Privacy-Preserving Contact Tracing and Public Risk Assessment using Blockchain for COVID-19 Pandemic

Paulo Valente Klaine, Lei Zhang, Bingpeng Zhou, Yao Sun, Hao Xu, Muhammad Imran

***Abstract*—Due to the number of confirmed cases and casualties of the new COVID-19 virus diminishing day after day, several countries around the world are discussing on how to return to the *new normal* way of life. In order to keep the spread of the disease under control and avoid a second wave of infection, one alternative being considered is the utilization of contact tracing. However, despite several alternatives being available, contact tracing still faces issues in terms of maintaining user privacy and security, making its mass-adoption quite difficult. Based on that, a novel framework for contact tracing using blockchain as its infrastructure is presented. By integrating blockchain with contact tracing applications, user privacy can be guaranteed, while also providing people and government bodies with a complete public view of all confirmed cases. Moreover, we also investigate how public locations can aid in the contact tracing process by measuring the risk of exposure to COVID-19 to the general public and advertising it in a blockchain. By doing so, these locations can effectively notify of potential infection risks, while also guaranteeing privacy and trustworthiness in the information. Lastly, numerical results are shown in different scenarios and conclusions are drawn.**

***Index Terms*—Blockchain, contact tracing, COVID-19, coronavirus**

I. Introduction

In 2020, the whole world experienced and saw the effects of a pandemic caused by the severe acute respiratory syndrome coronavirus-2, known as COVID-19, with billions of people put into quarantine, self-isolation and full lockdown [1], [2]. However, as the number of infections starts to slowly decline, government bodies are discussing on how to adapt to life after the pandemic, the *new normal*, through maintaining social distancing, wearing masks in crowded spaces, and tracing contacts between people, in order to control the spread of the disease again [2].

Traditional contact tracing is a process in which health staff members help a person to recall everyone they had close contact during the time-frame they may have been infectious [3]–[5]. This is done with the objective of contacting the exposed people and warn them as quickly as possible in order to suppress the spread of the disease and reduce its reproduction rate. However, since traditional contact tracing relies on memory, its accuracy and efficiency are limited. In addition, recent studies show that current healthcare infrastructures are not prepared to perform contact tracing in such large scale, such as the COVID-19 pandemic. In the United States, for example, an additional 50,000 people would need to be hired and trained, while 3.6 billion dollars of funding would be needed [5].

Considering these issues, other contact tracing solutions are being developed and tested all over the world. Examples of solutions used to tackle the COVID-19 pandemic occurred in South Korea and Singapore, where the spread of the disease was controlled by adopting a strategy of test, trace and contain using Bluetooth technology [4], [6]. Another application that relies on Bluetooth is being jointly developed by Apple and Google, in which a random identifier is assigned to different users. This eliminates the need of requiring the user's identity, being more privacy oriented [7]. Another solution is the one from the United Kingdom's national health service; however, it saw several criticisms by the general public in terms of what and for how long data is collected and stored [8]. Other solutions to digital contact tracing (DCT) also exist, such as the utilization of electronic platforms that synchronize healthcare databases and have up-to-date contact information of all patients [3], or the utilization of the global positioning system (GPS) combined with Wi-Fi in order to collect users' location and position [2]. Thus, whenever an individual comes into contact with an infected person the application sends an alert to the person's device.

However, despite technology significantly helping in contact tracing, issues in terms of privacy still remain. In the aforementioned solutions, for example, there is the need to use a third party server to check for contacts and send alerts to users [4], [6], [7]. Moreover, because these solutions are centralized, they can suffer from malicious attacks in order to obtain a person's identity and its contacts, or even to spread fake information or alerts by impersonating health authorities. In addition, there is also the issue of contacts or test results being altered, depending on political or personal interests, or availability of these applications, since privacy laws can be different between countries.

In order to overcome these issues, it is obvious that novel DCT solutions that do not rely on trust of third parties, while keeping users' privacy, are needed. One alternative to overcome these problems is by utilizing blockchain. Blockchain consists of an open and distributed database, where no single party has control and transactions, such as messages ex-

P. Valente Klaine, L. Zhang, Y. Sun, H. Xu and M. Imran are with the James Watt School of Engineering, University of Glasgow, Glasgow, United Kingdom (e-mails: firstname.lastname@glasgow.ac.uk). Corresponding author: Lei Zhang (Lei.Zhang@glasgow.ac.uk)

B. Zhou is with the School of Electronics and Communications Engineering, Sun Yat-sen University, Guangzhou, China (e-mail: zhoubp3@mail.sysu.edu.cn)

changed when there is close contact between two devices, are securely recorded in blocks [9]. Since blockchain does not depend on a central server, it can pave the way for global accessibility of information, while also being more robust to malicious attacks. Blockchain can also enhance data integrity and security, since the information of each block is visible by all participants and cannot be tampered with, reducing the risks of impersonation or altering test results or close contacts [9]. As such, blockchain can play an important role in increasing the trustworthiness of contact tracing applications.

