Blockchain Based Real-Time Contact Tracing – A Secure Way to Mitigate Highly Infectious Diseases

Asit Bandyopadhayay
Austin Peay State University

Reshmi Mitra
Southeast Missouri State University

Srija Bandyopadhayay
Cape Girardeau Central High School

Contact tracing is an effective, data driven infectious disease control strategy that involves identifying cases of active virus carriers and their contacts in restricting further disease transmission. Despite the effectiveness of this strategy, there are serious concerns regarding the privacy and security of data that are collected in this process as individuals give up control over those data. This study aims to provide some building blocks for developing a secured blockchain-based mobile application for contract tracing to strengthen the infectious disease mitigation approach. It also attempts to understand the contrasting perspective of different stakeholders involved in the data collection process through stakeholder survey and their willingness to share/store identity and health-related data in a blockchain-based app. Finally, we suggest a framework in developing an app to automate contract tracing in a private, secure, maintainable environment. This study helps create a strategic roadmap for developing a secured contact tracing platform to mitigate highly communicable diseases.

Keywords: blockchain, contact tracing, COVID-19, data security & privacy, pandemic, communicable disease mitigation

INTRODUCTION

Coronavirus Disease 2019 (COVID-19) has been recognized as a worldwide pandemic that has been spreading exponentially in various nations. As of date, worldwide (COVID-19) has infected more than 676 million people and caused more than 6.8 million deaths and it is increasing on daily basis. Precisely, the United States has become the country with the largest number of known infections with more than 103 million cases and caused more than one million deaths and even increasing. Several new cases are around half a million every day across the world (JHU, accessed March 3, 2023). COVID-19 is caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), first identified in the city of Wuhan in the Hubei province of China in December 2019. It is one of the most devastating infectious diseases identified in

human history and on March 11, 2020, the World Health Organization (WHO) declared COVID-19 a worldwide pandemic (WHO, 2020).

Contact tracing is an effective disease control strategy, precisely for highly infectious diseases that involve identifying cases and their contacts and subsequently working with them to interrupt disease transmission. This includes asking the carrier of infectious disease to isolate and quarantine at home voluntarily so that they should not spread the disease further. Contact tracing has also been a key strategy to prevent the further spread of COVID-19 (CDC, 2020). It is also referred to as the identification, monitoring, and support of the individuals (contacts) who have been exposed to the patient and possibly infected themselves. Due to the high contact rates of infections, nations are trying to use technological procedures and innovations to keep track of the infection rates and prevent the further spread of COVID-19 contagions. Although contact tracing is a difficult task, this process prevents further transmission of disease by separating people who have (or could have) an infectious disease from people who do not.

By tracking patient movements, public health officials will be able to provide real-time data about infected zones. This will also help identify virus-free zones and help maintain quarantine standards. To prevent future outbreaks, healthcare officials need to reduce the risk of information falsification which implies increasing the reliability of trusted sources. This will ensure accurate real-time information is being provided to the healthy population in a tamper-free and transparent manner. This raises crucial questions about user identity management and various degrees of data access rights based on the capabilities of the stakeholders.

Even though the use of technological advancements may be beneficial when collecting large amounts as well as ranges of data, the main concern arises when the data systems are incapable of securing the confidential data of the users. Technological advancements such as artificial intelligence (AI), blockchain, the internet of things (IoT), intelligent mobile apps, etc. can be leveraged to address this crucial contact tracing problem. Recently, several contact-tracing mobile applications have been developed using Bluetooth-embedded technology (Song et al., 2020). Using such technology, it is possible to record close encounters between mobile phones, wearables, and IoT devices. However, the biggest concerns with these methods are to ensure data security and privacy for their users. Personal information sharing even in case of a pandemic situation such as COVID-19 is governed by the policies of the federal and state government. Current work from MIT, Apple, and Google have announced their tracking solutions by storing users' data in the cloud (Song et al., 2020), whereby the user may lose ownership of their data.

Government agencies and organizations may access the health medical data of all people and go beyond the scope of their responsibility and duty. For example, some government health departments may find the personal information of infected patients, and then compel them to move to a centralized isolation center, resulting in additional infections, and restricting personal freedom. The application developed by Apple and Google will share the infected individuals' information with health authorities (Apple Newsroom, 2020), which means people's data privacy and human rights are being violated without their knowledge and their personal information is not secure in such situation.

To address the above shortcomings, the main objective of this work is to investigate user data privacy concerns towards building a viable blockchain-based mobile application (henceforth app). Blockchain is a viable solution to address these privacy concerns as it ensures that the data is immutable and auditable with the use of advanced cryptographic techniques. It primarily comprises a chronologically ordered list of encrypted signatures, and a secure distributed ledger containing permanent transaction records which are shared by all members in the network (Marbouh et al., 2020). Blockchain for trustworthy computing is receiving tremendous research interest both in industry and academia for various applications. Powered with this upcoming technology, the proposed solution that will be derived from this study has significant potential for planning and mitigation efforts for COVID-19 and future highly infectious diseases.

