

# Securing Contact Tracing in the COVID-19 Pandemic: Leveraging Block chain for Privacy Protection

Vidyashree R,  
Dept. of CSE, UVCE,  
Bangalore, India

Sunil Kumar G  
Dept. of CSE, UVCE,  
Bangalore, India

## Abstract

*In order to stop the illness from spreading further, the COVID-19 pandemic outbreak has highlighted the critical need for efficient contact tracking technologies using mobile phone applications. However, because of the sensitive nature of contact tracing, privacy concerns raised by the public have created a barrier to the current solutions, which is having a big impact on how widely contact tracing apps are being used. In order to desensitise the user ID and location information, we propose to employ blockchain technology to bridge the gap between the user/patient and authorised solvers in our work, which presents a privacy-preserving contact tracing system enabled by blockchain technology. Our technique exhibits superior security and privacy when compared to recently suggested contract tracing systems. It also has the added benefits of being battery-friendly and internationally accessible. The necessary resource is shown to be viable from both the server and cell phone viewpoints. By addressing public privacy concerns, the suggested approach can offer a timely framework that will enable government agencies, businesses, software developers, and researchers to quickly create and implement efficient digital contact tracking tools in order to quickly contain the COVID-19 epidemic. In the meanwhile, this project's open initiative enables global cooperation and integrates current tracking and location technologies using blockchain technology.*

**Keywords:** COVID-19, coronavirus, distributed ledger technology, blockchain, electronic contact tracing, privacy-preserving, pandemic.

## I. INTRODUCTION

The viral condition known as COVID-19 is brought on by the SARS-CoV-2 virus, which causes serious acute respiratory syndrome [1]. As a result of the disease's global spread, billions of people are under lockdown and health systems throughout the world are straining to keep up. As of May 18, 2020, 188 nations and territories have confirmed cases totaling 4,769,177, and 316,898 fatalities [2]. As at the time this research was written, COVID-19 vaccines were still unavailable. Therefore, some nations across the world have started using non-pharmaceutical measures (NPIs), which try to slow down the disease's transmission by lowering the pace at which members of the general public come into touch with one another [3]. NPIs primarily target social distancing, often referred to as physical distancing, which is defined as maintaining a specific distance from other people and avoiding congregating in big groups [4]. Most nations implement harsh policies, such as shutting offices, schools, and public gathering places as well as imposing travel restrictions.

In the absence of available vaccinations, NPIs were shown to be highly effective during the H1N1 flu pandemic (1918–1919), the final disease pandemic on the same size as the COVID-19 pandemic [9]. Early COVID-19 pandemic implementation of NPI by towns and cities has successfully decreased the total amount of infections while the implemented measure is still in effect. The mortality rate significantly decreased as a result of this. Strict controls, however, immediately jeopardise the economy. This is important since economic downturns negatively impact many facets of society, including health. According to Goldman

Sachs' forecast, the US economy may contract by 24% in the subsequent quarter of 2020—more than twice as big as any previous contraction ever noted [10]. The majority of nations on the planet are creating well-rounded plans that take into account both the economy and the COVID-19's potential recovery. For several decades, tracking contacts has been a crucial component of public health efforts to manage contagious diseases. It has demonstrated efficacy in mitigating COVID-19 in some nations. Since vaccinations appear to be far off [11], most governments throughout the world—including those in the US, Portugal, UK, Italy, Germany, and other countries—are focusing more on the track and trace method when it comes to reducing social distancing regulations. Once the lockdown is lifted—or at least partially lifted—and society adopts a "New Normal," this strategy will not only serve to save lives but also to salvage the economy.

#### Contact tracing

The process of locating individuals who may have had contact with a person with the infection and then gathering further data about these connections is known as "contact tracing" [12]. In the early stages of epidemiology, traceability of contacts is done using labor-intensive procedures. Contact tracking has an extensive record of helping prevent infectious illnesses. The memory of a (i.e. from exhaustive) list of individuals with whom they had communicated during the preceding weeks, or the places where the verified individual had been, was a major component of the procedure. Those who could be reached can be informed by emails, phone calls, or letters. Thus, using a standard contact tracing technique like this limits the list's completeness and correctness as well as the tracing's timeliness and efficiency.

