based access mechanism, users get a granular access to the system according to their assigned role ensuring that the security of the patient’s personal medical data is not compromised, and the access is provided to only the authorised users of the system. For secure data sharing, symmetric key mechanism (encryption/decryption) is used.
- In order to solve the problem of blockchain’s scalability, our proposed framework uses off-chain scaling mechanism of Interplanetary File System (IPFS). IPFS is also a favourable choice for storing critical and sensitive data due to its cryptographic capabilities.
- We perform real-case scenario of various users performing different functions on the framework to assess the performance of our framework. We conducted performance evaluation using Apache JMeter version 5.3 and Apache Version 2.0. Apache JMeter is a desktop performance testing tool which is used for analysis and testing of applications.

The work in this paper is as follows. Section 3 narrates the basics of Contact tracing and its undertaking series of steps. Section 4 discusses the benefits and challenges of blockchain technology. Section 5 contains the proposed system model, architecture and its workflow. Results and its discussion are provided in Section 6. In Section 7 conclusion and future work is presented.

3. Contact Tracing

Contact Tracing is a process of identifying, assessing, and managing people who are in close contact with confirmed index case. These contacts are then tracked and informed about their risk to get care and treatment beforehand to prevent further transmission of the virus [7]. Hence this method has successfully reduced case numbers and large-scale outbreak for decades. Before the advent of modern technology, contact tracing relied heavily on paper-based system to store list of potential virus carriers that have been in close contact with confirmed cases over the defined time period [17]. Calls, letters or direct meetings with potential contacts were some methods used to inform who might be contacted. Using these traditional contact tracing approaches had limited the tracing efficiency and delayed the information process. This paper-based tracing system was alterable, incomplete, unorganized, inaccurate and insecure. It was also ineffective due to problem of data redundancy.

Digitalized Contact Tracing was designed to overcome all these above challenges and issues to develop a system that is more reliable in all the above aspects [18]. For all the confirmed cases, it is of high importance to conduct contact tracing to get all the related information to minimize the outbreak. Fig. 1 depicts the series of steps in undertaking contact tracing effectively.

3.1. Defining contacts

For A contact is someone who has been in close contact with a COVID-19 case and has following exposures, within the period of 2 days before to 14 days afterward the case develops signs of infection [12].

- Being in a range of 1 m of a COVID-19 case for more than 15 min.
- Physical contact with patient of COVID-19 disease.
- Providing direct care to a confirmed COVID-19 case without using PPE (proper personal protective equipment).

3.2. Identifying contacts

Identifying contacts are critical, it requires a detailed case information that can be obtained by thorough case investigation and extensive interviews with the confirmed case of COVID-19 patient or their carer. Public health officials need to detect the contacts with respect to the local area context and cultural measures [12].

3.3. Informing contacts

The contact tracing workforce should then develop a list of individuals who had been in contact with the patient of COVID-19. Each contact that made it to the list should be informed and thus require monitoring. Context of informing the contact include information about the process of contact tracing, information on quarantine, during self-monitoring what symptoms to look out for, what to do if they become unwell or any specific query a patient might have.

3.4. Managing and monitoring contacts daily

There are multiple ways to manage and monitor the contacts, i.e., quarantine with the objective of monitoring their symptoms, direct monitoring by the contact tracing team or self-reporting that is determined according to each case specification. A contact with symptoms should self-isolate [12], and interact with medical provider that is suggested through referral pathway if symptoms becomes severe or worsen.
3.5. Data processes and analysis

All the data that’s been collected throughout the whole process of contact tracing should be saved in somewhere safe, tamper-proof for further descriptive analysis and for compiling performance indicators.

4. Blockchain

Distributed ledger technology called blockchain was invented by Nakamoto in 2008 [8] to solve the double-spending problem of first digital currency, i.e., bitcoin. Blockchain emerged as a digital currency, Bitcoin, it possesses high potential to change IT in the same way as open source software did a quarter century ago.

