JAMIA Open, 5(1), 2022, 1–9
https://doi.org/10.1093/jamiaopen/ooac019
Research and Applications

Research and Applications

CertificateChain: decentralized healthcare training certificate management system using blockchain and smart contracts

Jeffrey Tellew[1] and Tsung-Ting Kuo[2]

[1]Department of Computer Science, University of California Santa Barbara, Santa Barbara, California, USA, and [2]UCSD Health Department of Biomedical Informatics, University of California San Diego, La Jolla, California, USA

Corresponding Author: Tsung-Ting Kuo, PhD, UCSD Health Department of Biomedical Informatics, University of California San Diego, 9500 Gilman Drive, San Diego, CA, USA; tskuo@ucsd.edu

Received 28 March 2021; Revised 27 January 2022; Editorial Decision 21 February 2022; Accepted 2 March 2022

ABSTRACT

Objective: Managing training certificates is an important issue in research that can lead to serious issues if not addressed properly. For institutions that currently do not have a dedicated management system for these training certificates, a central database is the most typical solution. However, such a system suffers from several risks, such as a single-point-of-failure.

Materials and Methods: To address this issue, we developed and evaluated CertificateChain, a decentralized training certificate management system by using peer-to-peer blockchain and automated smart contracts. We developed an efficient certificate dividing-and-merging algorithm to overcome the transaction size limit on blockchain.

Results: We performed experiments on the system to evaluate its performance, then created a web app and tested the system in a real-world scenario. CertificateChain scaled linearly in terms of time compared with the total number of certificates added and could be quickly queried for existing data stored on-chain.

Discussion: CertificateChain was able to store and retrieve the training certificates on the blockchain network, with limitations including a comparative analysis of other systems, evaluation of different consensus protocols, examining certificates off-chain, a thorough comparison with a centralized system, and the extension to the main public Ethereum network.

Conclusion: We believe that these results indicate that blockchain technology could be a viable decentralized alternative to traditional databases in this use case. Our software is publicly available at: https://doi.org/10.5281/zenodo.6257094.

Key words: healthcare training certificates, data sharing, interoperability and health information exchange, privacy and security, blockchain distributed ledger technology

LAY SUMMARY

In many research scenarios, certifications are required for data access requests. Institutions must manage the relevant certificates to avoid potentially serious scenarios that could impede research. Most existing systems suffer from risks such as single-point-of-failure, a scenario in which an entire system can be rendered ineffective with the failure of only one node in the network. To solve this problem, we developed CertificateChain, a decentralized certificate management system that adopted blockchain and smart contract (programs running on blockchain) technology and stores the certificates on-chain. To evaluate the system's performance, we performed experiments on it by storing Collaborative Institutional Training Initiative (CITI) certificate files to test its scalability and speed, as well as real-world testing using an accompanying web app. We found that in terms of time, the system scaled linearly, and could quickly be searched for any existing certificates. The limitations include the evaluation of other blockchain consensus protocols, verification of certificate authenticity before and after uploading, the scalability of upload file size, as well as an in-depth comparison to existing centralized systems. After developing and evaluating the system, we believe that CertificateChain shows potential to be a viable decentralized alternative for existing centralized systems.

INTRODUCTION

Background and significance

When performing research, especially when handling things like private health information, training certificates such as Collaborative Institutional Training Initiative (CITI, Figure 1A)[1] are typically required. Researchers must renew these certificates when they expire and will sometimes be asked to present the digital certificates to access data. Failure to properly manage training certificates can lead to various issues. The inability to present a valid certificate can delay the release of funding of an awarded grant, the consequences of which could be very significant. Lack of a certificate needed to access data could also delay research, and thus any resulting publications as well. As such, it is important to have a system in place for managing these training certificates.

The traditional method for managing certificates in many institutions is to use email to exchange the PDF files, as shown in Figure 1B. Although this solution worked well enough to meet the minimum requirements, it had several issues. First, finding a PDF and then emailing it to someone whenever they need it is slow and inefficient. In one study, it took faculty an average of 5.1 days to respond to a survey,[2] a metric that one could assume would likely be similar for a response to a request for their certificate PDF. Additionally, it is prone to human error; emails can go unnoticed amongst the many other researchers may receive daily, or they might be sent to the wrong person. Finally, email also provides no way to know if a certificate is going to expire without manually checking the expiry date.

A typical approach to this kind of problem would be to set up a central database where certificate-holders can upload their certificates (Figure 1C). This would allow the party in need of certificate confirmation to quickly and directly get the information that they need. Although this solution solves many of the issues seen in the emailing system, it is not without problems of its own. Having only a single central database leaves the system with a single-point-of-failure, rendering it vulnerable to a malicious attack or simply a hardware or software malfunction. There may also be conflicts when determining who will be responsible for hosting and maintaining the database when there will be several parties using it.

