**Faculty of Computing and Technology**
**University of Kelaniya**

## CSCI 23072 Group project

## Final Report

# Blockchain based COVID-19 Contact Tracking System

This final report was submitted in partial fulfilment of the requirements of the above module in the B.Sc. (Hons) in Computer Science degree

Under the supervision of

Dr. Rajitha Tennekoon
Senior Lecturer
Department of Computer Systems Engineering

in

July 2022

Group 02

1. CS/2018/014 – Gunarathne A.D.D.
2. CS/2018/021 – Kavinda K.B.
3. CS/2018/030 – Niroshanan S.
4. CS/2018/036 – Rupasinghe W.A.I.M.
5. CS/2018/044 – Thilakarathne D.G.S.P.

# Abstract

The COVID-19 pandemic has caused significant disruption worldwide, affecting more than 574 million people at the end of July 2022. One of the best ways to combat this is to minimize transmission. Digital contact tracing is an effective technique that can be used for this purpose as it eliminates the manual contact tracing process and could help in identifying and isolating data subjects. However, users are reluctant to share their location and contact details due to concerns about the privacy and security of their personal information, impacting implementation and widespread adoption. Blockchain technology has been used in various fields and has proven to be an effective approach to securely handling data transactions, making it an ideal choice for digital contact tracing apps. Blockchain properties such as timestamps and data immutability can facilitate transparent retrieval of accurate virus trace information, while data encryption ensures the integrity of the information provided. Additionally, the anonymity of the user's identity mitigates some of the risks associated with privacy and confidentiality concerns. This report provides a detailed discussion of the blockchain-based digital contact tracing mobile app called "CovidTrack". Additionally, this report introduces the potential challenges related to other available contact tracing apps and describes how this app overcomes these challenges by using a blockchain-based decentralized network.

## Acknowledgements

We would like to express our deepest appreciation to Dr. Chamli Purshpakumara and Ms. Malsha Mahawatta for their contribution in stimulating suggestions and continuous encouragement to go through this project. Furthermore, we would also like to acknowledge with much appreciation to our supervisor Dr. Rajitha Tennekoon who has invested his full effort in guiding the team in achieving the goal. We must appreciate the guidance given by him also, thanks to all our colleagues and parents for their support of them to make this project successful.

# Table of Contents

# List of Figures

# List of Tables

# 1 Introduction

## 1.1 Motivation for carrying out the project

SARS-CoV-2, known as COVID-19 was unknown before it spread in Wuhan, China in late 2019. The infection started with 27 people in Wuhan and has now grown to more than 574 million people worldwide. Within a month of the initial outbreak, COVID-19 was declared a global health emergency by the World Health Organization (WHO). This is usually transmitted from infected people to healthy people through physical and close contact. Infected people can be symptomatic or asymptomatic, but both types of patients can transmit the virus. Therefore, the only way to control the spread is to keep infected people isolated for 14 days. Therefore, everyone must follow some simple practices every day, such as avoiding gatherings, maintaining social distance, washing hands, using hand sanitizer, and wearing masks and gloves when going out.

To overcome this virus, governments around the world are taking various measures to avoid social contact between people and minimize the spread. Full lockdowns have been imposed in several countries, sealing off national and international borders, closing schools and universities, asking employees to continue working from home, closing malls and markets, suspending gatherings and events, etc. All of these efforts are being made to limit human contact as much as possible. Nonetheless, the impact of these measures on the economy has raised global concerns, making it important to strike a balance between preventive mechanisms and economic activity. Healthcare organizations around the world manually track people who may have been in contact with COVID-19-positive individuals, but this process is time-consuming, error-prone, and inefficient. Therefore, a digital contact tracing system is required to identify, assess and manage the people that have been exposed to COVID-19 infected patients to prevent the spread of the virus and break the chain.

Digital contact tracing is a mechanism that uses the concepts of technology as a data-gathering tool to identify contacts and prevent transmission. However, contact tracing means continuous monitoring of data such as personal details and whereabouts of users and infected patients, creating a sense of fear in society that their movements will be tracked and transmitted to the app managers. Additionally, protecting the data of individuals becomes an issue in a pandemic situation as people become unsure of how the government will use this collected information.

Hence, this is a global problem and there isn`t any clear solution for this matter, the team wanted to take this challenge and help the world to overcome this problem. Therefore, the application has

been developed as a mobile application that is based on blockchain to trace people. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a network [7]. There are some great properties in blockchain technology such as timestamps and data immutability which can facilitate transparent retrieval of accurate virus trace information, also data encryption ensures the integrity of the information provided. Additionally, the anonymity of the user's identity mitigates the risks associated with privacy and confidentiality concerns. This report demonstrates how the team developed the blockchain-based contact tracking mobile app and how the team has overcome the issues and challenges that impose on society.

## 1.2 Project Objectives

Develop a blockchain-based contact tracking mobile app, focusing more on user privacy and security.

## 1.3 Scope of The Project

**Scope description**

The blockchain-based COVID-19 contact tracking app will have the following features. The app should be accessible by all modern android phones. Users should be able to log in or register to the system and provide the necessary details. The system should have a self-assessment survey to identify the risk level of the user for COVID-19. The system should track users and need to protect user privacy. The system should be able to generate reports and notify the user if the user has contact with an infected person.

**Deliverables**

- Project proposal presentation
- Functional and nonfunctional requirements
- Interim report
- Final report

**Constraints**

- The app should be released by the end of August 2022
- Time/ resources/ personal limitations

**Assumptions**

- Team members have all the required skills
- Team members have all the required resources.

## 1.4 Limitations

- Limited resources access
- Lack of knowledge in blockchain and android technologies
- The app is only available in English
- Only developed for android devices.

# 2 Background

## 2.1 Wider context of the problem

Contact tracing is a mechanism for identifying infected individuals, tracking others who may have been in contact with them, and gathering relevant information about those contacts to take timely action to minimize the spread of contagious diseases. Traditional contact tracing has historically been used to stem the spread of several communicable diseases. This is based on tracking people for days or weeks. Traditionally, these details were kept on paper, and those at risk of infection were notified by mail or phone call. This is a tedious and error-prone method that requires too much work. Over time, digital solutions to contact tracing are explored. Digital contact tracing is a mechanism that can track these details through cell phones, which can be used to identify people who may have been in contact with an infected patient. According to WHO, there are three steps in the contact tracing mechanism

- Contact Identification: If a person is diagnosed with a communicable viral disease, their contacts will be identified by asking about the routine and activities of the infected person. These contacts can be anyone who has meet the patient, such as family members, friends, colleagues, or healthcare professionals.

- Contact list: After determining the people who have been in contact with the infected person in the last few days, a list of these contacts is created. These contacts are then briefed on the situation and guided on the procedures to follow if they develop any symptoms. Contacts are also advised to remain in isolation or quarantine if necessary

- Follow-up of contacts: Periodic and regular follow-ups of contacts are mandatory as they help in the timely monitoring of health symptoms and test results and prevent further spread of the disease.

Digital contact tracing introduces certain issues and challenges related to the privacy and security

of users' personal information. As users' information is collected, tracked, counted, and sent to the network, it is necessary to maintain confidentiality and prevent disclosure of the user's identity. Also, need assurances to users that only data relevant to tracking the spread of COVID-19 is collected and nothing else. Several apps have been developed as a solution for dealing with the COVID-19 pandemic via contact tracing. However, all these apps face the same issues related to the security and privacy of user data. Most have their central server that stores and manages data, which creates vulnerabilities such as data theft, data tampering, data leakage, single point of failure, etc. Furthermore, these apps do not offer any verification mechanism to ensure whether a specific person is infected or not, due to the possibility that a malicious user inserts fake information into the app to cause panic among other users, causing issues related to trust and reliability of the app. In addition, the personal data collected by the apps remains the main concern of the app users. Since these apps are constantly collecting user information for contact tracing, user data privacy and security is still the biggest issue and needs to be addressed. People are hesitant in sharing their information, as they are not sure how their data will be used, who is going to be in charge of their data, and for how long.

Contact tracing apps must gather data in compliance with the General Data Protection Regulation (GDPR). In terms of health care data, the GDPR requires more protection, in the context of digital contact tracing apps, the wireless technology and app managers receive the data along with user identifiers, making it their responsibility to keep the data anonymous. All the strategies for contact tracing available today employ one simple and common mechanism that tracks the movement of the carrier of the virus and does not protect the privacy of users. Therefore, the people who have been diagnosed with the disease are afraid of losing confidentiality since details about their location are broadcasted publicly. Although the actual identity of the individual is not disclosed, they can be mapped easily due to the limited number of carriers on the same route. Once identified, people can start making speculations about their personal lives, develop incorrect perceptions, or generate rumors.

Apart from privacy issues, digital contact tracking systems can be compromised by malicious attacks such as:

- Trolling attacks: The attacker spreads false information to create panic among users, leads them to run diagnostic tests, and leads to a loss of trust in the system

- Blue-Jacking attacks: Attacker make use of Bluetooth and sends spam messages to other devices that have their Bluetooth turned on
- Blue-Bugging attacks: Attacker tries to gain unauthorized access to a device and attempts to give commands
- Spoofing attacks: Attackers make use of GPS signals near a mobile device and transmit incorrect location data that affect the tracing system and results.
- Backend impersonation attacks: Attacker replacing their identity with someone else's identity. Then false information is broadcasted to other devices within the network.
- Deanonymization attacks: Disrupt the privacy of users.
- Ransomware: Attacker develops fake contact tracing apps to gain information and data of users through their phones.
- Jamming attacks: Specific to GPS-based contact tracing systems. Prevents genuine signals from being received by users. Disrupt tracking via GPS signals.

Above, the report discussed the problems which people face when using contact tracing systems. Apart from them, there are some other matters which directly affect the accuracy of the system, such as:

- Data quality: COVID-19 generates considerable amounts of data such as information on infected people, hospitalization and death rates, transmission details, etc. However, it is necessary to analyze this data to gain insights and make better and more efficient decisions because fighting against the spread of COVID-19 depends on these decisions and the research conducted. Therefore, it is important that the data analyzed is accurate and the quality of the data is assured. It must consist of metadata and context to avoid misperceptions or discrepancies as lives are at stake.
- Lack of medical understanding: COVID-19 is a highly communicable disease that can also spread through the air, rather than by physical contact. This makes tracking difficult as a person can become infected without even physically contacted with an infected person. Another issue complicating the implementation of contact tracing is that scientific data on COVID-19 varies. For example, one patient has difficulty breathing and dies, while others

have no symptoms but turn out to be COVID-19 positive. In addition, asymptomatic and pre-symptomatic patients can also infect people, making it difficult to trace the source of contamination.

- Availability of testing: The efficiency and accuracy of contact tracing depend on the scope of testing. Currently, the government is only testing people who have had past contact with an infected person or have symptoms related to COVID-19. In addition, the fees for the diagnostic tests are very high, making it difficult for people in poor areas to get themselves tested.
- Technical Inefficiencies: Digital contact tracing techniques such as GPS tracking and Bluetooth have certain issues in terms of surveillance, malicious users, snoopers, etc. The problem with Bluetooth is it depends on the strength of the signal, which becomes weak when there are any obstacles in between. This makes it less effective. Although GPS has been used to get users' location details, it is not very secure and efficient because it is easy for malicious attackers to create false information on GPS networks.

## 2.2 Review

As the report discussed the biggest issue in contact tracing is how to guarantee user privacy and security. To overcome this issue blockchain technology can be used in the system. This technology can play an important role in contact tracing as it supports distributed peer-to-peer connectivity of network nodes, bridging the gap between users and the app. The technical features offered by blockchain allow the exchange of information while preserving the privacy of users. Table 1 provides a brief description of how the standard properties provided by blockchain technology can be used for contact tracing apps.