Up until recently, several governments created and implemented smartphone apps for digital contact tracking as a way to get around the labor-intensive approaches' obstacles. Detecting interactions with COVID-19-positive individuals using smartphone Bluetooth signals is one of the common contact tracing methods. This method does not track users' whereabouts or keep that information. With this method, minimal action might be required if someone shows signs of COVID-19, alerting others to the possibility that they may also be infected. The centralised and the decentralised models are the two variations of the Bluetooth-based contact tracking. A centralised model is Trace Together in Singapore [5]. However, with the decentralised approach, the user has greater power because the information is stored on their smartphone. In a decentralised paradigm, analysis and matching for individuals who may have visited COVID-19 are done on the user's smartphone. Furthermore, because it encourages consent, openness, and privacy, the decentralised approach has been supported by an international coalition that includes Apple and Google [6]. In the former, the server receives collected anonymized data that is uploaded. If someone begins to exhibit COVID-19 symptoms, matches are created with other contacts through server processing. To keep things simple, we will refer to the cell phone app-based digital method of tracking contacts as "contact tracing" in the following instead of using the word "digital."

## II. LITERATURE SURVEY

We examine four of the most current contact tracing strategies that have been suggested: the China Health code system [8], the Google/Apple collaborative contact tracing effort [6], the NHS COVID-19 App [7], and Trace Together from Singapore [5]. The location or grouping gadgets, power consumption, technological security, coverage, and degree of privacy protection are among the indicators we evaluated in our review.

The Bluetrace [5] protocol-powered app Trace Together uses Bluetooth with reduced energy (LE) to find and locally capture clients that are close to the user. Because the user must maintain their gadget in an active streaming state for this strategy to work, the user device's battery is depleted. Due to its open wireless interface, Bluetooth technology raises security risks. Bugging, sniffing, and jamming are among the most common attacks against Bluetooth-based contact tracing systems. Replay attacks are a serious threat to the contact tracking network, and they might potentially spread widespread public concern.

Because hardware identification on the Wireless physical layer could remain hidden and expose actual hardware, the Bluetooth protocol may be used for user security in the meantime.

While this kind of privacy could be seen as protected from the larger public, inside a smaller group that is vulnerable to radio frequency interference, it is practically visible. Meanwhile, current wireless interference and the user device's transmission power restriction restrict the problem of regionally triggered proximity solutions. As we previously established, Trace Together is a centralised service with regard to of the user's true identity and notifications, but the authority is the only party that knows about the user's privacy. Consequently, if the harmful action originates from the central service provider, it is seen to be non-true privacy-serving.

With Bluetooth LE, Google Ios Contact Tracing also uses a comparable strategy. In terms of user privacy, it differs from Trace Together since the product or service provider maintains user anonymity by not obtaining their true identify. To match and notify contacts, the user must utilise their central server, which raises privacy concerns with trajectory attacks and makes it possible to rebuild the user's profile using server access data. In a similar vein, there is a chance that the National Health Service's COVID-19 App might expose user privacy.

The Health Code System differs from the previously mentioned techniques in that it doesn't rely on Bluetooth or proximity sensing. The method works by scanning the user-associated Quick Response code, which is based on structural cross-match. Because of centralization, user privacy is violated in this system, and the real identity of the individual using it is not concealed from the authorities. But because the health indicator is only checked when a checkpoint is passed, it doesn't utilise data and saves the user's battery. Additionally, the coverage is easily expandable due to its very central hierarchy. Aarogya Setu, COVID Safe, Decentralised Secure Proximity tracking, Pan-European Privacy-Preserving Proximity Tracing, and many other protocols and solutions are being developed to address pandemic contact tracking [13]–[16], among others. With their modifications to certain aspects, they resemble the solutions previously mentioned.

#### Blockchain basis for contact tracing

Due to the necessity of gathering, matching, and dispersing information, contact tracing poses privacy issues. Providing for the identity protection of COVID-19 users is one of the other concerns. Although some control over involvement may be provided via the opt-in option, it is unclear how we will make sure that only pertinent data is shared. In order to desensitise the individual's ID and location information, the blockchain can act impartially in a distributed manner as a mediator between the client/patient and the approved solutions. It can offer an alternative to depending on users adhering to laws or regulations in a centralised system for privacy preservation through technical design. Additionally, users' identities may be further protected by combining blockchain technology with technologies for anonymization and encryption. Since blockchain technology is non-regional by nature, it offers an appropriate worldwide access platform for tracking and managing the COVID-19 epidemic. A transparent feature can shield the public from deliberate false information disseminated by government agencies or other outside parties.

#### Blockchain As The Backbone For Privacy-Preserving Information Sharing

Blockchain technology might solve the trust, security, confidentiality, and openness problems associated with the current contact tracing technologies. Blockchain technology has shown great potential in a number of fields, including finance, energy trading, logistics, authentication, and the Web of Things (IoT) [18], [19]. Blockchains comprise distributed databases arranged in an irreversible, tamper-proof hash tree structure [20]. Specifically, information added to the blockchain network is arranged into blocks. Every block contains a hash value that is unique to it; this value also applies to the block before it, ensuring a linkage between blocks that is retroactive. In a distributed system devoid of trust, blockchain technology provides an unchangeable, visible, safe and auditable ledger for confirming the accuracy and manageability of data and assets across time.