Therefore, the purpose of this study is two phases. In the first phase of the study, we plan to conduct a market study in understanding feasibility criteria, especially privacy concerns in developing a mobile application (henceforth app) for highly infectious diseases. In this phase, we conduct a survey with the different administrative stakeholders (healthcare institutions, public health officials, information systems

administrators, government, and other institutional administrators) in knowing the data privacy concerns they have while using such an app.

In the second phase, we propose a framework to automate contract tracing through a blockchain-based mobile app for highly infectious diseases in a secure, maintainable environment. The main contributions of this paper are a) capturing the sentiments of stakeholders from diverse fields to understand organization-specific concerns about contact tracing and information flow and b) developing a framework to automate contract tracing.

This paper is organized as follows: Section 1 talks about introduction; section 2 reviews contact tracing and blockchain technology-related work from literature; section 3 discusses blockchain technology as a secured and powerful tool for contact tracing; section 4 talks about contact tracing framework development methodology; section 5 deliberates results and discussion; section 6 talks about our proposed contact tracing framework, and finally conclusions are available in section 7.

LITERATURE REVIEW

This section has two parts – in the first part we reviewed the most recently proposed COVID-19 contact tracing approaches across the world and in the second part we studied blockchain as a tool for contact tracing.

COVID-19 and Contact Tracing

The ultimate goal of contact tracing is to identify individuals who are carrying or have symptoms of carrying an infectious virus as early as possible, so that they may be quarantined, tested, and monitor on their health progress. Another purpose of contact tracing is the identification, monitoring, and support of the individuals who have been exposed to the infected patient and possibly infected themselves as the disease is contagious in nature. By identifying and isolating such individuals from the circulating population, the spread of the virus may be diminished. Contact tracing is effective in preventing infectious diseases. The process relied heavily on remembering the list and location of the people whom they have been in contact with over a certain period. Manual processes (for example phone calls, text messages, emails, etc.) can be used to inform people who might be contacted. Therefore, accuracy, as well as completeness of the list of contacts, timeliness, and efficiency of the tracing, is limited by such a traditional manual contact tracing method. With the extensive use of smartphones, digitized contact tracing with the help of it has been developed and implemented in some countries to solve the problems of manual contact tracing methods.

Currently, we have two popular contact tracing systems - location-based and individual-based. Location-based contact tracing always provides a centralized service and records if there are infections in the given locations without the knowledge of infection movement (we-care. world, Feb 2021). The individual-based tracing systems only focus on person-to-person contact via Bluetooth. Here, Bluetooth signals from smartphones are used to detect interactions with people infected with COVID-19. This approach does not use or store users' location as well as data, and if someone develops COVID-19 symptoms, an alert could be sent to others that they might have been infected, with the least intervention. There are two variants of Bluetooth-based contract tracking - the centralized model (TraceTogether used in Singapore is an example of this model (Bay et al., 2020)) and the decentralized model (BeepTrace, proposed by Xu et al. (2021)). However, Bluetooth technology-based contact tracing solutions have security concerns as it has a vulnerable wireless interface, and threats that include sniffing, jamming, etc.

Google Apple contact tracing (Exposure Notification, 2020) employs a similar approach to TraceTogether. MIT PACT protocol suggested by Rivest et al. (2020) also has similar products and projects. All these solutions are based upon either a centralized database that is built into the system or incomplete privacy protection provided to its users. Such designs cannot meet the requirements of user privacy and data security. The difference lies between TraceTogether and Google Apple contact tracing in the user's privacy perspective. In Google Apple contact tracing, since the service provider cannot use the user's real identity, to some extent it can protect privacy of its users. However, the main concern here is the

user is required to use their central server for contact matching and notification, which brings the concern about compromised user privacy and enables the reconstruction of the user's profile using access information to the server. In the same way, U.K. NHS COVID-19 app (Levy, 2020) has risks of potential exposure of user privacy. Other contact solutions such as China's health code system (Mozur et al., 2020); India's Aarogya Setu (Gupta et al., 2020); Australia's COVIDSafe (Currie et al., 2020); Pan-European Privacy-Preserving Proximity Tracing (Team, 2020) are like the concept described here with minor tweaking on certain features.

Contact Tracing and Blockchain Technology

As COVID-19 has taken its name into the worldwide crisis, many global concerns such as the downfall of an economy were taken into consideration. Many nations like the U.S. expected their economy to plummet due to the lockdown brought down by the pandemic. To tackle such downfalls, Xu et al. (2021) state that contract tracing along with social distancing can help nations limit the spread of the virus and prevent longer lockdowns in the future; however, a further question arises when taking into account privacy issues regarding contract tracing. To handle this issue, the authors suggest the use of BeepTrace, a Bluetooth enabled Blockchain contact tracing, which globally distributes user information in a decentralized manner using two distributed blockchains so that the users have direct authority over their information without the involvement of any centralized authority where confidential data can be compromised. Unlike centralized contact tracing apps like TraceTogether and Google/Apple, BeepTrace will provide complete transparency in data which will further prevent inaccuracies in data systems. The contract tracing app will keep track of the tracing cycle for 14 days - the minimum days recommended by World Health Organization (WHO) to limit the further spread of infections; further geodata information about geographical intersections involved in contract tracing will be stored in ciphertext which will only be accessible to the users. The authors state that BeepTrace will further avoid using proof of work (PoW) and proof of stake (PoS) consensus mechanisms and will instead use direct acyclic graph (DAG) based consensus mechanisms to provide faster and more secure transactions with low computing power. Overall, the authors claim that BeepTrace can effectively desensitize user identity and geodata while preserving battery life, security, and privacy in one go.