Immutability, a unique property of blockchain that ensures no third-party interference to this continuously growing chained data. All the data introduced in blockchain is stored using blocks that are connected and secured using cryptography. Each block contains hash of that block, transaction data, cryptographic hash of previous block and a timestamp. Based on a P2P (peer-to-peer) topology, blockchain is a decentralized ledger that is not owned by any single entity. With no third-party intervention, blockchain is more secure, irreversible, transparent and more performant.

Blockchain technology has exposed great abilities in various fields and can be integrated with contact tracing application to solve problems in existing schemes such as security, trust, transparency, and privacy [19].

When someone joins the network, it gets the full copy of the blockchain for the nodes to verify that everything is in order. The new block is sent to everyone in the network, each node than verify the block to make sure they haven’t been tampered with. After successful verification each node adds this block in to their blockchain. All the nodes in this network create consensus. They agreed on which blocks are valid and which aren’t. This validation is performed by the nodes which are connected in the network using specific consensus mechanism to ensure the new member is authentic. This process of validating the transaction is commonly known as mining and miner are the node performing this validation. The other nodes will reject such blocks that are tampered with in the network.

Blocks that are tampered with will be rejected by other nodes in the network. So, to successfully tamper with the blockchain one needs to manipulate with all the blocks of the chain, do the proof of work for each block again and take control over 50% of the P2P network. Only then your tamper will be accepted by all others. So, this is almost impossible to do. After validation that block is added to the blockchain and the transaction is completed.

4.1. The three pillars of blockchain technology

4.1.1. Decentralization

In a decentralized blockchain system, the information is distributed across the network and not stored by one single entity. Decentralization solves trust issues as users don’t have to trust a central authority and it authorize multiple participants to manage a network. It gains user confidence because of its lower risk of systematic failure.

4.1.2. Transparency

Transparency add much needed, level of accountability that is required by many businesses. All transactions are traceable and searchable in open blockchain. This feature may contradict with blockchain’s privacy and security but they can work together. Blockchain can provide granular access to some authorized users while protecting your data from unauthorized users.

4.1.3. Immutability

This immutability property of blockchain is game changer for many industries. Once data is entered in the blockchain, it cannot be tampered with. The reason for this blockchain’s property is because of cryptographic hash function. Each block has unique identification through cryptographic algorithm.

---

![Fig. 1. An overview of contact tracing process.](image-url)
4.2. Challenges of blockchain technology

The main concerns related to blockchain is lack of scalability and lack of interoperability. Storage capacity of blockchain is quite limited thus introducing voluminous data of contacts would highly affect the efficiency of blockchain [20]. Using off-chain storage mechanism would effectively minimize the storage burden off from the blockchain.

Technology has certain advantages and limitations to certain groups of people, mostly elders and minors. That may affect the rolling out of transactions of any system, but there are ways to incorporate them. Many advanced technologies such as wireless IoT and wearable gadgets can enable them for using any system.

It’s a fact that centralized systems are more efficient in terms of economics than decentralized systems. On the other side, the decentralized blockchain system can preserve privacy a lot better than a centralized system that can effectively diminish the resistance of using the technology because of the fear of human rights violation. This will increase the uptake of our proposed system among the citizens and eventually be of supreme importance in saving billion lives each day.

5. Proposed system model

In this section, our proposed system model that is blockchain based contact tracing is discussed. The proposed solution ensures trusted information sharing between patient and trusted authority. The proposed system is developed in a secure environment for trusted contact tracing communication and tackles various challenges of the contact tracing.

5.1. Architecture overview

Our proposed solution model allows the development of the distributed Contact Tracing in an efficient manner. Model of the proposed system is illustrated in Fig. 2 that is intended to meet the requirements and challenges of Contact Tracing. Three different types of user exist, which are: Contact Tracer, patient and administrator. All these users have granular access to the system according to their level of authority over the system. Every authorized member of the app pledges to commit to the privacy policies and procedures to safeguard Personal Data. These users would interact with the system’s GUI of DApp browser where all the functionality of the proposed framework is being displayed. According to their roles, the users would react with other modules of the system. Functionality of the proposed framework is implemented on blockchain. Blockchain is based on peer to peer mechanism where all nodes have equal rights and creates a distributed platform that suits best for our proposed system. Blockchain follows some consensus rules for each transaction to be secure and temper-proof.

