ITC 4/50

Information Technology and Control
Vol. 50 / No. 4 / 2021
pp. 674-685
DOI 10.5755/j01.itc.50.4.29064

COVID-19 Information Sharing with Blockchain

Received 2021/05/08

Accepted after revision 2021/10/25

http://dx.doi.org/10.5755/j01.itc.50.4.29064

HOW TO CITE: Aslan, B., Ataşen, K. (2021). COVID-19 Information Sharing with Blockchain. *Information Technology and Control*, 50(4), 674-685. https://doi.org/10.5755/j01.itc.50.4.29064

COVID-19 Information Sharing with Blockchain

Bora Aslan, Kerem Ataşen

Department of Software Engineering, Faculty of Engineering, Kırklareli University, Kırklareli, Turkey
e-mails: bora.aslan@klu.edu.tr, atasenkerem@klu.edu.tr

Corresponding author: bora.aslan@klu.edu.tr

COVID-19 is a disease caused by a novel coronavirus originated in Wuhan, China. The virus rapidly spread over more than 200 countries around the world and caused deaths of more than 690.000 of people. To prevent rapid spreading of this disease, the information sharing related to the findings about the COVID-19 disease must be fast and secure between countries. Since the COVID-19 related health data such as the symptoms and private patient records are confidential, such information requires privacy protection. The blockchain and smart contracts are well-suited solutions for speed, privacy, and security needs of dissemination the COVID-19 related information. Blockchain based e-health solutions have been discussed for years. However, a pandemic is more important than the regular health problems. Thus, this study proposes how critical pandemic related information should be shared between the participating countries and can be accessed by health data actors such as researchers, doctors, laboratory staff, authorized institutions of different countries as well as the World Health Organization.

KEYWORDS: COVID-19, Blockchain, E-health, Smart Contracts, Security and Privacy.

1. Introduction

COVID-19 is a disease caused by a new coronavirus that detected in humans or animals first appeared in Wuhan, China. Following the spread of the virus of many countries around the world, World Health Organization (WHO) assessed that COVID-19 can be classified as a pandemic [12]. Since this novel coronavirus can easily be transmitted effectively from human to human, disease detection at a highly accurate rate gained importance [7], [16], [21].

Polymerase Chain Reaction (PCR) is one the methods employed to detect this disease [33]. PCR has 2 different versions which are quantitative and digital.

Reliability of the digital PCR equipment and software such as FastPCR [11] is open the discussion due to its centralized structure. The software code is generally closed to global access, i.e., it is not open source. Open-source software allows any people to analyze the code behind de program while closed source software does not permit that [27]. Closed-source programs only run on one machine which belongs to a certain company; hence, the company has an opportunity to use the PCR data for their benefits or for any other reason. The companies can even manipulate the PCR test results. In addition to these factors, the company which manufactures the PCR test, and the PCR test software owner might be two different companies. It means that the software owner can also involve in data fraud or other similar interventions. Because of the centralized structure of the dPCR machine, the dPCR machine also has the weakness of single point of failure which can be seen in many machines prone to failure. Once the software crashes, all machines will be out-of-service since all machines use the same software. Once the machines crash, the software will have nothing to do. In addition to above concerns, there are issues related to privacy since COVID-19 related data is an electronic health record. According to almost every data protection regulations and legislations (abbreviated as DPRL in rest of this paper) such as HIPAA [1], privacy-preserving EHRs have four requirements: patients must be able to define privacy policies concerning the information related to them, to check whether the agreed privacy policy has been enforced, in case of undesired information flow, they should be able to detect the data leak, the patient should not be forced to trust anybody but those parties directly involved with the treatment and common certification authorities and the information gained from linking different flows of medical data should be insufficient to establish profiles of or gain new knowledge about patients. Since the COVID-19 data is an EHR, the same requirements are available and applicable.

All these concerns point out the same thing: there is a great need for a highly available, secure and redundant system in the hardware and software perspectives for the environment of the dPCR test for SARS-COV-2 detection and COVID-19 e-health data sharing. Narayan et al. [23] proposed some techniques that guarantees security and privacy of the EHRs on cloud. Their work shows that how new primitives in attribute-based cryptography can be used to create a privacy-preserving and secure EHR system that make it possible for patients to share their health data among healthcare providers in a dynamic, flexible, and scalable way. Seol at al. [29] proposed a EHR model based on cloud computing solutions that performs attribute-based access control using extensible access control markup language to have fine-grained access control on the EHRs. Nonetheless, storing the patient health data in the third-party servers in a centralized manner as in [23] and [29], is a leading problem for keeping balanced data privacy and the need for patients and providers to regularly interact with the data.

The use of blockchain technology for the EHRs can be found in [13] and [18]. Both studies focus on the privacy and security aspects of the health data. However, these studies do not emphasize which cryptography techniques can be used to achieve those goals.

Wang et al. [32] proposed attribute-based encryption and identity-based encryption to achieve confidential medical data for patients, hospital, and insurance companies. However, their study does not connect countries to prevent fast dissemination of diseases.

Cao et al. [6] proposed a secure blockchain based EHR system to guarantee that medical data is not tampered. However, they are not proposing to connect different countries for fast and secure information sharing to prevent and take precautions for illnesses' dissemination.

Blockchain is a highly distributed, secure, and available network of machines where all machines could be thought as redundant, therefore, these machines will never crash in case of any failure on one machine [23]. All machines in a blockchain network keep the same record of transaction history. In case of dPCR tests, this data can be thought as dPCR test results. Since all machines keep the same data, manipulation of the test results will never be successful where the manipulated data will be invalid. The linked structure of blockchain also has tamper-proof feature for blockchain-based structures. The applications which run on the distributed network is also called the decentralized applications (DApps). dPCR software can run on the blockchain network as DApps, which means it will never crash-down due to highly available blockchain network structure.