Applications for contract tracing can benefit from the integration of blockchain technology by adding much-needed safety, confidence, transparency, and privacy that are either lacking or only partially provided by the current systems. In addition to being a chain-link data structure, the Consensus Mechanisms (CM) is crucial to realising the special advantages of blockchain technology. The CM assures the blockchain's consistency and integrity across geographically dispersed nodes, as well as an obvious ordering of transactions. Blockchain system performance, including transaction throughput, latency, node scalability, security level, etc., is mostly determined by the CM. As a result, many CMs for blockchain have been investigated, based on application situations and performance requirements. When choosing a content manager, it's crucial to take into account factors like network performance, latency, storage, and scalability. Proof of Work (PoW), Proof of Stake (PoS), and Direct Acyclic Graph (DAG) based CM are examples of frequently used CMs.

PoW's fundamental concept is the competition of processing power, and it was first shown in the initial blockchain application (Bitcoin). Every node in the CM competes for access spot in the new block whilst earning bonuses by using its processing power for the hash process. This results in the use of computer resources and unnecessary energy utilisation. Conversely, PoS depends on coin ageing competition instead than processing power competition. Thus, PoS benefits the affluent miner and may lead to near-monopolies, which may give rise to the emergence of a strong third party.. Given that user privacy is at risk in this endeavour, this might potentially provide a hurdle. Such an issue can be addressed by design by using a more fair weighting mechanism on coin age. PoW and PoS chain architectures are both compatible with one other. The CM needs to lower the access frequency of new blocks in order to keep users on just one instance of the blockchain [18]. This may result in some obstacles when implementing PoW and PoS CMs for an extensive amount of contact tracing users (such as those in populous nations like China or India).

Specifically, the CM will use a lot of resources, which is excessively expensive for such a limited in resources system, in order to lower the pace of new block access and shield the PoW or PoS determined by this system from assault. Moreover, the system won't be able to handle the exponential rise in user numbers due to the restricted capacity of the additional PoS and PoW blocks. For example, in Ethereum, the throughput is often restricted to 20 to 30 TPS, but in Bitcoin, it is typically limited to 7 TPS [21]. A lengthy confirmation latency for the CMs is implied by the low entrance rate of fresh chunks in PoW and PoS CMs.

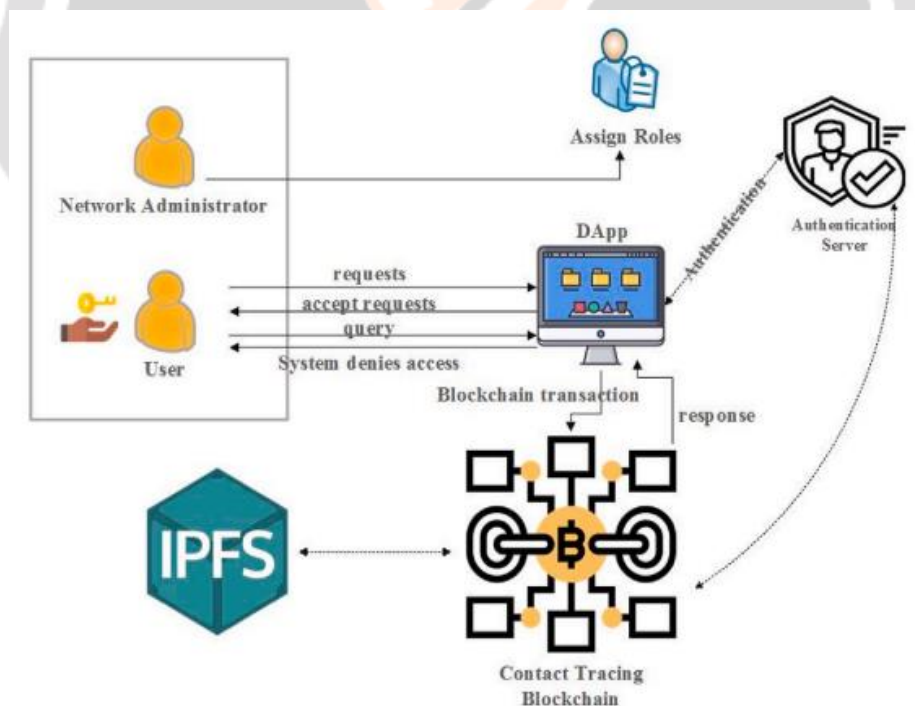
For this system, the typical verification delays of three minutes for Ethereum and sixty minutes for Bitcoin are insufficient since additional network delays including access and processing delays also need to be taken into account. However, by lowering the amount of rigorous computation security level difficulty (e.g., no need to wait for block confirmation following 6 blocks are created after it), efficiency and delay performance may be greatly improved. Furthermore, contact tracing might be done in a city with a small to large population.

