Blockchain and Contact Tracing Applications for COVID-19: The Opportunity and The Challenges

Mohamad Kassab[1], Giuseppe Destefanis[2]
[1]*Pennsylvania State University*, Malvern, PA, U.S.A.
muk36@psu.edu
[2]*Brunel University*, London, U.K.
giuseppe.destefanis@brunel.ac.uk

***Abstract*—Contact tracing mobile applications have been emerging as potentially automating surveillance technology to help stem the spread of the novel coronavirus (SARS-COV-2) by tracking individuals and those they come into exposure with. The avalanche of these apps left the software security researchers' with concerns about vulnerabilities in hastily written software. On the other hand, the COVID-19 pandemic has motivated the recent interest of leveraging blockchain for healthcare-related scenarios, including proposing and developing blockchain-based contact tracing apps. Utilizing the cryptographic concepts of blockchain to secure the collected data could help in winning the level of public engagement required to fight the spread of COVID-19. But will blockchain be a panacea to all the challenges accompanying these apps? Motivated by answering this question and following a twofold process, this paper: (i) explores the current landscape of contact tracing mobile apps, (ii) examines how blockchain technology can contribute positively to this landscape, and (iii) reports on the technical and social challenges that still accompany the deployment of blockchain-based contact tracing apps.**

***Index Terms*—Blockchain; COVID; Contact Tracing; security; performance.**

I. Introduction

Since the genesis case was confirmed in Wuhan, China, in late 2019, the novel coronavirus (SARS-COV-2) that causes the Coronavirus Disease 2019 (COVID-19) has spread all over the world at an unprecedented rate. The epidemic has worsened to the extent that the World Health Organization (WHO) declared the situation a pandemic by March 11, 2020. By end of November 2020, the number of reported COVID-19 cases surpassed 60 million worldwide according to the data from John Hopkins University & Medicine Corona Virus Resource Center [1]. Almost immediately, public health systems began struggling to treat incoming patients with symptoms, delivering syndromic and disease surveillance, and performing clinical research for vaccinations and medical treatment.

In lieu of an existing vaccine, the large-scale deployment of digital surveillance has become a "beacon of hope" in curbing the pandemic. Digital surveillance has been deployed to i) track confirmed and potentially impacted cases with the virus, ii) enforce lockdown when necessary, and iii) generate a much-needed source of data and statistics to the authorities.

Smartphone-enabling technologies such as Bluetooth, RFID tracking, built-in sensors, and NFC allow it to be an integral part of the digital tracking sphere. Starting the month of April 2020, we saw an avalanche of contact tracing mobile apps to help stem the spread of the virus by tracking individuals and those they come into exposure with.

While these apps may have slightly different approaches on how tracing contacts, at their core, they are tracking programs using Bluetooth or GPS to track an individual's exposure to cases. Users elect to share data and are alerted if they have been within proximity to COVID-19 cases. If an individual is found to be infected with the virus, all of the people that have recently been near him/her are alerted and asked to follow the public health authorities' guidelines. Not all existing contact-tracing apps serve as digital tracking applications from the authority perspective. Depending on the design, public health authorities may (or not) receive data that users choose (or asked) to share to enhance contact tracing.

While several countries are racing to develop contact tracing apps to control the COVID-19 virus spread, the mad dash has left some places with a confusing mishmash of options and the software security researchers' community has worried about vulnerabilities in hastily written software. Indeed, little contemporary data exists that documents the landscape of these applications.

Conversely, despite the privacy concerns, recent studies have shown that users have felt more comfortable to use contact-tracing apps as the pandemic proceeds. For example, a survey was conducted by Metova firm, a leading provider of custom software solutions for IoT, with 2000 residents of the United States on contact tracing and exposure notification apps use in the fight against COVID-19. The survey found 77% of participants would want to be notified via their mobile phone if someone they recently came in contact with was tested positive for COVID-19, and 85% are willing to anonymously share a positive COVID-19 status for the greater good [2].

Surprisingly, and despite the reports indicating the high level of willingness among the general population to download contact tracing apps, and share data through [2], the actual numbers of downloads is still relatively slim. A recent study by the University of Oxford's Big Data Institute estimates

978-1-7281-9630-5/21/$31.00 ©2021 IEEE
DOI 10.1109/SANER50967.2021.00092

that at least 60% of the population in a given area would need to use an automated contact tracing apps for it to be considered effective in containing the virus [3]. On March 20, 2020, Singapore became one of the first countries to deploy a voluntary contact-tracing app, "TraceTogether" [4] but only about 26% of the population had it installed two months after its inauguration. While some level of compliance is still better than none, the low rates of adoption in parts of the world is a challenge for these apps to provide any breakthrough.