Despite DCT being a good alternative for controlling the spread of the disease, it is only natural that whenever restrictions are lifted, more agglomerations start to occur. In such cases, DCT solutions can be insufficient, thus it is vital that public spaces have some alternative to inform the population about potential risks. Current solutions involve workers monitoring parks, supermarket or shop entrances in order to control the number of people inside. However, from the general public perspective, there is no effective way to monitor if such place is safe or when is the best time to visit such locations in order to minimize the risk of exposure. As such, it is vital that public places aid in the process of contact tracing by monitoring the number of people and calculating a *risk level* depending on certain conditions. However, if the same approaches considered in DCT are applied, similar issues in terms of privacy and trust in third parties arise. In this case, it can be even more concerning, since public locations would not like to advertise their risk levels in order to reduce the number of people, potentially leading to loss of revenue. Thus, it is vital that some sort of control and trustless mechanisms are envisioned in order to keep the general public informed and safe.

Based on that, we propose a framework that integrates blockchain as the underlying infrastructure of DCT and risk assessment in public locations. In DCT messages between users can be exchanged and confirmed cases can be stored in the blockchain, whereas in risk assessment, public locations can advertise their risk levels to the chain, so that it is visible for all participants. Despite [10] being a good example of blockchain applied to DCT, BeepTrace suffers from high computing and complexity when it comes to the architecture with many involved parties. In addition, in contrast to [10], which adopts a passive positioning and contact tracing methodology, using geographical data (BeepTrace-Passive), this paper focuses on Bluetooth as the main technology for positioning and tracing, in what we refer as BeepTrace-Active. Also, in [10] matching is done at the blockchain level, whereas in this paper, we opt to perform matching of contacts at the user mobile phone (local matching). Moreover, in this work we also investigate the role that public areas can play in contact tracing, and provide a novel solution that integrates public locations in the contact tracing process. By leveraging the power of blockchains, the need for a specific company or government to hold contact information is eliminated, data integrity is guaranteed and a more transparent and immutable platform for end-users can be provided. Based on this idea, the main objectives and contributions of the paper are as follows:

- We propose a framework relying on blockchain for DCT, namely BeepTrace-Active, in order to increase user privacy, security and transparency;
- We investigate the idea of public places acting as points of interest and publicizing its information in a blockchain and analyze the number of close contacts in such locations;
- We produce simulation results and analyze the impact and performance of blockchain in DCT, while also providing some guidance on contact tracing solutions.

II. Preliminaries

A. Gain Contact Information

There are many well-developed location sensing solutions for contact tracing, such as Bluetooth, GPS, WiFi-Direct, 4G/5G [2], [6], [10], [11]. Generally, GPS has a good location resolution to sub-meters, while it works poorly in urban areas with buildings or in closed regions like shopping malls [12], whereas WiFi access point-based localization is applicable for indoor positioning. On the other hand, in outdoor regions, where WiFi is unavailable, cellular networks like 4G and the upcoming 5G, can be considered.

However, one of the most popular methods for DCT utilizes Bluetooth, a short-range device-to-device solution, which provides connectivity information of carrying devices between people. Specifically, Bluetooth provides contact information for devices based on their connectivity states [13]. The sensing range of Bluetooth is of approximately 10 meters, and devices in the same Bluetooth area are considered to be close to each other in location. WiFi-direct, another device-to-device solution, is similar to Bluetooth, while its sensing range is of 50 to 100 meters [14]. Naturally, a large sensing range covers more devices, and hence more people can potentially be identified. Therefore, it leads to an overestimation of contacts, increasing the length of contact list of confirmed cases, while the increased burden is affordable.

Unlike Bluetooth, which actively exchange messages between two devices, GPS, cellular and WiFi solutions provide location estimates, which can be translated to contact information, such as when two people come into close contact with each other. However, GPS and cellular device localization methods face serious concerns in terms of user privacy during the location collection process and have to involve significantly complex encryption to protect such systems [10]. Thus, in this article, only Bluetooth and WiFi-direct based device-to-device connection for managing people contact information are considered. Since both Bluetooth and WiFi-direct can be used to gain connectivity information of a user device to its nearby devices by broadcasting messages with each other, without requiring location labels of devices or user identities, user privacy is protected.

B. Blockchain

Blockchain has been proven a powerful tool in multiple industries including finance, supply chains, energy trading, IoT, and cryptocurrencies, due to its advantages [9]:

- Replacing a central authority by a distributed one, improving security and reducing costs;

- All information stored in the blockchain is immutable, which allows every participant to have access to this permanent record of events and prevents the data being tampered;
- Removing the risk of fraudulent messages and also providing greater transparency and efficiency to the general public.