A study by Song et al. (2020) addresses concerns regarding privacy security systems when understanding how centralized data systems can violate users' privacy when collecting data revolving around COVID-19 cases. Many companies like Apple and Google are using centralized data systems by storing user information in a cloud system which eventually leads the user to lose access to their data while making it easier for hackers to gain control of the confidential information. To prevent these mis-happenings while tracing COVID-19 cases, Song et al. (2020) suggest location and individual-based contact tracing systems using blockchain as well as smart contract technologies to effectively track infection movements in various locations while also securing the privacy of the people. To effectively use this method, users will be required to turn on their Bluetooth to detect other users and their infection trajectories. To maintain further privacy, Bluetooth would be generating random mac addresses stored in Blockchain databases to ensure that users are not being tracked by surrounding networks (Song et al.). Furthermore, the COVID-19 tracing system contains four layers: user interaction layer, mobile service layer, smart contract layer, and data storage layer. The user service layer enables the users to connect to Bluetooth to report their health status which later goes to the smart contract service layer to determine the infection status of the location. The mobile service layer, as a result, will be used to alert the user's direct and indirect contacts with other infected users. All these checks in data are secured in the data storage layer using the blockchain technology system. Furthermore, using the data, COVID-19 cases can be predicted using probability simulation. Blockchain technologies are especially difficult to maneuver which will ensure the security of data when being used in contract tracing apps.

Due to the COVID-19 global pandemic, many general challenges have been faced around the world. Some of them include social distancing, unemployment, hoax information, shortage of life-saving drugs, oxygen, and healthcare equipment, low distribution of food and charity funds, online scams, quality of education, etc. All these challenges came in complimentary with the already high infection rates. Kalla et

al. (2020) suggested these challenges can be controlled using technologies, especially using blockchain and smart contracts. Along with blockchain, smart contracts can be used to encode all the terms and conditions between different parties of the data to make sure that the data is not being stolen from an outside party. Furthermore, the use of blockchain technology can be vital when dealing with contract tracing and patient information sharing. Kalla et al. (2020) state that Bluetooth can be used to detect close encounters, and later the data can be retained through a blockchain database where all the user information is protected through pseudonymity. Thus, the data can be shared in a secure manner where the users and patients can have the majority of control over their information without having to be worried about data forging. Authors suggested that due to the high security in transactions and data storing, blockchain technology has the potential to be used in various other areas other than storing healthcare data, however, blockchain technology can be further utilized if it can ensure legal security, privacy, latency, and resource utilization which can hopefully be achieved through further research and improved algorithms.

The study of Marbouh et al. (2020) attempted to review various use cases of blockchain technology for COVID-19 and develop a blockchain-based trusted data tracking system. In this study, authors review various blockchain applications and opportunities in combating the COVID-19 pandemic and develop a tracking system for the COVID-19 data collected from various external sources. Authors propose, implement, and evaluate a blockchain-based system using Ethereum smart contracts and oracles to track reported data related to the number of new cases, deaths, and recovered cases obtained from trusted sources. They also presented a detailed algorithm that captures the interactions between stakeholders in the network and security analysis and the cost incurred by the stakeholders. Finally, the authors claim their work provides economically feasible solution that ensures data integrity, security, transparency, and traceability among its stakeholders.

Blockchain Based Secured Contact Tracing

Blockchain being an emerging field of research is experiencing a lack of research, however, this technology has enormous potential. Information security and privacy are the most important issues that any individual as well as business organizations are facing at present time. Information security and privacy cover potential threats to the privacy of the personal data stored in different organizational databases, unintentional threats to information systems, deliberate threats to information systems as well as what organizations can/should do to protect their information resources and information security controls. Blockchain technology can provide a robust solution in this area.