With the growing recognition of the distributed nature of health services, the technology of blockchain has enjoyed substantial deliberation in the past three years from the healthcare sector to implement numerous healthcare scenarios on the top of a blockchain [5]. The COVID-19 pandemic has incentified the recent interest of leveraging blockchain for healthcare-related scenarios, including proposing and developing blockchain-based contact tracing apps. While utilizing the cryptographic concepts of blockchain to secure personal data collected from these apps could help in winning the level of public engagement required to fight the spread of COVID-19, a question arises: Will blockchain be a panacea to the challenges accompanying these apps?

Motivated by answering the above question, three sub-research questions emerge:

- **RQ1**: What is the current landscape of contact tracing mobile apps?
- **RQ2**: How blockchain technology can contribute positively to this landscape?
- **RQ3**: What are the current technical and social challenges that accompany the deployment of the blockchain-based contact tracing apps?

To answer these questions, a twofold process was followed:

1) A sample of 52 contact tracing mobile apps that are already deployed or currently in development in different countries was scrutinized. The sample included 5 blockchain-based apps.
2) A search was executed in November 2020 on LionSearch engine using the string: "(Covid) and (contact tracing) and (blockchain)". LionSearch is an integrated search engine that is provided and maintained by the Pennsylvania State University's Library and it aggregates search results from over 950 database/search engines. The search retrieved 225 articles, including peer-reviewed and newspaper articles. The search was followed by conducting a deductive content analysis [6] on the extracted articles from the above search.

This paper presents a contemporary view of the results of the analysis following the above process along with a discussion on the implications and the future research avenues to pursue.

The remainder of this paper is structured as follows: Section 2 provides the background and related work. Section 3 presents the findings from the analyzed sample of apps, while Section 4 provides an overview of proposed blockchain-based mobile apps and discusses how blockchain can contribute to this landscape. Section 5 presents the technical and social challenges, and finally Section 6 provides the Conclusion.

II. Background

A. What is Blockchain?

Blockchain is a type of distributed ledger technology. New entries are added by appending them to the end of the ledger. Therefore, the ledger built is a chronological chain of data blocks, which justifies the name assigned to the technology. Blockchain technology is characterized by the **CoDIFy-Pro** principles. The uppercase characters represent the five principles that guide the blockchain technology: **Co**nsensus, **D**ecentralization, **I**mmutability, **F**inality, and **Pro**venance, explained as follows.

Consensus and Decentralization. A blockchain consists of a set of nodes connected through a peer-to-peer network. Each node in the network maintains an exact copy of the blockchain creating a decentralized structure. When a new block is presented to the chain, all the nodes of the network need to reach a consensus on the validity of that block. The consensus mechanisms are protocols that ensure all nodes on the network are synchronized with each other and agree on which transactions are valid (and only those are added to the blockchain). These consensus mechanisms are critical for a blockchain to work correctly. Examples of deployed consensus mechanisms include Proof of Work, Proof of Stake, Proof of Capacity, Proof of Human-Work, Proof of Activity, Proof of Authority, and Proof of Elapsed Time.

Immutability. Blocks on the blockchain can't be modified or deleted (in contrast with a traditional relational database). Each block contains a cryptographic hash and a timestamp creating an immutable record of all the transactions in the network.

Finality. A single and shared ledger provides one unique place to determine ownership of an asset or completion of a transaction.

Provenance. Network participants have access to the knowledge of where an "asset" came from and how its ownership changed over time.

A blockchain can also be both permissionless or permissioned. A public blockchain is permissionless where anyone can join the network. A private blockchain is permissioned network that will require the pre-verification of the participants. A blockchain containing Electronic Health Records (EHRs) is a potential use case for a permissioned blockchain, for example.

B. Related Work on Blockchain to Combat COVID-19 Pandemic

In a previous work [5], multiple views were presented from a systematic literature review on existing peer-reviewed studies on utilizing blockchain solutions in the healthcare domain. In that review, 52 extracted primary studies were mapped into five healthcare-related scenarios. At the time, only 17 studies presented already implemented solutions in practical settings. A summarized mapping of the 52 studies is provided through the link "https://bit.ly/32dJ0MS".