Blockchain consists of a distributed ledger that keeps everyone's data in an open, auditable, and tamper-proof distributed storage solution, solving trust and transparency issues with user privacy and accessibility in mind [10]. Blockchain is a chain-like data structure consisting of blocks with a header and a body, where the chain is organized using a hash tree [9]. Each block has a header with hash value associated to the previous block's content, establishing a retroactive connection from the latest block to the genesis block, the first block in the chain. It provides an unbreakable linkage to the fully traceable records in the order of blocks, as such, users can verify the integrity and authenticity of any known block by calculating the hashed value and comparing it with the next block. Thus, any changes to the previous block will tamper its integrity, leading to a verification failure.

Every participant in the network holds a copy of the data, in order to locate the latest block on the longest chain, which makes the network distributed. Besides its unique data structure, the basis of blockchain's trust comes from a collective effort, the Consensus Mechanism (CM). Due to the special needs of DCT, different blockchain CMs, such as, Proof-of-Stake/Work and voting based mechanisms (practical Byzantine fault tolerance) can be used [15]. The former is better in terms of scalability, while the latter shows supremacy in terms of transaction per second and confirmation delay. However, as it will be verified by our simulations, both CMs are applicable to DCT, with varying performance depending on the number of confirmed patients or required notification speed.

III. Proposed Solution

A. Architecture

A high-level architecture of BeepTrace-Active, our blockchain-based privacy-preserving contact tracing, is illustrated in Fig. 1. As shown, there are three identities including (i) on-device personal blockchain-based DCT application, (ii) blockchain, (iii) hospital (or similar health authority).

The function of each identity is summarized as follows:

- **On-Device Personal Application**: The application takes charge of contact list management and case inquiry. Based on the real-time information from Bluetooth or WiFi-direct, the application creates a contact list for users, in case they had a close contact or were in the same public area at the same time. The application is also responsible for inquiring the blockchain to check for potential matches between the positive cases recorded in blockchain and the ones stored locally.
- **Blockchain**: The blockchain records the pseudo-IDs of confirmed cases based on medical reports from health authorities. In addition, its data is open for case inquiry from the application.
- **Health Authorities**: The health authorities take charge of conducting virus tests of potentially infected people. Health personnel upload the pseudo-IDs of positive cases to the blockchain, forming a transparent and unalterable record of positive case IDs.

As shown in Fig. 1, the workflow of the proposed scheme is described as follows:

- *(Step 1) Generate Pseudo-ID*: The application of each user periodically generates a temporary pseudo-ID (e.g., on each day or each hour). This ID includes a series of random letters, used to distinguish users, and the created time stamp. Since it is periodically generated at random, it prevents the user location from being tracked, preserving user privacy. Even, when health authorities upload the information to the blockchain, only the pseudo-IDs of confirmed patients are visible, fully preserving their identities. Moreover, to avoid privacy leakage by people monitoring a device's Bluetooth name, other protective measures can be taken, such as the DCT application periodically changing the Bluetooth name together with the pseudo-IDs, as in [6].
- *(Step 2) Broadcast Pseudo-IDs:* During the wireless connection period of a user's mobile phone using either Bluetooth or WiFi-direct, the ID is distributed to its neighbors connecting with the UE's mobile phone.
- *(Step 3) Form Contacts List*: A user can receive multiple IDs in proximity in one day, and the application stores these IDs locally, forming a contact ID list for this user. As it will be shown in our simulations, the amount of data required per day is less than half of an MB, thus the proposed scheme would not require more than a couple MB to store a couple of weeks worth of data.
- *(Step 4) Virus Test*: At any given time, people can go to a hospital to perform a virus test.
- *(Step 5) Upload Positive Cases*: In case a person is tested positive, health authorities are responsible for uploading the IDs of confirmed cases. Since pseudo-IDs change frequently, the application should also store the most recent used IDs (in the last 14 days, for example). Thus, it can upload all its previously used pseudo-IDs to the blockchain.
- *(Step 6) Record Positive Cases*: The blockchain includes the IDs of those positive cases in a new block, recording the list of all positive-case IDs. Since these IDs do not have any personal information and block generation is distributed, there is no privacy concern.
- *(Step 7) Periodic Update*: The application downloads data from the blockchain (e.g., on a daily basis). This data consists of the pseudo-IDs of all people who have tested positive during that day.
- *(Step 8) Local Matching*: The application compares if any of the pseudo-IDs downloaded from the blockchain is present in the contact list created in the user's mobile phone. Since this process is performed locally in the mobile phone, it is also privacy preserving.