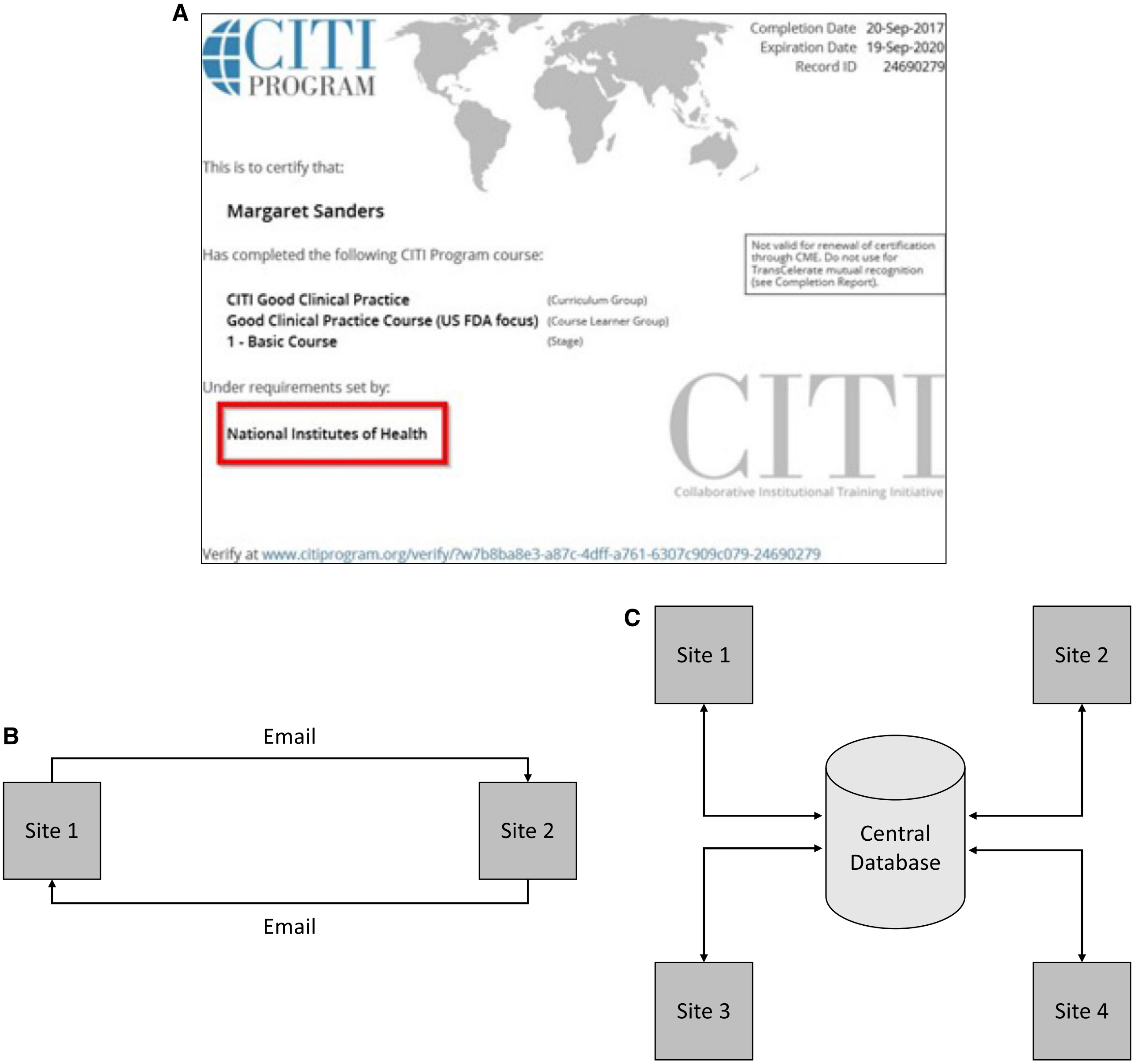
To address the above-mentioned issues for an email-based or centralized training certificate management system, we propose a decentralized system that could act as a single database without being vulnerable to single-point-of-failure. Although it would be possible to create backups and increase redundancy with traditional databases to avoid this issue, this is essentially what blockchain, a novel distributed immutable ledger technology originally proposed for crypto-currencies, was designed for with its system of nodes.

Blockchain largely rose to popularity in late 2017 when Bitcoin became a viral sensation. Bitcoin is just one of many implementations of blockchain technology, which was originally created to support a decentralized digital currency now commonly referred to as 'crypto-currency.' It accomplishes this by creating a peer-to-peer ledger that keeps track of all transactions that occur on the network and then updates on each participating machine, or "node," in the network. Therefore, there is no single-point-of-failure in a blockchain network.

Also, blockchain provides several other useful benefits for the situation.[3] By providing immutability, blockchain ensures that nobody can tamper with the data after it is uploaded. Additionally, it eliminates the need for any one entity to manage and set up a database, instead delegating the task to the entirety of the participants in the network, who each set up a node that keeps track of the state of the blockchain.