For developing more security and privacy, the cryptographic mechanism is proposed for reliable communication. Each user has assigned with a unique address for using proposed framework, which is used to build trust between users in a communication network.

5.2. Contact Tracing workflow

Contact Tracing is crucial to be conducted for all the confirmed cases to break new transmission chains. A contact is someone who had been in close contact of about 1 m with a confirmed case for more than 15 min or had any form of direct physical contact with the confirmed case or providing direct care to the confirmed case without using proper protective gears. First step of Contact Tracing is identifying contacts. Best methods for identification are by interviewing and conducting detailed case investigation of the patient or it can be their caregiver as well. The contact tracing workforce needs to identify contacts based on the local context and society norms. Contact Tracing Team would develop a list of people who are interacting physically with the confirmed patient while providing care. Each person confirmed as contact should be notified and provided with information on self-quarantine, what symptoms to look out for, if the condition worsen who to refer for testing and treatment and any other query or concern raised by the contact. Contacts observing self-quarantine needs to self-report any signs or symptoms or even no signs or symptoms. After a specific time, contact should discontinue self-quarantine if found asymptomatic.

5.3. Smart contract

Smart Contracts are used to perform basic operations. They are an important part of DApps. These contracts grant access to the users of the system and allowing them to perform various procedures on the records.
The contract included in our proposed system is Contact Tracing Records. This contract contains the implementation of the functionality of our proposed contact tracing system. It defines roles and provide access accordingly to perform various operations. The algorithm of smart contract named Contact Tracing Records is given below. All the operations included in the proposed system are defined along with their conditions. Permitting access to different roles to perform particular functionalities are also explained in it.

5.3.1. Vulnerability analysis

Safeguarding the crucial and valuable data is vital part of any business. The code need to be free of risks of security breaches and any vulnerability that may lead to future lose [36]. The smart contract defines all of the functionality of our proposed system, to make it all rounded and free of security vulnerabilities, the code needs to be thoroughly tested. There are many security analysis tools that provide this facility for checking code. Oyente, a smart contract auto-auditing tool, analyze smart contracts and returns possible bug attacks on it including the famous DAO attack [35]. This was developed by researchers from National University of Singapore in Jan 2016. It provide analysis report with various attributes that verifies the availability of security threats. The analysis report for our smart contract is shown in Fig. 3. All the vulnerabilities are checked false that means there is no security bugs in our smart contract (see Figs. 6 and 7).

5.4. Transaction

The functionalities provided by the system how these are incorporated while the implementation of the system is explained in this section.

5.4.1. Assign roles

This phase of the DApp is handled by an administrative entity, which is trusted by the hospital and is assigned with the job of defining the roles of a user on the system. The Assign Roles sends (Role Name, Roll Address) to the Blockchain. These both act as the unique identification of a user on the system. Just like the system has two different users on the system, the roles would also be of two kinds i.e., Assign Roles might assign roles to Contact tracer or Assign Roles could also assign roles to Patient. The Assign Roles sends (Role Name, Role Address) to Blockchain that is stored in Role List for Patient and Contact Tracer that are separate to both of these entities. As this system in secured through symmetric key cryptography mechanism, user would first be authenticated and then can access multiple functionalities offered by the system.

5.4.2. Add Patient Records

At this stage, Patient is assigned the role to perform various functions on DApp. When requesting the Blockchain to add records related to biodata on the Blockchain, the patient sends record to be stored on Blockchain.

5.4.3. View Patient Records

The patient uses Role Address assigned to him to perform the view function on his medical records. The system would follow the steps below to perform this function,

- After logging in to the system, the system now matches the Patient’s address to whom its being logged in with the record stored in Blockchain.
- After validation at step 1 is done, the record R is available on the user’s system.

