Can blockchain take smartphones out of contact tracing?

Ikpobe, Oritsebawo; Easton, John

DOI:
10.31585/jbba-5-1-(1)2022

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Ikpobe, O & Easton, J 2021, 'Can blockchain take smartphones out of contact tracing?', *Journal of the British Blockchain Association*, vol. 5, no. 1, 30993. https://doi.org/10.31585/jbba-5-1-(1)2022

THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-5-1-(1)2022

Can Blockchain Take Smartphones Out of Contact Tracing?

Oritsebawo Paul Ikpobe, John M Easton
The University of Birmingham, UK

Correspondence: oxi700@alumni.bham.ac.uk
Received: 22 October 2021 **Accepted:** 8 December 2021 **Published:** 17 December 2021

Abstract
The global public health crisis caused by the emergence and spread of the coronavirus disease (COVID-19) has been devastating, prompting the need for immediate countermeasures to curb its spread, especially in the absence of any approved treatment shortly after its onset. This crisis has highlighted the gap in current contact tracing systems, which require massive public participation to be effective but lack a high degree of public acceptance. This low acceptance is mainly due to concerns regarding personal data privacy and guaranteed data protection, hindering the success of existing systems. We evaluate the use of blockchain to improve contact tracing and provide a solution to effectively track the spread of an epidemic, using COVID-19 as a relevant use case. The key requirements of the proposed system include protecting user data, maintaining full transparency using a decentralised system, and eliminating the need for global positioning system or personal data for contact tracing. A proof-of-concept system uses a private blockchain to secure and manage data collected at various locations using a mobile application or stored-value contactless smart cards. Contact tracing is performed via smart contracts over the blockchain using the collected data. We confirm the improvements provided by the proposed system for contact tracing.

Keywords: *blockchain, contact tracing, smart contract, Hyperledger Fabric*
JEL Classifications: *I100, Y800*

1. Introduction

Contact tracing allows us to identify persons who have been in close contact with others infected by diseases such as the coronavirus disease (COVID-19). Yap and Xie [1] highlighted the importance of collecting accurate epidemiological data via contact tracing. Such data are key for deploying preventive measures against outbreaks in a country and promoting situational awareness in the public. This has been evident throughout the COVID-19 pandemic and further emphasised in the COVID-19 report of the World Health Organization, which also lists various precautionary measures: 'rapid diagnosis and immediate isolation of cases, rigorous tracking and precautionary self-isolation of close contacts' [2]. The report also mentions the primary issue hindering the implementation of these measures: 'an exceptionally high degree of population understanding, and acceptance of these measures are critical for countries to curb ongoing outbreaks' [2].

The lack of any approved treatment during the early propagation of COVID-19 made prevention crucial, especially due to the unique properties of the virus including 'non-specific features of the disease, infectivity even before the onset of symptoms in the incubation period, transmission from asymptomatic people, long incubation period, prolonged duration of the illness and transmission even after clinical recovery' [3]. While the release of approved COVID-19 vaccines has put the end of the pandemic in sight, extensive measures will still be required to curb its spread and avoid new outbreaks as countries gradually reopen their borders for business and tourism.

The pandemic has exposed gaps in control of disease outbreaks and the urgency with which countermeasures should be adopted for potential outbreaks in the future. These aspects are important for potential outbreaks of diseases such as Ebola, severe acute respiratory syndrome, Zika, and variant strains worldwide, which can increase over time, as shown in Figure 1. More frequent outbreaks can be attributed to various global trends. First, increased globalisation means that humans are more connected through travel and trade. Consequently, outbreaks can spread across the globe in a matter of days. Even within countries, increasing urbanisation, with 68% of the world population projected to live in urban areas by 2050 [5], and the concentration of people living in often unhygienic conditions can promote the spread of diseases.

Human displacement resulting from natural disasters, emergencies, poverty, or conflict has also led to large groups of people having to relocate outside their home countries. Under poor conditions, these people are often vulnerable to

infectious diseases. Moreover, climate change directly impacts environmental health and can alter the transmission patterns of infectious diseases. In particular, water-borne diseases and zoonoses may have their transmission season lengthened and geographical ranges altered, as seen with Zika, malaria, and dengue [6].