With the COVID-19 outbreak, blockchain's research and practitioners communities have been stimulated to conceive solutions to combat the pandemic. In [7] the authors provided a brief abstract recommending blockchain for sharing COVID patients' diagnostic information, managing monetary donations, and preventing the spreading of false information regarding infectious diseases. Nguyen and colleagues [8] provided a view on the research efforts and applications utilizing blockchain and AI technologies to combat the COVID-19 pandemic. Their work cover scenarios exclusively related to tracking, user privacy, safe operation, and supply chain.

Pragmatic surveillance blockchain-based solutions to combat COVID-19 are also emerging and include:

- **MiPasa**: Cointelegraph reported on March 28, 2020, that the WHO joined forces with IBM, Oracle, Microsoft, and the enterprise firm HACERA in building the open data hub called MiPasa on the top of Fabric hyperledger [9]. The tool uses various data sources and analytic tools to detect and recognize COVID-19 infection hot spots.

- **HashLog**: With the help of public data from the US Centers for Disease Control and Prevention (CDC) and WHO, Acoer's HashLog visualization engine interacts in real-time with Hedera Hashgraph's distributed ledger technology to ensure real-time logging and data visualization of the spread of the disease [10]. Each transaction is recorded through a verified hash reference on Hedera's ledger which provides epidemiologists with legitimate data.

Given that the COVID-19 outbreak is still recent, there is a scarcity of peer-reviewed studies particularly investigating the potential of blockchain to combat the pandemic. The world experienced deadly virus outbreaks over the recent years (e.g., SARS (2002-2004), Ebola (2013-2016), Zika (2015-2016)), and there have been some studies proposing blockchain solutions for tackling the surveillance scenario for communicable diseases (e.g., [11], [12]). The difference with COVID-19 is that it's much more contagious than the others. For example, Ebola is spread primarily via infected fluids, whereas COVID - being a potent strain of the common cold - is easily spread via respiratory droplets. The basic reproduction number (R_0); which is the expected number of cases directly generated by one case in a population where all individuals are susceptible to infection, is projected to be between 2 to 6 for COVID-19, comparing to 0.19–1.08 for SARS; and 1.5–1.9 for Ebola. In effect, COVID-19 is characterized by a much larger healthcare and economic burden as a global pandemic; and disease surveillance as presented in [11], [12] is only one facet of the solution.

TABLE I
EXTRACTED INFORMATION FROM ANALYZING EACH APPLICATION

1. Application name
2. Centralization (Centralized, Decentralized)
3. Mobile Operating System
4. Tracking Technology
5. Source Code Availability
6. Country of Development or Deployment
7. Development Sector (Private / State)
8. Approximate Number of Downloads
9. Providing Privacy Policy
10. Personally Identifiable Information (PII) Collected
11. Data Encryption
12. Privacy Policy Provided
13. Data Storage Duration

III. RQ1: WHAT IS THE CURRENT LANDSCAPE OF CONTACT TRACING MOBILE APPS?

At the most general level, surveillance of humans can be defined as "regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these. A central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category)" [13]. Contact tracing is one particular type of surveillance. Before the COVID-19 era, contact tracing has been mainly conducted manually. The process involved interviewing infected patients to trace their recent contacts, then the authorities reach to each identified contact to check for existing symptoms. This typical manual process is relatively slow and requires massive human resources which cannot effectively cope with the speed that the SARS-CoV-2 virus has been spreading at under loose distancing measures. The mobile contact tracing apps aim at automating this process.

To analyze their current landscape, we investigated a sample of 52 contact tracing mobile apps developed and/or deployed in 29 countries. The sample was retrieved from the outcome of our search on LionSearch tool using the string "(contact tracing app) and (COVID)". Thirteen pieces of information were extracted from each of the analyzed apps included in this study, as shown in Table 1.

Figure 1 provides an aggregated contemporary view of the analyzed apps. We posted the extracted data on each app through the link: https://bit.ly/2HeQNUh.

The findings from analyzing the apps against the mechanisms they employ for data collection and management indicates that only 15% of the overall sample was detected collecting anonymous data with no PII. Forty-three percent of the apps maintain Pseudonymized copies of the data, while the remaining 42% had no information on the data anonymity. Once collected, 47% of the sample store the data in a centralized location (e.g. authority server), while 26% retained the data locally on the mobile device (decentralized). Twenty-eight percent of the apps didn't report on how the data would be stored. Table 2 provides a summative comparison between the decentralized vs. centralized versions of these apps.

