Special Section: Consumer Technology-Based Solutions for COVID-19

Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach

Keping Yu
Sichuan Normal University
Waseda University

Liang Tan
Sichuan Normal University
Chinese Academy of Sciences

Xinglin Shang
Sichuan Normal University

Junjie Huang
Sichuan Normal University

Gautam Srivastava
Brandon University
China Medical University

Pushpita Chatterjee
Old Dominion University

***Abstract*—COVID-19 is a major global public health challenge and difficult to control in a short time completely. To prevent the COVID-19 epidemic from continuing to worsen, global scientific research institutions have actively carried out studies on COVID-19, thereby effectively improving the prevention, monitoring, tracking, control, and treatment of the epidemic. However, the COVID-19 electronic medical records (CEMRs) among**

Digital Object Identifier 10.1109/MCE.2020.3035520
Date of publication 3 November 2020; date of current version 2 February 2021.

hospitals worldwide are managed independently. With privacy consideration, CEMRs cannot be made public or shared, which is not conducive to in-depth and extensive research on COVID-19 by medical research institutions. In addition, even if new research results are developed, the disclosure and sharing process is slow. To address this issue, we propose a blockchain-based medical research support platform, which can provide efficient and privacy-preserving data sharing against COVID-19. First, hospitals and medical research institutions are treated as nodes on the alliance chain, so consensus and data sharing among the nodes is achieved. Then, COVID-19 patients, doctors, and researchers need to be authenticated in various institutes. Moreover, doctors and researchers need to be registered with the Fabric certificate authority. The CEMRs for COVID-19 patients uses the blockchain's pseudonym mechanism to protect privacy. After that, doctors upload CEMRs on the alliance chain, and researchers can obtain CEMRs from the alliance chain for research. Finally, the research results will be published on the blockchain for doctors to use. The experimental results show that the read and write performance and security performance on the alliance chain meet the requirements, which can promote the wide application of scientific research results against COVID-19.

In December 2019, people were strongly attacked by a new type of coronavirus pneumonia, COVID-19.[1] This virus causes a high rate of acute respiratory infections that are difficult to control.[2] According to data released by the World Health Organization, as of July 20, 2020, the cumulative number of confirmed cases worldwide has reached 14 million, and the deaths have exceeded 650 000. In order to control the spread of the virus, most countries have adopted measures such as quarantines and border closures, which have effectively contained the spread of the epidemic to a large extent. However, the epidemic has stalled the economies of many countries and disrupted global supply chains, which has also had a significant impact on world economic development.[3,4]

The most basic way to face this epidemic is to strengthen medical research cooperation and develop new coronavirus vaccines.[5] The development of the vaccine requires a large number of new cases of COVID-19 as a reference. Moreover, if data from researchers' experiments are not shared and recorded in a timely manner, it will not only lead to a large number of duplicate experiments around the world, but it will also not guarantee the accuracy of the results from medical research institutions.[6,7] However, in order to protect patient privacy, case data from each hospital are currently independent of each other and CEMRs cannot be made public and shared, which is not conducive to the in-depth study of COVID-19 at each research institution, nor is it conducive to the safe sharing of research results. To facilitate research on COVID-19, it is urgent for the current society to design a plan for sharing CEMRs. However, some pressing issues need to be addressed. For example, patient privacy must not be disclosed.[8] When sharing research results, it is important to protect the intellectual property rights of the researchers. Furthermore, the data shared must be authentic and cannot be tampered with the work of Yu *et al.*[9] and Guo *et al.*[10]