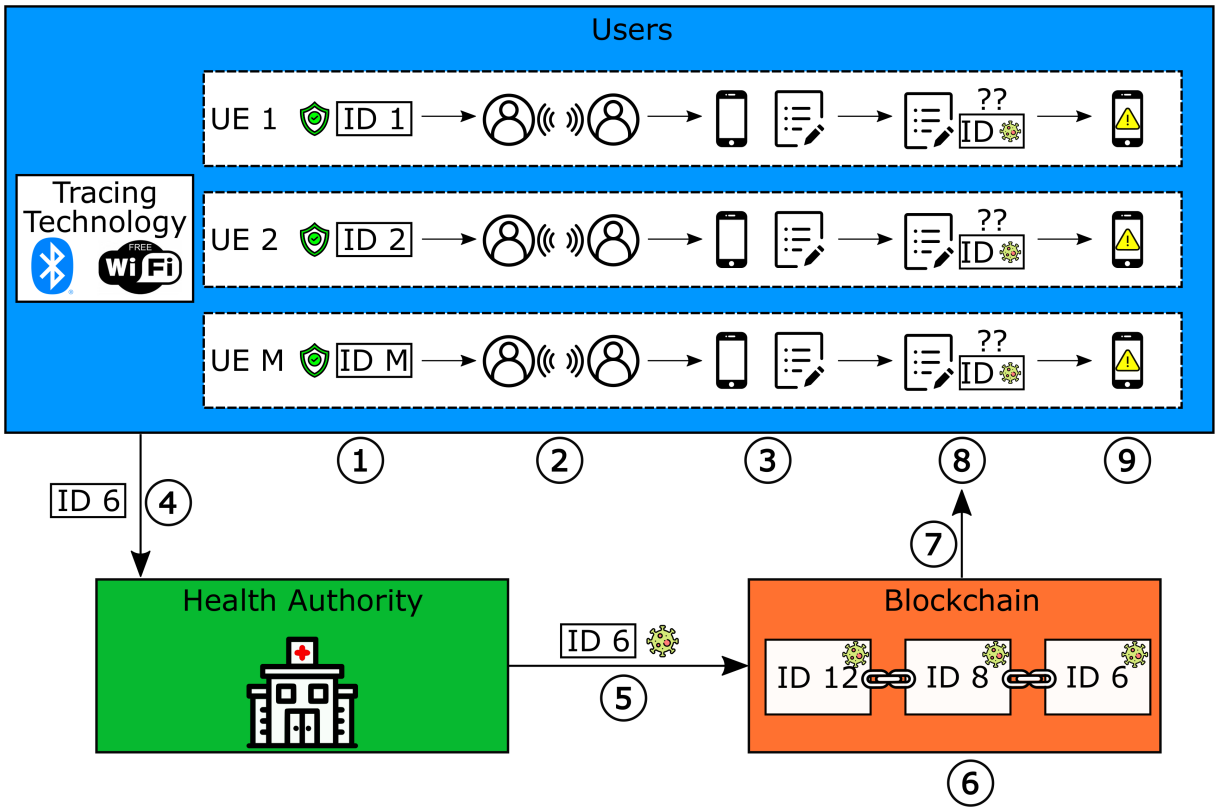


Fig. 1. Architecture of BeepTrace-Active, the proposed blockchain-based privacy-preserving DCT.

- *(Step 9) Alert Generation*: If the local matching returns any positive result, the user is alerted by the application, indicating to the user a high likelihood of exposure to COVID-19.

B. Public Areas

In addition to involving people in contact tracing, the possibility of risk level alerting for public areas, such as shops, malls, or pharmacies to aid in DCT is also investigated. Since these locations often act as gathering points, they can play an important role in informing users about the risk of visiting such places by, for example, estimating how many people are at the location at any given time, the average distance between people (given by the average number of people divided by the area), or by informing if there were any recent confirmed cases in the vicinity.

However, trusting third parties can be an issue, since such locations would try to avoid publicizing information due to personal, economical or political interests. In order to solve such issues and increase the trustworthiness of public areas, while also providing a safe environment for the general public, the utilization of blockchain as the infrastructure for the dissemination of such information is proposed. Based on that, public areas could have a metric, or a *risk level*, which could inform the public about the overall risk of exposure to COVID-19. For example, whenever shops are crowded, the shop's risk level would be increased and uploaded to the blockchain, so that users know that certain locations are riskier than others. This can be used to not only attract customers to certain locations, whenever the risk level of shops are low, but also to limit the amount of people that visit such locations.

The proposed workflow of the scheme is as follows:

- **People counting:** Based on the number of Bluetooth or WiFi-direct connections received by the hotspot of the building, the number of people staying within this area can be estimated. Because only the number of available connections is monitored, users can change pseudo-IDs without affecting the accuracy of the estimate.
- **Risk assessment:** Based on the obtained population information, the infection risk level of this area can be briefly estimated, in which a large population implies a high risk level. In addition, public locations can also have access to the pseudo-ID blockchains, in order to periodically download data and determine if any person that has visited the place recently tested positive for COVID-19. In case of a confirmed positive visit in the last 14 days (according to the World Health Organization – WHO, guidelines), the risk level of such locations can be increased and all pseudo-IDs that have visited the location can be notified.