Table 1: Features of blockchain technology

| Feature | Application |
|---|---|
| Decentralized network | The management of the data is user centric, which gives the power of data ownership to the users |
| Data security | The data within the blockchain is kept after applying encryption, which can only be decrypted by an authorized user |
| Data provenance | The information being entered in the blockchain is stamped with the digital signature of the source, which proves the legitimacy of the source as well as the data |

| Feature | Application |
|---|---|
| Data availability | The data are distributed among all the nodes within the network, which makes them available all the time to every user |
| Data immutability | The information in the blockchain is immutable, which means once a detail is entered it can never be modified. This provides reliability and transparency to all users |
| Time stamping | The data within the blockchain network is time stamped, which eliminates the chances of discrepancies being present |

To provide effective tracing without compromising users' identity and privacy, and to securely share the data for decision-making is difficult in a centralized network due to the risks of data manipulation. This could be handled in blockchain-based systems since the network is distributed and users' identities are anonymized, to begin with. With decentralized techniques, the details are only stored on the user's device, giving users both power and control over their personal information. Analysis and processing of contact tracing data also occur on the user's device, promoting transparency, privacy, and user consent. Aside from maintaining users' privacy, the app should also be effective in terms of contact tracing, network coverage, infection protection, and so on. A blockchain-based decentralized network can provide accessibility and traceability on a global scale, connecting larger numbers of users from different geographic locations without compromising their privacy. In addition, the information shared on the blockchain can be collected by any technology means (Bluetooth, GPS, etc.) and enable better and richer interactions. Also, the blockchain network would be the best option for overcoming the spreading of false information and rumors as it allows for transparent contact tracing while maintaining verifiable privacy. In addition, data confidentiality should be maintained for the entire life cycle of the data from its creation to its disposal, which is typically 14 days in the case of COVID-19. Blockchain technology gives users full control over managing their data from start to finish, allowing them to share and withdraw their data at any time.

**Existing Digital Contact Tracing Solutions for COVID-19**

Recently, several apps have been developed to deal effectively with the COVID-19 pandemic. These apps help healthcare workers and the public gain insight into the situation to make appropriate decisions. Some of these apps are discussed below.

**Trace Together**

- TraceTogether is an app developed based on the BlueTrace protocol that utilizes Bluetooth low energy [BLE] technology to find out and record the proximity details of users [1]. To run this

app, users need to keep their phones in the active state, which always allows for the broadcasting of their location. Also, this app operates a centralized network.

**COVID Trace**

- Developed by Apple and Google, the Bluetooth technology-based app collects only necessary data like location concerning time and does not keep any recognizable user data thereby keeping the data anonymous (Google/Apple, 2020). If two individuals stay near one another for more than 10 minutes, tokens are exchanged and stored in the app. Whenever a person is diagnosed with COVID-19, this information is shared with the app server. These generated tokens are only shared with the public database with the permission of the user. This app keeps the users' location records for the past 3 weeks. App managers are responsible for the anonymization of user location while uploading. Moreover, the exact time is not disclosed and is rounded off for privacy reasons. The presence or absence of the disease is not verified. However, the user is required to use their central server for contact matching and notification.

**Health Code System**

- The health code system is contrasting from the above methods, as it does not use Bluetooth nor proximity detection. It is based on relational cross-match by scanning the QR code, which is associated with the user. In this system, user privacy is not respected due to centralization, and theidentity of the user is not hidden to the authority. However, the health code is only scanned at thetime of passing checkpoints, hence saves the user battery and does not consume data (Xu et al., 2020).

**ViruSafe**

- ViruSafe is based on GPS location sharing to enable institutions to act accordingly in caseof an emergency (Martin et al., 2020). The app has a location tracker based on GPS coordinates, enabled voluntarily by the user, to create a heat map with potentially infected people. The users can also share any chronic diseases they may have. Additionally, the app can notify users under quarantine when the quarantine period is over. The data are collected in a central registry. All collected data are accessible by the Ministry of Health.

Table 2: Comparison of Existing Contact Tracing Solution

| Name of the Solution | Positioning Technology | Power Usage | Security of Technology | Privacy Preserving |
|---|---|---|---|---|
| TraceTogether | Bluetooth | High | Low | No |
| Google/Apple Covid Tracing | Bluetooth | High | Low | Yes, partially |
| Health Code System | QR code | Low | Medium | No |
| ViruSafe | GPS | High | Low | No |

Table 2 shows the comparison of the existing contact tracing solutions. Above apps vary in the way of contact tracing positioning technology. Some of the apps use GPS and QR codes to track the user's movement, while others use Bluetooth to identify close contacts. Some governments have mandated the use of their apps, while others encourage voluntary adoption. Most apps are using a centralized database to store data. Hence, anyone who has access to the database can manipulate these data. Therefore, People are hesitant in sharing their information, as they are not sure how their data will be used, who is going to oversee their data, and for how long. Also, most apps use Bluetooth or GPS and track every step and location of the user, and because of this users' privacy was interrupted. Another common matter indicates in other apps is that they always rely on the COVID-19 test results. Therefore, users who haven't tested themselves cannot go forward through these apps.

## 2.3 Methods or tools that could be used

### Android Studio IDE for application development

There are a lot of methods to create mobile applications in the present world. Since the team is going to build only an android application the most popular and oldest method. In research, there are lots of materials to follow about the android studio, and it is a great IDE to start android programming. Android Studio contains lots of new and cool features and directly supports the

google environment because of that integrating google services through it will be very easy. Android Studio is based on IntelliJ IDEA so it provides a very fluid and very convenient coding experience to the developer. And it consists of all the tools which need to build an application, So Android Studio is a very great IDE for android developers.

**Java programming language is used for interim codes in android studio**

The IDE is supported mainly by two programming languages one is Kotlin and the other is Java. Since Java is one of the most popular object-oriented High-level programming languages at present, this is the language that will use in the project.

**GitHub**

Since this is a group project which going on for a certain time, project revision management is a necessity. Therefore, the team used GitHub to achieve the project revisioning and sharing.

**Google Firebase Database**

Google Firebase Database will be used as one of the databases in the application. It used to store user information and generates reports.

**Web3j**

Web3j is a lightweight, highly modular, reactive, type-safe Java and Android library for working with Smart Contracts and integrating with clients (nodes) on the Ethereum network. This allows you to work with the Ethereum blockchain, without the additional overhead of having to write your integration code for the platform.

**Solidity Command Line Interface (Solc)**

Solidity is an object-oriented programming language for writing smart contracts. Solc is the command line compiler that use to generate contract binary and ABI.

**Bluetooth**

The Android platform includes support for the Bluetooth network stack, which allows a device to wirelessly exchange data with other Bluetooth devices. The app framework provides access to Bluetooth functionality through Bluetooth APIs. These APIs let apps connect to other Bluetooth devices, enabling point-to-point and multipoint wireless features.

**Blockchain**

In the blockchain technology, each transaction is verified by the majority of participants of the system. It contains every single record of each transaction. There is no Central Server or System

which keeps the data of Blockchain [3]. The data is distributed over Millions of Computers around the world which are connected with the Blockchain.

# 3 Design

## Overall design proposed

### Proposed Design

COVID-19 is a deadly communicable disease and by using a contact tracing mechanism government can minimize the spread of this disease. Therefore, the team decided to develop a blockhead base COVID-19 contact tracking app to help the government in this cause. Below describes the design of the full app.

When a user starts the app, the user needs to provide Bluetooth and location permissions to continue the app. Once they provide both location and Bluetooth permissions app will direct them to a login page. Here registered users can access their existing profiles, while new users need to register to the app. When a new user registers the details of the user will add to the firebase database. These details will use to generate reports and login purposes. When the user is registered or logged in, they have to go through a self-assessment. According to the user entered answers, the system will automatically generate a COVID-19 risk level for the user. There are 5 risk levels such as negative, low risk, moderate risk, high risk, and positive. If the user's risk level is moderate, high, or positive then the system will display corresponding isolation protocols for each level of the risk. Then the user directs to the home interface. Users can update their health status at any time from the home interface.

In the home interface, using Bluetooth technology the app will automatically scan and find close contact IDs every 15 minutes. Then the app will store those IDs in the local storage. Once an ID is entered into the local storage it will automatically delete after 14 days. According to generated user health status, only the positive and negative user`s health status and phone number into the blockchain. At the end of each day, the app takes a positive user list from the blockchain and compares it with the close contact list from local storage. When comparing, if the app finds a match, it will automatically identify the user as close contact and inform the necessary quarantine protocols. Additionally, from the home interface users can generate some reports about COVID-19.

Figure 1 illustrates the app framework.

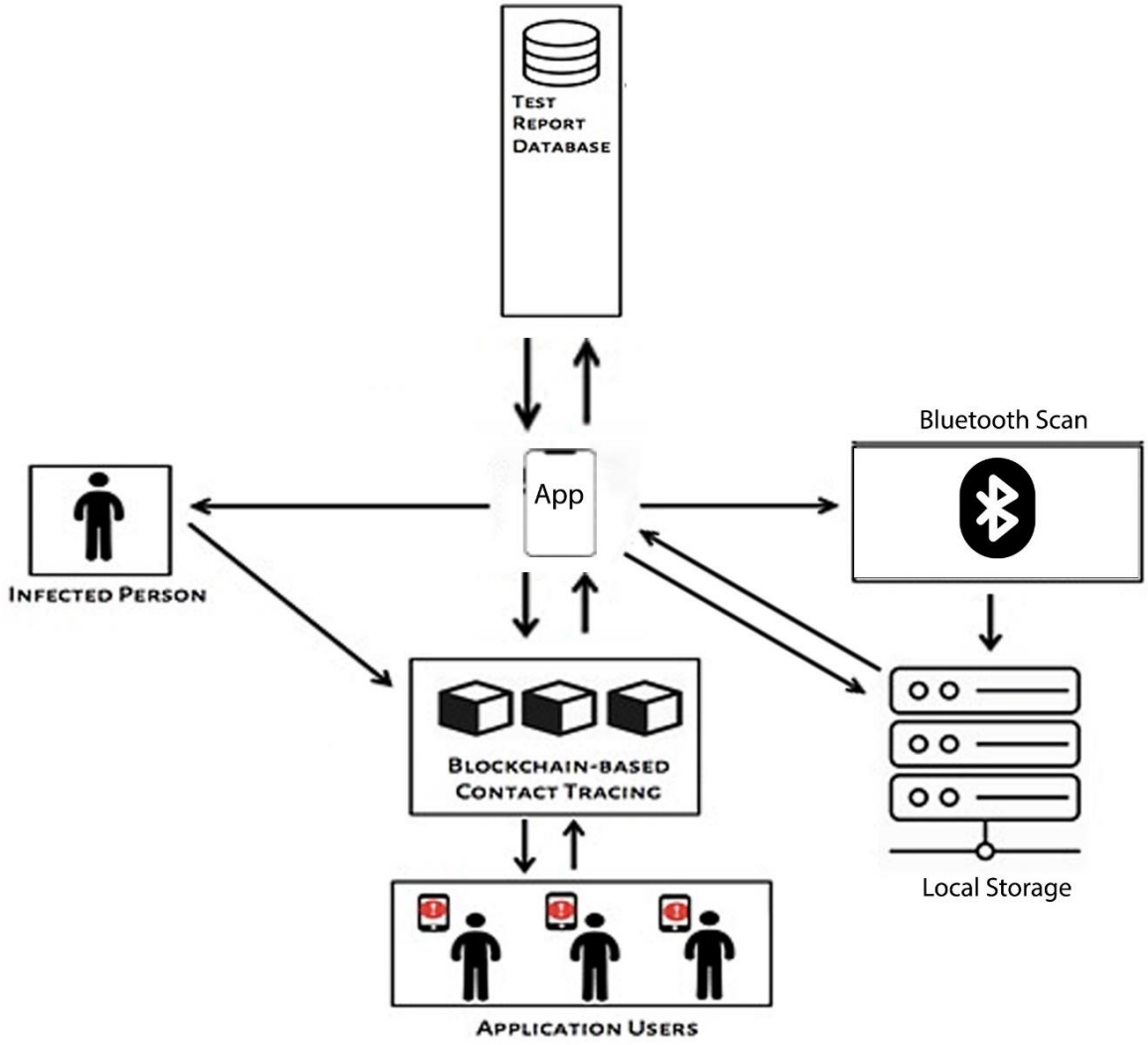


Figure 1 App Framework

**Use Case**

Figure 2 illustrates a use case of close contact scenario. When two users contact each other, the apps will automatically scan and exchange the Bluetooth mac IDs, then those exchanged IDs were stored inside their local storage. In figure 2, the blue user will store the yellow user's ID in his local storage and the yellow user will store the blue user's ID in her local storage. Those IDs in local storage will automatically be deleted after 14 days. After a few days, the blue user tested positive for COVID-19. Then he updates the self-assessment and marks himself as a positive patient. Then the app will send the blue user's health status and phone number into the blockchain. Once this is added to the blockchain, the yellow users` app will fetch a positive ID list from the blockchain into

her app and compare it with local storage IDs. If the app finds a match, will immediately consider the user as close contact and provide the necessary quarantine protocol instructions that she should follow for the next 2 weeks. Here the yellow user has contacted with blue user a few days ago. So her local storage has the ID of a blue user. Therefore, when comparing the local storage with the blockchain yellow user finds that she has had close contact with a positive patient.