Currently, clouds or databases maintained by administrators are often used to manage data, which can lead to the destruction and manipulation of private data. Blockchain is a distributed database ledger that is decentralized, traceable, and nontamperable.[11,12] Blockchain nodes are able to share data and maintain the ledger collectively, using consensus mechanisms to ensure data consistency.[13,14] In addition, blockchain has a time sequence, which can solve the problem of copyright of scientific research results. When research results are successfully uploaded to the chain, ownership can be determined based on a timestamp[15]. Thus, blockchain is superior to cloud and database in terms of tamper-proofing, privacy protection, and temporal sequencing. To

this end, this article proposes a blockchain-based COVID-19 medical research platform for CEMRs. This platform uses the characteristics of the alliance chain to be safe, trustworthy, and nontamperable so that data can be shared in a timely and safe manner. Hospitals and medical research institutions are respectively used as nodes in the alliance chain. Among them, node users such as patients, doctors, and researchers need to register and authenticate on the blockchain before data transmission and query. In order to protect the privacy of patients, this platform uses a pseudonym mechanism to share CEMRs. The CEMRs of patients are stored on the platform, and researchers can obtain the patients' CEMRs and upload relevant research results from the platform. The application platform based on the alliance chain in this article can not only quickly share data, but also ensure the copyright issues of research results. To jointly overcome the COVID-19 hurdle and facilitate research progress, a shared medical research support platform is the optimal choice.

The rest of this article is organized as follows. The "Problem Statement" section describes the problems faced. The structure and functions of the platform are illustrated in the "Blockchain-Based Medical Research Support Platform" section, and the "Security Analysis" section mainly shows the performance analysis of the experiment. Finally, "Experiment Analysis" section summarizes the full text.

PROBLEM STATEMENT

AT PRESENT, researchers and medical experts are actively combating COVID-19. With the joint efforts of countries around the world, measures to prevent and control COVID-19 continue to be improved. However, there are still many problems need to be solved in the current medical environment.

Problem 1: Although vaccines are being developed globally based on patient conditions, vaccine research is also in a closed state. Medical research institutions are unable to share vaccine research data in a timely manner, which results in a relative lag in vaccine research.

Problem 2: Doctors in each hospital only study cases based on patients in their own hospitals. Although hospitals around the world have accumulated enough medical information, the medical information held by each hospital is usually not comprehensive. Therefore, real research on COVID-19 cases has the characteristics of small research samples, high repetition rate, and small amount of effective data, resulting in insufficient research on COVID-19, which is not conducive to the prevention and treatment of COVID-19 patients.

Problem 3: The sharing of COVID-19 research results across hospitals is not well developed, this may result in the most advanced research results and treatment options not being disseminated to every hospital at the first opportunity. It will cause patients to miss the best treatment period. Therefore, the slow disclosure and sharing of research results is also an urgent issue in the current healthcare environment.

Question 4: Although traditional sharing schemes such as databases and cloud storage can provide sufficient capability to share sample data in a timely manner, they cannot guarantee the immutability of data and the intellectual property rights of research results.

BLOCKCHAIN-BASED MEDICAL RESEARCH SUPPORT PLATFORM

In order to solve the above problems in the "Problem Statement" section, a blockchain-based medical research support platform is proposed to promote the sharing of CEMRs and COVID-19 research results. The platform can protect the privacy of patients and the research results and intellectual property rights of doctors, as well as hospitals and medical research institutions.

The platform is based on the alliance chain and integrates node access control mechanisms. Figure 1 describes the architecture of blockchain-based medical research support platform, which includes four entities as follow.

1) *Fabric Alliance Chain*. Fabric alliance chain is used to store the CEMRs of COVID-19 patients and the COVID-19 research results of medical researchers. The nodes of the alliance chain are composed of