Thus, our scheme can be used together with on-site review of health authorities on infected people for their recent contacts, improving the efficiency of DCT. Moreover, by integrating

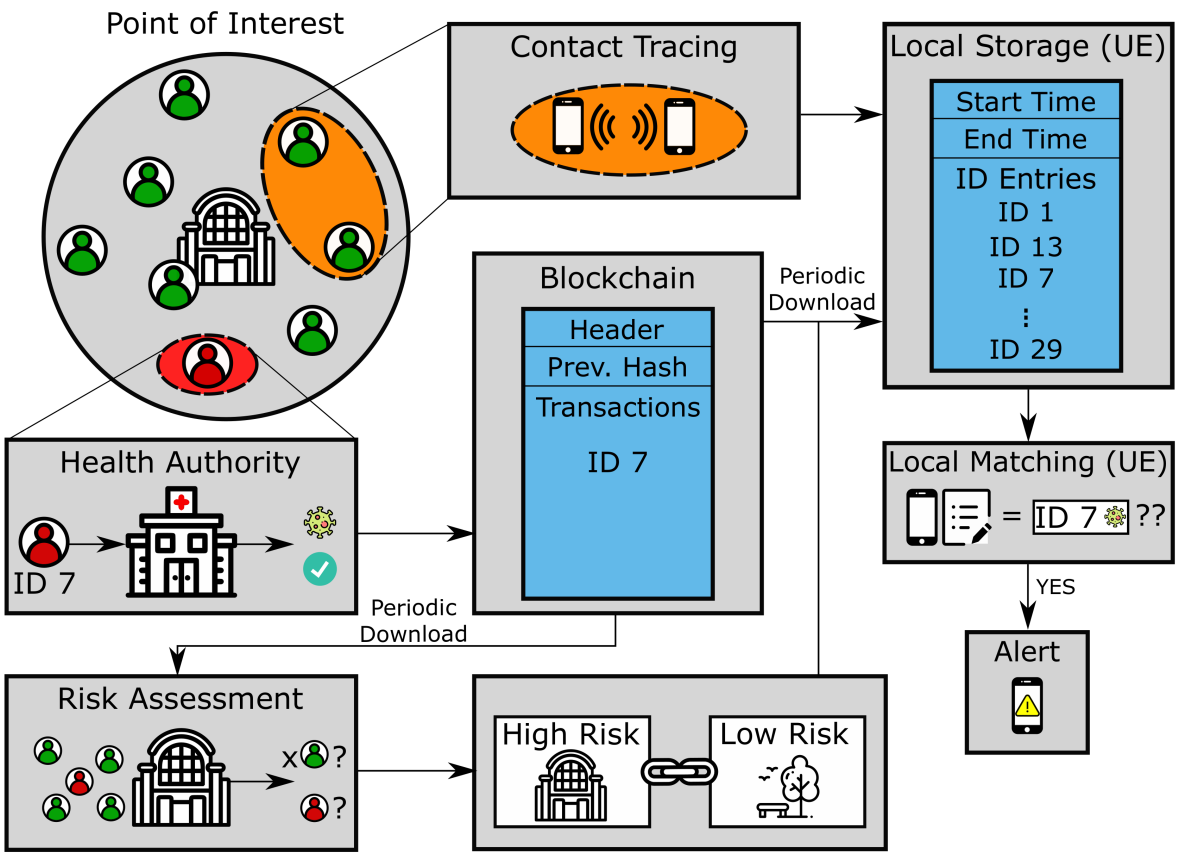


Fig. 2. Framework for blockchain as an infrastructure for both DCT and public risk assessment.

public areas in the DCT process, it can bring significant benefits in order to quickly and effectively control the spread of the disease, as more people can be alerted.

C. Blockchain Procedure

In BeepTrace-Active we use blockchain as the medium for information broadcasting, and storing the pseudo-IDs supplied by confirmed patients. The local storage identified in Fig. 2 is a list of all pseudonyms by users, it is worth noting that the user personal information is never shared in any case, avoiding privacy leakage. By publishing the pseudo-IDs via blockchain, the data is protected by it with ultimate privacy-preservation, as the access information is not trackable if a user matches the record in locally. This leaves the user with more security and privacy, and eliminates the possibility of malicious manipulations of test results. In addition, Fig. 2 also shows how public locations can advertise information in the blockchain. By estimating the number of people in a determined location, or by periodically downloading data from the blockchain, the risk of public locations can be determined and uploaded to a separate chain. This data can also be downloaded by users, so they can assess the risks of going outside or visiting certain places. Despite blockchain being widely used as a distributed ledger for recording information agreed by different parties that perform transactions, in this manuscript the application scenarios of blockchain are further extended. By integrating blockchain into DCT, confirmed COVID-19 cases can be published in the chain, allowing a tamper-free and public access to this data in order to perform local matching. This enhances user privacy, minimizes misinformation and can also lead to an increase trust and, potentially, to the adoption contact tracing, benefiting millions of people and mitigating the impact of future pandemics.