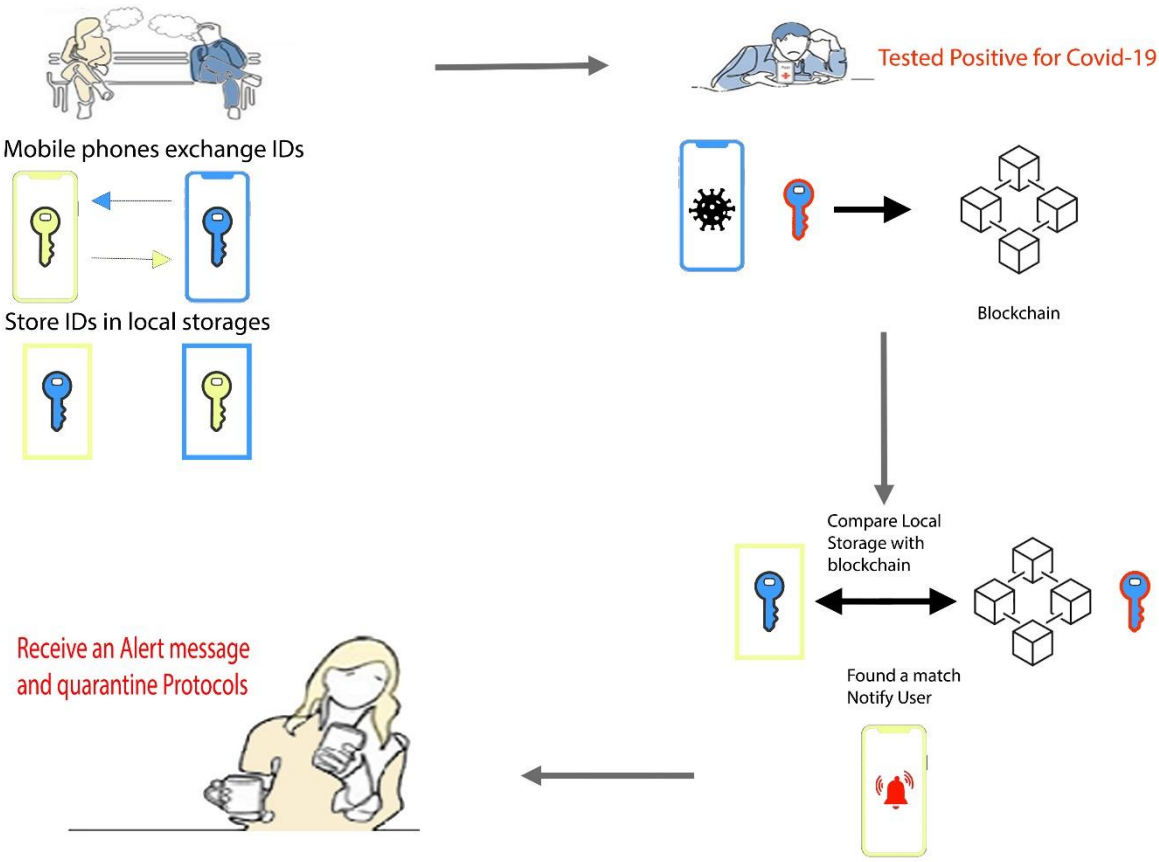


Figure 2: Use case of close contact scenario

**Diagrams**

Class diagrams are the blueprints of the system or subsystem. This project use class diagrams to model the objects that make up the system, show the relationships between the objects, and describe what those objects do and the services they provide**.** class diagram helps to understand the requirements of the project problem domain and identify its components. Figure 3 shows the system class diagram without attributes and methods.

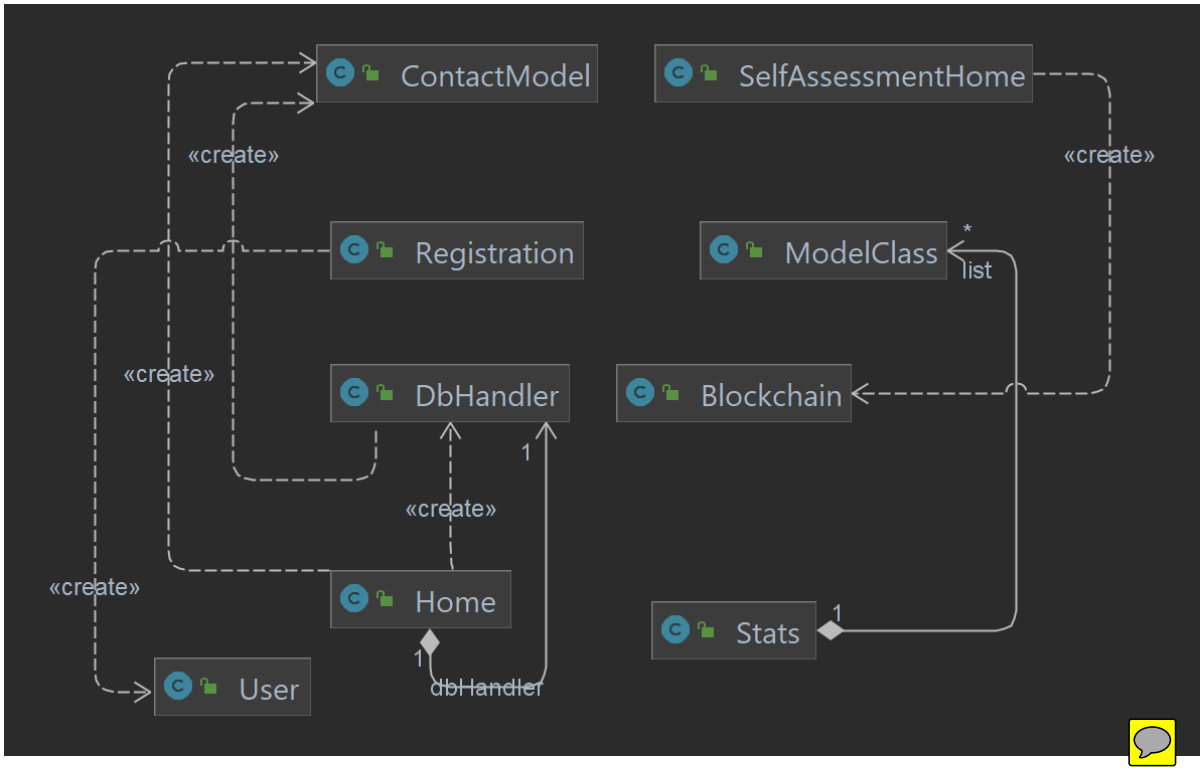


Figure 3: Class diagram without attributes and methods

Activity diagrams visually presents a series of actions in the system. These diagrams help both users and developers to come together and understand the same process and behavior. Below figure 4 and figure 5 shows the activity diagram of the login and registration.

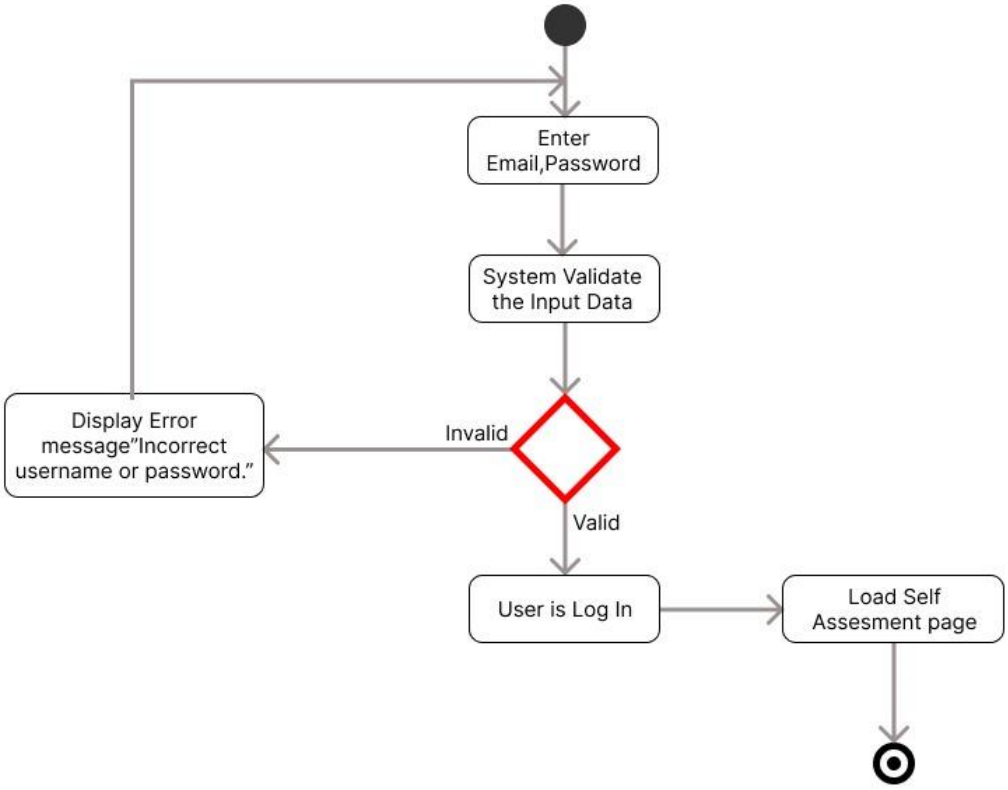


Figure 4: Activity diagram for login

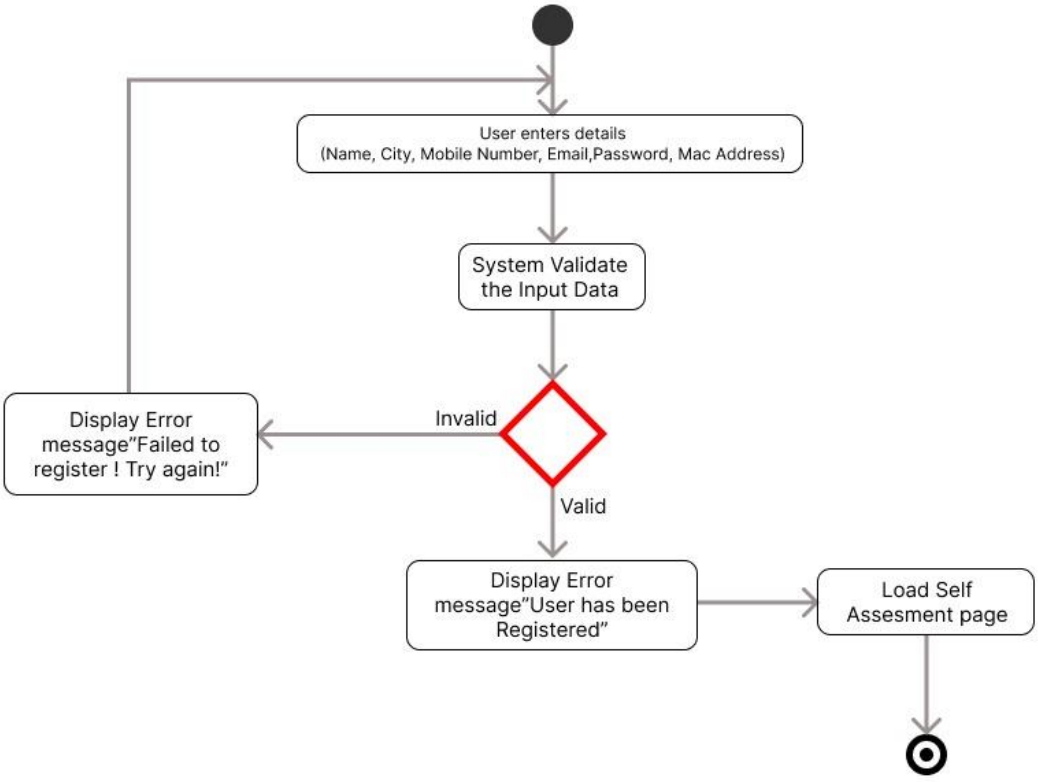


Figure 5: Activity diagram for registration

**Unique Features**

Digital contact tracing is a mechanism that uses the concepts of technology as a data gathering tool to identify contacts and prevent transmission. However, often mobile apps are used as the tool for digital contact tracing. A major benefit of using contact tracing apps is speed. Traditional contact tracing can be time-consuming, but an app has the potential to quickly notify contacts after a positive test result. There are several methods that can be used for tracking via mobile apps:

- Bluetooth
- Location-based
- Quick Response codes

From these methods, the team has decided to use Bluetooth technology because it is one of the common approaches used by contact tracing apps to uncover people who may have been around infected people. Most systems use Bluetooth or GPS for contact tracking and track every step of the user, because of this users' privacy was interrupted. But this project, the Bluetooth-based approach does not store users' location or data. They only notify the contacts of infected people with minimal intrusion into the user's privacy. This gives user the privacy they need and automatically helps them to protect from COVID-19. And also, when comparing with QR code method, Bluetooth is much easier for the users to use and handle, so it will help to improve the user experience.