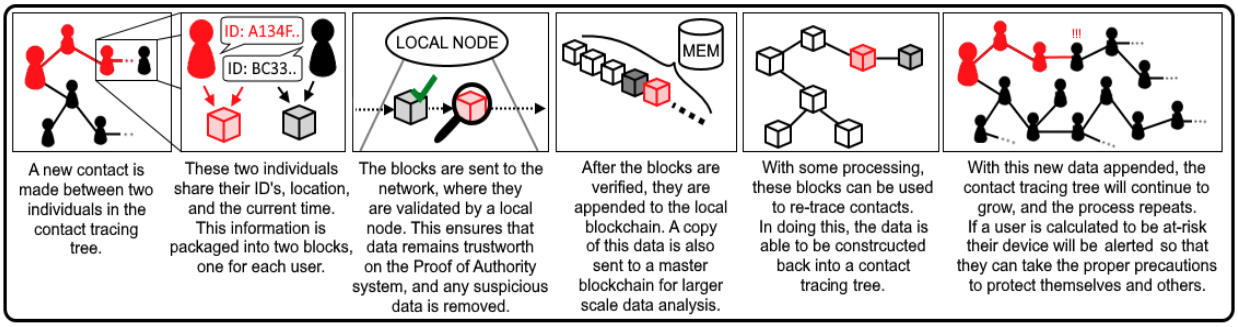
Blockchain has numerous benefits such as decentralization, persistency, anonymity, suitability, etc. and these benefits lead to some of the important blockchain applications such as cryptocurrency, financial services, risk management, internet of things (IoT) (Daneshgar et al., 2019). Because of the above unique characteristics, blockchain technology is becoming an important technology for the next generation of internet interaction systems particularly in smart contracts, public services, IoT, reputation systems, and security services. Working of blockchain technology provides a sequence of blocks, which holds a complete list of transaction records like a conventional public ledger (Chuen, 2015). For maintaining data security through blockchain, one such blockchain-based architecture is utilized for smart vehicles. Inter-connected services in smart vehicles offer sophisticated benefits to all stakeholders involved; however, these services expose the smart vehicles and their users to a range of security and privacy threats such as location tracking or remote hijacking of the vehicle. A study by Dorri et al. (2017) proposes BC-based architecture that protects the privacy of the users of smart vehicles, and increases the security of the vehicular ecosystem. Wireless remote software updates other emerging and relevant services such as dynamic vehicle insurance fees. By relying on the generic characteristics of blockchain technology, the authors qualitatively argue the resilience of their proposed BC-based architecture against common security attacks.

Based on the challenges and issues discussed in the previous section, the biggest concern is how to secure the collected personal information from contact tracing while maintaining users' privacy. We believe any tracking system should not compromise the user privacy, security, and systems performance; hence, we are a big proponent of blockchain-enabled contact tracing that satisfies security, privacy, and performance expectations.

The nature of contact tracing brings challenges to the privacy and security of users' information since it is to be collected, verified, and distributed. Another issue is the identity protection of users. Here, with its inherent feature, blockchain technology can play a neutral role in a distributed manner to protect the identity of the users by desensitizing the users' identification and location information. With its technical design, blockchain technology can provide a solution for privacy protection in a much simpler and better way compared to a centralized system. Additionally, blockchain technology combined with encryption techniques can further protect the user's identity. With the global nature of blockchain, it provides a suitable global access platform for contact tracing and control. Furthermore, the transparency feature of this technology can prevent users from intentional misinformation by external entities.

Blockchain is the technology behind Bitcoin, considered disruptive since many of its attributes have overcome the limitations of a centralized database. It is structured as a chain of blocks linked together using cryptography. Each block contains a complete list of transaction records, a timestamp, and a hash of the previous block, and they are shared by all members in the network (Zheng et al., 2017; Marbouh et al., 2020).). Blockchain is well-known for its decentralized nature. In a centralized system, people place trust in a single record keeper (Abadi & Brunnermeier, 2018) who may misuse their delegation to misreport, modify, or leak users' confidential data to a third party (Nofer et al., 2017). In contrast, with the usage of blockchain, data is distributed through several nodes in the network. Nodes use a consensus algorithm to agree on the truthful state of the data in the blockchain (Mingxiao et al., 2017). Additionally, a decentralized blockchain also eliminates the single point of failure problem posed by the centralization system (Nofer et al., 2017). Blockchain for trustworthy computing is receiving tremendous research interest both in industry and academia for various applications. Powered with this upcoming technology, the proposed solution that will be derived from this study has significant potential for planning and mitigation efforts for COVID-19 and future highly infectious diseases. Figure 1 depicts the functionality of blockchain-based contact tracing.

FIGURE 1
BLOCKCHAIN FUNCTIONAL FLOW DIAGRAM FOR CONTACT TRACING



To address the shortcomings identified from the literature, this study investigates user data privacy concerns towards building a mobile app where data privacy and security have the utmost priority. Based on past studies, it has been observed that blockchain is a viable solution to address these data security and privacy concerns as it ensures that the data is immutable and auditable with the use of advanced cryptographic techniques (Fusco et al., 2020; Kalla et al., 2020; Song et al., 2020). Additionally, there is a lack of concrete understanding of access rights (e.g., read, write, modify, store) and the usability of data amongst the data managers (e.g., admin, public health officials). Therefore, in this study, we conduct a survey analysis in understanding feasibility criteria, especially privacy concerns in developing a mobile app for controlling highly infectious diseases, and based on that we suggest requirement specifications for such an app to automate contract tracing for highly infectious diseases in a secure, maintainable environment. Finally, this study will help us answer the following research questions:

1) What are the users' major privacy concerns about sharing various self-identifying information including geographical location for infection-containment of highly infectious diseases such as COVID-19?
2) What minimum amount of information related to user identity and access rights should be stored in the blockchain for successful contact tracing?
3) What would be an ideal framework for developing such a mobile app?