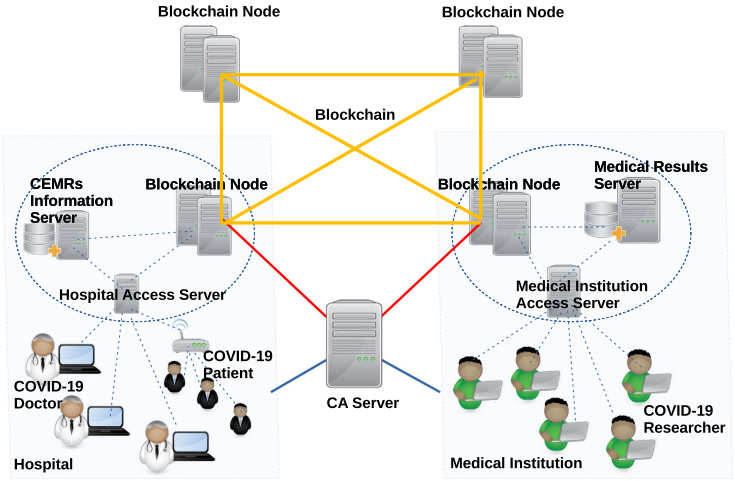

Figure 1. Architecture of blockchain-based medical research support platform.

hospitals or medical scientific research institutions.

2) *Fabric CA Server*. Fabric CA provides PKI-based identity authentication management service for Fabric. Fabric CA provides, based on Ecert and Tcert, can achieve very flexible permission control and audit according to business requirements, and provides Fabric with the foundation of trust for the alliance chain.
3) *Hospital*. Hospital is a medical organization that treats COVID-19, including personnel and basic information systems. Personnel includes managers, doctors, and patients. The basic information system includes an access control server and CEMRs information server.
4) *Medical Institution*. Medical institutions are specialized in COVID-19 research institutions. It also includes personnel and information systems. The personnel includes managers and scientific researchers, and the information system includes access control servers for medical institutions and medical results servers.

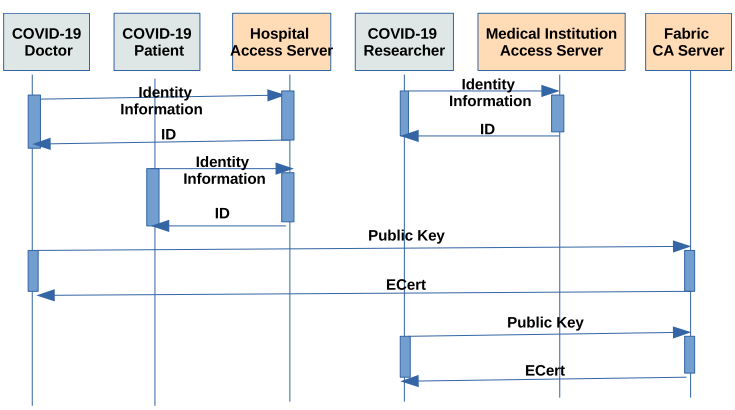

Figure 2. User registration in hospital, medical institution, and Fabric CA.

Registration

The registration of this platform includes two parts. One is that users of hospitals or medical institutions register in the access server. The other is that users of hospitals or medical institutions register in the alliance chain Fabric CA.

1) *User Registration in Access Server*. COVID-19 doctor and patient need to register in the hospital access server, while the COVID-19 researcher should register in the medical institution access server. As shown in Figure 2, the doctor and the patient send their identity information to the hospital access server, and after verifying the identity information, the hospital access server returns the legal ID to the doctor and the patient. The same applies to the researchers in the medical institution.
2) *Users Register in Fabric CA*. COVID-19 doctors in the hospital and COVID-19 researchers in the medical institutions register with the Fabric CA, as shown in Figure 2. The doctor sends the public key to the Fabric CA through the hospital access server and the Fabric CA issues Ecert to corresponding doctors through the hospital access server. The same applies to the researchers in the medical institutions.

Authorization

The alliance chain is created and managed by multiple business-related organizations, and can share CEMRs and COVID-19 research results among multiple hospitals or medical institutions. However, to protect the personal privacy of COVID-19 patients, doctors should obtain patient authorization before

uploading CEMRs. If patients agree to share CEMRs, doctors can share the patient's CEMRs with other hospitals or medical institutions under a pseudonym through the alliance chain. At the same time, to ensure that CEMRs and research results are only shared within the alliance chain, only users authorized by the nodes of the alliance chain can perform operations such as query and upload. The specific authorization process is shown in Figure 3.