Also, most of the available systems for contact tracing are using centralized techniques to store, analysis and store data. Therefore, anyone who has access to the database can manipulate these data. People are hesitant in sharing their information, as they are not sure how their data will be used, who is going to be in charge of their data, and for how long. To address this problem, the team decided to use decentralized techniques. Therefore, the analysis and processing of the data for tracking contacts are done on the user's device, which promotes transparency, privacy, and user consent. Figure 6 shows the difference between centralized and decentralized setups when work with digital contact tracing.

.

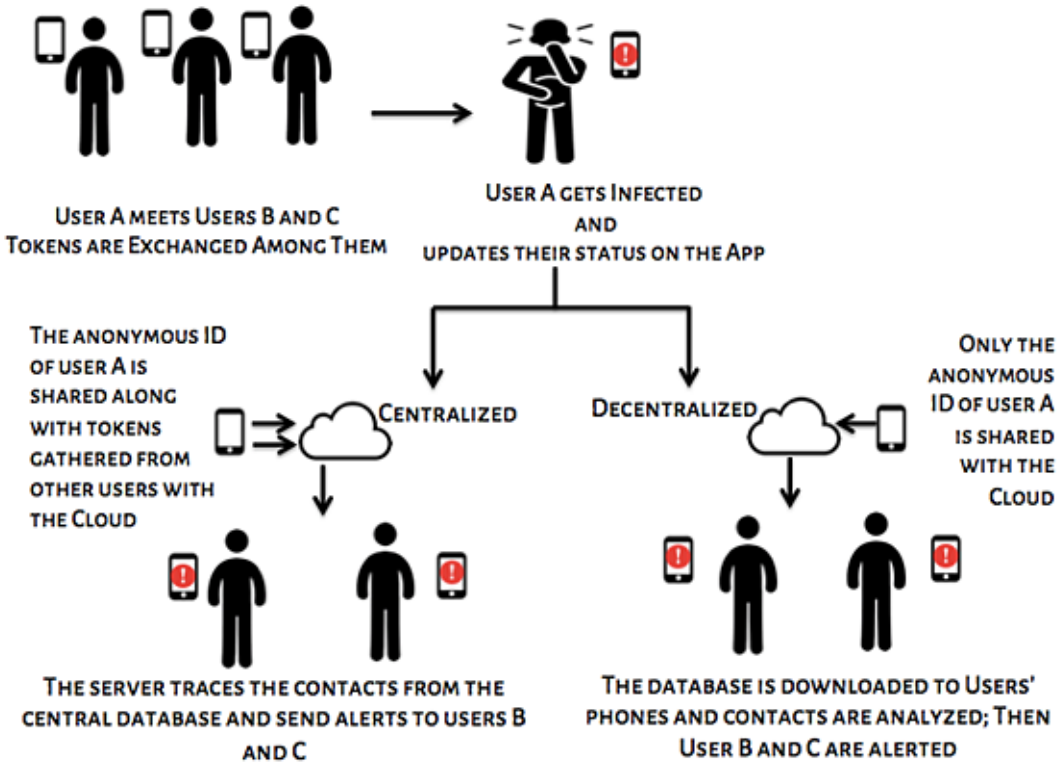


Figure 6: Digital contact tracing mechanism

From this project, the team has answered another common problem that presents in other apps. Most other apps, only rely on the COVID-19 test results. So people who haven't tested themselves in COVID-19 tests, cannot go forward through the app. Therefore, the team decided to include a self-assessment phase that every user must have to go through. From this assessment, application generate the COVID-19 risk level of each user according to the answers they made. These risk levels are generated according to the WHO standards. Also, this project will generate some important reports and provide that information back to the user in understandable ways.

# 4 Implementation

## 4.1 Technologies Used

The team developed an android application to track COVID-19 patients with Blockchain-based. Mobile phone is the most common device in society, so the best solution for detect patients build a contact tracing system with Bluetooth.

**Android Studio IDE & Google Firebase**

The development process is done through the Android Studio IDE with java (Gradle). The local database is built through Google Firebase. Registration details like full name, address, email, etc are added to the firebase. As a Real-time application, firebase is the better solution to store synchronized data. The application stores user's self-assessment data for 14 days and then generate instructions for high-risk and positive patients on how they should maintain their health and inform the application of their health status after 14 days again.

**Bluetooth**

The responsibility of the tracking part is fulfilled by the Bluetooth network. The application identifies nearby devices through this system. While the application running, it asked permission to enable the Bluetooth setting in your device, because a continuous Bluetooth network needs for the tracking process. The scanning process is happening in every 15 minutes. Also, the user must insert a Bluetooth mac address during the registration process.

The contact tracing concept in the project helped to identify infected people by tracking them with the real-time application. The important thing is application could give a list of close contacts who are identified in the Bluetooth network.

**Web3j**

The actual purpose of the application is to reduce the spread of COVID-19 by informing them that if they have any close contact with a COVID-19 positive patient, for that the team has to get information about the users. Then the team has to build a platform to inform each user can see if there was any close contact or any risk from a positive patient. As a better solution the team used the Blockchain platform to protect client privacy and make a distributed database for users. Basic blockchain coded with solidity language. Web3j (version 4.8.7) is the library that the team used for Ethereum support.

**Rinkeby**

Rinkeby FAUCET is the test network that the team used for the Ethereum blockchain. The Infura API suite provides instant access over HTTPS and WebSockets to the Ethereum. The team has to download MetaMask as a google chrome extension for Ethereum wallet. Through that Application could give higher privacy for users' details. Users can get the current update on their health status. The application can decide whether a user is in a high-risk or low-risk situation, then he or she can decide to quarantine or not. If someone got a positive or high-risk patient his or her mobile number and health status are stored in the blockchain, then after 14 days the application compares local

storage and the blockchain.