To get answers to the above research questions we survey with the different stakeholders (users of contact tracing apps, healthcare institutions, public health officials, and information systems administrators) in knowing the data privacy concerns the users have while using such apps. The stakeholders' survey in identifying their willingness to share/store input data in developing a mobile app for highly infectious diseases has helped us develop a requirement specification for the mobile app. The focus of our research is to examine users' data privacy and security concerns while using traditional contact tracing apps and how to provide a completely private and secure contact tracing environment. Thus, this study helps create a strategic roadmap for developing a secured contact tracing platform for highly communicable diseases.

CONTACT TRACING FRAMEWORK DEVELOPMENT METHODOLOGY

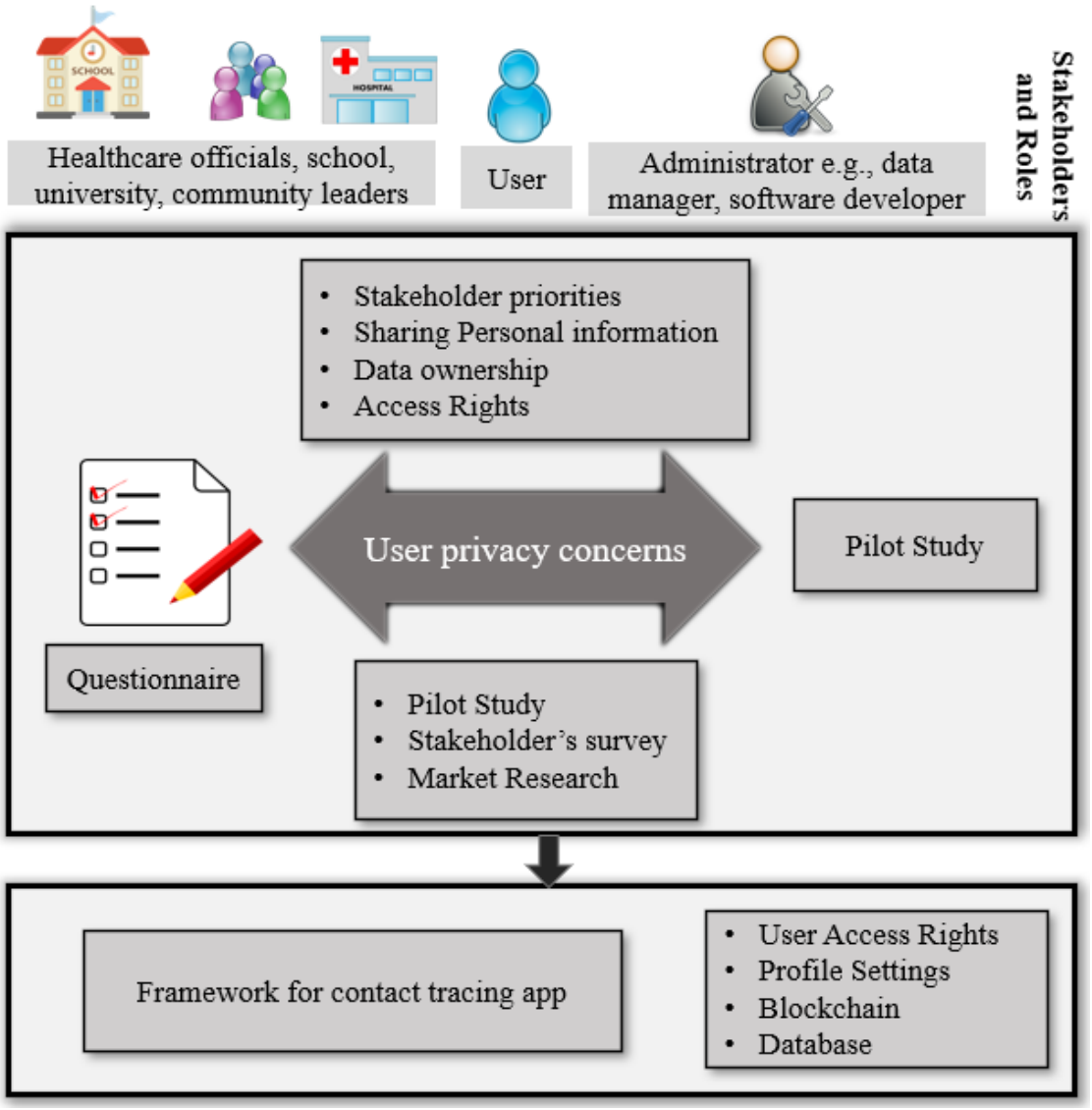
In this section, we provide a detailed workflow description of the framework development process and the methodology adopted for conducting the stakeholders' survey.

Workflow of the Framework Development Process

The preliminary workflow diagram for contact tracing mobile app development has been shown (in Figure 2) and explained below**.**

- Step 1: Need identification through a market study in understanding feasibility criteria, especially privacy concerns for developing a mobile app for highly infectious diseases.
- Step 2: Development of a preliminary questionnaire (pilot study) to collect data on stakeholders' willingness to share/store input data in a mobile app for highly infectious diseases. Based on the pilot study, we will finalize the questionnaire.
- Step 3: To Conduct a stakeholders' survey in identifying willingness to share/store input data in developing a mobile app for highly infectious diseases.
- Step 4: Based on the inputs received from the stakeholders' survey, we develop a framework for a blockchain based mobile app for contact tracing of highly infectious diseases.