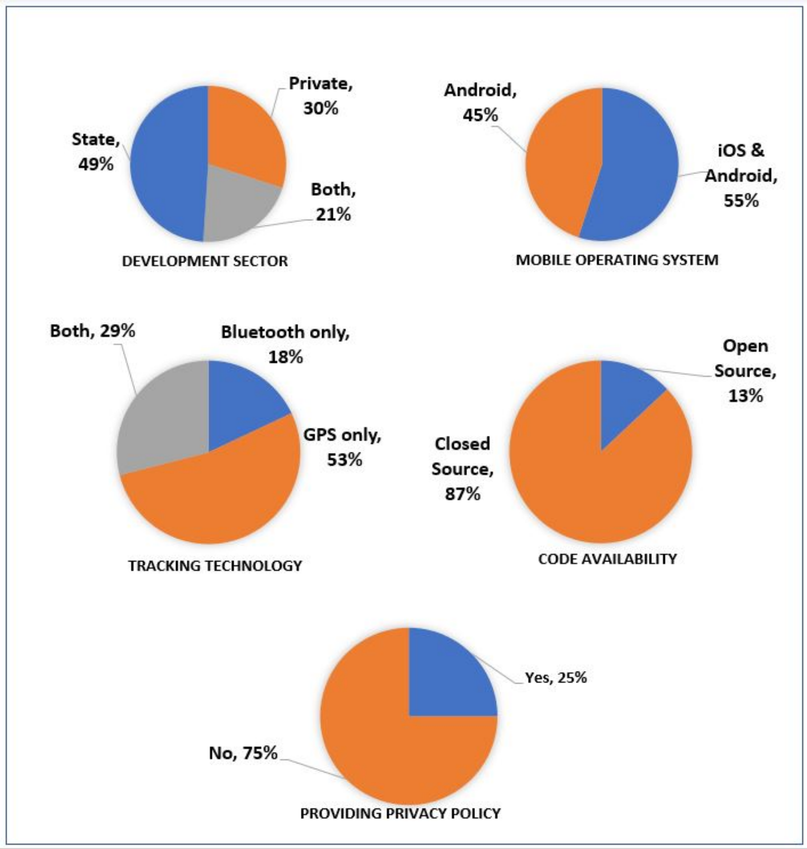

Fig. 1. Distribution of COVID-19 Contact Tracing Mobile Applications Analyzed Sample

The majority of the overall apps (58%) do not provide sufficient information regarding the data storage duration though. Only 21% reported temporary storage, while the remaining 21% store collected data for a period of one year or longer. 47% will store data in unencrypted format comparing to only 21% that store encrypted data.

It was surprising that code relating to Google advertising and tracking platforms (e.g., Google AdSense, DoubleClick) has been detected in 14 contact tracing apps from the analyzed sample. Code relating to Facebook advertising and tracking could also be found in 8 of these analyzed apps. Such a code allows publishers to make money by showing advertisements to their users from a vast array of sources. The presence of such a tracking code in contact tracing apps raises privacy concerns due to the targeting options offered by Google / Facebook advertisements platforms.

IV. RQ2: How Blockchain Can Contribute Positively to the Landscape of Contact Tracing Apps?

In both, the centralized and decentralized types of applications, a central database exists and it is potentially connected with millions of mobile users. Such an architecture suffers from several vulnerabilities and involves a single point failure. Besides, there is a potential for performance overhead with a delayed response.

With the "decentralization" and "consensus" features of blockchain, a user can opt to submit a device's unique Bluetooth identifier in encrypted form and the other participants on a ledger would be able to validate that a device has opted to share and receive anonymous information. This forms the basis of consent to be a participant in data sharing and subsequent tracking via blockchain. Everyone participating in the system could see if they have been near another person that owns a device that has been recorded on the network as infected (without that person being identified). Each block in the chain is secured with its own hash value.