5.4.4. Add patient symptoms and test record

Patient will monitor his own symptoms and daily submit it to the system for contact tracer to view and monitor his health. The system would follow the steps below to perform this function,

- After authentication, the patient can add the symptoms and test reports to an off chain named, IPFS.
- IPFS stores the information in distributed hash table.
- IPFS assigns hash to the information file stored.
- Sends the hash information to blockchain.

5.4.5. Get message

Patient can Get Message from the contact tracer related to the preventive measures or the emergency information incase things go wrong. After patient being logged in, system will automatically generate the message first up the screen from the contact tracer.

5.4.6. Add contacts

Patient can add contacts information if he test positive of the disease. Whosoever he’s in close contact with, approximately within the range of 1 m, for more than 15 min in last 3-4 days or 1 week, he will provide information of them all. So that contact tracer can track contacts as soon as possible to halt the spread of this disease.

5.4.7. Send message

After evaluating the symptoms of a particular patient, Contact Tracer would be able to send quick response to the patient regarding their health, preventive measures or emergency information. The system would follow the steps below to perform this function,

- Contact Tracer would specify the Patient’s address to whom he wants to send the message as well as the message.
- This message would store on the Blockchain and deliver to particular patient immediately.

5.5. Usage scenario for Algorithm 1

Privacy and misuse of data is a major concern of Contact Tracing and to overcome it role-based access is implemented in our proposed system. This also ensures that no third party would be allowed to manipulate the contact tracing records and only authenticated parties will have access to these functions explained in Algorithm 1. First function of this Algorithm 1 is Assign Roles, as the name suggest this function is used for assigning roles to the respective accounts so they have granular access to the system. This function is to be performed by the administrator different roles to different accounts. Next function is Add Patient Record that is performed by the patient after validation. All the data from will be saved once everything checks out.

Retrieve Data function can be performed by both contact tracer and patient but they need to validate themselves before accessing it. It needs a patient id as an argument to return the particular data according to the id. Add Test Records is a function that is also performed by the patient after validation for adding test records to the system. These test records would be saved through IPFS and its hash would be saved in blockchain. Next function is Send Message, this function sends message or
instructions to the patient and is performed by contact tracer. It requires patient id to be passed as an argument. It would send message to that particular patient’s id. Last function of Algorithm 1 is Get Message that is to be performed by patient, it takes an argument patient id. If there’s any message mapped to that patient id it will prompt on the screen once patient’s validation went successful.

Algorithm 1. Smart Contract for Contact Tracing

Assign Roles:

function Assign Roles (New Role, New Account)
add new role and account in roles mapping
end function

Add Data:

function Add Patient Record (contains variables to add data)
if (msg.sender == patient ) then
  add data to particular patient’s record
else Abort session
end if
end function

Retrieve Data:

function View Patient Record (patient id)
if (msg.sender == contact tracer || patient) then
  if (patient id) == true then
    retrieve data from specified patient ( id )
    return (patient record) to the account requested the retrieve operation
  else Abort session
  end if
else Abort if
end if
end function

Add Test Records:

function Add Patient Test Record (contains variables to add data)
if (msg.sender == patient) then
  Sends the information to IPFS
  IPFS stores the information in distributed hash table
  IPFS assigns hash to the information file stored
  Sends the hash information to blockchain
else Abort session
end if
end function

Send Message:

function Send Message (patient id)
if (msg.sender == contact tracer) then
  send message to particular patient
else Abort session
end if
end function

Get Message:

function Get Message (patient id)
if (msg.sender == patient) then
  if (patient id) == true then
    return (message) to the account that requested the get message operation
  else Abort session
end if
end if
end function
5.6. Workflow of proposed system

In the proposed distributed blockchain-based Contact Tracing, there are two main user entities, i.e., users and network administrator. Users are subdivided into Contact Tracer and Patient. It's the job of the administrator to define roles of the new accounts. Every user would have its role name and public account address. A list of all the users with defined roles are introduced in the proposed blockchain network.
Users communicate with the system for required services. The system would first verify from the list of roles assigned by the administrator then it would entertain the request and respond accordingly. All communications are encrypted throughout the blockchain network to ensure privacy. In the proposed model, AES128 cryptographic algorithm is used for encryption. IPSFS, a distributed secure record saving mechanism is used to store information provided by the users, after storing it generates corresponding hashes. These hashes are then stored in the blockchain network. All the other functions can also be performed on DApp browser.