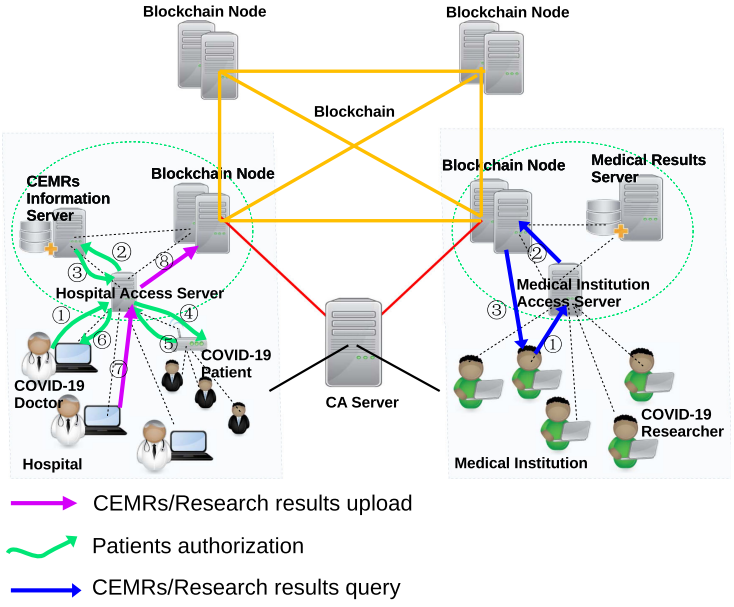

Figure 3. CEMRs sharing and user operation authorization.

CEMRs Sharing Authorization To protect the privacy of the COVID-19 patient, doctors uploading CEMRs must request authorization from patients, as shown in Figure 3. However, during the authorization process, a large number of patients may refuse authorization for fear of exposing their privacy. Therefore, the hospital will take steps to allay the patient's concerns. (a) Use a pseudonym mechanism to handle patient privacy information. When a doctor requests authorization from a patient, the patient can use his or her private key to generate pseudorandom numbers to replace the real name on the CEMRs. (b) Encourage patients to actively authorize with their doctors, and hospitals offer a partial medical fee waiver benefit to encourage patients to share CEMRs for COVID-19 research. The following is the process for doctors to request CEMRs authorization from patients.

Step 1: Doctor sends authorization request for use of CEMRs to hospital via ID distributed by hospital access server.

Step 2: After receiving the request, the hospital verifies whether the doctor's ID is legal. If the ID is illegal, the hospital will directly return the doctor's request as "reject the request." If the doctor's ID is legal, the hospital will check whether there is an authorized CEMR in the local database. If there is no authorized CEMR, it will proceed to *Step 3*. If there is an authorized CEMR, proceed directly to *Step 6*.

Step 3: The hospital sends a request to the COVID-19 patient, requesting to share the CEMRs of patient.

Step 4: Patients can choose whether or not to share their CEMRs. If COVID-19 patients agree to share CEMRs, the CEMR will be anonymized. First, the patient hashes his private key to generate a pseudo-random string, and then replaces the user name of CEMRs with the pseudo-random string as a pseudonym, and uses random data to replace private information such as contact information and address. Finally, send "Agree to authorize CEMRs" to the hospital. If patients do not agree to share CEMR, return "Refused to share CEMRs."

Step 5: If the hospital receives "Agree to authorize CEMRs," it will mark the CEMRs as authorized in the database, and then proceed to *Step 6*. If the hospital receives "Refused to share CEMRs," it will return to the doctor "Refused to authorize."

Step 6: The hospital will return to the doctor "a request for consent to use CEMR."