## 4.2 User Interface Design

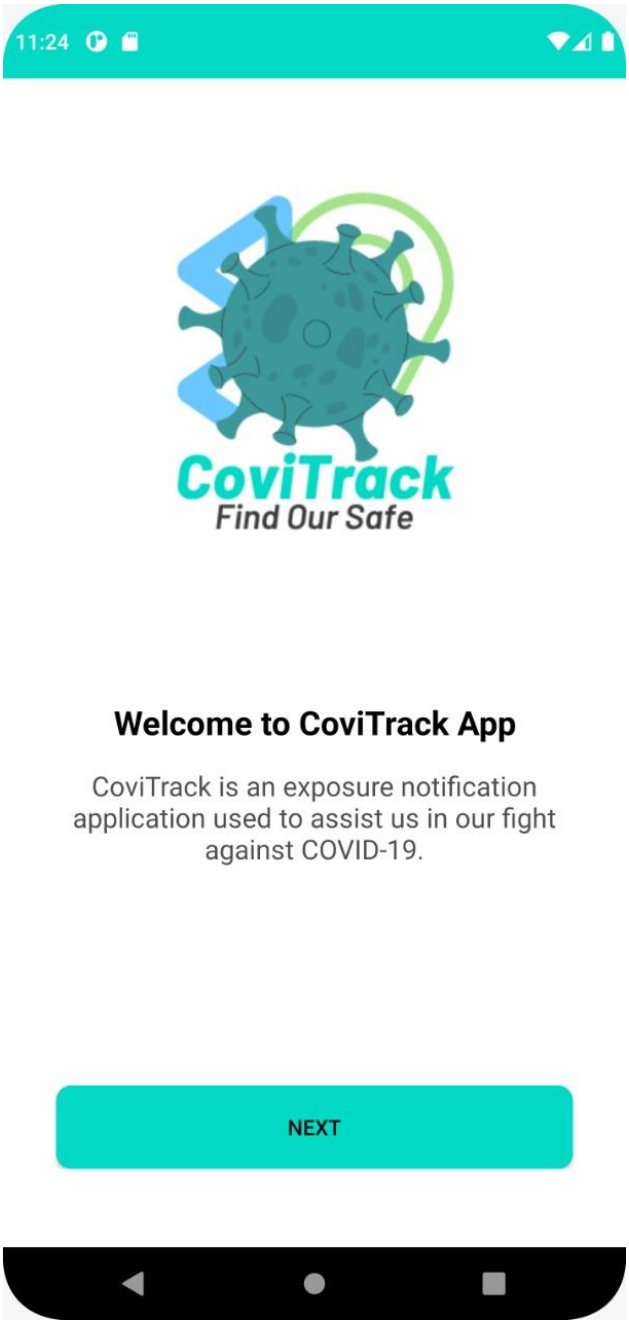


Figure 7: Start UI

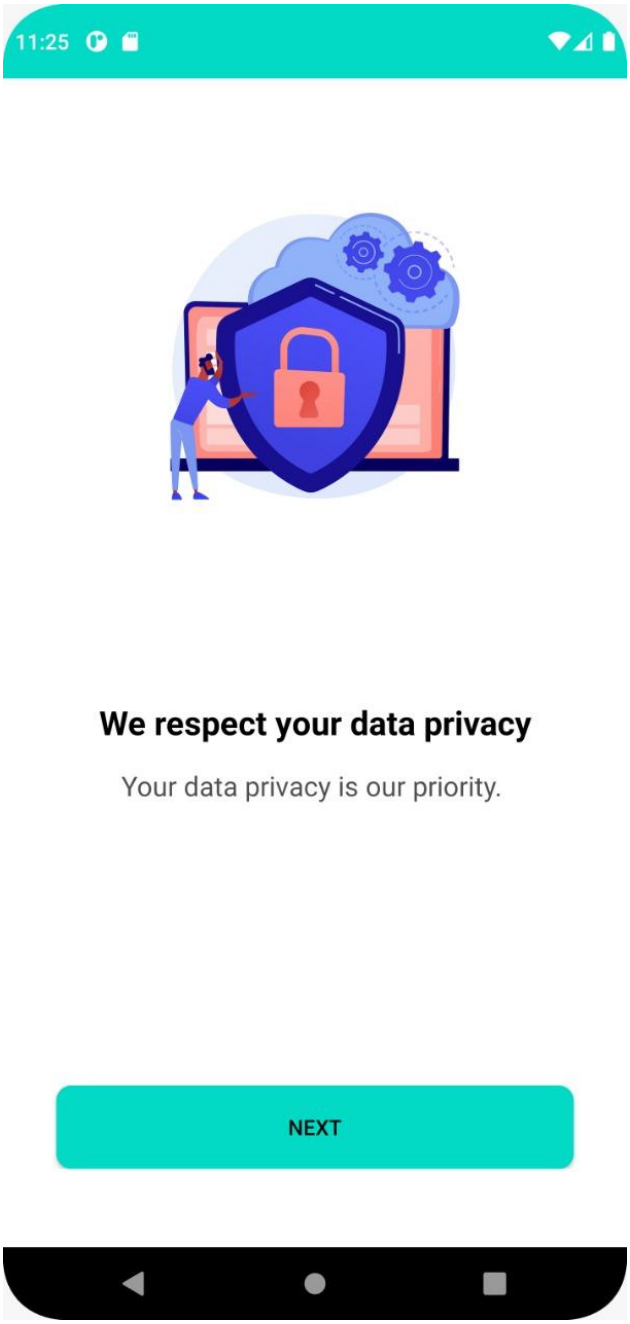


Figure 8: Privacy UI

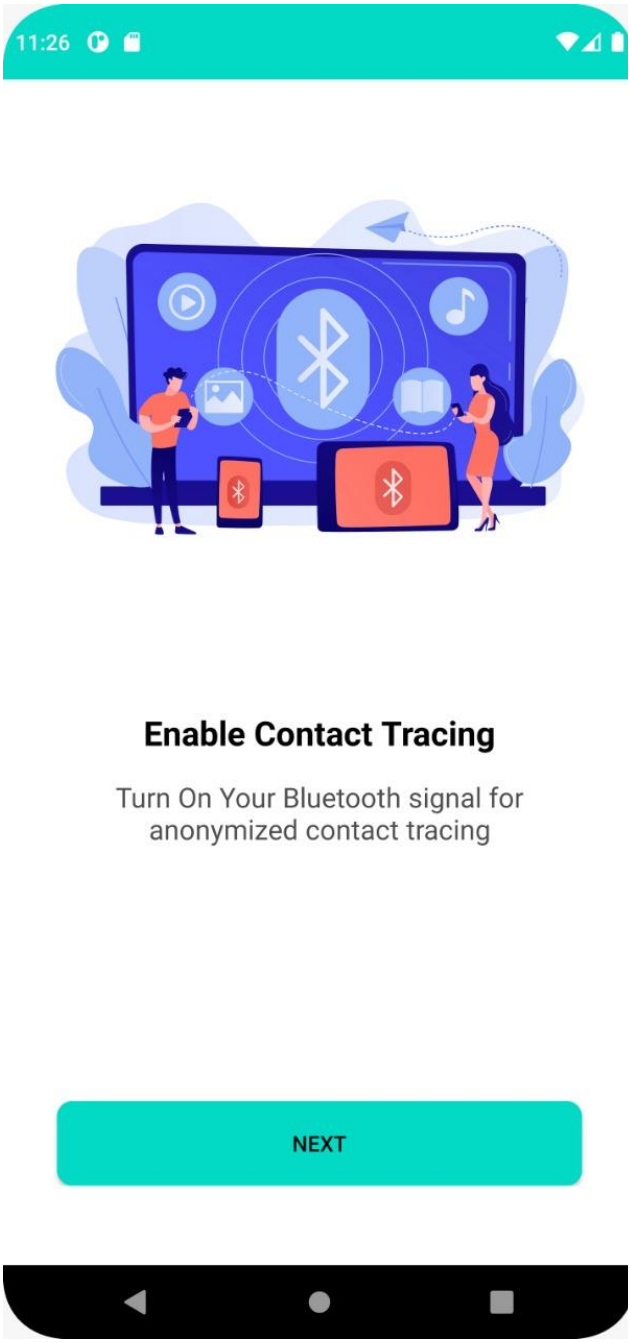


Figure 9: Bluetooth UI

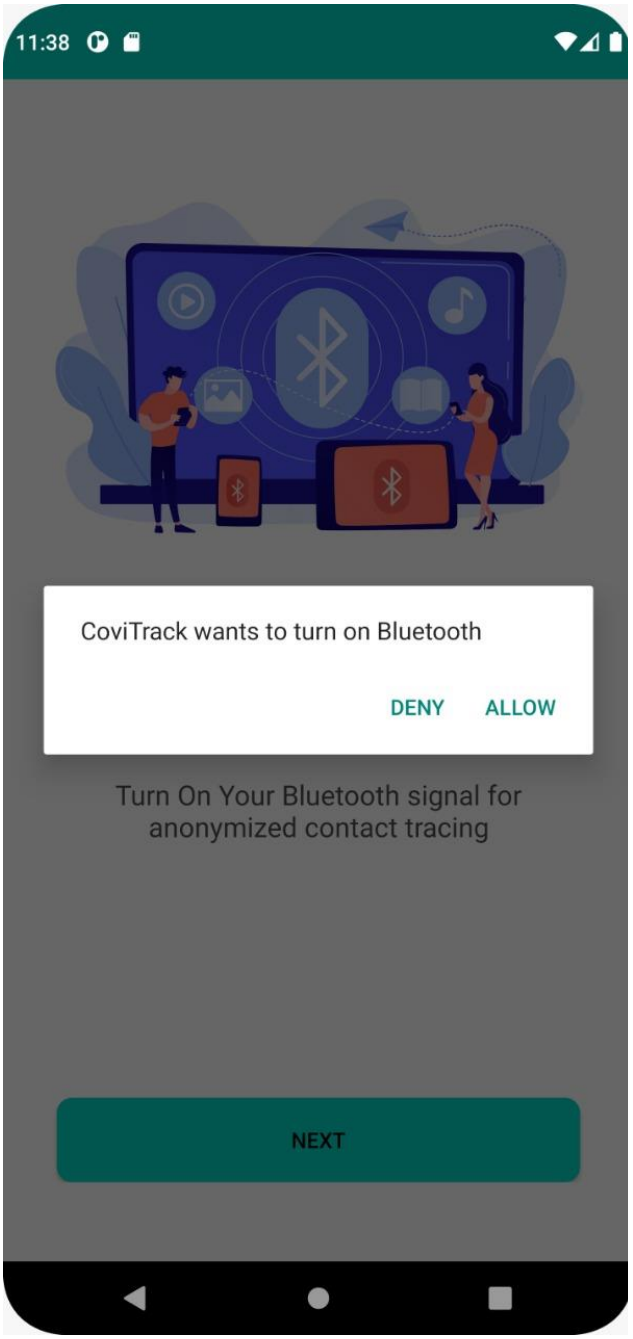


Figure 10: Bluetooth permission UI

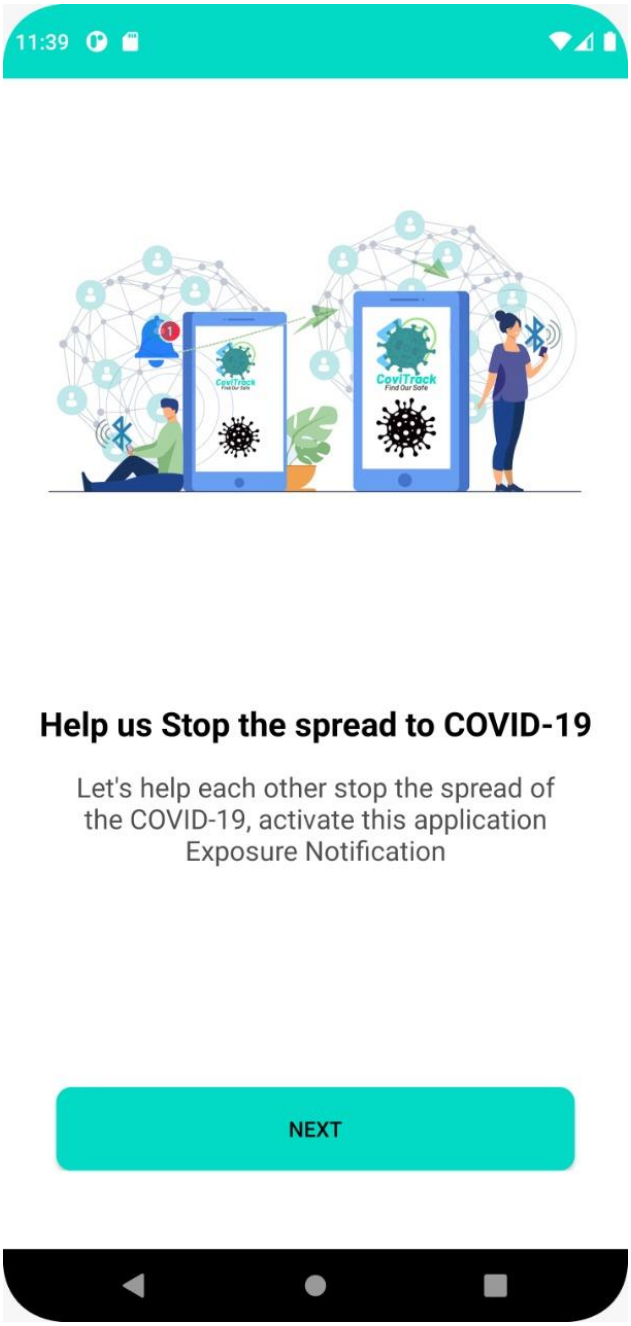


Figure 11: Get started UI

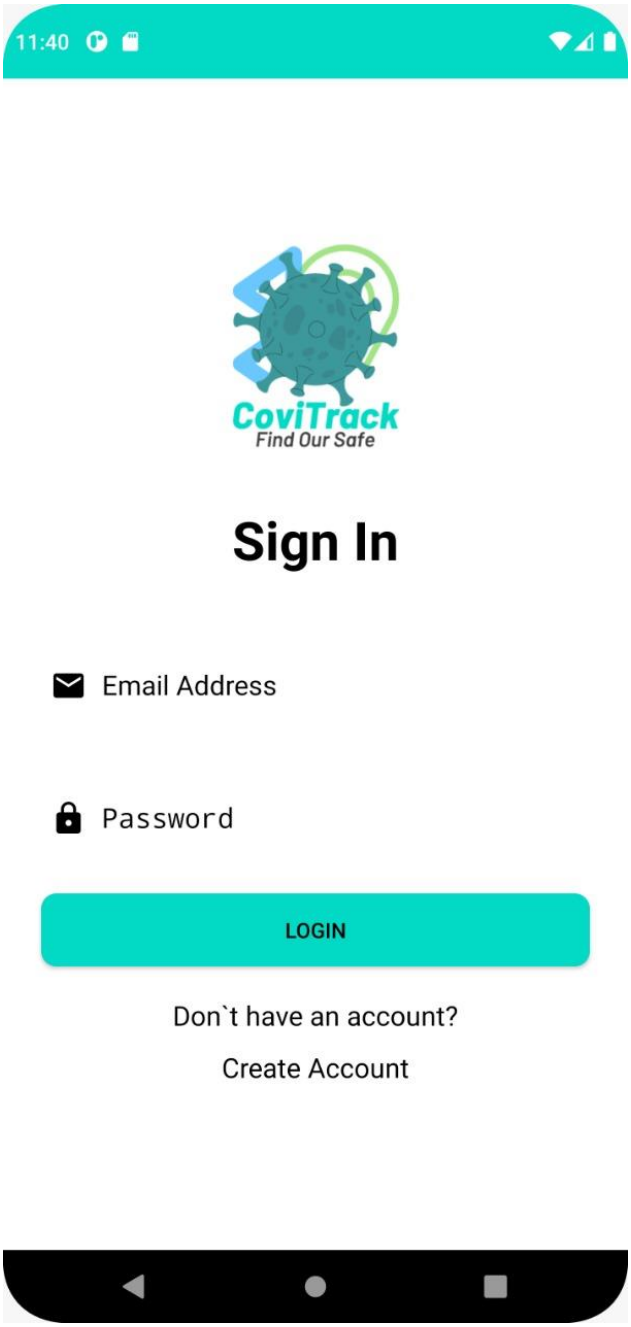


Figure 12: Sign in UI

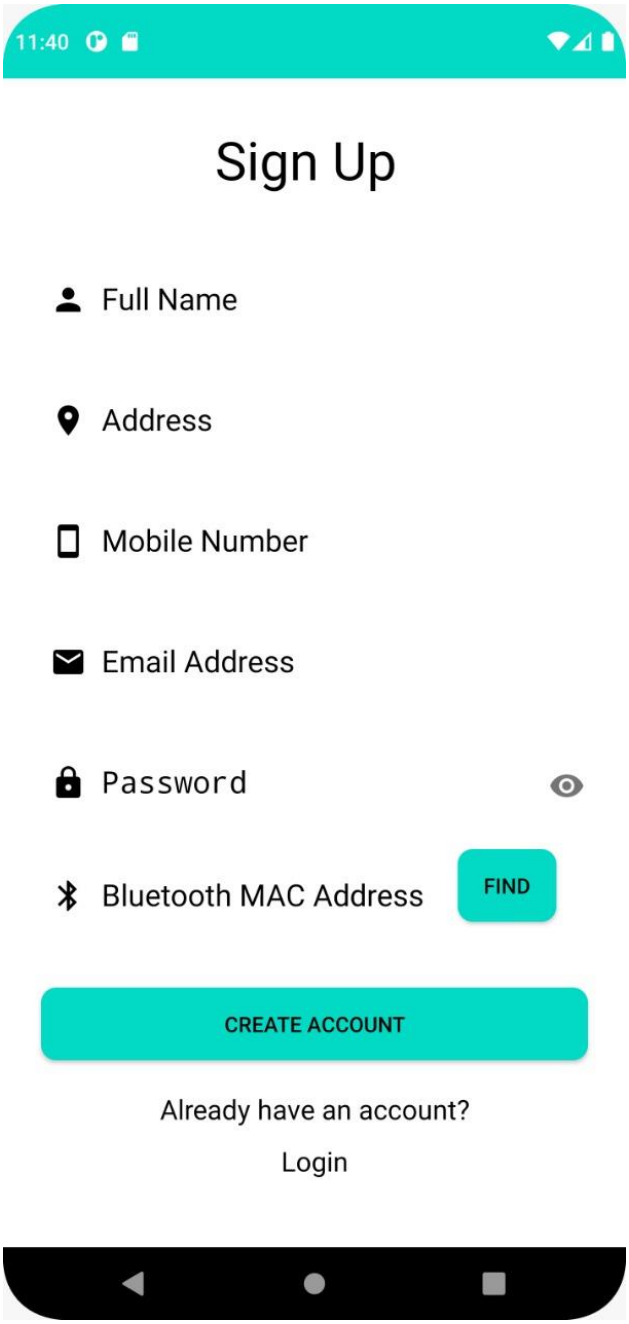


Figure 13: Sign up UI