FIGURE 2
WORKFLOW DIAGRAM FOR CONTACT TRACING MOBILE APP DEVELOPMENT



Survey Method

This is an exploratory study, and it follows a qualitative research design. semi-structured interviews (SSIs) administered via written questionnaire have been used as a data collection method. The SSI is designed to ascertain subjective responses from respondents regarding a particular situation or phenomenon experienced by them (McIntosh & Morse, 2015). Morse and Field (1995) argued that SSIs are normally used when the respondents have sufficient objective knowledge of the interview topic, but the subjective knowledge is lacking. SSIs are conducted using an interview questionnaire; however, it is important that these questions are open-ended and formulated in such a way that elicit unstructured responses and generate discussion. These questions are typically asked of each interviewee in the same way and order; however, the questions are semi-structured where interviewers are allowed the freedom to diverge slightly from the script (McIntosh & Morse, 2015). Because of this argument, we decided to adopt SSI for data collection. The questionnaire has three parts: in the first part of the questionnaire, we have given a brief introduction and the purpose of this study and we collected some basic demographic information. In the second part of

the questionnaire, we tried to understand the administrator's experience of covid-19, and how they handled it in their workplace. In the third part, they were asked about specific requirements they have for such an app without compromising the privacy and security concerns of the users. In this section open-ended questions like "what personal information do you think the users of such app will be willing to share?" and "How long do you think the data should be retained in the database?" were asked.

We conducted a small-scale pilot test with two professors of an AACSB-accredited business school, two organization executives, and four master students pursuing their MBA from AACSB-accredited business schools to assess the questionnaire's logical consistency, ease of understanding, and contextual relevance. Once we finalize the questionnaire, from the beginning of December 2021, we conducted the SSIs both electronically (video conferencing) and face-to-face. We followed a convenience sampling method based on some pre-decided criteria to choose our respondents. Twelve eminent administrators across the world from different sectors (healthcare, manufacturing, education, government, and information technology) and having more than 15 years of administrative experience were selected to provide expert stakeholder's opinions on specific requirements of the app and plausible data security and privacy concerns. We completed this data collection by the end of March 2022.

RESULTS AND DISCUSSION

Through this study, we desired to provide information to develop a contact tracing app that maintains users' privacy and information security. Although this study is a foundation for developing the app, we need to emphasize the practicality of this approach in helping the app developer to better understand the users' requirements and thereby provide a good requirement specification. To achieve this objective, we conducted an expert stakeholders' survey. Based on the inputs available from the open-ended questions asked to the expert stakeholders through SSIs, the results have been summarized and tabulated below:

TABLE 1
INPUTS ON PAST COVID EXPERIENCE

Questions	Sample responses	Most popular
Q1. Major concerns at the job site	• Making the workplace safe for employees, students, and visitors • Maintaining regular hygiene • Continued service with the same efficiency and productivity as pre-Covid period • Addressing the Fear psychosis of Covid • Employee attendance during lockdown • Prioritizing work schedule with poor employee attendance • Implementing lockdown measures within a short span of time (i.e., 2 weeks)	Providing sufficient verified information about the pandemic situation
Q2. Communication method used	• Emails • Phone calls • WhatsApp group messaging • Video conferencing applications such as Google Meet, Zoom • Microsoft Teams	Telework, videoconferencing

Q3. Technique for keeping track of active infections	• "Aarogya Setu" app • Thermal screening • Minimal concern because of poor employee attendance • Emergency response control room was formed • Weekly reports to keep track of active infections and educate the entire workplace	Weekly report of active infections
Q4. Solutions applied to handle situations at workplace	• Internal survey conducted for gauging severity of problem • Active signage on-campus for information dissemination • Special support to take care of mental health of students • Flexible classes and additional documentation provided to students	Active signage for information dissemination
Q5. Precautionary measures suggested to employees	• Mandatory mask requirement • Sanitizing stations • Multi-step sanitization procedures for disinfection. • Social distances. • Work from home. • Preparing bulletin following government instructions.	Mandatory usage of mask and frequent sanitizing

TABLE 2
SPECIFIC REQUIREMENT FOR APP

Questions	**Sample responses**
Q1. How people will be accessing it	Download from Google play and iPhone App store
Q2. App use - mandatory or volunteer	Mandatory given the gravity of pandemic situation, once the pandemic is under control it should be voluntary
Q3. Application will be mobile based/web based/telephone	Mobile
Q4. What personal information do you think the users of such app will be willing to share?	• Age, health information and past medical complications • Syncing the person's health info with insurance company • Gender and ethnicity of users to understand susceptibility of infection for certain groups • Information about immediate family members to better control the spread of contagions
Q5. (Access to past data) How long data should be retained in the database?	Till the pandemic is under control 3 weeks (typical infection period) Can be retained for future research purpose but privacy should never be compromised

Questions	Sample responses
Q6. Other comments/suggestions	Personal information should be secured and safe Incentivize user for using the app App should work without internet connection or lower bandwidth App should be a part of insurance or vaccine program Active notifications to maintain social distancing or containment zone Avoid false reporting of data such as under- or over-reporting