Because data is stored on a *"decentralized"* network, there is no single point of attack [14], which reduces the risk of unavailability to patient record keeping. With blockchain, healthcare providers and authorities can also have access to near real-time data: "Blockchain would ensure continuous availability and access to real-time data. Real-time data would allow researchers and public health resources to rapidly detect, isolate, and drive change for environmental conditions that impact public health. For example, a virus break within a community could be detected earlier and contained."[15]. The "immutability" feature creates a single source of truth of who

TABLE II
CONTACT TRACING APPS COMPARATIVE ANALYSIS: CENTRALIZED VS. DECENTRALIZED

Category	General Description	Analysis
Centralized	"Anonymized" data gathered and uploaded to a remote server where matches are made with other contacts, should a person start to develop Covid-19 symptoms.	• The matching between infected and potential infected occur on the authority server. • Advantage: Possibility of generating a trove of data that epidemiologists can use to track the spread of Covid-19. • Advantage: Information such as GPS location history and a list of everyone a person has come in contact with, could help governments make better public health decisions. • Concern: Data collected for one purpose can be abused and used for things it was never intended to be used for.
Decentralized	Most of the decentralized apps allow for the data to be stored locally on mobile devices. Devices exchange pseudonymous tokens. First, two phones come near one another, then the phones exchange unique codes that change frequently. Each phone logs the code it received and the one it transmitted. If a person tests positive, they can upload the log of the codes they transmitted to a public database. Other phones periodically check that database for the codes it has received from other phones. If a match is found, the phone knows it was near a person who later tested positive and triggers an alert. Participants' volunteered data can be transferred to a centralized location through which is managed by authority (e.g. cloud-based, or server).	• The matching between the infected and the potential infected happen on the infected's phone. • Advantage: offering a higher degree of privacy in comparison to centralized apps. • Concern: Public database can still be a point of attack or alteration. Even if private identifying information is not stored directly on the database, altering the public database can generate false alarms which may consume healthcare resources that need to be preserved.

opted in which can be searchable by health authorities while medical information associated with an anonymous device identifier is kept on locally on each device. The *immutability* feature also implies the availability of the entire history of health records. Figure 2 provides a mapping of the key benefits of building contact tracing apps on top of blockchain technology.

We detected five apps from the sample we analyzed in Section 3 as blockchain-based. Table 3 provides a brief overview of these apps.

V. RQ3: WHAT ARE THE TECHNICAL AND SOCIAL CHALLENGES FACING BLOCKCHAIN-BASED CONTACT TRACING APPS?

Recommending the contact tracing apps is perhaps understandable in the heat of the early stages of the pandemic; however, much deliberation must be given towards considering the long-term consequences of building such digital infrastructure across society. A report published by a global public policy firm for the tech sector recalled that 49% of the world remains digitally unconnected and affirms that "*virus fightback must start with adoption of policies that enable countries to take advantage of great leaps in pandemic-busting ingenuity*" [21],[22]. The Centers for Disease Control and Prevention (CDC) defined the preliminary criteria for minimum and preferred characteristics of digital contact tracing tools to help health departments overcome the challenges in the COVID-19 contact tracing workflow [23]. The World Health Organization also published interim guidance in May 2020 to regulate these apps [24].

Despite the advantages discussed in the previous section, in its current state, blockchain will not offer the complete answer for all the challenges for the contact tracing apps.

Firstly, within a blockchain deployment, the "decentralization", "provenance", and "consensus" imply that all the blocks are stored on every fully participating client node within the network which leads to large disk space coverage. As the health data volume will be on constant increase, a demand on each participating node will also increase to provide the required scalability. In the last two years, Bitcoin blockchain ledger size has grown at the rate of 50GB per year from 150 GB to 250 GB. The Ethereum size has been growing at three times more than that of Bitcoins. While according to Moore's law, hard disk storage prices will decrease with time, the blockchain-based contact tracing platform that maintains a significantly large volume of users data has to be proven in production settings as of yet.

Secondly, because of the blockchain's "immutability" characteristic, users' records can't be changed or removed from the network. Will this be appropriate when a lockdown is lifted? The "finality" characteristic of the blockchain can also diverge from existing legislation such as the European GDPR [25] or the recently announced Brazilian LGPD [26] that provides all citizens the capacity to govern their own data including the right to request an institution to delete personal data being processed based upon consent.