Smart contracts can be explained as a software running on the blockchain network, not only on a machine. The contracts can be written on the blockchain and executed by all nodes on the block. The contracts can be executed automatically when the terms of the agreement are fulfilled and self-implemented due to its decentralized structure without intermediaries by enabling protection against interferences [18]. Once a smart contract is deployed on the blockchain network, it cannot change by someone else, or it cannot fail. COVID-19 data sharing and accessing policies can be implemented as smart contracts. Besides that, some parts of the PCR software, i.e., decision-making or result returning parts, can be implemented on smart contracts.

In this paper, after explaining the core terms such as blockchain, smart contracts, PCR and so on, we proposed a secure blockchain based COVID-19 information sharing network, 3 different COVID-19 related data interaction algorithms for patients, authorized countries and authorized COVID-19 laboratories, and decentralized COVID-19 test software operation. Eventually, we proposed a secure and trusted COVID-19 consortium blockchain network that includes Turkey, USA, China, and India as participating countries of that network.

The remaining part of the paper is organized as follows: Section 2 has a brief history of COVID-19 pandemic and fundamental information on PCR technology. In Section 3, blockchain technology, smart contracts and decentralized applications are explained with some use case examples. Section 4 has our contribution and explanation. In Section 5, some concerns and future works are argued.

2. Blockchain and COVID-19

2.1. COVID-19 History

In the last days of 2019, it was confirmed that a group of patients with an unknown pneumonia was infected with a novel coronavirus, which has not been previously detected in humans or animals. This novel virus originated in Hubei Province, Wuhan, the People's Republic of China. Subsequently, this virus was named 2019-nCoV, novel coronavirus [8] [36]. The epidemiological data obtained from the observed patients revealed that the majority of these patients went to a local seafood market in Wuhan and the gene information of the virus obtained from these patients, 2019-nCoV, was highly similar to the coronavirus in the bats [19]. On the following days, this virus was called SARS-CoV-2 due to its similarity to the SARS coronavirus, which is also known as "severe acute respiratory syndrome" [17]. This virus managed to spread to nearly 200 countries in approximately 3 months [25].

In response to the spread of the virus and immediately after the unexplained pneumonia cases in Wuhan, a firm called BGI sequenced the genome of the SARS-CoV-2 virus by using genome sequencing technic and developed a test kit with RT-PCR (reverse transcription-polymerase chain reaction) technology to detect this virus by using a test [3]. PCR is a powerful technique that allows enzymatic amplification, obtaining multiple copies of specific regions of the DNA without using traditional cloning procedures [26]. The qPCR (quantitative PCR) method which occurs in real-time or quantitatively was later used with the dPCR (digital PCR) technique by offering solutions to overcome some problems in the current qPCR technique. The strengths and weaknesses of the dPCR technique for qPCR technique benefits are shown in Table 1 [15]. The '+' sign indicates that the technique is stronger, while the '-' sign indicates the weakness. The '*' sign indicates that two different techniques for the related benefit cannot provide a significant advantage.

The test results of the test conducted in the digital environment are either positive or negative according to certain threshold values. This result is controlled by

Table 1
Comparison of qPCR and dPCR

Criterias	qPCR	dPCR
Measurement Accuracy	-	+
Assay Content Sensitivity	*	*
Inhibition Resistance	-	+
Measurement Standardization	-	+
Vulnerability from Target Sequence Variability	-	+
Application Awareness	+	-

algorithms, regardless of the simplicity or complexity behind the measuring devices. However, in both cases, central software was used for controls, that is, the necessity of trusting a third party which in this case corresponds to the test device providers.

Same as the PCR software, electronic health record software such as LIMS and PHMS are also centralized. That means, all health records, in this case COVID-19 data, belongs to one authority. Central software means that a software run on a specific machine may not work properly for some redundancy problems. To express it briefly, it has a single point of failure weakness. When the machine is down or has some security problems, this might allow manipulating test data, testing software, LIMS or PHMS. Thus, the test results will become unreliable. As a result of these weaknesses, irrecoverable consequences may occur.

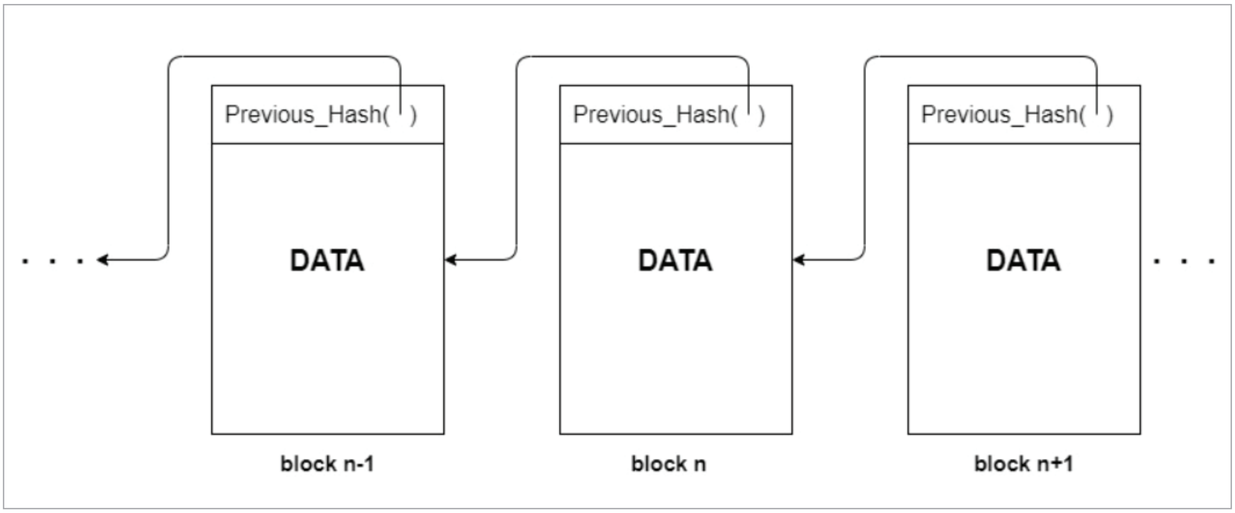
It is possible to ensure for the software to produce test results with smart contract-based mechanisms that are decentralized, reliable, tamper-proof, and fast on a blockchain network. Since it will be possible to express the existing algorithms behind the test mechanism with programming languages like Solidity [10] developed for programming smart contracts on Ethereum blockchain network or any other programming languages like Golang and JavaScript in the smart contracts, a test software deployed on the blockchain network will also benefit from all the features of the blockchain. Since a blockchain network consist of many computers, there will be no single point of failure problem while running the test software. Considering the cost of existing test software on instruments [20], the costs will also be reduced significantly by using smart contract-based test software running on the blockchain network. This way, access to test software problems will not be experienced, and the possibility of everyone in the world to benefit from this service at anytime and anywhere will be significantly increased due to the high availability property of the blockchain technologies.