In this system, DAG-based CM may overcome the drawbacks of PoW and PoS consensus. In contrast to PoW and PoS, all transactions in DAG are related, either directly or indirectly, and there are no contests to build new blocks. As long as they execute the previous transactions, users can add their blocks to the ledger at any moment using the DAG-based consensus method. Forking would occur as a result of the simultaneous generation of several branches. In DAG-based CM, forking allows for infinite TPS and confirmation rate. Furthermore, when forking is integrated into DAG, it might need relatively little resources for a user to build a new block, which makes it ideal for the system. Zero transaction costs and cheap processing power are two other important advantages of DAG-based CM that make it more appropriate for this system..

### III. BLOCKCHAIN ENABLED PRIVACY-PRESERVING CONTACT TRACING

We provide a thorough process description and a clarification of important ideas in this part. We will first go over the system's entities, their functions, and how they interact with one another in the sections that follow. After outlining the contact tracing framework's workflow, we will get into the specifics of creating and exchanging blockchain pseudonyms.

It is important to note that the framework is an open initiative that enables contact tracing data to be shared with various authorities, methods, and cryptography. It can also develop into an open interface data tracing hub for all contact tracing providers that protect privacy worldwide. Furthermore, neither the blockchain's incentive system nor its choice of blockchain central manager are restricted by the suggested structure. The CM can be included into the framework as long as it satisfies the performance requirements of the network. Furthermore, the framework has no restrictions on the positioning services that might be chosen.



#### A. Entities, functions and interfaces

The parties participating in this project are defined below, along with an explanation of each person's position and interface:

Users refers to contact tracking app users on their mobile devices in an abstract way. In the remainder of the paper, we will refer to the user gear (UE), the application, and the device as "user." Every user will read from the message on the chain for self-verification and post their encryption Trace Code to the tracing blockchain.

Geodata from verified COVID-19 users is diagnosed by diagnosticians, who then approve it with a signed preface and submit it to the monitoring blockchain for solvers matching.

The trusted user or third party's server, known as the geodata solvers server, engages with the geodata and offers support for the notification chain. sends the matched data to the notification blockchain after reading the raw data from the tracing blockchain for matching.

A trustworthy third party (such as governments or public health organisations) engages in key distribution to the user, diagnostician, and solvers through a Public Key Infrastructure (PKI)/Certified Authority (CA).

positioning service providers, such as WiFi, Bluetooth, GPS, and cellular towers, among others, depending on the user's support. In this article, the data provided by the supplier shall be referred to as geodata.

The Tracing blockchain is one of the two chains that allow users and diagnosticians to register Trace Codes; the other chain will be covered in more depth. The solver reads it as well in order to match geodata.

*B.* Notification The chain used for risk registering to the impacted users' Trace Code is called blockchain.

Trace Code is a masking name for the distributed ledger address that is presented in the article. It consists of two parts: the prefix, which is the user fake name, and the suffix, which is the geodata cyphertext.

#### IV. METHODOLOGY

In order for the government to easily track down everyone who comes into contact with someone who has COVID-19 symptoms and place that person under quarantine in order to stop the disease from spreading further, it would be helpful to automatically detect or trace everyone who exhibits COVID-19 symptoms and interacts with other people.

The last COVID pandemic put the entire globe on lockdown since the necessary technology was not available to identify the infected individual and his contacts in time to isolate them, preventing the virus from spreading quickly and averting such circumstances. In order to inform users about social estrangement and COVID-19 patients, mobile-based tracing was introduced. However, this method was not very successful because elderly people are not familiar with mobile operations, and it can take a long time for mobile devices to process and send trace data to centralised or decentralised servers. Additionally, there is a risk of server hacking, which could expose every user's information to hackers.