Thirdly, compared to the centralized data storage alternatives, the blockchain technology does not reach far enough upstream to resolve the questions: how do we ensure the identity of who is accessing patient records on blockchain in the first place? Who is the real endpoint? Even if medical symptoms data sets are kept in distributed databases outside the blockchain, then it would be interesting to know how data will travel between blockchain and distributed databases seamlessly without any privacy breach. Chang and Park [27] provided a taxonomy on the potential security attacks that

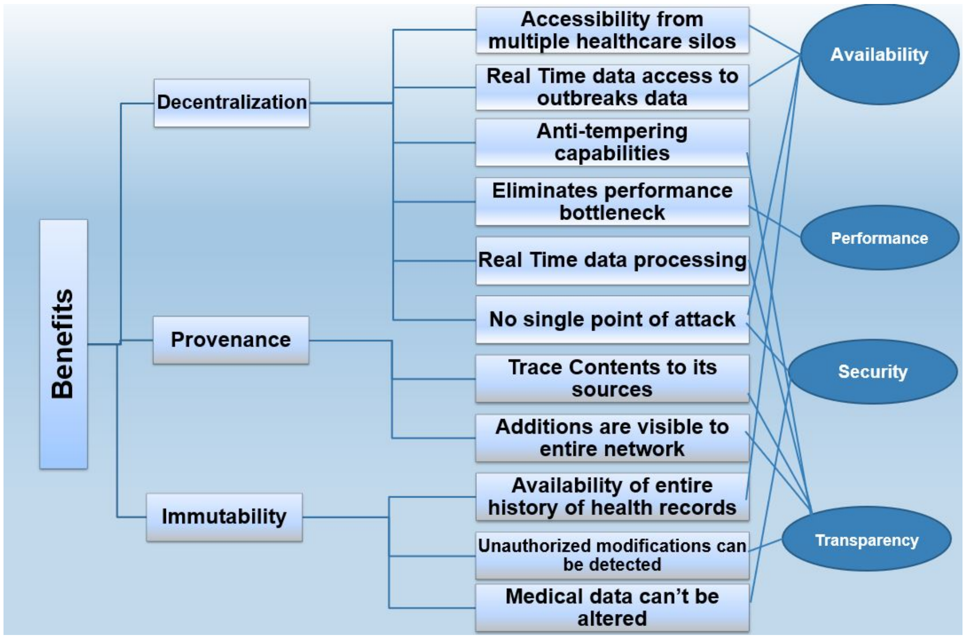

Fig. 2. Mapping of the Key Benefits Of Building Contact Tracing Apps on Top of Blockchain Technology.

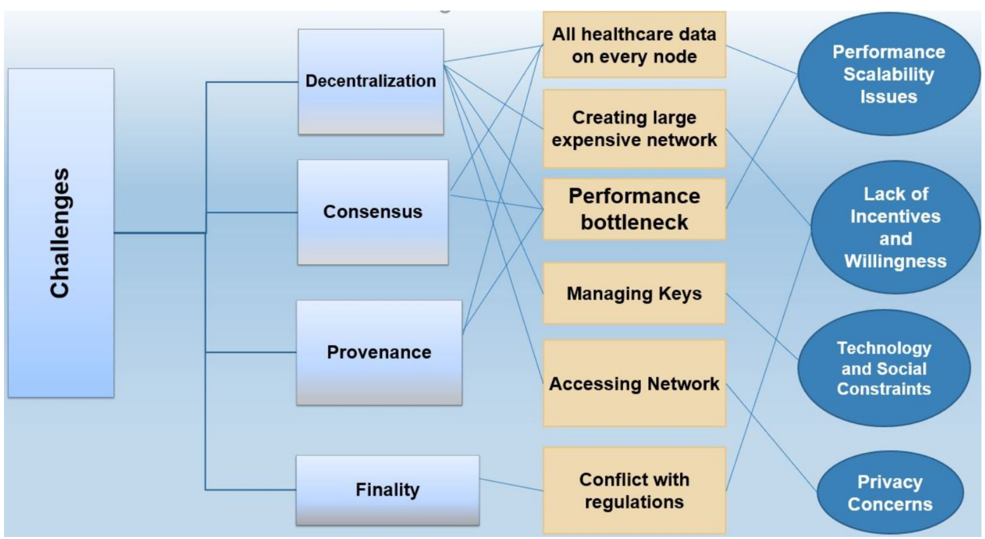

Fig. 3. Mapping of the Key Challenges Of Building Contact Tracing Apps on Top of Blockchain Technology.

blockchain technology may face. The high level of the taxonomy includes eight types of attacks that need to be addressed: Key attack, Identity attack, Manipulation attack, Quantum attack, Service attack, Malware attack, Application attack, and reputation attack.