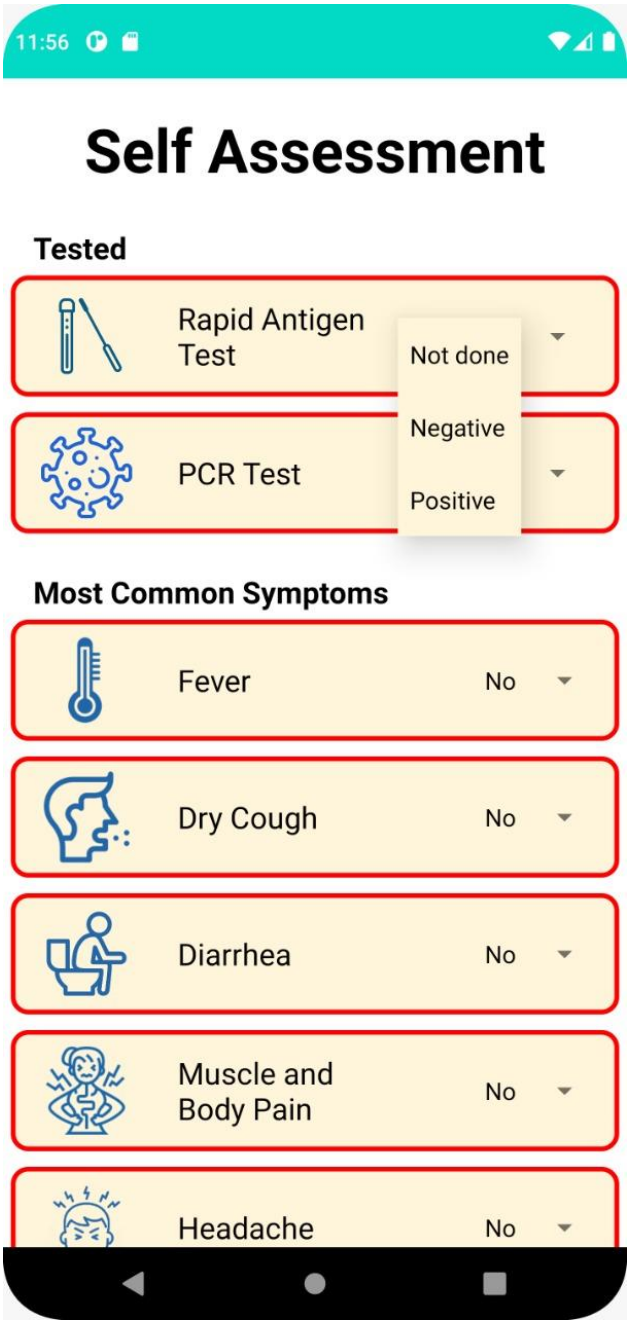


Figure 14: Self-assessment UI

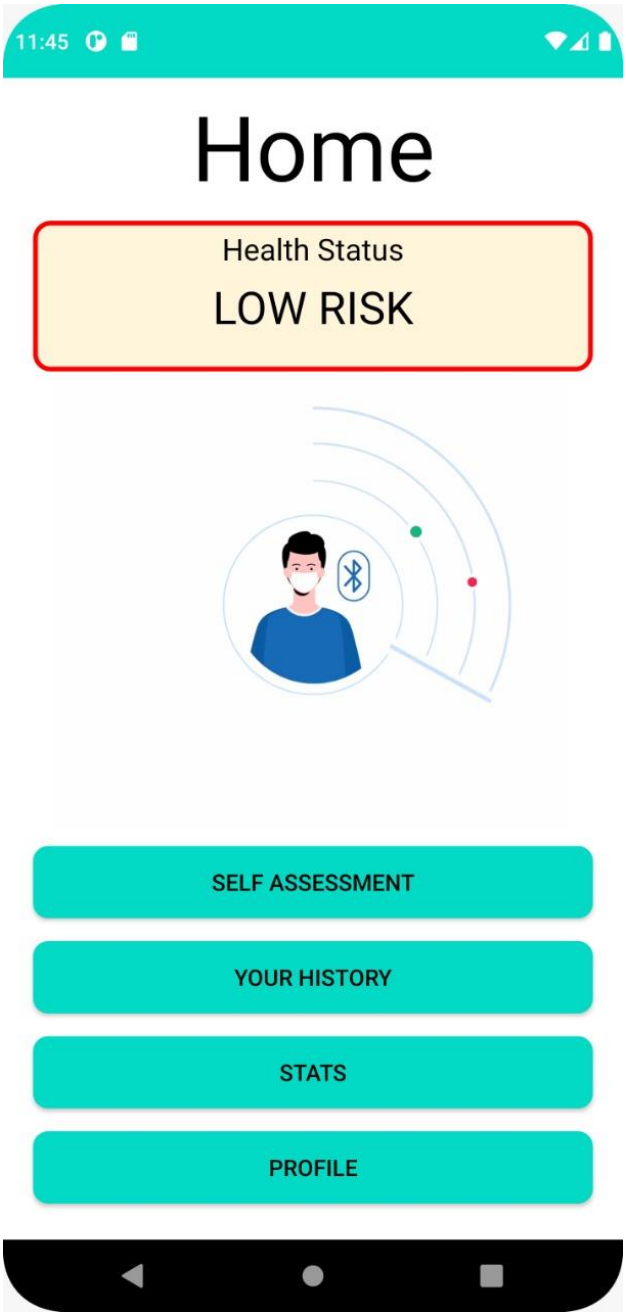


Figure 15: Home UI

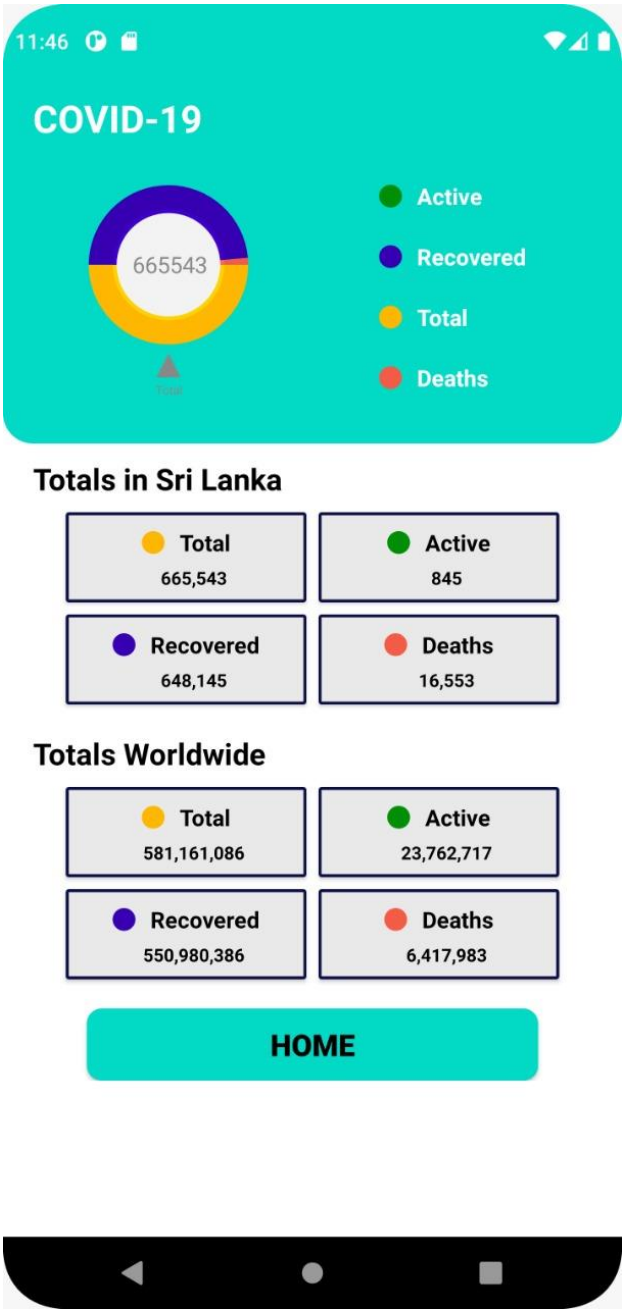


Figure 16: COVDI -19 stat report UI

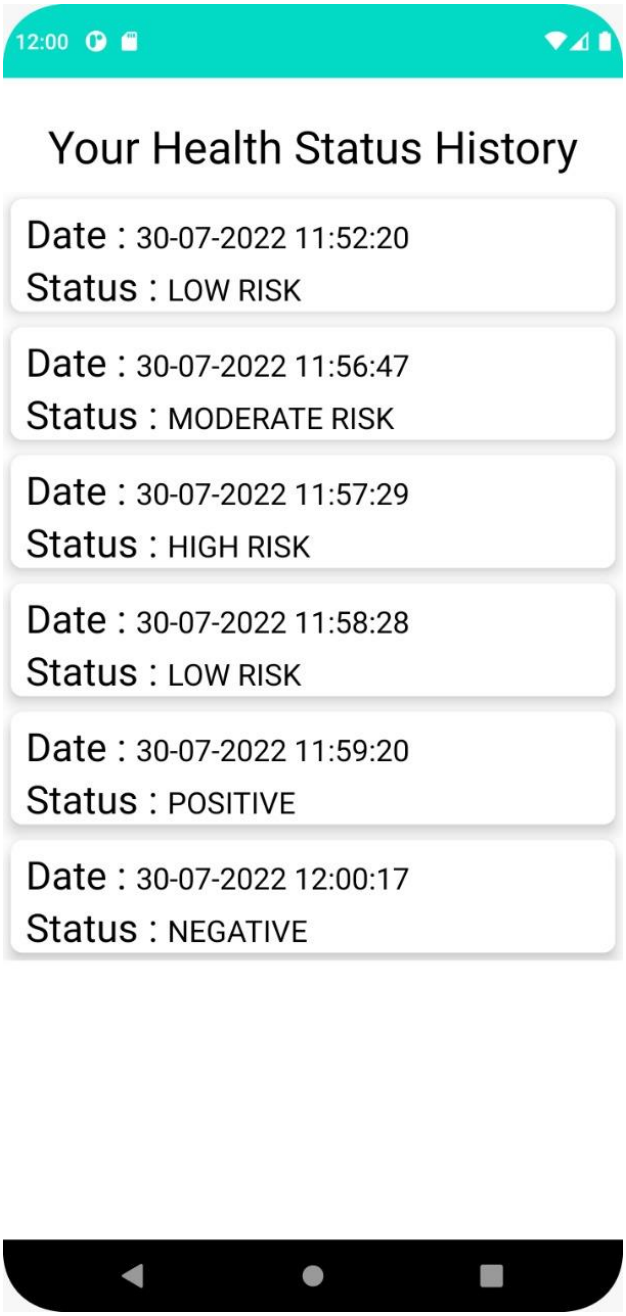


Figure 17: User health history UI

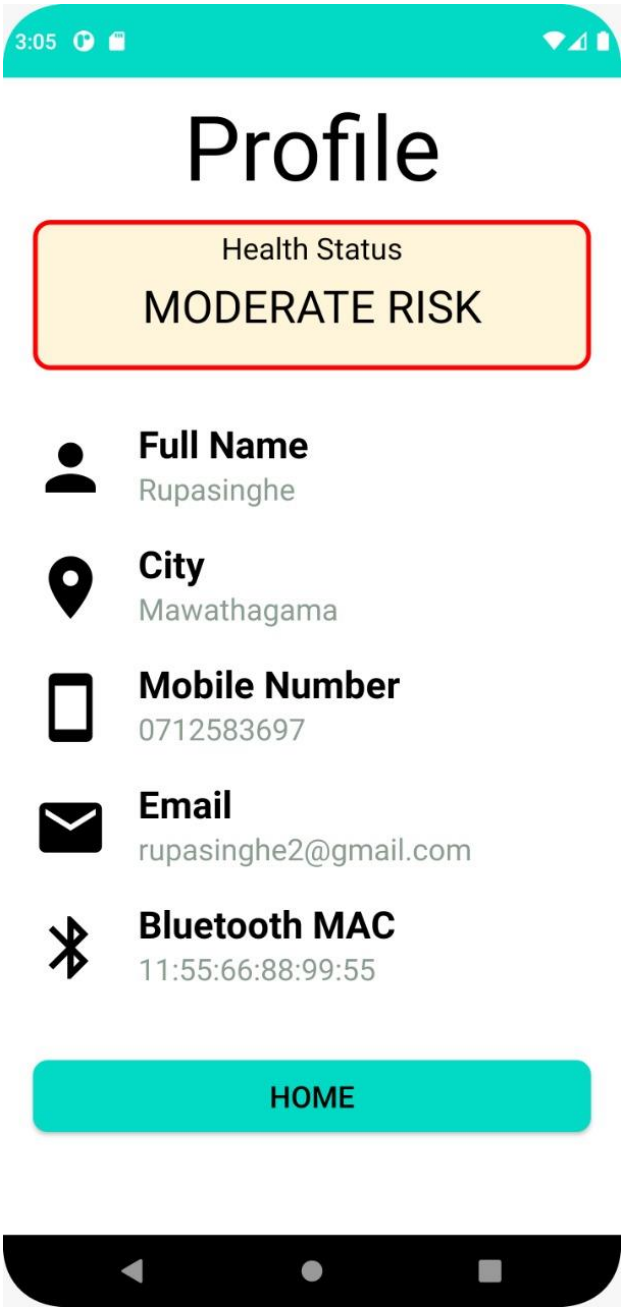


Figure 18: Profile UI


Figure 19: Moderate Instruction UI


Figure 20: High risk Instruction UI

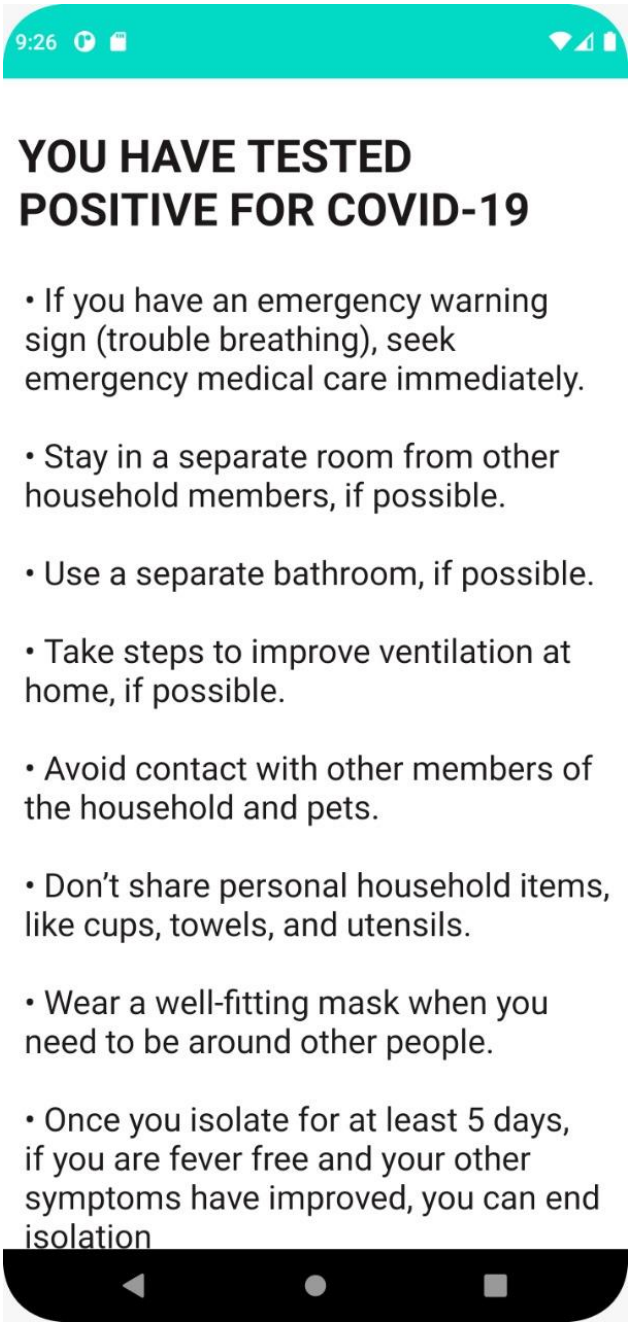


Figure 21: COVID-19 positive instruction UI