IV. Simulation Results

In this section, the performance of BeepTrace-Active is evaluated. We first illustrate the simulation settings of this work, and then compare results of two contact tracing technologies, Bluetooth and WiFi-direct tracing. The following three metrics are utilized to compare the two solutions:

1) Number of average close contacts: the total number of contacts stored in the user's mobile phone, sensed in the last 14 days.
2) Mobile phone storage required per day: the amount of data that each user needs to store every day, generated by close contacts. This data is used for conducting a mapping with daily confirmed cases, and is calculated by multiplying the number of transactions (number of daily confirmed cases) by the size of each transaction.
3) Number of required transactions per second: the number of transactions per second in the blockchain network to support our DCT mechanism.

A. Simulation Settings

We set the population density as $3333.3/km^2$, the same as the city of Glasgow. We set a total of 200 hotspots (such as shopping malls, supermarkets, and parks) where people can visit. Due to the special situation of COVID-19, we assume that each user travels at most once per day and the probability of a specific user to go out for a trip is set to p, which is related to personal habit, government policy, the current situation, etc.. In this simulation, we use two values $p = 0.2$ and $p = 0.6$ to denote *low-activity* and *high-activity* scenarios, respectively. The trips can start at any given time, and their durations are randomly distributed, 1–4 hours. The total simulated time in all scenarios is of 14 days.

For the two tracing methods considered in this paper, the range (the radius of sensing area) is set as 10 and 50 meters for Bluetooth and WiFi-direct, respectively. The sensing frequency for both methods is set as 1 minute, meaning that each outdoor user broadcasts his/her own temporary ID every minute. For the pseudo-IDs, it is considered that they change at every half an hour, for the sake of privacy preserving. Regarding the blockchain, only the pseudo-IDs (of recent 14 days) of confirmed cases are recorded into blocks as a transaction. We set the length of a pseudo-ID to 64 bytes and the time of transaction arrival is randomly distributed as the randomness of the time distribution of confirmed cases in our system.

B. Simulation Results

Fig. 3 shows the number of average close contacts of the two tracing methods for a varying number of users. We can see that the number of close contacts of the two tracing methods increase approximately linearly with the number of users. This occurs because the same population density is assumed throughout this experiment. Furthermore, we find that the number of close contacts of WiFi-direct tracing is 1 to 2 times larger than that of Bluetooth, although the sensing area is 25 times larger. This implies that increasing the sensing range is not an efficient way for contact tracing. This occurs because of an unbalanced user distribution, where more people gather around hotspots, thus, increasing the sensing range is not very effective in non-hotspot areas. Moreover, based on calculations, we find that under the same sensing method (Bluetooth or WiFi-direct), the number of close contacts in the high-activity scenario is up to 8 to 10 times larger than that of the low-activity scenario, even through the travel probability is only 2 times higher.

Fig. 4 compares the cumulative distribution function (CDF) of required storage of both tracing methods under the two activity levels. We can see that the amount of storage under all four scenarios is always less than 0.4MB. Moreover, considering that there is also the possibility of the application deleting the data after a certain number of days, these numbers demonstrate that BeepTrace-Active requires only a little amount of storage (up to several MBs in 14 days). We also estimate how much data needs to be downloaded from the blockchain on a daily basis. Given that users are active only 8 hours per day, the size of a pseudo-ID is 64 bytes, and pseudo-IDs change twice per hour, a single person produces exactly

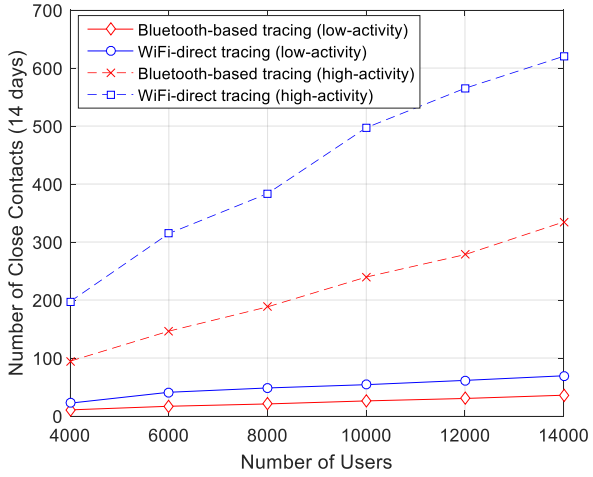


Fig. 3. Number of close contacts vs. Number of users.

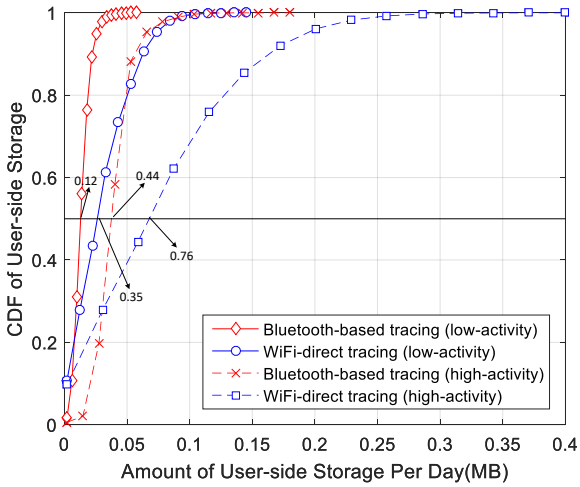


Fig. 4. CDF of per day storage required at a user's mobile phone.