5.7. Usage scenario for proposed framework

Access Granted: Let us now understand the flow of activities for a user i.e., patient who intends to add his records and daily observations on the system. The Fig. 4 below depicts the whole process of this scenario’s activity flow. This whole process starts from the Administrator, who is some trusted individual inside the hospital or healthcare organization. The administrator is responsible for assigning the Roles to various users of the system. This individual would obviously have some technical skills and experience as well for understanding and using the system. So, the first activity would be that administrator assigns roles and this would include Role Name and Account Address of the user who is being assigned that role. Every user of this proposed system would have a role name and account address for using the system. So, after administrator assigns this user some role, that role name and account address is stored in a roles list for validation purpose required in later steps.

After roles are assigned, now when a patient wants to perform some operations on the proposed system, he would at first request to perform them. The system would verify the patient’s role name and account address from the Roles List and allows the patient to perform those functions after validation returns success. The patient would perform the desired functions and the system would store the information on the Blockchain that would perform transactions for that information. Once the transaction is confirmed the system receives the message of success from the blockchain layer that patient can view on the DApp browser on which the whole proposed system is being visible.

Access Denied: Let us now understand the scenario when a user who is not assigned a role by the administrator or is not using the account address that is assigned the roles would try to access the system functions. As seen in Fig. 5 below in such a scenario system would deny access to the user requesting to use the function. In this process when a user requests to access dashboard of the system, the system checks Roles List to determine that should the user be allowed or not to use the various functions of the system. If the user is not assigned a role for performing these functions the system denies access to the user and indicating the user failed to authorize.

6. Simulations and results

In this section, the performance of the proposed solution is discussed. Comparison with related frameworks and challenges derived with this novel technology is also presented in this section.

6.1. Simulation environment

For performing simulations, Ethereum, a distributed blockchain network is used just like popular Bitcoin [8]. As compare to bitcoin, Ethereum possesses user friendly environment and can perform a greater number of transactions in 1 s. Decentralized Application usually known as DApps is a blockchain-based environment that is supported by Ethereum. Solidity is the programming language supported by Ethereum that can easily be customizable according to the needs of programmers [21]. Smart contract contains the main functionality of Ethereum and it is developed using solidity language. An Ethereum transaction regardless of types contains following elements [21]:

- From – sender of the message using the blockchain to the recipient. Both sender and recipient have a 20-bytes address.
- To – message recipient, also having a 20-bytes address.
- Value - the fund amount (wei) transferred from sender to recipient
- Data (optional) – contains the message that is being sent to the recipient
- Gas – For every transaction on the Ethereum blockchain the sender needs to pay some fees for performing that operation this fee is known as Gas. Every transaction contains the gas limit and gas price in it. This process is secure because the gas not consumed in a transaction is refund to the sender. And sender is charged for the only gas he consumes during transaction [21].
  - v, r, s – used for creation of the signature that is used for identification of transaction sender
  - nonce – keeps the count of number of sent transaction
  - init – used for contract initialization for the first type of transaction i.e. Contract Creation

6.1.1. Ganache

For developing decentralized applications on Ethereum, Ganache is used for development of DApps, deployment of smart contracts and running tests [22]. It is also called virtual blockchain that provide some accounts with unique address for development purposes. These addresses contain pre-defined virtual ethers. It looks like a virtual network of nodes but acts like a real-world application of Ethereum having nodes connected on its network.