User Operation Authorization To protect the sharing of CEMRs and research results in the alliance chain, users on the chain need the authorization of organization to perform operations such as querying and uploading data. When a user is registered, each institution assigns an ID to facilitate identification of the user. When a doctor is registered, the "doctorID" is returned. Similarly, when patients

and researchers are registered, "patientID" and "researcherID" will be returned. Then when the user sends an operation request, the organization verifies whether the identity is legal according to the user ID and then processes the request. Here, we take the example of a researcher, as follows.

Step 1: Researcher sends an "operation request" to medical institutions. This "operation request" is divided into two types: query CEMRs /research results and upload research results.

Step 2: The medical institution checks whether the identity of the researcher is legal according to the researcher ID. If the researcher ID is legal, the medical institution will agree to the request and execute the request. Otherwise, the medical institution will reject the request.

CEMRs and Research Results Upload and Query

All CEMRs and research results on the alliance chain are shared with the node organizations on the chain, and legally authorized users in each organization can query data through the access server. In order to ensure the validity and credibility of uploading CEMRs and research results, different institutions have different permissions. Currently, most hospitals use real-name registration methods to assign IDs to COVID-19 patients. Patients are assigned IDs and CEMRs addresses when registering. Among them, CEMRs include treatment data and user names, contact information, and patients' other private information. Therefore, when COVID-19 doctors request CEMRs for authorization, patients will use a pseudonym mechanism to anonymously process CEMRs and authorize them in order to avoid privacy leakage.

CEMRs or Research Results Upload Doctors and researchers who have obtained user operation authorization upload CEMRs/research results to the alliance chain through access server, and the uploaded CEMRs/research results can be viewed by doctors and researchers together. The upload operation process of CEMRs is as follows.

Step 1: The doctor sends ID, Ecert, and upload request for authorized CEMRs to the hospital access server.

Step 2: The hospital access server determines whether the doctor belongs to the hospital based on the ID. If it is not a doctor in this hospital, the request will be directly rejected. Otherwise, the hospital access server will check the doctor's request and perform *Step 3*.

Step 3: If the request is to upload CEMRs, the hospital access server will send the pseudonymous addresses of Ecert and CEMRs to the hospital blockchain node. The hospital blockchain node will verify whether the Ecert is valid. If the Ecert verification is valid, the smart contract is used to upload the pseudonymous addresses of CEMRs to the alliance chain. Otherwise, the upload fails.

In addition, the process of uploading research results to the medical institution's blockchain node is similar to the process described above. The only difference is that it does not require anonymization for research results in the *Step 3*.

CEMRs or Research Results Query Doctors and researchers can query CEMRs/research results to the alliance chain through access server. The process for a doctor to query CEMRs/research results from a hospital is as follows.

Step 1: The doctor sends the ID, Ecert, and query request to the hospital access server.

Step 2: The hospital access server judges whether the doctor is legal according to the ID. If not, the request will be rejected. Otherwise, the hospital access server will check the doctor's request and perform *Step 3*.

Step 3: If the request type is to query CEMRs/research results, the hospital access server will send Ecert to the hospital blockchain node, and the hospital blockchain node will verify whether the Ecert is valid. If the Ecert verification is valid, the hospital blockchain node returns CEMRs/research results to doctors through the hospital access server. Otherwise, the query fails.

Moreover, the process by which researchers request medical institutions to inquire about CEMRs/research results is similar to the process described above.

SECURITY ANALYSIS

1) *Privacy Protection.* This solution uses a pseudonym mechanism to deal with the patient's private information. When a

doctor sends an authorization request to a patient, the patient will use his or her private key to generate hashed pseudorandom strings to replace the real name on the CEMR for privacy protection.

2) *Anti-Tampering*. The composition of the block contains Merkel root, and according to the characteristics of the hash function, once a transaction is tampered with, it will result in a change in the hash of the entire block. Therefore, the blockchain is the best means to prevent tampering.
3) *Copyright Protection of Scientific Research Results*. Blockchain has a temporal sequence, and the ownership of scientific research results can be guaranteed by time stamps, which can avoid the legal problems due to copyright.