2.2. Blockchain and Smart Contract

A blockchain is essentially a linked list which has cryptographic hashes as pointers that keep records of all digital events or the transactions that have been executed and shared among participating members of distributed network with a distributed ledger manner. Each transaction added to the chain is agreed on by a majority consensus of the blockchain network members. The blockchain is an append-only ledger where information can never be erased or updated. The blockchain contains exact, traceable and verifiable record of every transaction ever made on the chain [24]. A general structure of a blockchain is shown in the Figure 1.

Bitcoin, the decentralized peer-to-peer digital currency, is the most popular and the first example that uses the blockchain technology which is announced

Figure 1
Blockchain Data Structure



in 2008 [22]. The digital currency Bitcoin itself is highly argumentative but the underlying blockchain technology has found wide range of applications in financial and non-financial worlds.

Decentralization is a core strength for blockchain since a copy of the blockchain data is owned by all actors. It provides a highly redundant infrastructure. To ensure the integrity of each record on different nodes, a consensus algorithm is required. The consensus algorithm allows the network members to ensure that each added block is legitimate and not falsified. The blockchain does not require trust. Therefore, it does not require any third party to provide a trusted environment for transactions. It creates a trust model based on a group consensus that the network verifies transactions and allows the block to be added to the chain.

Blockchain has roughly three types of networks: public, private and consortium [4]:

- *Public* – No one owns public blockchains. All records in the public blockchain are visible to the public and everyone could take part in agreeing on a consensus. This blockchain network type is theoretically the most decentralized form.
- *Private* – For the private blockchain, only nodes belong to a particular organization would be allowed to join the consensus process. A private blockchain can be thought as a centralized network since it is under the control of one organization.
- *Consortium* – The consortium blockchain is constructed by the participation of several organizations. It is semi decentralized since only a small number of nodes would be selected to join the consensus process.

Due to the hierarchical structure of our contribution, private blockchain used at first level and consortium blockchain networks are used at second level. In the light of the above-mentioned properties, blockchain has four main characteristics [31]:

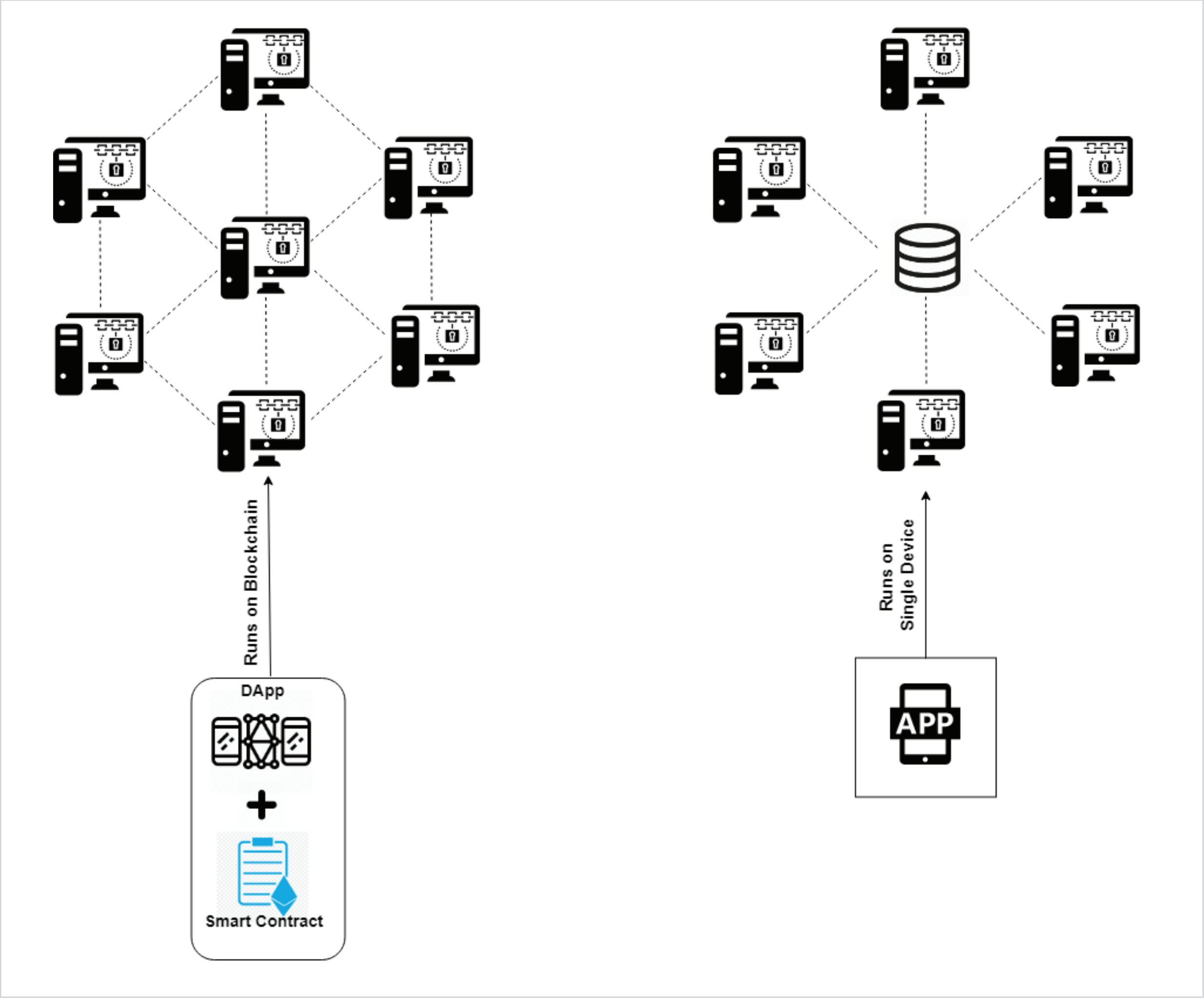
- *Decentralized (Redundant)*: All blockchain network member nodes have a copy of the blockchain file. This creates decentralization and redundancy for the transactional history.
- *Tamper-Proof (Immutable)*: The blockchain keeps the transaction records in a permanent manner. Once a block is added to the chain, it is not changeable since the block includes a hash pointer for the previous block on that chain. Since all blockchain network members keep the same copy of data, any altered blocks on that chain will be invalid. Thus, such alteration can easily be noticed by the other blockchain network members and the block is discarded.
- *Consensus Oriented:* In other words, the main principle is the verification of trust. To add a block to the blockchain, the block must be verified via a consensus algorithm to prove that the required consensus is achieved.
- *Transparency*: Since the blockchain data is stored on an open file, every participant of the current network can access this data and analyze all transaction history.