Although Bitcoin was the first use of blockchain, its rise to popularity brought the technology into the public eye and resulted in a large increase in the number of alternative crypto-currencies with the new technology of smart contracts.[3] Smart contracts, adopted in blockchain platforms such as Ethereum[4] and Hyperledger,[5] are programs that users can write and then run on the blockchain automatically to manage data on-chain. Smart contracts are beneficial to the system because the code stored on-chain is completely transparent and immutable. That is, everyone on the network can see the code (and who wrote it) but cannot change it. If a revision of a smart contract is needed, it can be deployed to the network as a new version, but the contract it is replacing in function will stay in the history of the blockchain for all to see. The technical features mentioned above for blockchain (ie, no single-point-of-failure, data immutability, decentralized management, and high availability) and smart contracts (ie, code transparency and code immutability) are highly desirable for a training certificate management system.

Although there are many proposals[6,7] for adopting blockchain and smart contracts in healthcare,[8–14] the feasibility and scalability of storing certificates on-chain are yet to be fully evaluated. Several previous papers explored theoretical applications of blockchain within the field of healthcare,[6] but any actual testing was yet to be conducted. Others created a system to store electronic health records,[7] while our study focused on managing the certificates. Another recent paper proposed using blockchain as a secure method for storing educational class credits.[15] There are a several other studies[16–20] that attempt to use blockchain to verify certificate authentic-



CITI PROGRAM

Completion Date 20-Sep-2017
Expiration Date 19-Sep-2020
Record ID 24690279

This is to certify that:

Margaret Sanders

Has completed the following CITI Program course:

Not valid for renewal of certification through CME. Do not use for TransCelerate mutual recognition (see Completion Report).

CITI Good Clinical Practice	(Curriculum Group)
Good Clinical Practice Course (US FDA focus)	(Course Learner Group)
1 - Basic Course	(Stage)

Under requirements set by:

National Institutes of Health

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w7b8ba8e3-a87c-4dff-a761-6307c909c079-24690279

Figure 1. (A) Example training certificate issued by the CITI program (citiprogram.org) for the National Institutes of Health (NIH), source: https://irbo.nih.gov/confluence/display/ohsrp/CITI+Portal+Access+and+Completion+Records. (B) Current management scheme of emailing certificate PDFs between parties. (C) System with 4 parties using a central database.

ity, but only store hashes[16,17] or states[18–20] of the certificates that can be used to prevent forgery, and do not upload the certificate itself nor contain any useful information about the certificate like its expiry date on the actual blockchain. Although these studies demonstrate some of the benefits of blockchain, it is still unclear if storing the training certificates on-chain may be a plausible solution due to the increased data load. That is, existing systems focus only on handling small pieces of data such as authentication information, as opposed to full certificate files, which jumps from mere bytes in the normal use case to several kilobytes or even megabytes when storing PDFs.

Objective

We aimed at developing a training certificate management system named CertificateChain using blockchain and smart contract and evaluating its feasibility and scalability empirically. The rest of the article is organized as follows: first, we will introduce blockchain and smart contracts, our novel certificate dividing-and-merging algorithm, our newly developed user web interface, and experiment settings in "Materials and Methods" section. Then, the results of certificate storing as well as web application will be shown in "Results" section. Finally, we will discuss the findings and limitations of this study in "Discussion" section, followed by the conclusions in "Conclusion" section.

MATERIALS AND METHODS

Blockchain platform and smart contracts

Based on our previous survey of blockchain platforms,[21,22] we chose Ethereum as the underlying blockchain for CertificateChain. Ethereum provides great support for advanced smart contracts, as well as