1KB of data per day. Given that whenever a user tests positive it needs to upload the pseudo-IDs used in the last 14 days, it can be concluded that a positive case generates 14KB of data. Considering that in most small countries, such as in Europe, after restrictions were lifted, the peak of COVID-19 cases is of about 3,000 cases, we estimate that no more than 42MB of data needs to be downloaded everyday. In more extreme cases, such as when the COVID-19 pandemic was at its worse and the number of cases in countries reached 10,000 or 20,000 per day, the blockchain can also have a location stamp, so that only users of that region download its data, drastically reducing the download size.

Lastly, Fig. 5 shows a key performance metric in blockchain networks, the transactions per second (TPS), against a different number of daily confirmed cases, starting at $1,000$ (typical value for a specific country) up to $200,000$ (typical value for the whole world). Note that the number of TPS is not related to the two sensing methods, thus the results of the two methods should be the same, shown as Fig. 5. As expected, we find that the number of TPS increases linearly with the

number of daily confirmed cases (sudden changes occur due to the non-linearity of the X-axis, which is set for an easier comparison). Specifically, the number of TPS of high and low-activity scenarios is about 30 and 10 respectively when the number of daily confirmed cases is $8,000$. Moreover, even for the whole world, in the scenario of $200,000$ daily confirmed cases, we calculate that the required number of TPS is about 75 and 63 for both high and low-activity scenarios. These numbers reveal that the number of TPS is not the bottleneck of the proposed DCT system, since even traditional PoS-based blockchain can achieve more than 100 TPS [15].

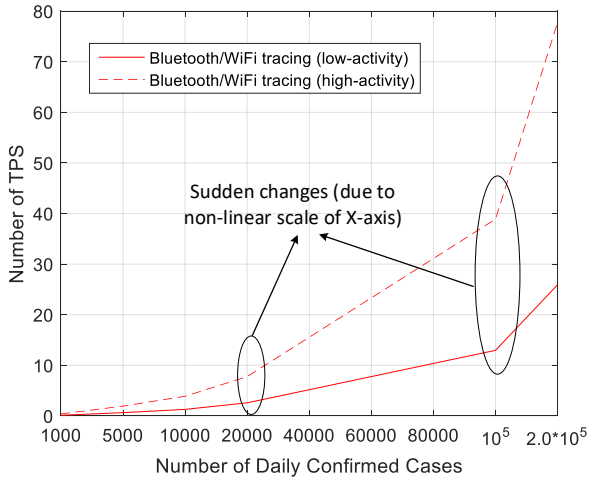


Fig. 5. Number of TPS vs. Number of daily confirmed cases.

V. Conclusions

In this article we overviewed current solutions for contact tracing and the most popular tracing methods. We have shown that contract tracing has several privacy issues and have presented a novel framework based on blockchain in order to preserved the privacy for DCT. Based on this framework, we have presented a framework on how blockchain can act as the underlying infrastructure behind DCT and increase the trust and privacy of its users, named as BeepTrace-Active. We have also investigated how public locations can aid in DCT, specially in publicly advertising their *risk levels* in order to alert people on which locations are safe and which ones are not. Based on these conditions, we analyzed the performance of the proposed solution under different scenarios, and have demonstrated that BeepTrace-Active is valid and efficient for DCT in the battle against COVID-19.

References

[1] W. H. Organization *et al.*, "Coronavirus disease 2019 (covid-19): situation report, 85," 2020.

[2] A. Hekmati, G. Ramachandran, and B. Krishnamachari, "Contain: Privacy-oriented contact tracing protocols for epidemics," *arXiv preprint arXiv:2004.05251*, 2020.

[3] K. T. Eames, C. Webb, K. Thomas, J. Smith, R. Salmon, and J. M. F. Temple, "Assessing the role of contact tracing in a suspected h7n2 influenza a outbreak in humans in wales," *BMC infectious diseases*, vol. 10, no. 1, p. 141, 2010.

[4] The Government of the Republic of Korea, "How Korea responded to a pandemic using ICT: Flattening the curve on COVID-19," 2020.

[5] C. Watson, A. Cicero, J. Blumenstock, and M. Fraser, "A national plan to enable comprehensive COVID-19 case finding and contact tracing in the US," 2020.

[6] 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," *Government Technology Agency-Singapore, Tech. Rep*, 2020.