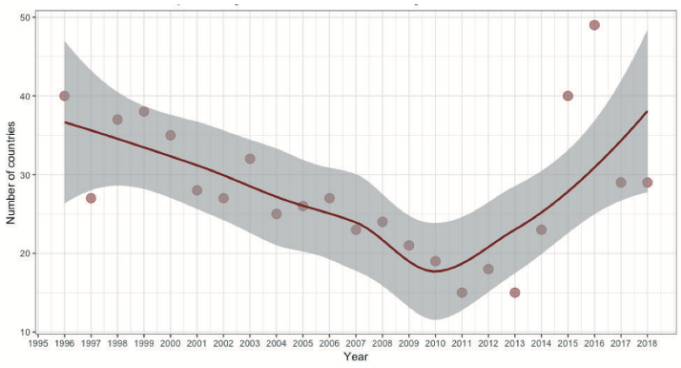

Figure 1: Number of countries experiencing disease outbreaks between 1995 and 2018 [4].

In June 2018, the abovementioned trends converged, and for the first time ever, there were outbreaks of six out of the eight categories of diseases in the Priority Diseases list of the World Health Organization [7]. As each of these diseases has the potential to cause global disruption if allowed to spread [8], the development of effective countermeasures becomes imperative to prevent outbreaks and prepare for epidemics.

In the absence of digital contact tracing, patients reporting their symptoms to medical professionals are expected to collect and trace all their recent close contacts, being an unrealistic procedure in the modern world. On the other hand, digital contact tracing allows the use of smartphone data for health surveillance while protecting individual privacy and providing safeguards against data breaches [9]. Accordingly, we explore how blockchain can be integrated into an Internet-of-Things system to achieve contact tracing towards the development of a trustless system to tackle the continued spread of disease outbreaks.

2. Existing Contact Tracing Technologies

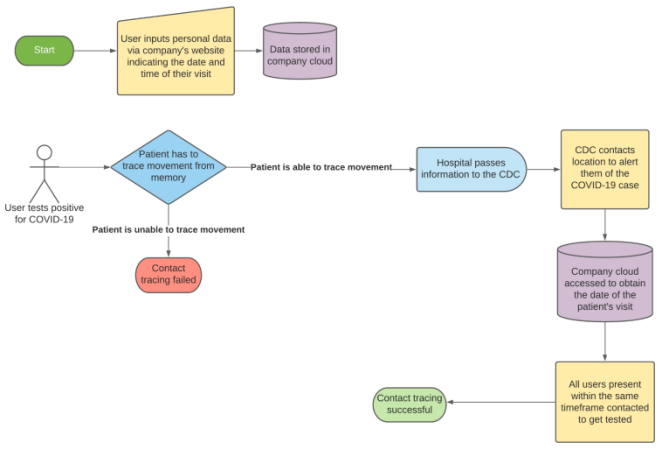

Figure 2: Workflow of typical contact tracing.

Current models for contact tracing should be analysed to devise potential improvements. Figure 2 shows the workflow of a typical contact tracing system. It shows the disconnection between users and hospitals as well as the delays in contact tracing due to the involvement of multiple intermediaries.

More modern systems include spatiotemporal reporting over networks and GPS (global positioning system) data to determine the locations for contact tracing [9]. Similar systems developed by Apple and Google [10] work with Bluetooth protocols and temporary keys in smartphones to preserve user privacy successfully. Thus, smartphones are inevitable in current digital contact tracing solutions.

However, these systems may cause concerns regarding individual data privacy and data protection, leading to low public acceptance. Most solutions are critically dependent on the number of participants, showing a low effectiveness if not widely used [11]. In addition, trust plays a major role along with preference, location, and jurisdiction in the multitude of available contact tracing apps (mobile applications), which further dilute the pool of participants.

We propose a solution considering COVID-19 as a use case. Although the epidemiology of COVID-19 was used as the basis for the model, it can be modified to fit different cases. To solve the problems of contact tracing, the proposed system is designed considering the following primary prerogatives:

- Must comply with the General Data Protection Regulation [12]
- Must secure user data
- Anonymous contact identification: Contact tracing must be done without compromising user privacy
- User notification: Users must be notified of their exposure to a disease (e.g. COVID-19).

The complete list of requirements is provided in the Appendix, which covers the design requirements at various levels.

3. Methodology

Based on the contact tracing requirements, we conducted a survey of the available permissioned blockchain frameworks and selected Hyperledger to develop the proposed system. Hyperledger provides several frameworks for different implementations, as outlined in Table 1. The listed characteristics allowed us to narrow down the framework selection for the proposed system.