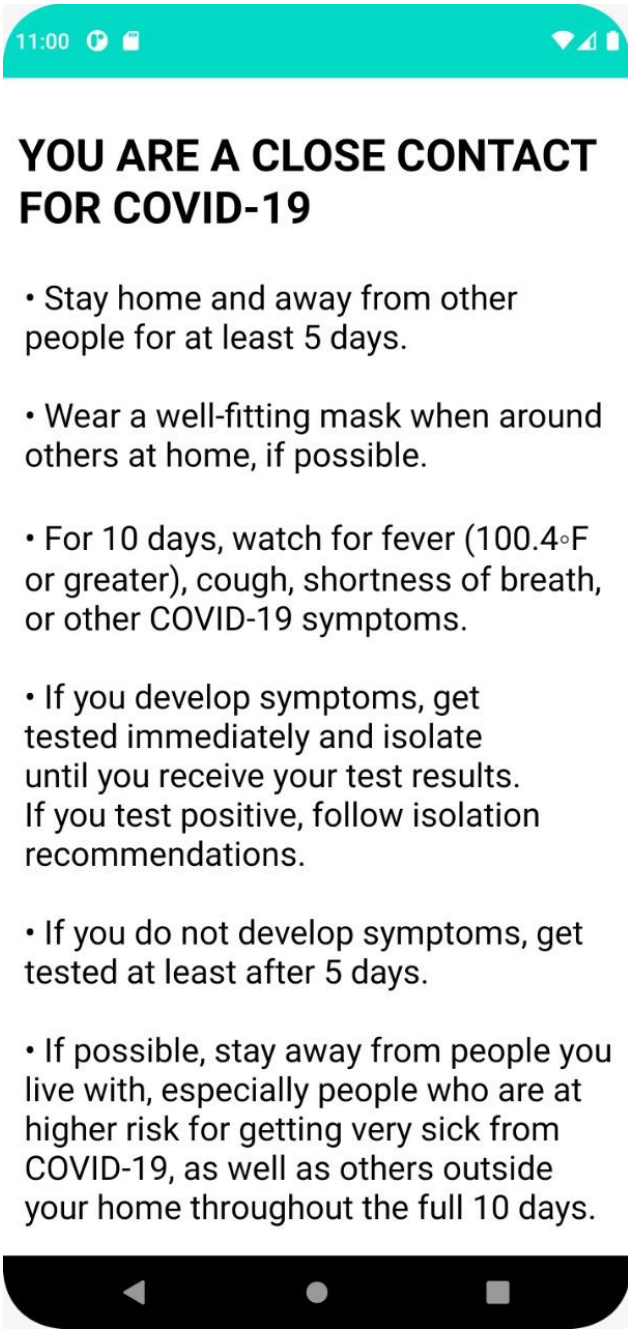


Figure 22: COVID-19 close contact instructions UI

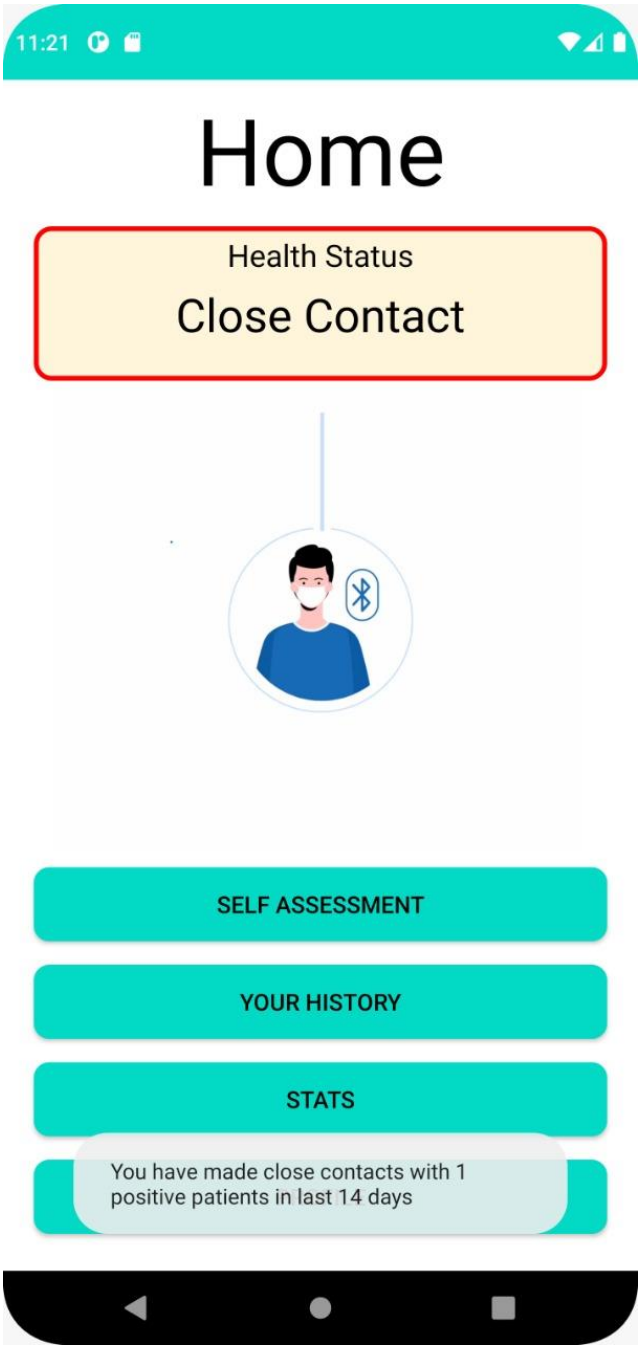


Figure 23: Close contact detected alert

## 4.3 Reports Generated

The blockchain interface was developed through the Rinkeby faucet web browser. When a high-risk or positive patient is detected, the application passes the id to the blockchain. Then the block will be generated. As the given figure:24, which gives the report of the transactions.