EXPERIMENT ANALYSIS

Experimental Environment

The consortium chain used by the medical platform in this article is implemented by Fabric v1.4.0. The operating environment is Ubuntu Linux 20.04LTS, Intel core i7-5500u CPUx4 2.40 GHz, and the memory is 8 GB. In order to verify whether the blockchain-based medical platform meets the performance requirements of reading and writing and whether it is superior to traditional databases, we use Hyperledger caliper to evaluate the framework and give the following three metrics.

1) *Throughput*: Throughput is an important indicator for evaluating the performance of a blockchain network. It represents the number of transactions that the network can process per second. In the medical support platform, if the number of CEMRs or research results that can be processed per second is greater, it proves that the platform can provide doctors or researchers with more CEMRs and research results per unit time.
2) *Resource Consumption*: Caliper supports the evaluation of memory, CPU and other resource consumption when fabric is working. When doctors or researchers query and upload CEMRs or research results through the client, the ability to consume resources reflects the availability of the medical platform. Therefore, resource consumption is also an indicator that needs our attention.
3) *Latency*: Latency is also a performance indicator that the blockchain network focuses on. It refers to the time delay from initiating an upload to a successful upload. In caliper, the average delay, maximum delay and minimum delay can be measured. Combined with the above indicators, it can be evaluated whether the blockchain-based medical support platform is better than the traditional database.

Experimental Process

This experiment uses a multimachine multinode organization method to construct a fabric network, and mainly builds and installs related dependencies on the Fabric network environment to ensure that the final network can operate normally. To verify the feasibility of the blockchain-based medical platform solution, the fabric network topology we designed includes two hospital organizations, a research organization, and a sorting service. The consensus method of the sorting service is based on kafka. In addition, in order to enable the medical platform to operate, the fabric network needs to be built. The overall building process is as follows. (1) Generate public and private keys and certificates, creation blocks, and channels. (2) Configure the hospital organization, research institution organization, sorting service, and client. (3) Use docker to start the fabric container. (4) Create a channel. (5) Add hospital organizations and research institutions to the channel. (6) Install the chain code on the peer node of the hospital organization or the research institution organization and instantiate it.

When the network is successfully built, it enters the FABRIC container and can query or upload CEMRs and research results using the command call chain code. In this experiment, the databases of both hospital and research institution nodes use leveldb to store CEMRs or research results, and we choose Hyperledger caliper, a general framework for blockchain performance testing, to test the performance of fabric networks, such as CPU occupancy and other

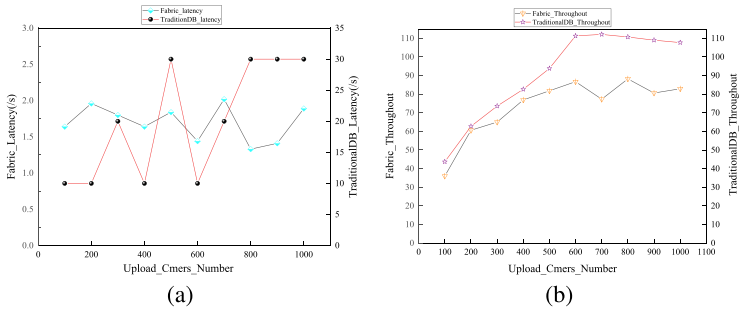

Figure 4. (a) Latency comparison between Fabric and traditional database for uploading CEMRs. (b) Throughput comparison between Fabric and traditional database for uploading CEMRs.

performance indicators. The complete testing process is as follows.

(1) Install Hyperledger caliper v0.2.0 by using local npm install.

(2) Bind the fabric version number through caliper.