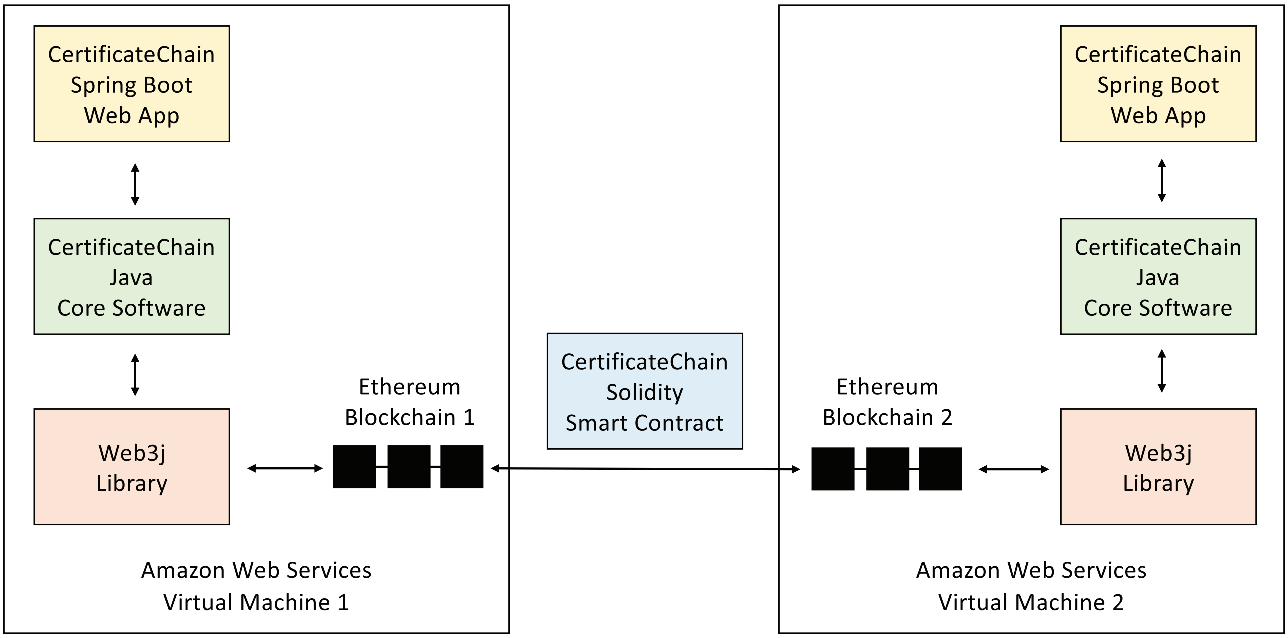


Figure 2. The system architecture for evaluating the CertificateChain system. This example shows a blockchain network with 2 Virtual Machines (VMs). Each VM hosts its own copy of the Blockchain, which communicates with each other via the Smart Contract and with the user via the Web App. The intermediate layers between the Web App and the Blockchain include the CertificateChain core software, as well as the Web3j blockchain library.

running private networks, and is well-supported by a very active community due to its popularity as a crypto-currency platform. We adopted Ethash,[23] a Proof-of-Work (PoW) consensus protocol for Ethereum. We developed smart contracts using Solidity[24] that allowed us to store and retrieve full PDF files from an Ethereum blockchain. Solidity is Ethereum's own special smart contract language taking inspiration from C++, Python, and JavaScript, and is Turing-complete which provides much more freedom to smart contract developers, such as the capability to use loops, when compared with what is available for a platform like Bitcoin.

Efficient certificate dividing-and-merging algorithm

An intuitive solution to store certificates on blockchain is to enclose each certificate in a transaction. However, there is usually a limitation of transaction size, for example, the Go-Ethereum implementation only allows up to 32 KB in a transaction.[25] To overcome this limitation, we developed a dividing-and-merging algorithm, which split each certificate into 30 KB slices before sending to the blockchain. Our algorithm then reconstructed the file into a byte array on the chain. As such, the contract is not limited to PDF files but could be used to store any file type or digital data using the same method.

A straightforward way to store/retrieve the slices is to reconstruct the slices of the file in order as a byte array on the blockchain. However, this required "sequential transactions" which can limit the rate of the file transfer to the rate at which blocks were mined/created while moving only one slice per mined block. To further improve the efficiency of the certificate logging and querying, we designed a mechanism to instead store the slices as objects at a predefined index within a hash table, which mapped slice indexes to the raw byte data. This was done by taking the original file, which was represented as a byte array in the Solidity smart contract and dividing it into smaller byte arrays that satisfied the transaction data size limit. Using the certificate ID, which is unique to each certificate, along with a simple incremental ID for each subarray, which was passed in the transaction along with the data itself, a map could be created for the certificate that allowed for easy reconstruction of the pieces as they arrived in any arbitrary order. Due to the incremental nature of the slice IDs, the map could be iterated over in order of the IDs whenever the full byte array was required, such as when a user requested to download the original file, and simply append the pieces to reproduce the full file.

With this design, any slice of the file could be added at any time if it ended up in the right position within the mapping on the blockchain, which was guaranteed via the mapping instead of the actual chronological order of the arrival of the slices. This parallelization of the transactions allowed us to perform all the storage/retrieving at once, reducing the time required for a full file transfer to match the time until the next block was mined, where previously only one slice could be transferred in this same time span.

User web interface

Since most potential users might not be familiar with blockchain technology, it was necessary to create an interface that abstracted the inner workings of the system away from them and allowed them to interact with it in a familiar manner. We created a web application using Spring Boot[26] to allow other UCSD DBMI members to upload their certificates as a test on the system, and utilized Web3j,[27] a Java Ethereum library, to connect the web application and the underlying Ethereum blockchain network. The web app took the certificate metadata and PDF and uploaded them to be stored on the chain.