When the idea of smart contracts appeared towards the end of the 1990s, these contracts were defined as digital contracts which operate when the necessary conditions occur like the traditional contracts [30]. According to Christidis and Devetsikiotis, smart contracts can be expressed as digital programs based on a platform-specific blockchain consensus protocol, which will be executed automatically when the terms of the agreement are fulfilled and self-implemented due to its decentralized structure, without intermediaries and by the protection against interferences [9]. It is not possible to run smart contracts on every blockchain platform. Blockchain platforms like Ethereum [35], Hyperledger Fabric [5] and NEM [14] can store and run smart contracts.

Unlike today's centralized Web or mobile applications (CAPP), DApps are transparent, traceable, flexible, and better incentive anti-centralized applications that do not run on a central server or machine. The information about the application is also not stored in a central database. Data is stored on blockchain or distributed storage solutions like Storj [34] and IPFS [2]. Due to the decentralized operation of the DApps on the blockchain network and the data being distributed on the blockchain, the failure of any machine in the blockchain network will not make the application and data inaccessible [28]. Because the same data and application will exist in any blockchain member and be accessed from any members of the blockchain network. In our case, it means that COVID-19 test software will never crash down. The operation logic of a DApp and a centralized application is given in Figure 2.

Figure 2

DApp vs CApp



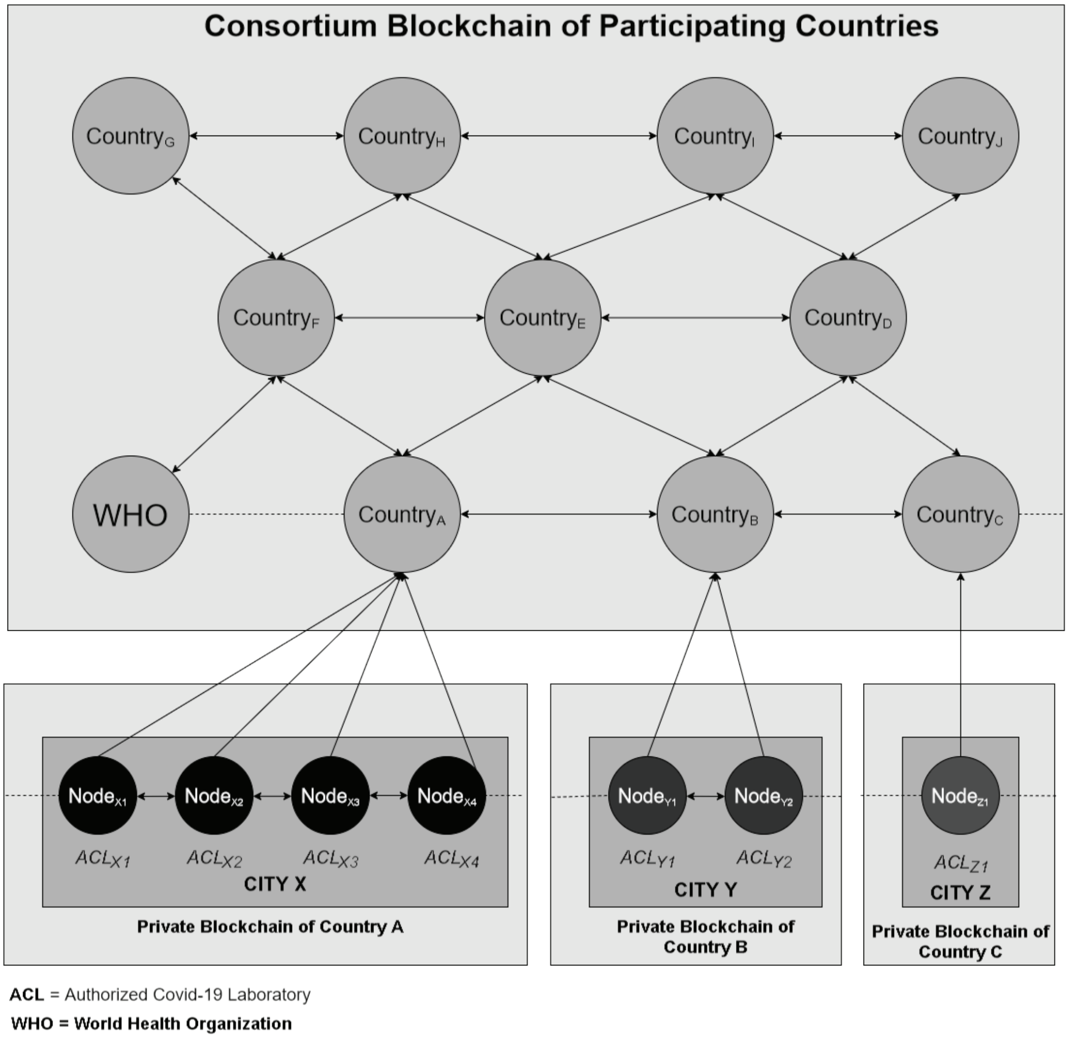
3. Secure Information Sharing for COVID-19