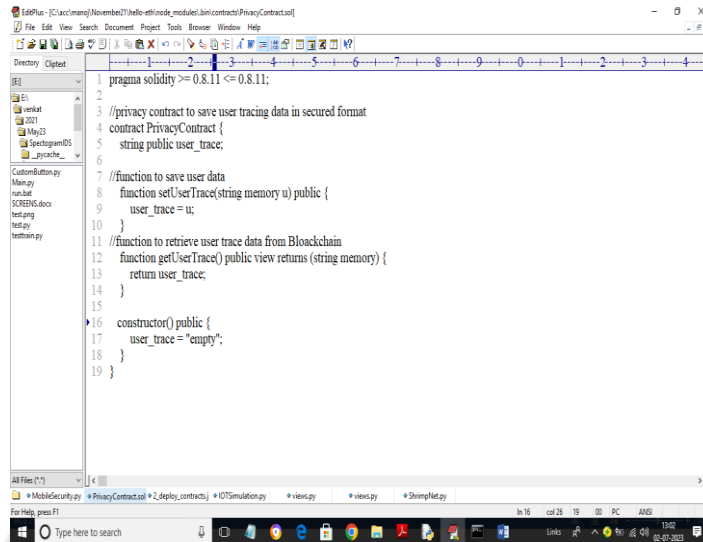
The author of this study is using blockchain technology, which has built-in support for providing user data privacy by encrypting all details, to get over the aforementioned problems. Blockchain technology ensures that data is safe and cannot be altered. The author uses an Edge Computation server to track down and process all user data before sending it to servers. Compared to mobile devices, edge servers can process information more quickly and use less energy.

Every individual will be equipped with a small sensor that will detect their location and health status. This sensor will then report to an edge server, which will determine whether the user is ill. If the user is, the edge server will send the location of the affected person and all other contacted individuals to a server where government officials will track down and quarantine all of those individuals.

Thus, we can track down every user and place them under quarantine to prevent the spread of the illness by using the suggested approach. Because the edge server operates at a fast speed and uses less power, we can also conserve processing power.

*C.* Since we lack real sensors or servers at the edge for processing, we have set up this project as a simulation in which users move around the screen as dummy objects. We then report all of the locations to a server for proximity computation, storing all of the processed data to a blockchain. Subsequently, the government body will choose the desired username and password and then get or track down every additional user information that the selected person interacts with.

*D.* With SMART CONTRACTS, which have functionality for storing and retrieving data, blockchain can save and retrieve data. The screen below displays SMART CONTRACT code created with the SOLIDITY programming language.



```
1 pragma solidity >= 0.8.11 <= 0.8.11;
2
3 //privacy contract to save user tracing data in secured format
4 contract PrivacyContract {
5     string public user_trace;
6
7 //function to save user data
8     function setUserTrace(string memory u) public {
9         user_trace = u;
10    }
11 //function to retrieve user trace data from Blockchain
12     function getUserTrace() public view returns (string memory) {
13         return user_trace;
14     }
15
16     constructor() public {
17         user_trace = "empty";
18     }
19 }
```

In above smart contract code we have functions to save and get user tracing data and now we need to deploy above contract to Block using Truffle tool. To deploy contract go inside 'hello-eth/node\_modules/bin' folder and then double click on 'runBlockchain.bat' file to get below screen



```
C:\Windows\system32\cmd.exe -holla develop
Microsoft Windows [Version 10.0.19H3.1807]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\jacc\mango\November21\hello-eth\node_modules\bin

C:\jacc\mango\November21\hello-eth\node_modules\bin>truffle develop
Truffle Develop started at http://127.0.0.1:9545/

Accounts:
(0) 0xc7851c115271e1d9e9ff93848d3c638313f
(1) 0x0e577c0c471a1351d770e0f49e0208039e
(2) 0xc430395f581686d395f6d8113741e4e112
(3) 0x029f63888361e7408f7d61f1acc39615d114
(4) 0x2431d8a222f9e4c547342431a1f5d5894a7f0
(5) 0x07178f9bca09474483351a7681c1e0f70e0
(6) 0x726f8c0ea353480e7120277e83c4f97e0b3
(7) 0x55f46977edc1ccccch30eb02a67770a293
(8) 0x5F9a8364f6c53c28478f38f4688011603a425
(9) 0x04279682985727f0808ce22ace90e0ac89

Private Keys:
(0) b4f17e4e134e78820441d56f28c4e17020835446f9e21633080f0c5e
(1) 1ee422008986f9c3015ab059e0494f97309e407368130411e8301
(2) 3721888073a20e19074806770f6261c639e4e86c01505277094e91f5
(3) 0x083a707a8db041f709830813e1a3404A0815e835a7c563805aa706ff
(4) 77f6407938f98c3ac170d1db45a88309103f7550e4ek11ee2c80cc2c
(5) 57837005d88811e7707c1f071530604053839ca4188421c7e65f498d2
(6) 0374005792ca284a25ac11eecc790835425f7e0b0e381696a20012543
(7) 5c44e0d5f781468f30005f840712b2673491f0a077a8e14221a1f8
(8) 8340b70489a05f5452518086c6ba137456418c3a087309245660a527
(9) 3638511387304c040ee340e04f3f0e91f3609f2d08e8a011e1d0405

Mnemonic: repeat kitten art call plastic talent gather canon cabbage stove find convince
Important: This mnemonic was created for you by Truffle. It is not secure.
Ensure you do not use it on production blockchains, or else you risk losing funds.

truffle(develop) > migrate

Compiling your contracts...
-----
> Compiling ./contracts/Migrations.sol
> Compiling ./contracts/PrivacyContract.sol
> Compilation warnings encountered:
```