(3) Specify the caliper's baseline configuration file and the fabric's configuration file behind the npx caliper launch master to generate a performance report in html format. Based on this performance report, it is confirmed that the blockchain-based medical support platform outperforms the traditional database.

Performance Analysis

CEMRs storage Different organizations are deployed throughout the network, and the deployed organizations can implement CEMRs upload operations in the container. According to the performance analysis report of caliper, a comparison chart of the delay in uploading CEMRs between traditional databases and blockchain-based medical platforms is obtained, as shown in Figure 4(a). Figure 4(a) points out that the delay of uploading CEMRs on this medical platform is in the range of 0–3 s, while the delay of traditional databases is in the range of 9–30 s. Figure 4(b) shows the throughput comparison of traditional databases and blockchain-based medical platforms when uploading CEMRs. From the comparison of throughput, it can be seen that although the throughput of uploading CEMRs in traditional databases is slightly higher than that of medical platforms, from the perspective of overall read and write, medical platforms based on blockchain have more advantages than traditional databases.

CEMRs acquisition When CEMRs are uploaded to the Blockchain Node, either doctors or researchers can read the CEMRs through the client. Caliper's test report concluded that the medical platform not only meets the needs of doctors or researchers for querying CEMRs, but also shows that the medical platform outperforms the traditional database in terms of latency and throughput. As shown in Figure 5(a), for querying CEMRs in the range of [0–1000], the latency of this medical platform always fluctuates in the range of 0–0.45 s, while the traditional database is within 0–7.5 s. Figure 5(b) gives the throughput comparison for querying CEMRs. As shown, when the number of query CEMRs is 600, the throughput of the traditional database is slightly higher than Fabric and the rest are lower than Fabric, which proves that the designed blockchain-based healthcare platform is superior to the traditional database in terms of throughput.

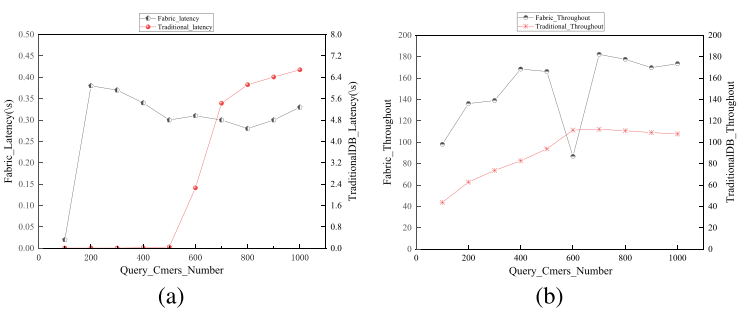

Figure 5. (a) Latency comparison between Fabric and traditional database for querying CEMRs. (b) Throughput comparison between Fabric and traditional database for querying CEMRs.

CONCLUSION

To cope with COVID-19, hospitals and medical research institutions should make full use of existing networks and blockchain technology to share CEMRs of COVID-19, thereby effectively improving the treatment, prevention, and vaccine development of COVID-19. In this article, we

propose a blockchain-based medical research support platform against COVID-19. This platform employs the characteristics of the alliance chain to be safe, trustworthy, and nontamperable so that CEMRs and research results can be shared in a timely and safe manner. Hospitals and medical research institutions are respectively used as nodes in the alliance chain. Among them, users such as patients, doctors, and researchers need to register and authenticate on the blockchain before CEMRs and research results transmission and query. In order to protect the privacy of patients, this platform uses a pseudonym mechanism to share CEMRs. The medical research support platform based on the alliance chain can not only quickly share CEMRs and research results, but also ensure the copyright issues of research results. In order to jointly overcome the COVID-19 difficulties and promote the progress of research, this proposal is efficient and effective.

ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61373162, in part by the Sichuan Provincial Science and Technology Department Project under Grant No. 2019YFG0183, in part by the Sichuan Provincial Key Laboratory Project under Grant No. KJ201402, and in part by the Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research (KAKENHI) under Grant JP18K18044. Liang Tan is the corresponding author.