By only requiring users to upload their certificate once using this web interface (instead of accessing it multiple times as is required by current email systems), we aim at reducing the possibilities for human error to cause any issues. This web interface also allowed users to query certificates from the chain to view their information or download the PDF file to their local machine. Importantly, it also enabled users to easily view any valid certificates and to check

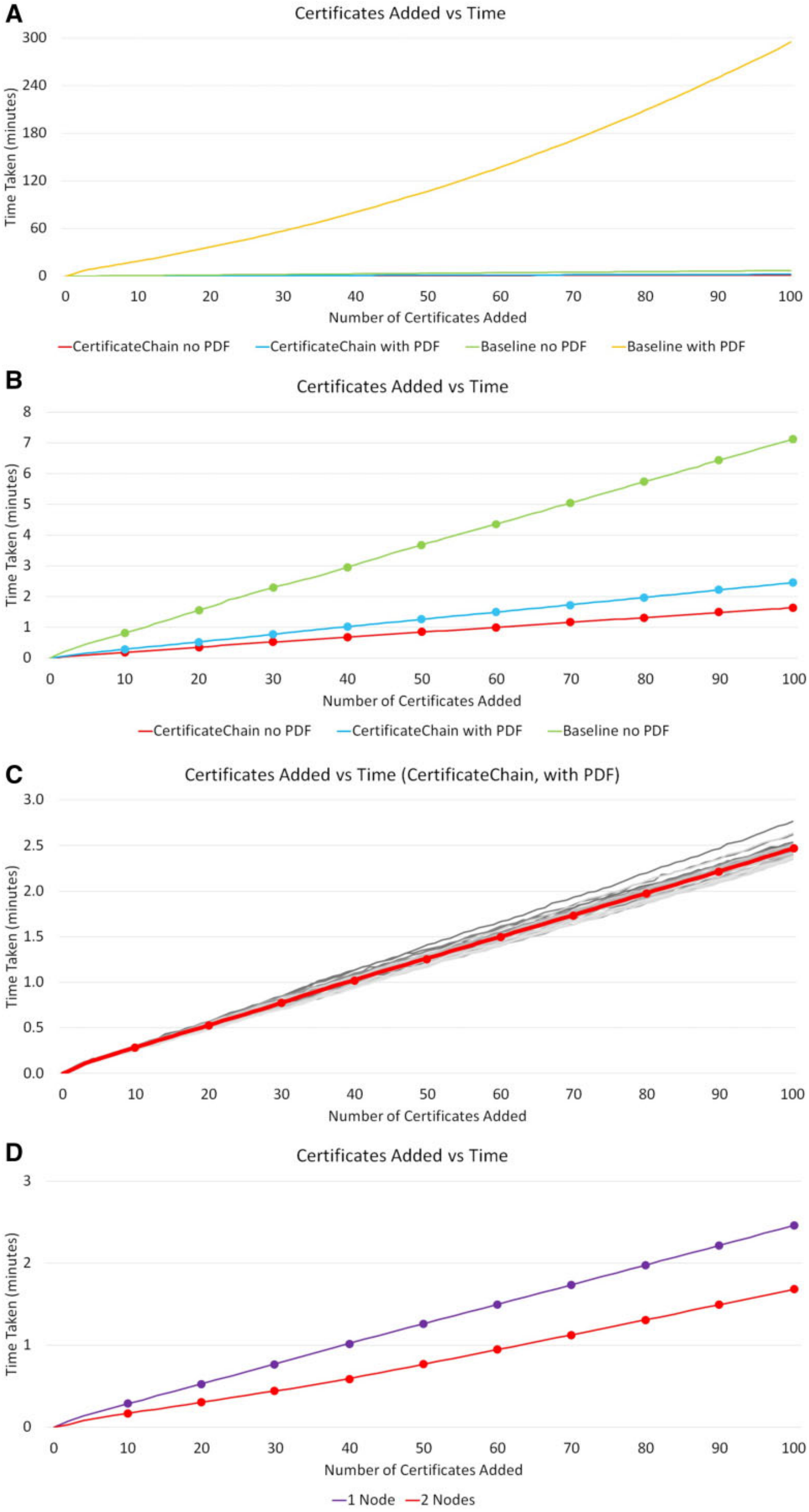


Figure 3. (A) Comparison between the number of certificates added and the average total time taken for both the baseline method and CertificateChain, storing the full certificate PDF or only the metadata. (B) The same as results but zoomed further in on the 3 lower lines for clarity since the slowest time was dramatically longer. (C) Average (red line) of 30 trials (gray lines) comparing the number of certificates added to the total time taken for CertificateChain with PDF files storage. (D) Comparison of average time to add 100 certificates with a 1- and 2-node system.

Table 1. Average time to add 100 certificates across 30 trials for the baseline system and CertificateChain, both with and without PDF files

System	PDF upload	Time (min)
Baseline	Yes	294.49
	No	7.13
CertificateChain	Yes	2.46
	No	1.64

whether a given researcher had a currently valid certificate, rather than having to contact them personally.