Considering the system specifications, Hyperledger Fabric was selected because it is a base framework that implements pluggable components, enabling system streamlining using only the necessary services.

4. Implementation

Figure 3 shows the workflow of the proposed solution with a blockchain streamline that automates contact tracing and

removes intermediaries. A blockchain is primarily used for data management, taking advantage of its immutability and transparency, which creates trust among the public. Data are collected via nodes at different locations through a mobile application (app) or a stored-value contactless smart card, which possesses a unique ID serving as public key for the distributed ledger. The smart card removes the necessity of smartphones in contact tracing to improve accessibility. In addition, an algorithm implemented by smart contracts uses these data to highlight locations where users test positive for COVID-19 and automatically flag users who likely had contact with the infected patient.

Table 1: Characteristics of Hyperledger Frameworks

Requirement	Fabric	Sawtooth	Iroha	Burrow	Besu	Indy	Grid
Permissioned Blockchain	✓	✓	✓	✓	✓	✓	✓
Modular Architecture	✓	✓	✓	✓			
Flexible smart contract deployment	✓	✓	✓	✓	✓		
Flexible coding language	✓	✓					
Adaptable Consensus Mechanism	✓	✓	✓		✓		
Mobile Application Synergy	✓		✓			✓	
Versatile	✓		✓				
Case-specific		✓			✓	✓	✓
Simple	✓			✓			

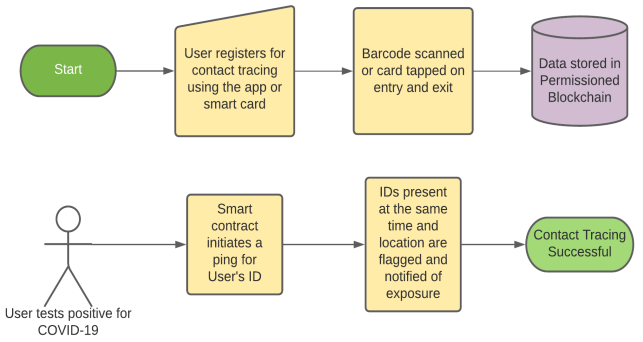

Figure 3: Workflow of proposed blockchain-based contact tracing.

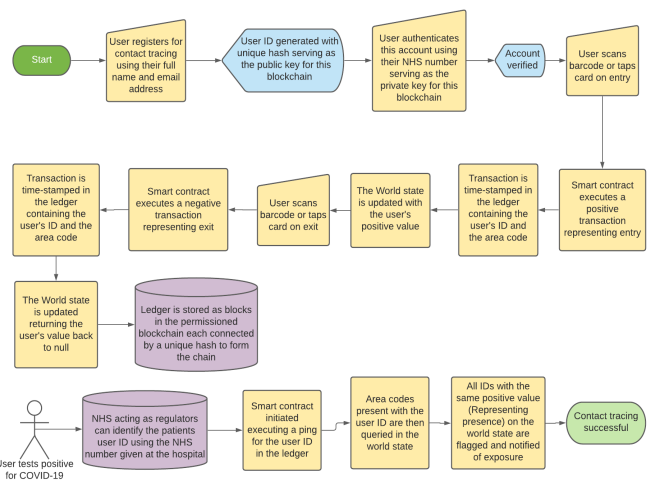

Figure 4: Blockchain contact tracing dataflow.

Figure 4 shows the dataflow of the proposed system including acquisition, processing, and storage of user data to be used by smart contracts when addressed.

Full transparency is maintained in two stages. The first stage involves linking the user's private key to a national medical record or identity number for authentication according to the country of implementation. For this use case, in the event of a contagious disease outbreak such as COVID-19 in the United Kingdom, the National Health Service (NHS) could act as regulators of the client application, working with admin access. The NHS is the only party with complete access to the client application as NHS numbers are used for authentication and the NHS acts as a regulator of the client application. Hence, a seamless transition between hospitals identifying cases can be achieved as the hospitals already possess and manage NHS accounts. In the event of an emergency outbreak, the approach can be modified by using any national medical records or identity numbers for authentication according to the country of implementation. Second, the proposed system enables the backtracking of the IDs of COVID-19 patients at hospitals through their identity numbers upon hospitalisation. Allowing patients to be checked against the ledger can minimise human error and enables system redistribution of pings over predetermined exposures, improving the pinpointing accuracy.