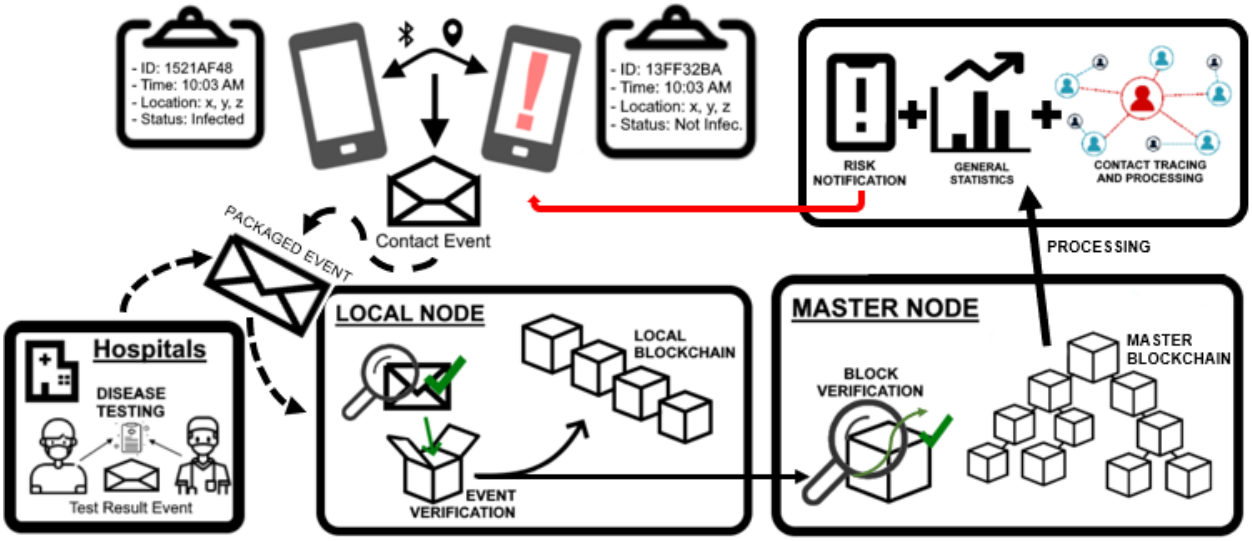
The results show that all the respondents agree that given the pandemic situation, the use of apps should be mandatory till the situation is under control and the app should be accessed through the Google play store or iPhone app store. More than 80% of the respondents are of the view that the app should collect demographic and health information of the users to better understand the vulnerable group of people and thereby provide speedy healthcare facilities to them. 50% of the respondents are of the view that access to past data should be available till the pandemic is under control, 33% of them suggested retaining the users' data for no more than the active infection period of three weeks and the remaining 17% are of the view of retaining these data for future research purposes, however, users' privacy cannot be compromised at any cost and at any point in time. Based on the stakeholders' feedback we propose a framework for a blockchain-based automated contact tracing system in figure 3.

Contact Tracing Framework

Our framework proposes a system that allows the collection and processing of contacts among individuals in real-time and use them to alert any individuals who have a potential risk of getting infected. The entire contact tracing process consists of four main steps from data collection to data processing: a) blockchain creation, b) contact tracing, c) data entry, and d) data viewing. Our very first step is the process of blockchain creation by which we propose to create a specialized and anonymized blockchain distributed among a hierarchy of nodes. This hierarchy is composed of different categories of reporting nodes, and the users who will be using this system, allowing this structure to restrict access to potentially sensitive data from nodes lower in the hierarchy. Our proposed blockchain system is different from a standard blockchain as it is not distributed freely and has flexibility in what types of data can be stored in it. This flexibility allows servers in different areas to collect and interpret external data outside of what is collected under normal operations.

The second component of our system is the contact tracer. A tracer is a module, which is given a timeframe and a set of users or a single user to focus on, which can query its local blockchain for contact events, infection events, and recovery events to portray an accurate representation of the transmission of infection between people within that node's scope. The third component is a data entry website, where authorized medical personnel reports user test results, submitting infection events and recovery events into the blockchain for later processing. The last component is data viewing. This is also done via a website, allowing authorized medical personnel to perform a trace for visualization (risk calculation and timeline visualizer) and view raw, anonymized blockchain data (blockchain viewer).

FIGURE 3
BLOCKCHAIN-BASED AUTOMATED CONTACT TRACING FRAMEWORK



CONCLUSION

Highly infectious diseases such as COVID-19 can be effectively controlled by contact tracing. This process of tracking down and recording several thousand infected persons and their respective contacts for a substantial period is extremely complex and tedious. In addition, there are privacy concerns due to access control issues for personal information. To address these shortcomings, we are proposing a blockchain-based mobile app for managing this contact tracing problem. To understand the organization-specific concerns, we are summarizing our findings from the semi-structured interviews of stakeholders and community leaders and thereby proposing a comprehensive blockchain-based contact tracing framework. This study provides a groundwork for developing the contact tracing app by helping the app developer to better understand the users' requirements. It will also help to develop a preliminary design that can lead us into developing an effective contact tracing mobile app. In the future, we will be developing the backend and frontend components of this contact tracing app that will help in mitigating contagious infectious diseases and thereby saving thousands of human lives.