Finally, blockchain technology is relatively new, and leveraging it for constructing architectural solutions in healthcare scenarios requires accounting for some constraints and architectural drivers. The cryptographic concepts of blockchain transactions will be unfamiliar to most people. In the context of medical records sharing, the proposed schemes from the existing research articles [5] require patients to manage their key pairs (public/private) to provide cryptographic signatures, and authorize access to their medical data. That said, the structural complexity of managing the keys should be concealed behind web and/or mobile application with a user-friendly interface [28]. But special consideration and provision must also be made towards many populations who do not have smartphones, internet access, or even traditional forms of physical identity credential.

The lack of access to smartphones can also be an obstacle to the "proximity tracing" applications which rely on a high

TABLE III
BLOCKCHAIN-ENABLED CONTACT TRACING APPS

Application	Description
Tracy [16]	Tracy is the first blockchain-based solution that was developed for quarantine management and contact tracing. On April 29, 2020, it has been reported in an announcement that the new app Tracy will be supported by the Matic Network for contact tracing and quarantine management, as the solution also uses decentralized data storage solution, MóiBit, to store sensitive data.
BeepTrace [17]	BeepTrace is a proposed blockchain-enabled privacy-preserving contact tracing scheme bridging the user and the authorized solvers to desensitize the user ID and location information. The initial validation results show higher privacy and better battery consumption in comparison to other non-blokchain based apps.
COVID19-Alert [18]	"To trace users the app algorithm issues time-sensitive anonymous temporary IDs that are used to identify the user to all third parties. When two users of the app pass by, the devices exchange temporary IDs and store them in a contact history log. This log chronicles every user the patient has encountered in the last X days and is stored exclusively on the user's device. Once a user tests positive for an infection he can optionally share their log, it is sent via API to other devices where they match the stored temporary IDs with contact information. If a user opts out, their contact information is deleted from the API database. Blockchain technology is used to ensure that the validated code with which the app is written cannot be adapted any more and to report labtests in the APP."
Viri [19]	The application mission is to allow organizations across multiple domains to plug into a single global contact tracing network while allowing them to adhere to their own privacy policies and applicable healthcare-data regulations. The application utilizes a hybrid backend architecture that leverages permissive blockchain technology. Data stored on the blockchain are anonymous generated ID and symptoms.
Coalition [20]	Based on Whisper Tracing V3 protocol. The protocol works by tracking contact events using Bluetooth while enabling notifications when exposure to infection occurs. The protocol can be coupled with a decentralized architecture leveraging IPFS and threads at the server level. Notifications of one's infectious state are executed by a user broadcasting its infected temporary IDs during one's interaction so that contact tracing can be performed at a server level or locally on mobile devices, and without a need to exchange PIIs.

level of inclusion. In addition, all the existing contact tracing mobile apps rely on GPS and/or Bluetooth capabilities which are not highly reliable still. Bluetooth's range, for example, is considerably wider than 6 feet which can trigger a high percentage of false positives regarding the exposure to the virus. Continuously enabled GPS/Bluetooth capabilities can also drain the battery quickly. A 2016 study found that with good signal strength, a battery of a GPS-enabled mobile phone depletes by 13% while a weak signal could cause the battery to drop up to 38% [29]. One solution scheme proposed by the developers of the blockchain based "BeepTrace" contact tracing app [17] is by separating the recording and uploading in two steps. By sending the data only when the mobile device is being charged, the solution becomes battery-friendly.

As the sphere of using blockchain for contact tracing apps grows, the interoperability in Business-to-Business (B2B) middle-ware integrated with enterprise systems at different locations worldwide will be critical for success. Blockchain does not deliver interoperability by itself but depends on it. Hence, blockchain should maximize the use of existing applicable interoperability standards, e.g. FHIR. The ability to transmit digital information freely among countries can be a constraint as well due to governmental regulations.

Figure 3 provides a mapping of the key challenges of building the contact tracing apps on the top of blockchain technology.

VI. CONCLUSION

The ultimate goal of the study presented in this paper was to examine the potential role blockchain technology can play in the sphere of contact tracing apps to combat COVID-19 crisis. To answer the three research questions introduced in this paper, a sample of 52 contact tracing apps were analyzed, including 5 blockchains based. Besides, a deductive content analysis was conducted on 225 articles, including peer-reviewed and newspaper articles addressing the subject of blockchain based contact tracing apps.