Smart contracts simulate contact by using positive and negative transactions for entry and exit, respectively. These transactions are triggered by the input from users over nodes via the app or the stored-value contactless smart cards. Only the user ID and unique area code assigned to the node are timestamped in the ledger. Upon occurrence of a positive COVID-19 test, the smart contracts are triggered to query the ledger for the corresponding ID. Presence is then identified in the world state by users possessing the same positive key–value pair, who are automatically notified of their exposure via the app or email.

Considering human factors, in the events of no-scan, tailgating, or a probable miss-read of IDs, a two-layer stop gap is set to minimise errors due to missed binary actions. First, a 24-hour timer is incorporated into the chaincode for entry scans. Using a conditional statement, a negative exit transaction is automatically executed to set the value of the ID back to null. A large time value was chosen to accommodate errors; however, the time value requires optimisation in the testing phase to avoid wasted ping transactions. To address wasted ping transactions within that time range, the second layer extends the conditional statement on entry transactions to return a recurring positive ID value to null. This process is crucial to preventing errors due to 'omnipresence', forgoing the timer in the event of a missed exit transaction. These steps potentially mitigate human error, optimised during quality checks using several sample scenarios.

Contact tracing can create awareness and provide information on the spread and demographics of a disease. In addition, it provides analytical data anonymously by interpreting the network statistics obtained using Hyperledger Caliper [13]. For

example, the number of cases in an area can be determined by the number of smart contracts triggered, and the number of blocks generated per day allows us to understand traffic and exposure across a region. Thus, the proposed system provides an additional source of accurate and trusted epidemiological data, which are essential to curb the spread of a disease.

5. Adoption and Usage

Contact tracing as an emergency countermeasure depends heavily on user behaviour, and its effectiveness is determined by public acceptance. These features are the greatest barriers facing the implementation of contact tracing, especially in countries with a general distrust in the government. In a cross-country survey [14] conducted across France, Germany, Italy, the United Kingdom, and the United States, findings were consistent with the general notion that contact tracing solutions should be delegated to a transparent public health authority for positive public acceptance. Hence, we used national medical records independent of government IDs for authentication in this study.

Even with such delegation, the general mistrust in tracking solutions for contact tracing is still highly apparent. Thus, users are more likely to opt-out of downloading or disconnect their devices from use when contact tracing apps are mandated. Other sources of mistrust include a genuine discomfort with the use of sensitive data (e.g. geolocation data) and fear of data protection during and beyond the use of a smartphone app.

General public concern on these matters is based on genuine fear and mistrust. The focus of our solution to overcome this fear is creating an incentive based on trust itself.

First, contact tracing requires public consent at the onset but has been mostly limited to the use of smartphones. Our solution aims to tackle this by creating an option through contactless smart cards, which require no device and are not traceable. Removing the necessity of smartphones also makes the solution accessible to an entire population, thereby creating a larger pool of users.

Second, with contact tracing made autonomous by using smart contracts in blockchain, the system runs independent of human interference on the back end, and user and admin interactions only occur on the front end via a client application. Eliminating the possibility of human interference is another key selling point for adoption and favours creating a trusted source of epidemiological data using network statistics. This is vital because distrust in governments and public media causes people to mistrust the epidemiological data released, impacting their overall awareness.

Lastly, by taking advantage of decentralisation and the high-level encryption of blockchain, our solution does not require personal data. Authentication only occurs on the front end using national medical records that are currently handled by hospitals, avoiding any dissemination of personal data.

6. Technical Solution

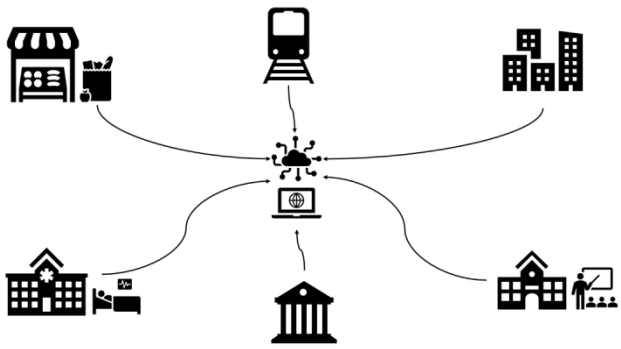

Figure 5: Grid diagram of implemented blockchain-based contact tracing.