6.1.2. Metamask

Metamask act as a bridge between Ganache and Web browser [23]. It allows the developers to view the working of the decentralized applications on the web browser. The addresses provided by Ganache run DApps on Metamask. This browser extension performs as Ethereum blockchain without running complete node of the blockchain.

6.1.3. System specifications

The specifications of system used for network simulations are:

- Intel Core (TM) i5-8250U CPU @ 1.60 GHz processor
- And 8.00 GB of memory with Windows 10 Home (64-bit)

6.2. Performance assessment

In this subsection, we will discuss how our proposed system would perform different functions by various users in real-case scenarios. For performance evaluation, we used Apache JMeter version 5.3, which is popular in testing environment. It is an open source testing software for analysis and measuring performance of various services provided by the applications [24].

<table>
<thead>
<tr>
<th>Function Caller, and Gas of proposed framework.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function Caller</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Admin</td>
</tr>
<tr>
<td>Admin</td>
</tr>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Contact</td>
</tr>
<tr>
<td>Contact</td>
</tr>
</tbody>
</table>
6.2.1 Average execution time

Time require to completely and successfully execute a specific function by a user, is known as execution time. With the increment in number of transactions, the time to execute them would also increase. The functions against we evaluated execution time in this subsection are defined in Algorithm 1 of section. For single user our system performed the functions Assign Roles, Add Patient Records, View Patient Records, Send Message and receive message for about 10.7 s, 1 min 9 s, 50 s, 9 s and 4 s respectively. This time would increase as the number of users using the system increases simultaneously.

6.2.2 Throughput

In Fig. 3, the throughput of different segments of Contact Tracing smart contract are analyzed, in terms of number of users ranging from 100 to 500 that are performing different functions explained in Algorithm 1. The unit for Throughput is in Data/time, i.e., KB/sec in JMeter.

A number of experimented performed on our proposed framework to evaluate the performance of the system. From this, we conclude that there is a smooth linear graph formed between number of users and overall throughput indicating the efficiency of the proposed framework.

6.2.3 Average latency

In Fig. 4, the average latency of our proposed solution is presented in terms of throughput. The latency is the time between the request sent to a system and the response received by the system. JMeter is used to evaluate latency for this proposed framework. Milliseconds is the unit for latency in JMeter. In this experiment, 13 ms is recorded as the highest latency.

The lower the latency, quicker would the app respond. According to NHS the number of New COVID cases reported on the 19th Nov were 30 in the city of ABERDEEN in UK with population of 189,120 [33]. This means that with the increase in users our system would support the upcoming users with minimum latency.

6.3. Cost analysis

We can calculate the transaction sizes of various functions of our proposed framework by using the data payload. Keeping in mind that transaction sizes are specifically calculated for various functions of Algorithm 1 through data payload point of view. All these transactions cost some gas or fee, that can also be calculated in 'ETH' with units wei or gwei. The transaction fee for a transaction is the product of gas consumed and gas price. It could be represented as follows,

\[(\text{gaslimit} \times \text{gasprice}) = \text{transaction fee}\]

We can calculate the transaction fee by using the recommended figure for gas consumed which is 66199 and is 20 Gwei for gas price. So,

\[\text{Transaction Fee} = 66199 \times 20 = 1323980 \text{ Gwei}\]

And to calculate the transaction fee of 1 ether, we know each gwei is equal to 0.000000001 ETH (10^-9 ETH).

\[1 \text{ Ether} = 1323980/1000,000,000 \text{ Gwei} = 0.0013 \text{ Gwei}\]

The transaction fees for various functions of Algorithm 1 are presented in Table 2.

6.4. Comparison of proposed framework with related work

In this section we discuss some parameters that made our proposed contact tracing system better in comparison with other systems. To cope up with the challenges, we present our blockchain-built contact tracing that fulfills both privacy and performance requirements. For post pandemic contact tracing all the below aspects are required for better capability to fight against this novel disease.