3.1. The Network for COVID-19 Information Sharing

First, we proposed a blockchain-based secure COVID-19 information sharing network. Then, we proposed a smart contract-based COVID-19 test software. Authorized COVID-19 Laboratories (ACL) exist in different cities around the world. Laboratory Information Management Systems (LIMSs) software is used in ACLs to keep records. When a COVID-19 test results is received, the information regarding the patient is recorded through this software. After recoding the COVID-19 data through the LIMS software, data is then made accessible from a main central software, which is the Public Health Management System (PHMS). Figure 3 outlines our contributions to this field which are the ability of multiple stakeholders, such as Authorized COVID-19 Laboratories, cities, countries and WHO to securely interact with the blockchain. PHMS software is used for country nodes, and LIMS software is used for ACL nodes.

Figure 3

Our Proposal: Blockchain Based COVID-19 Information Sharing Network


Consortium Blockchain of Participating Countries
CountryG
CountryH
CountryI
CountryJ
CountryF
CountryE
CountryD
WHO
CountryA
CountryB
CountryC
NodeX1
NodeX2
NodeX3
NodeX4
ACLX1
ACLX2
ACLX3
ACLX4
CITY X
Private Blockchain of Country A
NodeY1
NodeY2
ACLY1
ACLY2
CITY Y
Private Blockchain of Country B
NodeZ1
ACLZ1
CITY Z
Private Blockchain of Country C
ACL = Authorized Covid-19 Laboratory
WHO = World Health Organization

3.2. Proposed COVID-19 Information Handling Algorithms

Table 1 shows the abbreviations for variables used in the proposed algorithms. Algorithm 1 shows how patient nodes interact with their COVID-19 information, Algorithm 2 shows how country nodes interact with COVID-19 information of patients of other countries and Algorithm 3 shows that how ACL nodes are interacting with COVID-19 information of patients.

Table 2

Abbreviations for Algorithms

Variable	Explanation
P_{ID}	Patient ID
N_A	Network Admin
BC_N	Blockchain Network
C_{ID}	Country ID
ACL_{ID}	Authorized COVID-19 Lab ID
P_{C_REC}	Patient COVID-19 Record

Algorithm 1

Patient Interaction Algorithm

```
Result: Give grant to patient for writing, updating or reading its COVID-19 Records initialization;
while True do
    if $P_{ID}$ in $BC_N$ then
        if $P_{C\_REC}$ not in $ACL_{ID}$ then
            create_covid_records($P_{ID}$ , $P_{C\_REC}$ , $BC_N$)
        else
            update_covid_records($P_{ID}$ , $P_{C\_REC}$ , $BC_N$)
            read_covid_records($P_{ID}$ , $P_{C\_REC}$ , $C_{ID}$ , $ACL_{ID}$ , $BC_N$)
        end
    else
        not_in_records()
    end
end
```

Algorithm 2

Authorized Country Working Algorithm

```
Result: Get grant for adding or updating COVID-19 Records initialization;
while True do
    if $C_{ID}$ in $BC_N$ then
        if authorized($P_{C\_REC}$) in $C_{ID}$ then
            read_covid_records($C_{ID}$ , $P_{C\_REC}$ , $BC_N$)
            alter_covid_records($C_{ID}$ , $P_{C\_REC}$ , $BC_N$)
        else
            ask_authorization($C_{ID}$)
        end
    else
        not_in_records()
    end
end
```