We adopt a modular approach with a blockchain spanning a fixed geographical area to optimise storage and performance by minimising the traffic across the network. Figure 5 illustrates the implementation of this approach, where nodes are deployed across densely populated locations within an area interacting with the blockchain via the client application.

6.1. Blockchain Architecture

The private blockchain is a base ledger with a single organisation consisting of interoperable peer nodes and associated by their channels with each node represented by a unique area code.

As illustrated in Figure 6, client application A0 handles the proposal of smart contracts to be invoked by peers P*i*–P*n*, which are mediated by ordering node O through channel C1 to execute preconfigured smart contracts. A smart contract SC either updates ledger L1 with entry/exit transaction or queries the ledger for key–value pairs during a ping depending on the input from the client application. Configurations for organisation R0 and the channel are stored in certificate authority CA0 and channel configuration CC1, respectively, which are issued by the membership service provider during initialisation.

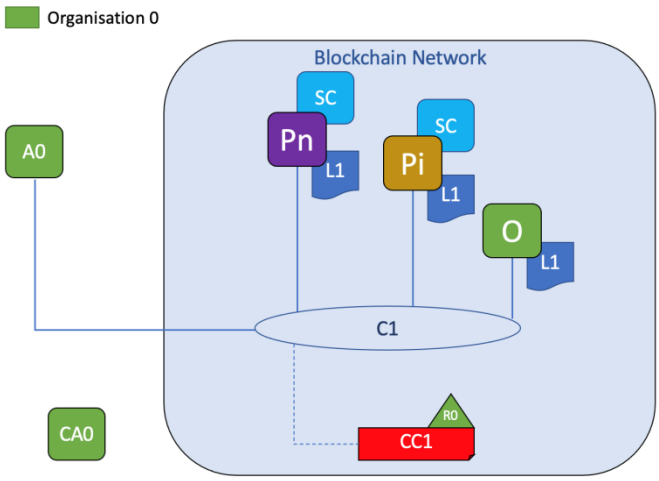

Figure 6: Blockchain architecture.

6.2. Storage Solution

To optimise storage, the proposed system minimises data collection by considering only timestamped user IDs and their respective area codes. Nevertheless, the defining limitation of blockchains is storage, and this use case requires storage to be on-chain. A key element to optimise storage is purging user data 20 days after a user reports infection with COVID-19. This is achieved by using the private data collection feature of Hyperledger Fabric [15, 16].

6.3. Private Data in Hyperledger Fabric

In Hyperledger Fabric, private data provide another layer of security in the permissioned blockchain. This framework grants access to a defined subset of organisations and peers to endorse, commit, or query sensitive data [16]. Hence, the NHS can be defined as a regulator, given exclusive access to read and write private data.

Data purging is performed in the collection policy configuration of the smart contract using property Blocktolive. This property determines the number of blocks for which private data are retained, removing data from consequent blocks but retaining their hash value to serve as immutable evidence [16]. In this case, purging is configured by estimating the number of blocks generated per day multiplied by 20 to satisfy the system requirements.

7. Proof of Concept

As a blockchain administration project, we evaluate the system design, structure, and implementation. Blockchain development on this scale requires a team of developers. Therefore, considering resource limitations, the key features of this specific solution are highlighted in a mock-up using the test network of Hyperledger Fabric [17].

Figure 7 shows the architecture of the blockchain for the test network. The architecture contains ordering organisation O and two peer organisations R1 and R2 with one peer node each (P1 and P2). The implemented architecture was run in a Linux Ubuntu terminal with chaincode written in JavaScript.

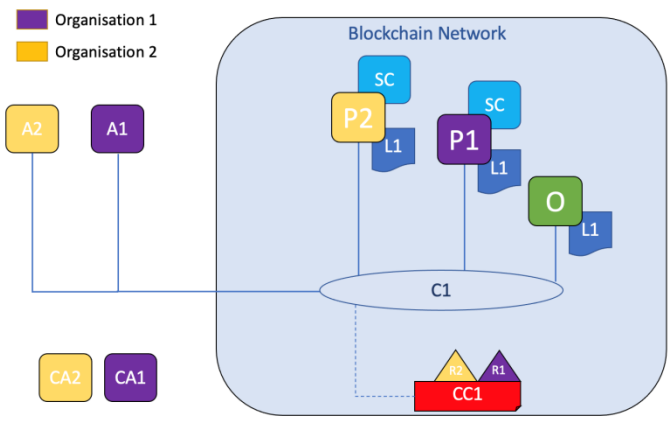

Figure 7: Test network of Hyperledger Fabric to implement blockchain architecture for proof of concept.