REFERENCES

Abadi, J., & Brunnermeier, M. (2018). *Blockchain economics* (No. w25407). National Bureau of Economic Research.

Abuhammad, S., Khabour, O.F., & Alzoubi, K.H. (2020). COVID-19 contact-tracing technology: acceptability and ethical issues of use. *Patient Preference and Adherence*, *14*, 1639.

Apple Newsroom. (2020). *Apple and Google partner on COVID-19 contact tracing technology*. Retrieved January 29, 2021, from https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Arifeen, M.M., Al Mamun, A., Kaiser, M.S., & Mahmud, M. (2020). *Blockchain-enable contact tracing for preserving user privacy during COVID-19 outbreak.*

Bay, J., Kek, J., Tan, A., Hau, C.S., Yongquan, L., Tan, J., & Quy, T.A. (2020). *BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders*. Government Technology Agency-Singapore, Tech. Rep.

Centers for Disease Control and Prevention (CDC). (2020). *Interim Guidance on Developing a COVID-19 Case Investigation & Contact Tracing Plan: Overview*. Retrieved October 9, 2021, from https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/overview.html

Currie, D.J., Peng, C.Q., Lyle, D.M., Jameson, B.A., & Frommer, M.S. (2020). Stemming the flow: How much can the Australian smartphone app help to control COVID-19. *Public Health Res Pract*, *30*(2), e3022009.

Dar, A.B., Lone, A.H., Zahoor, S., Khan, A.A., & Naaz, R. (2020). Applicability of mobile contact tracing in fighting pandemic (COVID-19): Issues, challenges and solutions. *Computer Science Review*, 100307.

Exposure Notification. (2020). Apple Inc., Cupertino, CA, USA and Google LLC., Mountain View, CA, USA.

Fusco, A., Dicuonzo, G., Dell'Atti, V., & Tatullo, M. (2020). Blockchain in healthcare: Insights on COVID-19. *International Journal of Environmental Research and Public Health*, *17*(19), 7167.

Gupta, R., Bedi, M., Goyal, P., Wadhera, S., & Verma, V. (2020). Analysis of COVID-19 Tracking Tool in India: Case Study of Aarogya Setu Mobile Application. *Digital Government: Research and Practice*, *1*(4), 1–8.

Idrees, S.M., Nowostawski, M., & Jameel, R. (2021). Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions. *JMIR Medical Informatics*, *9*(2), e25245.

Intersoft Consulting. (2021). *General Data Protection Regulation GDPR*. Retrieved October 8, 2021, from https://gdpr-info.eu/

Johns Hopkins University (JHU). (n.d.). *COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)*. ArcGIS. Retrieved March 3, 2023, from https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

Kalla, A., Hewa, T., Mishra, R.A., Ylianttila, M., & Liyanage, M. (2020). The role of blockchain to fight against COVID-19. *IEEE Engineering Management Review*, *48*(3), 85–96.

Levy, I. (2020). *The Security Behind the NHS Contact Tracing App*. Retrieved May 8, 2021, from https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

Lu, R., Heung, K., Lashkari, A.H., & Ghorbani, A.A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access*, *5*, 3302–3312.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I.A., Debe, M.S., Salah, K., . . . Ellahham, S. (2020). Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. *Arabian Journal for Science and Engineering*, pp. 1–17.

McIntosh, M.J., & Morse, J.M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research*, *2*, 2333393615597674.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, pp. 2567–2572.

Morse, J.M., & Field, P.A. (1995). *Qualitative research methods for health professionals* (No. 610.73072 M6).

Mozur, P., Zhong, R., & Krolik, A. (2020). In coronavirus fight, China gives citizens a color code, with red flags. *The New York Times*, *1*. Retrieved from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187.

Rivest, R.L., Callas, J., Canetti, R., Esvelt, K., Gillmor, D.K., Kalai, Y.T., . . . Zissman, M. (2020). *The PACT protocol specification*. Private Automated Contact Tracing Team, MIT, Cambridge, MA, USA, Tech. Rep. 0.1.

Song, J., Gu, T., Feng, X., Ge, Y., & Mohapatra, P. (2020). Blockchain meets COVID-19: A framework for contact information sharing and risk notification system. *arXiv preprint arXiv:2007.10529*.

Team, P.P. (2020). *Pan-European Privacy-Preserving Proximity Tracing*. Retrieved from https://www.pepp-pt.org/content

WeCare. (n.d.). *We care world covid 19 tracing*. Retrieved February 19, 2021, from https://we-care.world/

WHO. (n.d.). *"WHO Director-General's opening remarks at the media briefing on COVID-19—11 Mar. 2020,"* Retrieved January 29, 2021, from https://www.who.int/dg/speeches/detail/who-director-general-s-opening-r emarks-at-the-media-briefing-on-covid-19—11-march-2020.

Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W.J., & Imran, M.A. (2020). Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond. *IEEE Internet of Things Journal*, *8*(5), 3915–3929.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564.