Algorithm 3

Authorized COVID-19 Lab Working Algorithm

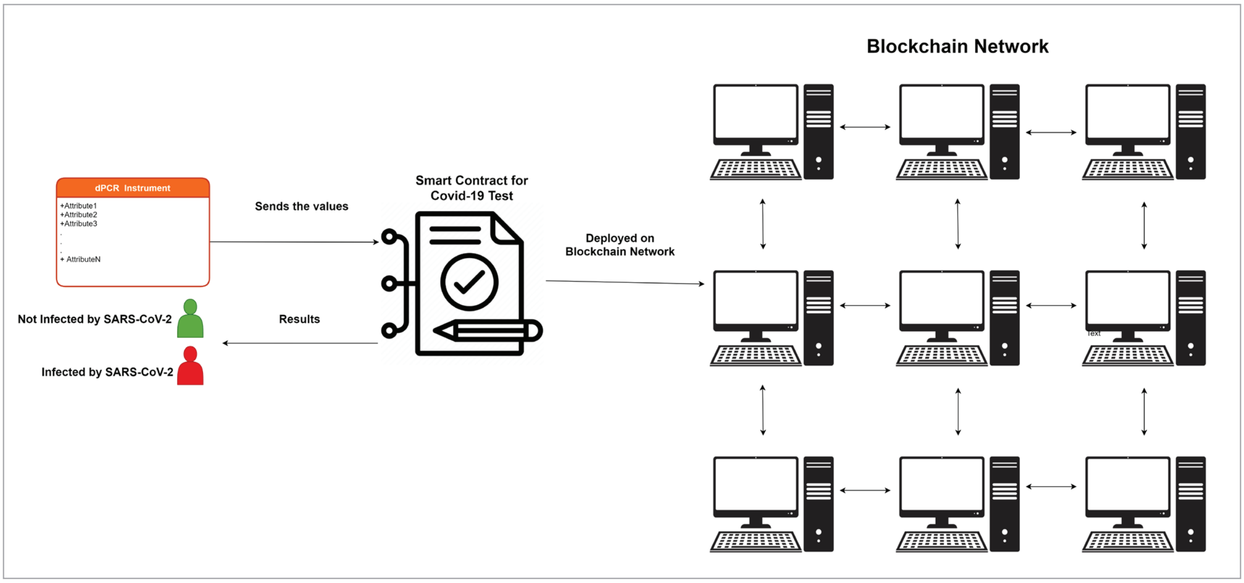
```
Result: Get grant for writing or reading COVID-19 Records initialization;
while True do
    if $ACL_{ID}$ in $BC_N$ then
        if authorized($P_{C\_REC}$) in $ACL_{ID}$ then
            read_covid_records($ACL_{ID}$; $P_{C\ REC}$;$BC_N$)
            write_covid_records($ACL_{ID}$; $P_{C\ REC}$;$BC_N$)
        else
            ask_authorization($C_{ID}$)
        end
    else
        not_in_records()
    end
end
```

3.3. Proposed Decentralized COVID-19 Test Software Operation

Taq DNA Polymerase Enzyme, Taq DNA Polymerase Buffer, forward primer, reverse primer, dNTP, $MgCL_2$, Genomic DNA template and nuclease-free water reagents are put in tubes with test swabs for PCR tests. Each reagent component must be vortex and spin before use to pellets of material forming in the storage tube. Those tubes with the compound put in the test instrument. In the present case after the test is finished, the results are shown in the centralized computer software. However, in our proposed decentralized case in Figure 4, decisive mechanisms of this test software can be programmed as smart contracts in a distributed manner. Attributes at dPCR instrument in Figure 4 represents compounds those include different patients' swabs. After the smart contract is finished its process test results will be written to blockchain that the current ACL computer participated. Any results request can made to blockchain after this process. According to our proposal in the Figure 4 smart contracts are deployed on the same consortium blockchain network where patient, country and ACL nodes exist.