Experiment settings

To test the scalability of CertificateChain, we measured the time CertificateChain required for adding 100 CITI certificates of 410 KB each to a newly created blockchain. We compared CertificateChain with a baseline method which added certificates to the blockchain using sequential transactions. We also ran experiments both with PDF file storage and without PDF file storage (ie, storing only the metadata, such as the name and expiration date) on-chain for benchmarking purposes. Then, we compared the speed when the certificates were added all from 1 blockchain node against the speed when they were added evenly from 2 blockchain nodes. We set up a private Ethereum network including Ubuntu Virtual Machines (VMs) in Amazon Web Services (AWS)[28] to serve as the blockchain nodes. We repeated each experiment mentioned above for 30 trials. The system architecture used for CertificateChain evaluation is demonstrated in Figure 2.

RESULTS

Certificate storing

As shown in Figure 3A and B, CertificateChain outperforms the baseline method in both scenarios with/without PDF file storage. At roughly 2.5 min to add 100 certificates, CertificateChain averaged about 1.5 s per certificate upload. The retrieval time is negligible when compared with the storing time.[29] In fact, CertificateChain with PDF file storage was even more efficient than the baseline method without PDF file storage. Each result is computed by averaging the time measurements of the 30 trials, as depicted in Figure 3C. Exact times for these experiments are listed in Table 1. We further compare the effect of adding certificates from more nodes. The results of adding certificates from 2 nodes (ie, adding 50 certificates from each node) compared with adding just from 1 node is shown in Figure 3D. The system with 2 nodes adding certificates performed better than the system with 1 node adding certificates, likely due to the increased computational resources available.

Web application

The web application we developed is shown in Figure 4A and B. We invited a total of 17 participants from UCSD Health Department of Biomedical Informatics, split between interns, faculty, and staff, who combined to submit 20 different certificates, including CITI and UCSD Health Insurance Portability and Accountability Act (HIPAA) trainings, to the experimental database using this web application. The CITI certificates were approximately 410 KB each and the HIPAA certificates were approximately 120 KB each. The detailed statistics of the participants and certificates are shown in Table 2.

DISCUSSION

Findings

Our results demonstrated that CertificateChain was able to store and retrieve the training certificates on the blockchain network in a reasonable time (1.5 s for storing a certificate). For the submission of certificates by participants, CertificateChain was able to handle uploads, queries, and downloads without any issues. No major usage hurdles were reported, and no unusual delays were observed interacting with the blockchain network. For the scalability test, CertificateChain provides a linear scaling of time with respect to the number of certificates added to the blockchain. Thus, we managed to securely store certificates on a blockchain in a manner similar in performance to traditional database systems, while gaining several benefits. When using the web app, users uploading a certificate would first select a certificate file, which the web app would then store in memory and upload to the blockchain in the background while the user continued with the rest of the process. This was done to keep the user experience fluid and consistent with what a typical user might expect from a web app in terms of performance. Combined with our web app, the system also reduces the opportunities for human error by requiring certificate uploads only once, compared with the numerous times a researcher may have to email their certificate without the system, and allows users to instantly check if a researcher has a valid certificate rather than having to contact them personally and ask.