6.4.1 Enhanced privacy as the main focus

Privacy is the most significant and alarming factor of contact tracing as information has to be collected, traced and distributed. Protecting the identity of users is also a major concern. Meanwhile, Information handling in centralized system has a risk of manipulation and corruption. Nevertheless, it is not a trouble for blockchain, it has the capability to bridge out these differences and create a distributed environment for the tracing participants. Rather than relying on rules and regulation in centralized system, Blockchain offers privacy preserving technical solution, where the identity is removed at the beginning and it can further combine with encryption technologies to provide ultimate confidence in privacy.

6.4.2 Access control

By controlling the access of the users, this framework ensures that no unauthorized party would be able to access the system. Using blockchain technology ensures no third-party intrusion, that makes our proposed solution more secure. Confidentiality ensures that the communication made between any two parties cannot be interpreted by anyone else. Therefore, unauthorized access to the data cannot take place. Confidentiality can be achieved through encryption. Therefore, in our solution, message encryption and decryption is achieved through systematic key encryption that ensures the authentication of the user. Every authorized user has a defined role and according to that specified role, user have granular access to the system ensuring security of personal records of the patients.

6.4.3 Scalability

One challenges that blockchain is facing is scalability that requires a solution. For developing a robust framework, we used Interplanetary File System (IPFS) that is off-chain storage mechanism [25]. The data is encrypted using symmetric key encryption. For data decryption a unique private key is required, that provide protection against malicious attacks because it’s not easily guessable, therefore security of the framework is not compromised. The IPFS hash is then stored in the blockchain, which has a trait of being tamperproof so it is difficult to perform any malicious activity. Hence, the data size of records stored in blockchain has now decreased and system performs adequately.

6.4.4 Trustworthy information

Misinformation can cause panic to the general public and leads to inaccuracy of data; hence it slows the process of pandemic prevention.
Information inaccuracy and information transparency are the main reasons for the misinformation. The higher authorities can have a motive to not disclose the accurate information or provide false records according to their indulgence in centralized mechanism. But that’s not the case with blockchain. Blockchain’s transparency feature comes handy for preventing data misinformation normally caused by third parties and authorities by providing verifiable trusted tracing information.

6.4.5. Fault tolerance

For overcoming the problem of single point of failure, we proposed to incorporate the benefits of IPFS in our system. This storage system is distributed that acts as a P2P network. To store, each file is broken down into different portions and then assign them a specific node on the network.

6.4.6. Availability

Interplanetary File System is used for data storage in our proposed framework. This distributed storage system generates hashes against each data storage. A request is sent to IPFS whenever the data is required and it will direct to that specific node where the data are kept. This distributed storage mechanism would ensure the availability of data while maintaining high throughput of the system.

7. Conclusion and future work

In this research work, a secure and resource effective blockchain-based data storage mechanism with role-based access for Contact Tracing is proposed. This is the merger of the blockchains and the Contact tracing app. Only authenticated and trusted individuals can access the proposed framework by this novel technology, i.e., blockchain. Challenges of centralized data storage is known worldwide and to tackle those IPFS, a distributed file storage system is considered. Blockchain technology in vision new advanced capabilities in contact tracing field and addressed some issues that faced by existing contact tracing solutions.

In future, we plan to implement the existing framework more general basically for all expected pandemics. We would develop a module where patients can get assistance online from doctor, merging contact tracing with healthcare sector [31]. Present decentralized frameworks are accessed to a local network, hence using third party suppliers would boost the coverage globally without much effort. Payment module for online assistance would also be developed in future research works.

Future versions would also include Blockchain interoperability and cross-chain functionalities that would widen the adaptability of blockchain [38]. We also aim to modify our current system with additional vaccine module in our future releases.

Author contribution

Nida Bari: Conceptualization, Methodology, Software, Validation, Data Curation, Writing.
Usman Qamar: Supervision, Project Administration.
Ayesha Khalid: Formal Analysis, Investigation, Resources.

Funding

Not applicable.

Consent

Not applicable.

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.

References


[42] Lazaroiu G, Roscia M. Smart district through IoT and blockchain. IEEE (ICRERA); 2017.