Figure 4

Our Proposal: Decentralized COVID-19 Test Software Operation

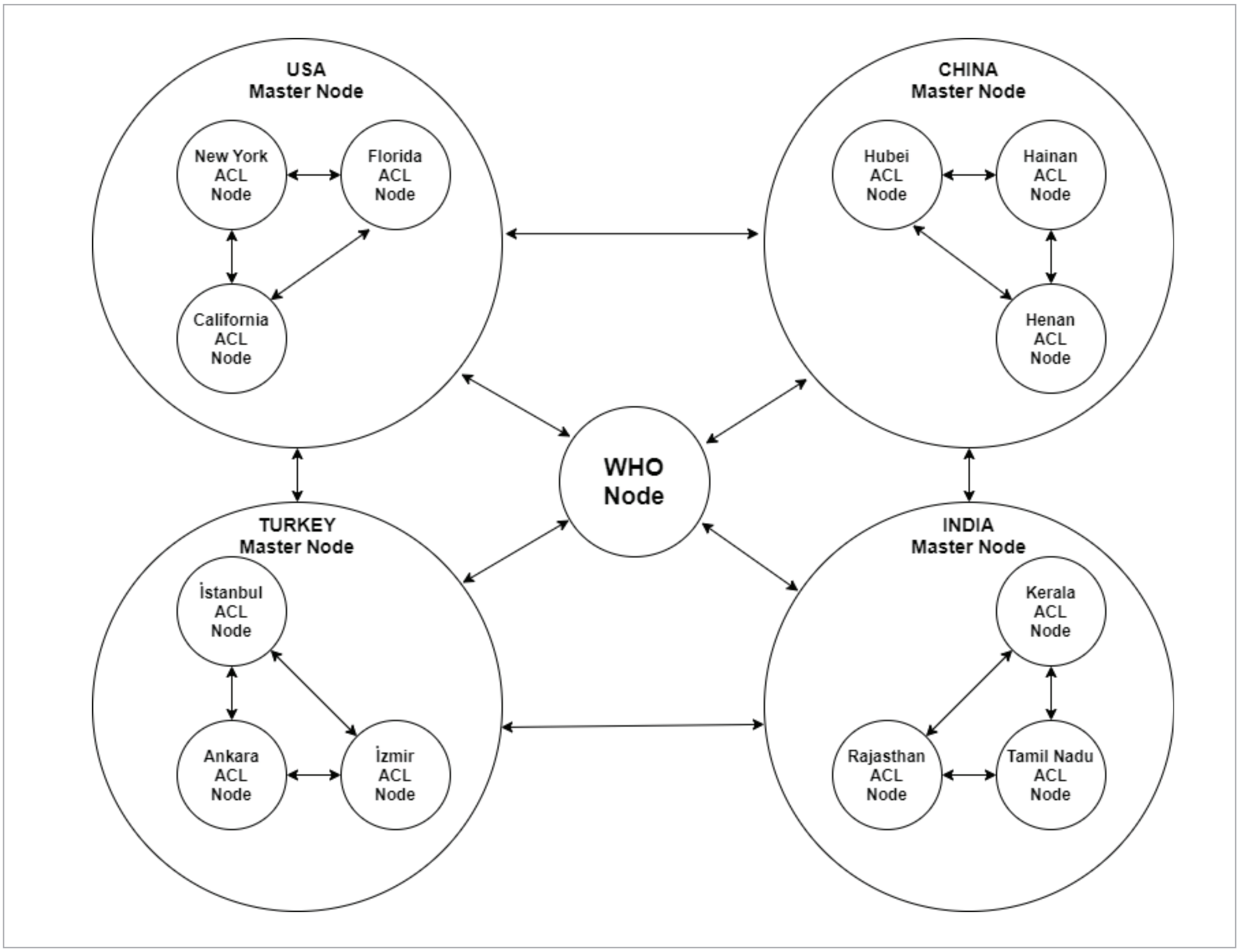


4. Case Study: Trusted Information Sharing Among Countries for COVID-19

As stated in Figure 5, our trusted COVID-19 information sharing among countries will be established in a distributed manner by using the blockchain technology. In our case study, the USA, China, Turkey, and India are considered as participants of our proposed trusted COVID-19 information sharing platform. We assumed that each of these four countries have at least one master node in that consortium blockchain network. These master nodes will belong to the state ministry of health institutions or an equivalent authorized institution of countries. These master nodes are also the members of different private blockchains of their specific countries. In Turkey example of these private blockchains, nodes are created from ACL computers, which keep COVID-19 information of patients in the related laboratories. In order to provide absolute and immutable accuracy for COVID-19 test results these ACL computers will run the distributed

Figure 5

Case Study: Consortium Blockchain for Trusted COVID-19 Information Sharing Between USA, China, Turkey, and India



software and smart contract that explained in Section 3.3. In addition to these a smart contract implementation of Algorithm 3 will audit the COVID-19 data interactions of those ACL workers.

That master nodes of countries are behaving as interfaces between the private blockchains and the consortium blockchain, which consists of the USA, China, Turkey, India and the WHO nodes.

In case of any information gathering request from one of the participating countries, the related master node implements the smart contract implementation of Algorithm 2 that will audit the COVID-19 data interactions of those master nodes to check the request owner authorization. If the owner of the request is authentic, then the information will be provided to requester master node.

A smart contract implementation of Algorithm 1 should be integrated with electronic health applications, such as e-Nabız application that belongs to Turkey Ministry of Health, for give grant to patients to manage their permissioned health records. In that case, decisive algorithms of e-Nabız must be implemented as smart contracts. Taking into account the possibility that not every country has such an application as e-Nabız or any other reasons like laws and regulations, not all participating countries can provide that. However, nobody can deny the fact that the blockchain technology and smart contracts will provide faster and more trusted COVID-19 information sharing and data integrity among the participating countries.

5. Conclusion and Future Works

It is obviously known that many of the software for health sector are highly expensive. This is due to the monopolized nature of this field. Since almost all software is closed source, it is almost impossible to analyze the code behind the software for security and privacy issues. All these conditions are the same for dPCR software. Blockchain technology presents a solution to prevent that monopolization. Any PCR software can be implemented as a decentralised application, DApp, to run on a blockchain network. However, there could be some privacy issues on health data. Therefore, the selection of an existing blockchain platform or creating a novel blockchain platform should be carefully considered. If there are any privacy or security issues in the selected blockchain platform, health data can also be used by malicious actors. Therefore, a proper implementation of our proposal will bring highly secure, private and a cheaper solution. However, any incorrect application will result in unpredictable results for both heath sector representatives and patients.

In our scenario, all participating parties of the consortium blockchain joins this network regardless of their privacy concerns. Therefore, we may say that some patients or countries will require some anonymization to protect their identifications and COVID-19 related health information. For this purpose, cryptological mixing methods can be used. This topic should be investigated in future studies.