Figure 8 shows the network components in the Linux terminal that lists all the docker containers currently running. After the network is running, a channel is created to allow interactions via smart contracts. These contracts handle interactions between peers by querying the ledger or invoking functions included in the chaincode.

Figure 9 shows the creation of assets in the ledger by invoking the smart contract followed by the query of all assets from the ledger to illustrate the querying process. Assets from the ledger can be queried in multiple ways according to the use case. Figure 10 shows a simple asset query by ID from the ledger using smart contracts, demonstrating querying by the unique user ID after a positive COVID-19 test.

Figure 8: Test network components implemented in Hyperledger Fabric.

Figure 9: Asset creation.

Figure 10: Basic query per user ID.

More complex functions can be implemented by smart contracts to query the ledger using key–value pairs [18]. The assets in the test network have five key–value pairs, excluding the asset ID. These pairs can be individually queried from the ledger using rich queries to pull all the assets with the same value. Figure 11 shows a rich query performed using key owner to pull all assets owned by an individual. This further demonstrates asset queries by their key–value pair to pull all users at a specific node using the area code and to determine their presence in the system.

Figure 11: Rich query based on key–value pairs.

8. Conclusion

We propose a contact tracing system that meets various requirements for application to a use case considering COVID-19. The proposed system may contribute to combating epidemics, improving current contact tracing systems by providing trust to users. In fact, securing personal data and maintaining full transparency without requiring smartphones can increase public acceptance, which is essential for creating a sufficient pool of data for digital contact tracing. Incorporating the system into the NHS operations creates a seamless transition between testing and identification of disease cases, establishing a new trusted source of epidemiological data. As countries are looking forward to reopening their economies, effective contact tracing becomes essential to prevent new outbreaks of COVID-19. The proposed system may be applied in the current COVID-19 pandemic as well as other epidemics or pandemics in the future to support prevention and control.

This study was limited to blockchain administration owing to resource constraints and our current unavailability of manpower and expertise necessary to develop the blockchain solution at a practical scale. Such implementation would involve quality checks beyond the system's successful operation for ensuring speed, efficiency, and a low failure rate in tests against various sample scenarios. In future work, we intend to use a complete build to evaluate the scalability and enhanced data analysis across modules using available Hyperledger tools. In addition, the proposed solution may be extended by integrating the vaccination status into the IDs to anonymously gather data and accurately determine the immunisation efficacy across multiple regions.

Appendix: Requirements of Proposed Blockchain-Based Contact Tracing System

Level	Requirement	Description
Stakeholder	Compliance with General Data Protection Regulation [11]	Lawful basis of processing: consent • Participants provide valid consent through app/smartcard registration
	Securing data of participants	Data secured by the blockchain immutability • Data stored on blockchain cannot be tampered with because each block contains the hash value of the previous block as its header
		No personal data needed for contact tracing by leveraging blockchain anonymity • NHS number is only used for account authentication, locked to the private key • NHS numbers are already handled by the NHS, avoiding data sharing
		Data offloaded after 20 days following positive cases of COVID-19 • Achieved using private data collection feature of Hyperledger Fabric • Private data are purged after a number of blocks defined in the collection policy of smart contract • An estimate can be set for the number of blocks created in a day multiplied by 20
User	Portability	Users interact with the system via app or stored-value contactless smart card
	Accessibility	Modular design allows for strategic deployment of nodes over a region
		Contact tracing initiated by preconfigured smart contacts

System	Contact identification	System should identify contact anonymously: 1. User presence is registered at nodes using app or stored-value contactless smart card 2. Smart contract is initiated on entry or exit, reflected in blockchain as a positive or negative transaction, respectively 3. User ID or public key is timestamped to ledger with each transaction 4. Ping smart contract initiated using ID of a user diagnosed with COVID-19 5. Smart contract acts by querying ID against world state 6. Any other IDs present with the same positive value (representing presence) are flagged
	User notification	All user IDs flagged by a ping are notified of exposure via app or email • Handled automatically by smart contract feeding back to client application
	Data management	User IDs are unique, random-generated hashes used as public keys for blockchain
		NHS numbers are locked to private keys used for account authentication • Allows backtracking of user IDs at hospitals
		Only IDs are timestamped in a block against area code assigned to node
		Ledger data are offloaded every 20 days
	COVID-19 identification	System handles identification only by input after a positive COVID-19 test • Input serves as trigger for smart contract
	Data analysis	Anonymous data received from nodes should be intelligible for epidemiological analysis • Number of ping smart contracts initiated represent new COVID-19 cases • New information available on spread and demographics of disease

Competing Interests:
None declared.