[7] Apple, Google, "Privacy-preserving contact tracing," 2020. [Online]. Available: https://www.apple.com/covid19/contacttracing

[8] "NHS COVID-19 app," https://www.nhsx.nhs.uk/covid-19-response/nhs-covid-19-app/, accessed: 2020-05-24.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[10] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. B. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and Beyond," may 2020. [Online]. Available: http://arxiv.org/abs/2005.10103

[11] A. L. Greiner, K. M. Angelo, A. M. McCollum, K. Mirkovic, R. Arthur, and F. J. Angulo, "Addressing contact tracing challenges—critical to halting ebola virus disease transmission," *International Journal of Infectious Diseases*, vol. 41, pp. 53–55, 2015.

[12] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 427–450, 2009.

[13] P. Kriz, F. Maly, and T. Kozel, "Improving indoor localization using bluetooth low energy beacons," *Mobile Information Systems*, vol. 2016, 2016.

[14] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "3gpp lte traffic offloading onto wifi direct," in *2013 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2013, pp. 135–140.

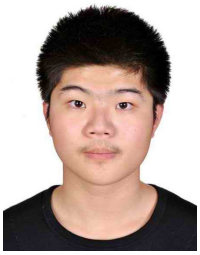
[15] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2018, pp. 1545–1550.

Paulo Valente Klaine (S'17, M'19) received his B. Eng. degree in electrical and electronic engineering from the Federal University of Technology - Paraná (UTFPR), Brazil in 2014, the MSc. degree from the University of Surrey, Guildford, U.K., in Mobile Communications Systems in 2015, and the PhD degree in Electrical and Electronics Engineering from the University of Glasgow, U.K., in 2019. He has 3 filed patents and authored/co-authored over 15 publications. He is currently a research associate at the University of Glasgow, U.K., and his research interests include self organizing networks, V2X communications, wireless blockchain and machine learning in wireless networks.

Dr. Lei Zhang (SM'18) is a Senior Lecturer at the University of Glasgow, U.K. His research interests include wireless communication systems and networks, blockchain technology, data privacy and security, etc. He has 19 patents granted/filed in more than 30 countries/regions. Dr Zhang has published 2 books and 100+ peer-reviewed papers. He received IEEE ComSoc TAOS Best Paper Award 2019. Dr. Zhang is a Technical Committee Chair of 5th International conference on UK-China Emerging Technologies (UCET) 2020. He is an associate editor of IEEE Internet of Things (IoT) Journal, IEEE Wireless Communications Letters and Digital Communications and Networks.

Bingpeng Zhou (16'S-17'M) received his PhD degree from Southwest Jiaotong University, Chengdu, China, in 2016. He was a Postdoctoral Fellow with the Hong Kong University of Science and Technology, Hong Kong, China, from 2016 to 2019. Prior to this, he was a Visiting Ph.D. Student at the 5G Innovation Centre, University of Surrey, Guildford, U.K. in 2015. Bingpeng Zhou is currently an Associate Professor with the School of Electronic and Communication Engineering, Sun Yat-sen University, Guangzhou, China. His research interests include visible light-based positioning, 5G wireless localization and intelligent internet-of-vehicles.

Yao Sun received the B.S. degree in Mathematical Science, and the Ph.D. degree in Communication and Information System, both from University of Electronic Science and Technology of China (UESTC), in 2014 and 2019, respectively. Dr. Sun is currently a Lecture with the University of Glasgow, Glasgow, UK. Before that, he was a research fellow with UESTC, Chengdu China. Dr. Sun has extensive research experience and has published widely in wireless networking research. He has won the IEEE Communication Society of TAOS Best Paper Award in 2019 ICC. His research interests include intelligent wireless networking, Internet of Things, blockchain system, network slicing and resource management in mobile networks.



Hao Xu is pursing PhD at the Communications, Sensing and Imaging CSI Research Group, School of Engineering, the University of Glasgow, U.K. He received his MSc Aerospace Vehicle Design (Avionics) with distinction from Cranfield University, and BEng (Aerospace/Avionics) from the University of Sheffield. His research interests covers wireless communication and wireless blockchain consensus.

Muhammad Ali Imran (M'03, SM'12) Fellow IET, Senior Member IEEE, Senior Fellow HEA is Dean University of Glasgow UESTC and a Professor of Wireless Communication Systems with research interests in self organised networks, wireless networked control systems and the wireless sensor systems. He heads the Communications, Sensing and Imaging CSI research group at University of Glasgow and is the Director of Glasgow-UESTC Centre for Educational Development and Innovation. He is an Affiliate Professor at the University of Oklahoma, USA and a visiting Professor at 5G Innovation Centre, University of Surrey, UK. He has over 20 years of combined academic and industry experience with several leading roles in multi-million pounds funded projects. He has filed 15 patents; has authored/co-authored over 400 journal and conference publications; has edited 7 books and authored more than 30 book chapters; has successfully supervised over 40 postgraduate students at Doctoral level. He has been a consultant to international projects and local companies in the area of self-organised networks.