References

1. Act, A. Health Insurance Portability and Accountability Act of 1996. Public Law, 1996, 104, 191.
2. Benet, J. Ipfs-Content Addressed, Versioned, p2p File System. arXiv PrePrint arXiv, 2014.
3. BGI. COVID-19 Local Laboratory Solution. accessed 2021-05-08]; Available from: https://www.bgi.com/global/covid-19-local-laboratory-solution/
4. Buterin, V. On Public and Private Blockchains. Ethereum Blog, 2015, 7, 180.
5. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016, Chicago, IL.
6. Cao, S., G. Zhang, P. Liu, X. Zhang, Neri, F. Cloud-Assisted Secure eHealth Systems for Tamper-Proofing EHR via Blockchain. Information Sciences, 2019, 485, 427-440. https://doi.org/10.1016/j.ins.2019.02.038
7. Carlos, W.G., C.S. Dela Cruz, B. Cao, S. Pasnick, Jamil, S. Novel Wuhan (2019-nCoV) Coronavirus. American Journal of Respiratory and Critical Care Medicine, 2020, P7-P8. https://doi.org/10.1164/rccm.2014P7
8. Chen, N., M. Zhou, X. Dong, J. Qu, F. Gong, Y. Han, Y. Qiu, J. Wang, Y. Liu, Wei, Y. Epidemiological and Clinical Characteristics of 99 Cases of 2019 Novel Coronavirus Pneumonia in Wuhan, China: A Descriptive Study. The Lancet, 2020, 395(10223), 507-513. https://doi.org/10.1016/S0140-6736(20)30211-7
9. Christidis, K., Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 2016, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339
10. Dannen, C. Introducing Ethereum and Solidity. Springer, 2017, 318. https://doi.org/10.1007/978-1-4842-2535-6
11. Digital, P. FastPCR is an Integrated Tool for PCR Primers or Probe Design. Accessed 2021-05-08]; Available from: https://primerdigital.com/fastpcr.html.
12. Director-General, W. Who Director-General's Opening Remarks at the Media Brieng on COVID-19, 2020.
13. Ekblaw, A., A. Azaria, J. D. Halamka, Lippman, A. A Case Study for Blockchain in Healthcare: «MedRec» Prototype for Electronic Health Records and Medical Research Data. In Proceedings of IEEE Open & Big Data Conference, 2016.
14. Foundation, N. NEM Thr Smart Asset Blockchain. Accessed 2021-05-08; Available from: https://nem.io/.
15. Hall Sedlak, R., Jerome, K. R. The Potential Advantages of Digital PCR for Clinical Virology Diagnostics. Expert Review of Molecular Diagnostics, 2014, 14(4), 501-507. https://doi.org/10.1586/14737159.2014.910456
16. Huang, C., Y. Wang, X. Li, L. Ren, J. Zhao, Y. Hu, L. Zhang, G. Fan, J. Xu, Gu, X. Clinical Features of Patients Infected with 2019 Novel Coronavirus in Wuhan, China. The Lancet, 2020, 395(10223), 497-506. https://doi.org/10.1016/S0140-6736(20)30183-5

17. Ji, W., W. Wang, X. Zhao, J. Zai, Li, X. Cross-Species Transmission of the Newly Identified Coronavirus 2019-nCoV. Journal of Medical Virology, 2020, 92(4), 433-440. https://doi.org/10.1002/jmv.25682

18. Linn, L. A., Koo, M. B. 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, 2016.

19. Lu, H., C. W. Stratton, Tang, Y. W. Outbreak of Pneumonia of Unknown Etiology in Wuhan, China: The Mystery and the Miracle. Journal of Medical Virology, 2020, 92(4), 401-402. https://doi.org/10.1002/jmv.25678

20. Markets and Markets. Digital PCR (dPCR) and Real-time PCR (qPCR) Market. Accessed 2021-05-08; Available from: https://www.marketsandmarkets.com/Market-Reports/digital-pcr-market-174151204.html.

21. Munster, V. J., M. Koopmans, N. van Doremalen, D. van Riel, de Wit, E. A Novel Coronavirus Emerging in China-Key Questions for Impact Assessment. New England Journal of Medicine, 2020, 382(8), 692-694. https://doi.org/10.1056/NEJMp2000929

22. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2019, Manubot Reproduction.

23. Narayan, S., M. Gagné, Safavi-Naini, R. Privacy Preserving EHR System Using Attribute-Based Infrastructure. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, 2010. https://doi.org/10.1145/1866835.1866845

24. Narayanan, A., J. Bonneau, E. Felten, A. Miller, Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. 2016: Princeton University Press.

25. NCIRD. Locations with Confirmed COVID-19 Cases. Accessed 2021-05-08; Available from: https://www.cdc.gov/coronavirus/2019-ncov/global-covid-19/index.html.

26. Ochman, H., A. S. Gerber, Hartl, D. L. Genetic Applications of an Inverse Polymerase Chain Reaction. Genetics, 1988, 120(3), 621-623. https://doi.org/10.1093/genetics/120.3.621

27. Paulson, J. W., G. Succi, Eberlein, A. An Empirical Study of Open-Source and Closed-Source Software Products. IEEE Transactions on Software Engineering, 2004, 30(4), 246-256. https://doi.org/10.1109/TSE.2004.1274044

28. Raval, S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, 2016, O'Reilly Media.

29. Seol, K., Y.-G. Kim, E. Lee, Y.-D. Seo, Baik, D.-K. Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. IEEE Access, 2018, 6, 9114-9128. https://doi.org/10.1109/ACCESS.2018.2800288

30. Szabo, N. Formalizing and Securing Relationships on Public Networks. First Monday, 1997, 2(9). https://doi.org/10.5210/fm.v2i9.548

31. Viriyasitavat, W., Hoonsopon, D. Blockchain Characteristics and Consensus in Modern Business Processes. Journal of Industrial Information Integration, 2019, 13, 32-39. https://doi.org/10.1016/j.jii.2018.07.004

32. Wang, H., Song, Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. Journal of Medical Systems, 2018, 42(8), 1-9. https://doi.org/10.1007/s10916-018-0994-6

33. Wang, W., Y. Xu, R. Gao, R. Lu, K. Han, G. Wu, Tan, W. Detection of SARS-CoV-2 in Different Types of Clinical Specimens. JAMA, 2020, 323(18), 1843-1844. https://doi.org/10.1001/jama.2020.3786

34. Wilkinson, S., T. Boshevski, J. Brandoff, Buterin, V. Storj a Peer-to-Peer Cloud Storage Network, 2014. Accessed 2021-05-08; Available from: https://www.storj.io/storj2014.pdf.

35. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 2014, 151(2014), 1-32.

36. Xu, X.-W., X.-X. Wu, X.-G. Jiang, K.-J. Xu, L.-J. Ying, C.-L. Ma, S.-B. Li, H.-Y. Wang, S. Zhang, Gao, H.-N. Clinical Findings in a Group of Patients Infected with the 2019 Novel Coronavirus (SARS-Cov-2) Outside of Wuhan, China: Retrospective Case Series. BMJ, 2020, 368. https://doi.org/10.1136/bmj.m606