Ethical Approval:
Not applicable.

Author's Contribution:

Funding:
None declared.

Acknowledgements:
I would like to share my sincere and heartfelt thanks towards Dr John M Easton for his guidance and support throughout this project. Without his active guidance, cooperation and encouragement, I would not have been able to complete this project. I also want to thank my parents, family members, and friends who have always supported me morally. Lastly, We would like to thank Editage (www.editage.com) for English language editing.

References:

[1] K. Y. Yap and Q. Xie, "Personalizing symptom monitoring and contact tracing efforts through a COVID-19 web-app", *Infectious Diseases of Poverty*, vol. 9, no. 1, pp. 1–4, 2020.

[2] World Health Organization, "Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)", 2020. https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf [Accessed: 19 Aug 2020].

[3] T. T. Zhou and F. X. Wei, "Primary stratification and identification of suspected Corona virus disease 2019 (COVID-19) from clinical perspective by a simple scoring proposal", *Military Medical Research*, vol. 7, no. 1, pp. 1–4, 2020.

[4] World Economic Forum, "Outbreak readiness and business impact: Protecting lives and livelihoods across the

global economy", 2019. http://www3.weforum.org/docs/WEF%20HGHI_Outbreak_Readiness_Business_Impact.pdf [Accessed: 25 Aug 2021]

[5] United Nations Department of Economic and Social Affairs, "2018 Revision of World Urbanization Prospects", 2018. https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html [Accessed: 25 Aug 2021].

[6] World Health Organization, "Climate change and human health". http://www.who.int/globalchange/climate/summary/en/index5.html [Accessed: 25 Aug 2021].

[7] L. Weber, "More dangerous outbreaks are happening: Why aren't we worried about the next epidemic?", *HuffPost*, 2018. https://www.huffingtonpost.com/entry/outbreaks-epidemic-preparedness_us_5b4f85fbe4b0de86f4892daa [Accessed: 25 Aug 2021]

[8] World Health Organization, "Prioritizing diseases for research and development in emergency contexts", 2021. https://www.who.int/activities/prioritizing-diseases-for-research-and-development-in-emergency-contexts. [Accessed: 26 Aug 2021].

[9] S. Wang, S. Ding, and L. Xiong, "A new system for surveillance and digital contact tracing for COVID-19: Spatiotemporal reporting over network and GPS", *JMIR mHealth and uHealth*, vol. 8, no. 6, e19457, 2020.

[10] Apple, "Privacy-Preserving Contact Tracing - Apple and Google", 2021. https://covid19.apple.com/contacttracing. [Accessed: 23 Nov 2021].

[11] W. J. Bradshaw, E. C. Alley, J. H. Huggins, A. L. Lloyd, and K. M. Esvelt, "Bidirectional contact tracing could dramatically improve COVID-19 control", *Nature Communications*, vol. 12, no. 1, 2021.

[12] UK Legislation, "Data Protection Act 2018, c. 12", 2018. http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed: 30 Nov 2020]

[13] Hyperledger Foundation, "Hyperledger Caliper – Hyperledger Foundation", 2021. https://www.hyperledger.org/use/caliper. [Accessed: 29 Nov 2021].

[14] S. Altmann et al., "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study", *JMIR mHealth and uHealth*, vol. 8, no. 8, p. e19857, 2020. doi: 10.2196/19857.

[15] Hyperledger, "Private data", 2021. https://hyperledger-fabric.readthedocs.io/en/latest/private-data/private-data.html [Accessed: 19 Apr 2021].

[16] Hyperledger, "Private Data—Concepts", 2021. https://hyperledger-fabric.readthedocs.io/en/latest/private-data-arch.html#endorsement [Accessed: 19 Apr 2021]

[17] Hyperledger, "Using the Fabric test network", 2021. https://hyperledger-fabric.readthedocs.io/en/latest/test_network.html [Accessed: 21 Apr 2021].

[18] Hyperledger, "Using CouchDB", 2021. https://hyperledger-fabric.readthedocs.io/en/latest/couchdb_tutorial.html [Accessed: 23 Apr 2021].