REFERENCES

1. R. Abbas and K. Michael, "Covid-19 contact trace app deployments: Learnings from Australia and Singapore," *IEEE Consum. Electron. Mag.*, vol. 9, no. 5, pp. 65–70, Sep. 2020.
2. T. Singhal, "A review of coronavirus disease-2019 (covid-19)," *Indian J. Pediatrics*, vol. 4, pp. 281–286, 2020.
3. C. Rothe *et al.*, "Transmission of 2019-NCOV infection from an asymptomatic contact in Germany," *New England J. Med.*, vol. 382, no. 10, pp. 970–971, 2020.
4. M. A. Rahman, M. S. Hossain, N. A. Alrajeh, and N. Guizani, "B5g and explainable deep learning assisted healthcare vertical at the edge: Covid-19 perspective," *IEEE Netw.*, vol. 34, no. 4, pp. 98–105, Jul.\Aug. 2020.
5. C. Huang *et al.*, "Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China," *The Lancet*, vol. 395, no. 10223, pp. 497–506, 2020.
6. V. Rahmanian, M. H. Rabiee, and H. Sharifi, "Case fatality rate of coronavirus disease 2019 (covid-19) in Iran—a term of caution," *Asian Pacific J. Tropical Med.*, vol. 13, pp. 328–330, 2020.
7. R. F. Sear *et al.*, "Quantifying covid-19 content in the online health opinion war using machine learning," *IEEE Access*, vol. 8, pp. 91886–91893, 2020.
8. H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "Beeptrace: Blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond," in *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.3025953.
9. K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 8, pp. 2072–2085, Aug. 2015.
10. Z. Guo *et al.*, "Robust spammer detection using collaborative neural network in internet of thing applications," in *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2020.3003802.
11. L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77 215–77 226, 2020.
12. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "Authprivacychain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70 604–70 615, 2020.
13. C. Feng *et al.*, "PDKSAP : Perfected double-key stealth address protocol without temporary key leakage in blockchain," in *Proc. IEEE/CIC Int. Conf. Commun. China*, 2020, pp. 151–155.
14. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Inf.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
15. W. Liang, D. Zhang, X. Lei, M. Tang, K. Li, and A. Zomaya, "Circuit copyright blockchain: Blockchain-based homomorphic encryption for ip circuit protection," in *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2020.2993032.

Keping Yu is currently a Visiting Professor with the College of Computer Science, Sichuan Normal University, Chengdu, China. He is also a Researcher with Waseda University, Tokyo, Japan. He serves as the Editor for IEEE Open Journal of Vehicular Technology and Guest Editor for Sensors, Peer-to-Peer Networking and Applications, Energies, Intelligent Automation and Soft Computing, and IEICE Transactions on Information and Systems. Contact him at keping.yu@aoni.waseda.jp.

Liang Tan is currently a Professor with the College of Computer Science, Sichuan Normal University, Chengdu, China, and with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China. His research interesting includes cloud computing, big data, trusted computing, and network security. Contact him at jkxy_tl@sicnu.edu.cn.

Xinglin Shang is currently working toward a master's degree in computer application technology with Sichuan Normal University, Chengdu, China. Contact her at 1250919363@qq.com.

Junjie Huangis currently working toward a master's degree in computer application technology with Sichuan Normal University, Chengdu, China. Contact her at 929300141@qq.com.

Gautam Srivastava since 2014, has been a tenure-track position with Brandon University, Canada. He received the B.Sc. degree from Briar Cliff University, Sioux City, IA, USA, in 2004, and the M.Sc. and Ph.D. degrees from the University of Victoria, Victoria, BC, Canada, in 2006 and 2011, respectively. Contact him at srivastavag@brandonu.ca.

Pushpita Chatterjee is currently with the Old Dominion University, VA, USA. Contact her at pushpita.c@ieee.org.