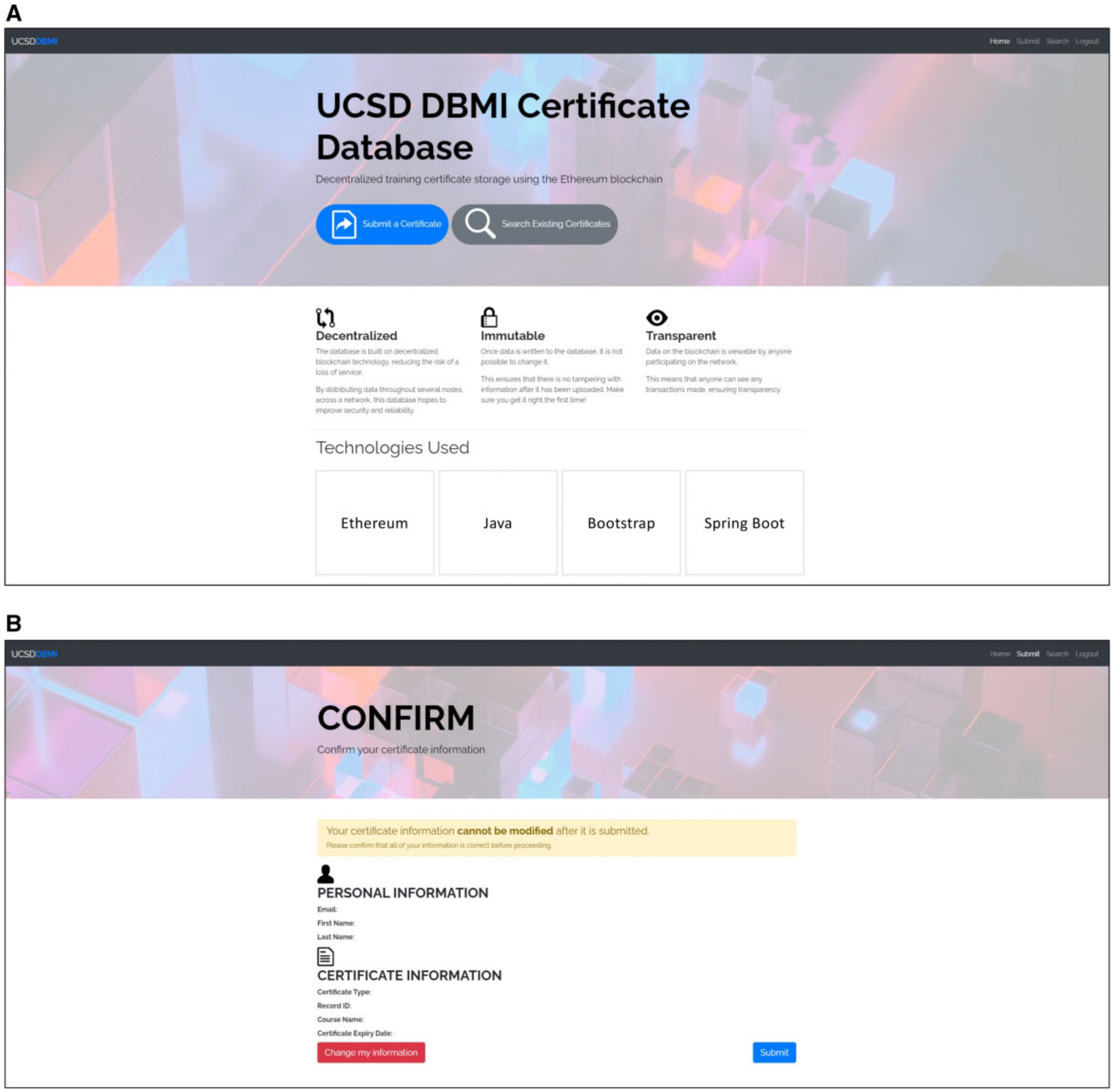
Public blockchain testnet

Although CertificateChain was designed for private blockchain networks, we also conducted a test on the public Ropsten "testnet" (ie, a public test blockchain network of which the crypto-currency has no real monetary value)[30] to understand the performance of CertificateChain with PDF file storage in a setting with many participating blockchain nodes and thus transactions. Using a transaction timeout of 100 min, we uploaded certificates 1 at a time (as opposed to 100 at a time) and recorded the time to upload each certificate. In general, the time to store a certificate was between 14 and 90 min. The storage speed was influenced by various factors such as the number of other nodes mining on the network at any given time or the number of other transactions waiting to be processed. These evaluation results are not directly comparable to the results shown in Table 1, because of the very different configurations between the private and the public blockchain networks.

Limitations

The limitations for this work are as follows. First, our method focuses on storing actual certificate files on-chain. We are yet to conduct a thorough comparative analysis to compare our method empirically with existing studies which store hashes or states of the certificates.[16–20] Also, while we adopted Ethereum in our system, there are other blockchain platforms, such as Solana[31] or Hyperledger Fabric,[32] that might be viable alternatives to Ethereum. We are yet to implement CertificateChain on these blockchains to enhance the generalizability of our system.

Second, we are yet to investigate other blockchain consensus protocols, such as Proof-of-Authority (PoA)[33] or Proof-of-Stake (PoS). This study was conducted exclusively using PoW. However, Ethereum has since begun a transition to PoA/PoS,[34,35] and as such we expect it to be significant moving forward. Additionally, we performed experiments on the public Ropsten testnet to "emulate" the scenario of having numerous blockchain nodes. However, we are


A
UCSDDBMI
Home Submit Search Logout
Submit a Certificate
Search Existing Certificates
B
UCSDDBMI
Home Submit Search Logout
Change my information
Submit

UCSD DBMI Certificate Database

Decentralized training certificate storage using the Ethereum blockchain

Decentralized

The database is built on decentralized blockchain technology, reducing the risk of a loss of service.

By distributing data throughout several nodes across a network, this database hopes to improve security and reliability.

Immutable

Once data is written to the database, it is not possible to change it.

This ensures that there is no tampering with information after it has been uploaded. Make sure you get it right the first time!

Transparent

Data on the blockchain is viewable by anyone participating on the network.

This means that anyone can see any transactions made, ensuring transparency.

Technologies Used

Ethereum | Java | Bootstrap | Spring Boot

CONFIRM

Confirm your certificate information

Your certificate information **cannot be modified** after it is submitted.
Please confirm that all of your information is correct before proceeding.

PERSONAL INFORMATION

Email:
First Name:
Last Name:

CERTIFICATE INFORMATION

Certificate Type:
Record ID:
Course Name:
Certificate Expiry Date:

Figure 4. (A) The home page of the web app interface. (B) The confirmation page of the web app interface.

yet to investigate the performance of the system on a large private blockchain network. Although in a private network one could potentially consider participating nodes to be trustworthy, some of blockchain's benefits are not guaranteed unless a network is large enough to prevent a single entity from controlling most of the nodes. Therefore, further experiments could further ensure the feasibility of CertificateChain when the number of private blockchain nodes is large. Besides, the main scope of our study was limited to a private network use case, where several institutions seek to replace an internal exchange of certificates. A significant redesign of the system for public blockchain networks would be required to properly evaluate the feasibility in a use case where the system is open to the public as opposed to a controlled private network.