In above screen Blockchain started with default accounts and private keys and now type command as 'migrate' and press enter key to deploy contract and get below output

```

C:\Windows\System32\cmd.exe
> Blocks: 0      Seconds: 0
> contract address: 0xB048920F343E31813C96C457D781A1F216C5A
> block number: 1
> block timestamp: 150028035
> account: 0x178641812271E1E6FFA1868483C18313F
> balance: 91.88658281
> gas used: 24954 (0.3115)
> gas price: 2 gwei
> value sent: 0 ETH
> total cost: 0.000497788 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost: 0.000497788 ETH

_deploy_contracts.js
=====
Deploying 'PrivacyContract'
-----
> transaction hash: 0x15149f681265a77c8138980c4881f9151b41296466c1391af38f45440a
> Blocks: 1      Seconds: 4
> contract address: 0x004F45C1c08cF31cbab8848c817040485
> block number: 3
> block timestamp: 150028075
> account: 0x178641812271E1E6FFA1868483C18313F
> balance: 90.88658281
> gas used: 25332 (0.3186)
> gas price: 2 gwei
> value sent: 0 ETH
> total cost: 0.000758384 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost: 0.000758384 ETH

Summary
=====

```

To implement this project we have designed following modules

**Generate Tracking Users Simulation:** using this module we will generate user simulation output

**Calculate User Location & Proximity:** using this module we will make all simulation users to move and then report locations to edge server for computation and if any user violates or comes too close to another user then system will alert them with red colour mark.

**Stop Simulation:** using this will stop simulation

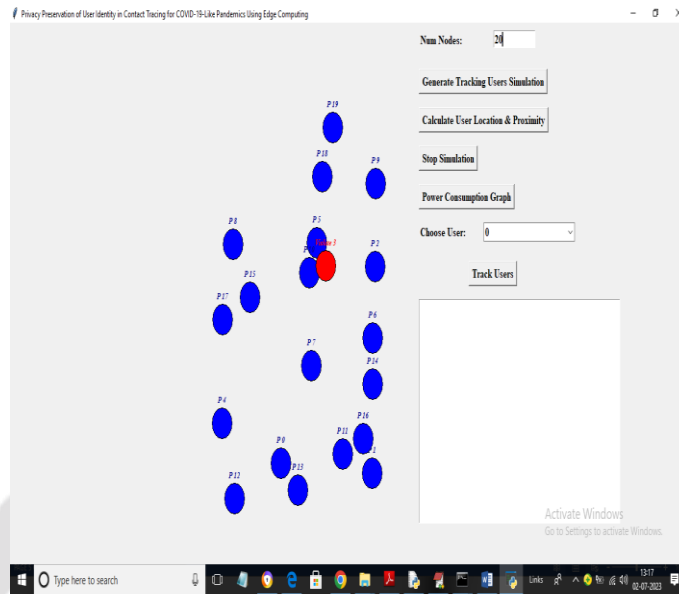
**Power Consumption Graph:** using this we will plot power consumption graph which is consumed using Mobile Processing and Edge Server processing. Apple and Google are using Mobile processing to compute user proximity and in propose work we are using Edge Servers where mobile or sensors will sense data and offload to edge servers which will perform computation and send to Blockchain server for storage

**Trace Users:** using this module government authority can selected desired user and then application will trace all user details with whom selected users comes in contact.

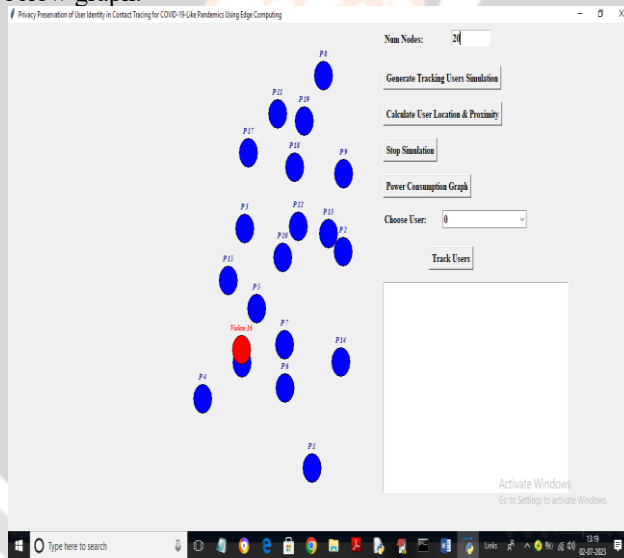
## V. EXPERIMENT RESULTS

In the below screen, first text fields I entered number of nodes or users as 20 and after pressing first button we got above output where each blue colour circle consider as one user and each circle is placed at screen X and Y location which will consider as real latitude and longitude and now click on 'Calculate User Location & Proximity' button to allow users to move and then compute proximity and get below output.

we can see user are moving and if any user comes too close then Edge server will mark or alert him with red colour. Similarly as long as simulation runs then edge server will continue processing.