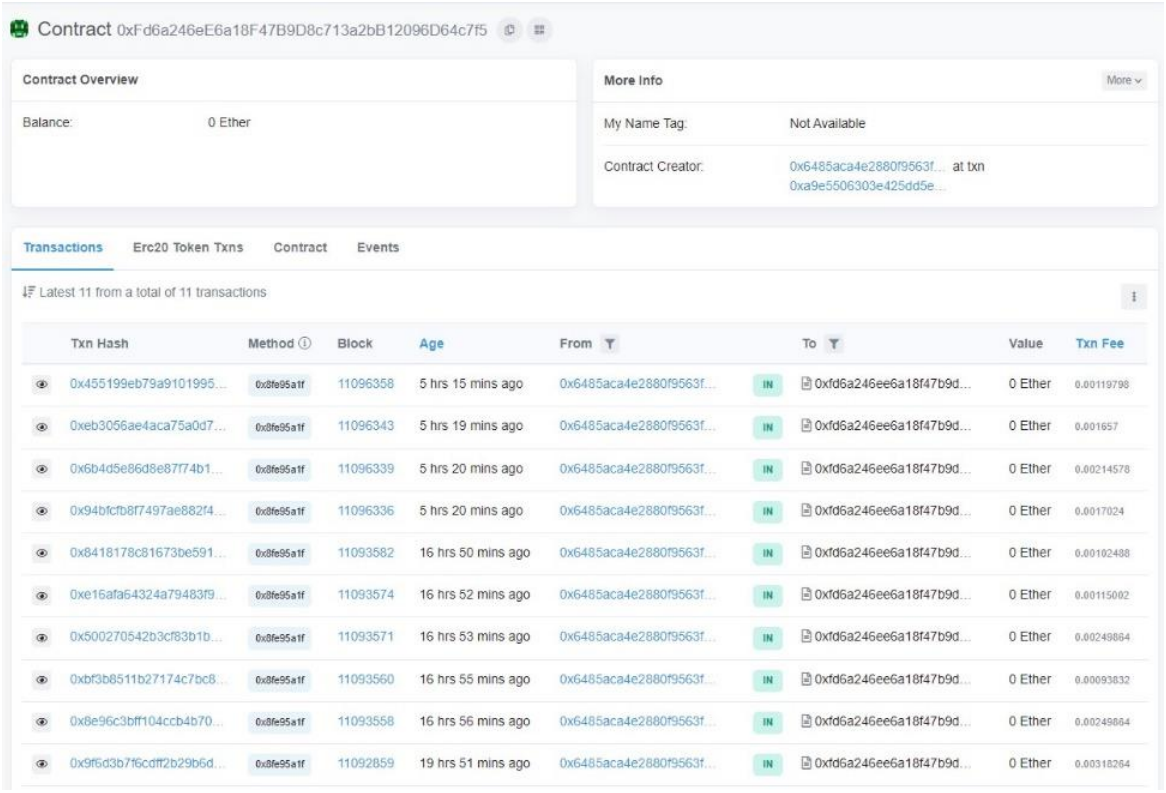


Figure 24: Blockchain report

The application generates the user's health status when they fill the self-assessment. At every login moment, it generates and stored data in the local database for 14 days. In figure 25 shows the users's health history with the time when the user fill the self-assessment.

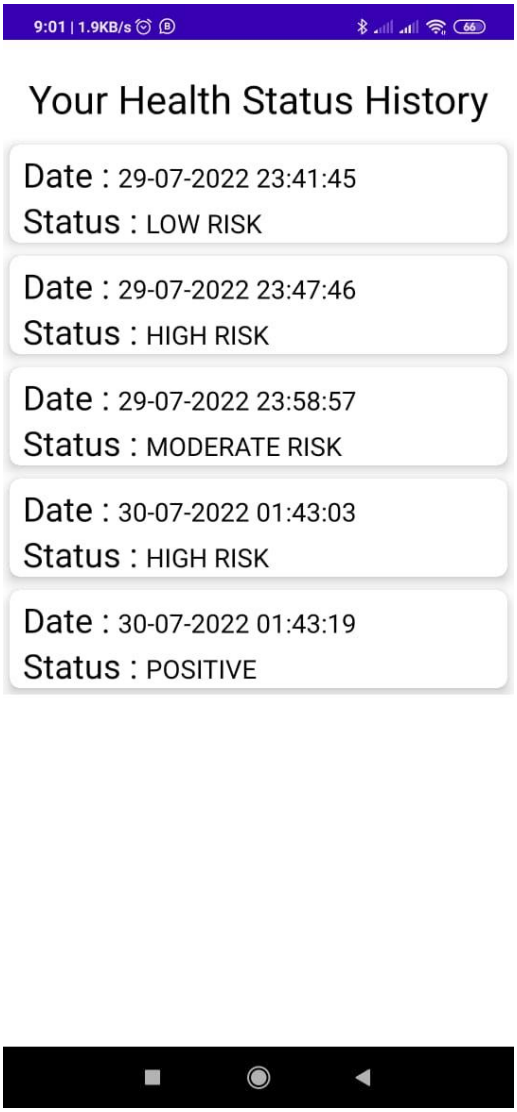


Figure 25: User health history UI

Through the figure 26, the application shows the overall summary of the spread through the world so users can update how the current situation of the pandemic.

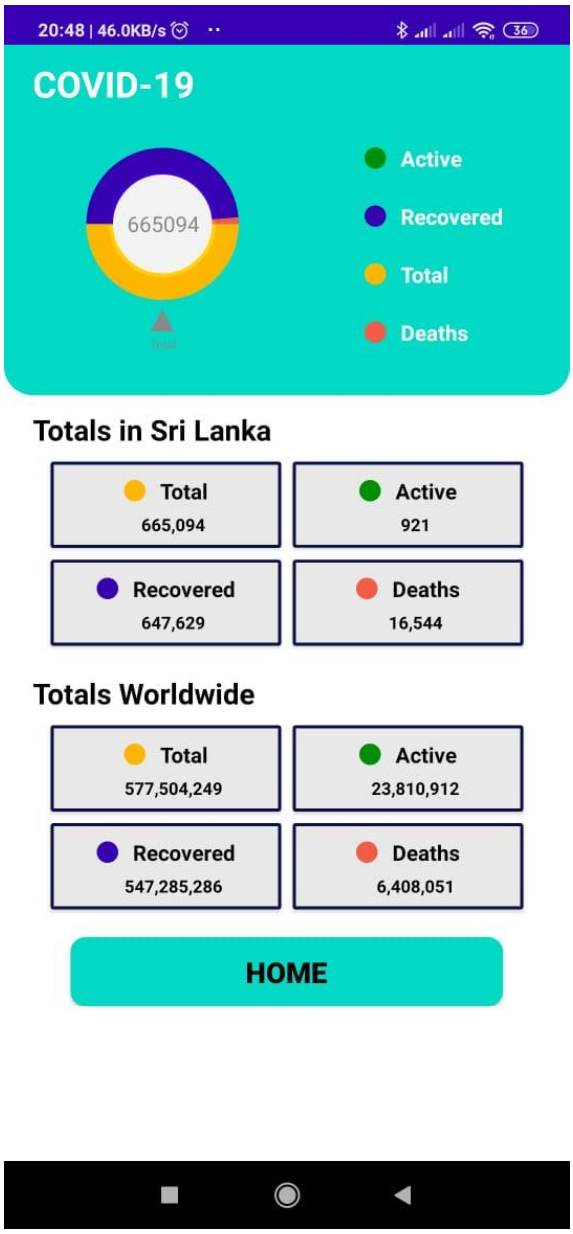


Figure 26: COVID -19 stat report UI

The application gives several instructions for positive, moderate, and high-risk patients on how they should maintain their health in the upcoming days. Figure 27 illustrate those instructions which generate by the application those users.


Figure 27: Example for instructions

In google firebase, the application stored registration details and the health status of each user. those are stored in. json format. so all their details are stored in locally, as mentioned earlier only positive and high-risk patient ids are stored in blockchain. Both figure 28 and 29 shows the status.


Figure 28: Registration details

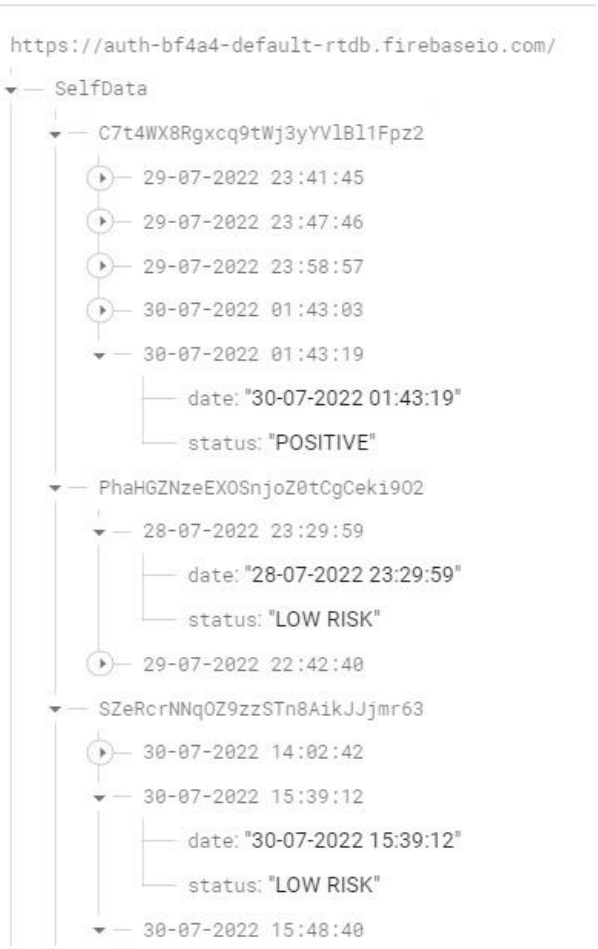


Figure 29: Health status

# 5 Discussions and Conclusions

## 5.1 Discussion of the development process

This project was separated mainly into two parts. The first part of the project, focuses on finding close contacts. In the latter part, the project focuses on the block chain. Mobile phones are widely used in society. Therefore, the team decided to create a mobile app with Bluetooth technology for contact tracing purposes. Every mobile phone has a unique Bluetooth mac id. It helps to identify each user uniquely. the team decided to deploy this system on a native android application. In this project, local storage is used to store close contact IDs. Thus other third party cannot track user close contacts.

In this project, the team had a problem identifying user health status. The team decided to implement a form in mobile application to get user health details. Using that method, this system can verify a

user's health status correctly.

The next step, the team had to store user health status and mobile numbers in blockchain when someone gets positive for COVID-19. Blockchain with java application still has many resources. Here the team used the web3j library to connect the blockchain with the mobile app. Using Solidity, the team implemented a smart contract on the blockchain and deployed it on the Rinkeyby test network. The development method used for this project is a combination of agile and scrum. This was chosen mainly due to the flexibility of improving and changing the requirements and the ease of adding components during the development of the application, without hindering productivity. The functionality of the mobile application and the progress were discussed in the meetings with the team supervisor.

## 5.2 Conclusions

The COVID-19 pandemic continues to affect the way of life of everyone. The contact tracing apps are likely to play a vital role in aiding health authorities quickly identify individuals that may have been exposed to the COVID-19 virus. The imminent interest and adoption of tracing app technology will improve the tracing capability of health authorities.

## 5.3 Proposed Future Work

The following areas can be further developed for the COVID-19 contact tracking system project that uses blockchain technology

- The mobile application can add a location track and get live updates about user location.
- Positive cases live updates can be shown on the map
- The Application can inform to close contacts second and third level.
- The Application can check positive patients and close contacts following self-quarantine rules and advice through live location sharing.
- Warning the user about the danger zone when the user enters an area with many patients.

# References


1. Bay, J., Kek, J., Tan, A., Sheng Hau, C., Yongquan, L., Tan, J. and Anh Quy, T. (2020). *A privacy-preserving protocol for community-driven contact tracing across borders*. BlueTrace.

2. Euromoney.com. 2022. Blockchain Explained: What is blockchain? | Euromoney Learning. [online] Available at: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain#:~:text=Blockchain%20is%20a%20system%20of,computer%20systems%20on%20the%20blockchain.

3. Google/Apple (2020). *Privacy-Preserving Contact Tracing - Apple and Google*. [online] Apple. Available at: https://covid19.apple.com/contacttracing.

4. Idrees, S.M., Nowostawski, M. and Jameel, R. (2020). Blockchain based Digital Contact Tracing Applications for Pandemic Management (COVID-19): Issues, Challenges, Solutions and Future Directions (Preprint). *JMIR Medical Informatics*.

5. Labs, W., 2022. Web3j. [online] Docs.web3j.io. Available at: https://docs.web3j.io/4.8.7/.

6. Martin, T., Karopoulos, G., Hernández-Ramos, J.L., Kambourakis, G. and Nai Fovino, I. (2020). *Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps*. [online] Wireless Communications and Mobile Computing. Available at: https://www.hindawi.com/journals/wcmc/2020/8851429/.

7. Medium. 2022. An introduction to Ethereum Development on Android using Web3j and Infura. [online] Available at: https://medium.datadriveninvestor.com/an-introduction-to-ethereum-development-on-android-using-web3j-and-infura-763940719997.

8. Shahroz, M., Ahmad, F., Younis, M.S., Ahmad, N., Kamel Boulos, M.N., Vinuesa, R. and Qadir, J. (2021). COVID-19 digital contact tracing applications and techniques: Areview post initial deployments. *Transportation Engineering*, 5, p.100072.

9. Worldometers.info. 2022. COVID Live - Coronavirus Statistics - Worldometer. [online] Available at: https://www.worldometers.info/coronavirus/.

10. Xu, H., Zhang, L., Onireti, O., Fang, Y., Buchanan, W.J. and Imran, M.A. (2020). BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond. *IEEE Internet of Things Journal*, [online] pp.1–1. Available at: https://arxiv.org/pdf/2005.10103.pdf