Our findings from this review show that blockchain has generated the interest and attention to be implemented as a platform to improve the authenticity and transparency in contact tracing apps. While blockchain; like any technology, is not a solution itself, it can act as an enabler to early detection of outbreaks through a network of connected nodes whose only purpose is to remain alert about outbreaks. Nevertheless, this study also demonstrated that there are challenges that still exist in utilizing blockchain systems. These challenges should be considered as research opportunities.

REFERENCES

[1] John Hopkins University & Medicine. (2020) Coronavirus Resource Center. Available at https://coronavirus.jhu.edu/map.html. Last seen on 15 November 2020.

[2] Marketing Technology Insights. (2020, June) New survey reveals growing acceptance around covid-19 contact tracing and exposure notification apps. Available at http://tiny.cc/n47asz.

[3] Coronavirus Fraser Group. (2020) Oxford's Openabm-Covid19 Model Helps the UK and Other Countries to Control the Coronavirus Epidemic. Available at https://bit.ly/3j3ONMx.

[4] TraceTogether. (2020) Available at https://www.tracetogether.gov.sg/.

[5] M. Kassab, J. DeFranco, T. Malas, P. Laplante, V. V. G. Neto *et al.*, "Exploring research in blockchain for healthcare and a roadmap for the future," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[6] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering." in *EASE*, vol. 8, 2008, pp. 68–77.

[7] M. C. Chang and D. Park, "How Can Blockchain Help People in the Event of Pandemics Such as the COVID-19?" *Journal of Medical Systems*, vol. 44, pp. 1–2, 2020.

[8] D. Nguyen, M. Dinh, P. Pathirana, and A. Seneviratne, "Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-like Epidemics: A Survey," *Preprints 2020*, 2020, yet unpublished.

[9] S. HAIG. (2020, March) World Health Organization Launches Blockchain Platform to Fight COVID-19. Available at http://bit.ly/3bC2FfJ.

[10] Hedera Hashgraph. (2020, February) Acoer Coronavirus Tracker, Powered by Hedera Hashgraph, Now Freely Available to General Public with Added Clinical Trial Data. Available at http://bit.ly/3i7KEHB.

[11] S. Bhattacharya, A. Singh, and M. M. Hossain, "Strengthening public health surveillance through blockchain technology," *AIMS public health*, vol. 6, no. 3, p. 326, 2019.

[12] V. K. Chattu, A. Nanda, S. K. Chattu, S. M. Kadri, and A. W. Knight, "The Emerging Role of Blockchain Technology Applications in Routine Disease Surveillance Systems to Strengthen Global Health Security," *Big Data and Cognitive Computing*, vol. 3, no. 2, p. 25, 2019.

[13] G. T. Marx, "Surveillance studies," *International encyclopedia of the social & behavioral sciences*, vol. 23, no. 2, pp. 733–741, 2015.

[14] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.

[15] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.

[16] Cointelegraph. (2020) Matic powers a privacy-centric coronavirus tracking app.

[17] 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," *arXiv preprint arXiv:2005.10103*, 2020.

[18] covid19-Alert. (2020) Available at https://devpost.com/software/covid19-alert.

[19] Viri. (2020) Available at https://www.viri.io/.

[20] Coalition. (2020) Available at https://www.coalitionnetwork.org/.

[21] A. D'mello, "Report reveals privacy is taking back seat in global contact tracing efforts," *IoTNow*, May 2020. [Online]. Available: https://bit.ly/3jeKFJY

[22] Access Partnership. (2020) Digital contact tracing: A comparative global study. Available at https://bit.ly/36MZnSH. Posted on 27th May 2020.

[23] Centers for Disease Control and Prevention. (2020) Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19. Available at https://bit.ly/3fLAMSh.

[24] World Health Organization, "Ethical considerations to guide the use of digital proximity tracking technologies for covid-19 contact tracing: interim guidance," Tech. Rep., 2020.

[25] The EU General Data Protection Regulation. (2016) Available at https://gdpr.eu/.

[26] Brazilian General Data Protection Law. (2019) Available at https://www.lgpdbrasil.com.br/.

[27] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of Blockchain from Security Perspective," *Journal of Banking and Financial Technology*, vol. 3, no. 1, pp. 1–17, 2019.

[28] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, "How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept," *Journal of Diabetes Science and Technology*, vol. 13, no. 2, 2018.

[29] M. Tawalbeh, A. Eardley *et al.*, "Studying the energy consumption in mobile devices," *Procedia Computer Science*, vol. 94, pp. 183–189, 2016.