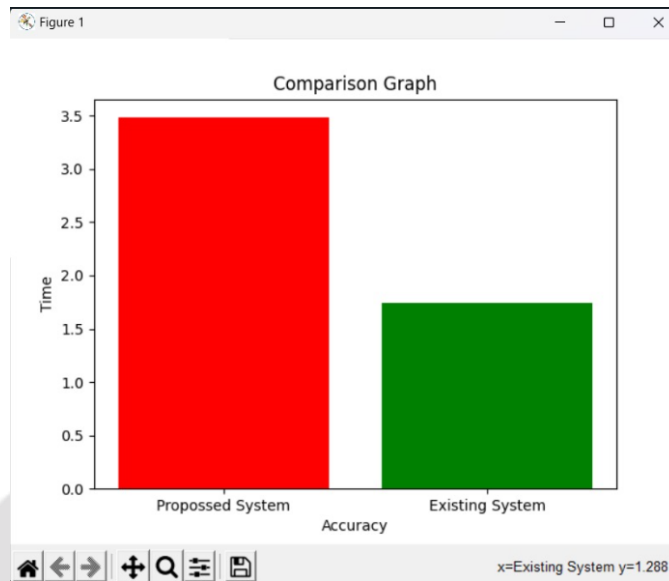


user 16 is violating COVID distancing rules and now click on ‘Stop Simulation’ button to stop simulation and then click on ‘Power Consumption Graph’ to get below graph.



In above graph x-axis represents number of user scan or sending data to edge server and y-axis represents power consumption and red line represents existing Mobile processing technique and green line represents Propose Edge server technique and in both techniques propose is consuming less power and now select desired user from drop down box like below screen.





In above screen in first column we can see selected user ID and his X and Y location and then 4th column we can see other user ID'S with whom this user comes in contact and we can see those users X and Y location with Proximity distance and with date and time.

Similarly by selecting any user we can trace all contacted user details automatically.

User ID	X (Latitude) Location	Y (Longitude) Location	Contact with Other User ID	Other User X Location	Other User Y Location	Proximity Distance	Date & Time
11	207	267	10	179	260	28.861739379323623	2023/07/02-12:43:13
11	269	264	2	257	260	12.649110640673518	2023/07/02-12:43:16
11	437	472	14	426	450	24.596747752497688	2023/07/02-13:18:10
11	297	416	7	303	426	11.661903789690601	2023/07/02-13:20:06

### VI. CONCLUSIONS

To address the crucial privacy-preserving problems in digital contact tracking for the COVID-19 pandemic, a blockchain-enabled approach is suggested. To desensitize the geodata to the user identification, blockchains with encryption allow communication between the client/patient and the approved solvers. To demonstrate the benefits, a comparison of each entity's activities and procedures in detail with those of current solutions is provided. Issues with blockchain performance, complexity of solvers, user storage and battery, and economic and societal factors are also covered. Our numerical findings demonstrate that, in terms of security, privacy, battery life, and coverage, the suggested approach comes out on top overall. In order to defeat the COVID19 pandemic, this solution offers governments, authorities, businesses, and research institutions around the world a timely foundation for creating a reliable platform for information exchange.

## REFERENCES

- [1] A. E. Gorbalenya et al., "The species Severe acute respiratory syndrome-related coronavirus: classifying 2019-nCoV and naming it SARS-CoV2," *Nat Microbiol*, vol. 5, pp. 536–544, 2020.
- [2] "Covid-19 dashboard by the center for systems science and engineering (csse) at Johns Hopkins University (JHU)." [Online]. Available: <https://coronavirus.jhu.edu/map.html>
- [3] M. C. J. Bootsma and N. M. Ferguson, "The effect of public health measures on the 1918 influenza pandemic in U.S. cities," *vol. 104*, pp. 7588–7593, 2007.
- [4] C. C. Harris, Margaret; Adhanom Ghebreyesus, Tedros; Liu, Tu; Ryan, Michael "Mike" J.; Vadia; Van Kerkhove, Maria D.; Diego; Foulkes, Imogen; Ondelam, Charles; Gretler, "WHO audio emergencies coronavirus press conference," 2020. [Online]. Available: <https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-press-conference-full-20mar2020.pdf>
- [5] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy, "BlueTrace : A privacy-preserving protocol for community-driven contact tracing across borders," p. 9, 2020.
- [6] Apple Inc. and Google LLC., "Exposure Notification," May 2020.
- [7] J. Snow and M. Mallon, "The security behind the NHS contact tracing app," pp. 1–14, 2020.
- [8] P. Mozur, R. Zhong, and A. Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," *New York, NY*, 2020. [Online]. Available: <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>
- [9] Neil. Ferguson et al., "Report 9: Impact of nonpharmaceutical interventions (NPIs) to reduce COVID19 mortality and healthcare demand," London: Imperial College London, Tech. Rep., 2020. [Online]. Available: <https://www.imperial.ac.uk/media/imperial-college/medicine/sph/ide/gida-fellowships/Imperial-College-COVID19-NPI-modelling-16-03-2020.pdf>
- [10] M. McKee and D. Stuckler, "If the world fails to protect the economy, covid-19 will damage health not just now but also in the future," *Nature Medicine*, pp. 1–3, 2020.
- [11] "The Coalition for Epidemic Preparedness Innovations. CEPI welcomes UK Government's funding and highlights need for \$2 billion to develop a vaccine against COVID-19," 2020. [Online]. Available: <https://cepi.net/news-cepi/2-billion-required-to-develop-a-vaccine-against-the-covid-19-virus/>
- [12] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dorner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, 2020. [Online]. Available: <https://science.sciencemag.org/content/368/6491/eabb6936>
- [13] India Government, "Aarogya Setu Mobile App," 2020. [Online]. Available: <https://www.mygov.in/aarogya-setu-app/>
- [14] Department of Health Australia, "The COVIDSafe Application," 2020. [Online]. Available: <https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-agency-response.pdf>
- [15] D.-T. task group, "Decentralized Privacy-Preserving Proximity Tracing," no. April, p. 33, 2020.
- [16] P.-P. e.V. i.Gr, "Pan-European Privacy-Preserving Proximity Tracing," 2020. [Online]. Available: <https://www.pepp-pt.org/content>
- [17] P. Voigt and A. v. d. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. Springer Publishing Company, Incorporated, 2017.
- [18] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, 2019.
- [19] H. Xu, P. Klaine, O. Onireti, B. Cao, M. A. Imran, and L. Zhang, "Blockchain-enabled Resource Management and Sharing for 6G Communications," *Digital Communications and Networks*, 2020.
- [20] S. Underwood, "Blockchain beyond bitcoin," Tech. Rep., tech. Rep. 11, Sutardja Center for Entrepreneurship & Technology Technical Report. UC Berkeley (jun 2016).
- [21] C. Bendiksen, S. Gibbons, and E. Lim, "The bitcoin mining network trends, marginal creation cost, electricity consumption & sources," *CoinShares Research*, vol. 21, 2018.
- [22] Apple, "Apple T2 Security Chip," Tech. Rep. October, 2018. [Online]. Available: <https://www.apple.com/euro/mac/shared/docs/Apple-T2-Security-Chip-Overview.pdf>
- [23] Department of Health, "Confidentiality: NHS code of practice," Published following a major public consultation, pp. 1–45, September 2003. [Online]. Available: <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf>
- [24] U. Department Of Defense, "Global Positioning System Standard Positioning Service," *Www.Gps.Gov*, no. September, pp. 1 – 160, 2008. [Online]. Available: <http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf>
- [25] OpenStreetMap, "OpenStreetMap." [Online]. Available: <https://www.openstreetmap.org/>

- [26] European Centre for Disease Prevention and Control, "Contact tracing: Public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union," European Centre for Disease Prevention and Control, Stockholm, Tech. Rep. February, 2020.
- [27] "John the Ripper benchmarks," 2020. [Online]. Available: <https://openwall.info/wiki/john/benchmarks>
- [28] R. Rivest, "The MD5 Message-Digest Algorithm," Tech. Rep., apr 1992. [Online]. Available: <https://www.rfc-editor.org/info/rfc1321>
- [29] Oak Ridge National Laboratory, "ORNL Launches Summit Supercomputer," Oak Ridge National Laboratory, Tech. Rep., 2018. [Online]. Available: <https://www.ornl.gov/news/ornl-launches-summit-supercomputer>.
- [30] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," IEEE Internet of Things Journal, 2019.
- [31] Y. Sun, J. Cao, M. Ma, H. Li, B. Niu, and F. Li, "Privacy-preserving device discovery and authentication scheme