Third, although each of the certificates we used contains a permanent link to the issuer's website that can be used to verify authenticity, for other types of certificates there might be concerns about the possibility of faking a certificate before uploading it to the chain, which warrants further study. In fact, the whole biomedical training process (eg, registration, participating lectures, and evaluations) could potentially be integrated into the blockchain, thus all the information will be recorded on-chain with reduced susceptibility to fraudulent activities. We believe that this application would be particularly well-suited to the blockchain, as the transparency and immutability that the blockchain provides have already been proven to be useful in demonstrating the authenticity of other items such as medicine.[36] We are also yet to evaluate the performance of storing large PDF files (eg, >10 MB) or using more certificates.

Fourth, we are yet to conduct a more in-depth analysis of the system's performance in comparison to a traditional database system, to further clarify whether the transparency/immutability benefits of

Table 2. The participants in the real-world testing and the breakdown of the certificates that were added to CertificateChain

Category	People	CITI	HIPAA	Certificates
Student	14	13	2	15
Staff	2	2	0	2
Faculty	1	2	1	3
Total	17	17	3	20

CITI: Collaborative Institutional Training Initiative; HIPAA: Health Insurance Portability and Accountability Act.

smart contracts in our system outweighs the potential obstacle of increased software engineering complexity when compared with current solutions involving centralized systems, and if so, whether it can do so at a competitive price. This experiment was run on the AWS cloud platform, which cost about $60 USD per month per machine, and due to the nature of private or test networks, required no actual crypto-currency to operate (ie, the crypto-currency in the system had no real monetary value). Although we consider this cost to be moderate for institutions who join the private blockchain network, further investigation would still be required to determine if this system, when scaled to the appropriate level, could be a financially viable alternative to the established database systems.

Finally, our system was evaluated on private or testnet blockchain networks, though it theoretically could also be extended for the "mainnet" (the public Ethereum network using crypto-currencies with real monetary values). That said, as of January 2022, the mainnet gas prices would result in a transaction fee of about $23 USD to upload 32 KB of data. With the 410 KB of CITI or 120 KB of HIPAA certificates used in our experiments, this would put the cost at $322 or $92 USD per certificate upload, respectively. These estimations show significantly increased costs when operating on the mainnet instead of a testnet or private network. To mitigate this issue, further methodology improvements such as storing a "preview" version of the certificates instead[8] would be required.

CONCLUSION

We developed CertificateChain, a healthcare training certificate management system based on blockchain and smart contracts. CertificateChain possesses desirable technical features that are important for managing training certificate PDF files, including no single-point-of-failure, data immutability, decentralized management, high availability, code transparency, and code immutability. We showed the linear scalability of CertificateChain by automatically submitting certificates via scripts. We also deployed a web application for participants to manually submit their certificates, providing a user experience comparable to that of a traditional database. CertificateChain represents a prototype that can serve as the cornerstone for future healthcare blockchain and smart contract studies. These findings support the use of blockchain technology as a transparent, immutable, decentralized, and highly available method of storing important data in general, showing that blockchain's uses extend well beyond crypto-currency and into the realm of healthcare.

FUNDING

All authors were partly funded by the National Institutes of Health (NIH) (R00HG009680, R01HL136835, R01GM118609, U01EB023685, and T15LM011271). T-TK is also partly funded by the UCSD Academic Senate Research grant RG084150. The use of the UCSD Campus Amazon Web Services (AWS) cloud network is supported by Michael Hogarth, MD. Research reported in this publication was supported by the NIH. The content is solely the responsibility of the authors and does not necessarily represent the official views of the NIH.

AUTHOR CONTRIBUTIONS

JT contributed to conceptualization, methodology, software, validation, formal analysis, investigation, data curation, writing (original draft), and visualization. T-TK contributed to conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing (review and editing), visualization, supervision, project administration, and funding acquisition.

ACKNOWLEDGMENTS

The authors would like to thank Lucila Ohno-Machado, MD, PhD, Jejo David Koola, MD, Kai W. Post, MS, Tyler Bath, and Nancy Herbst for very helpful discussions and support, as well as Cyd Burrows-Schilling, MS, and Randi Sutphin for the technical support of the UCSD Campus AWS cloud network.

CONFLICT OF INTEREST STATEMENT

None declared.

DATA AVAILABILITY STATEMENT

The data underlying this article are available in Zenodo at https://doi.org/10.5281/zenodo.6257094.

REFERENCES

1. CITI Home Page. 2021. https://about.citiprogram.org/en/homepage/. Accessed March 9, 2022.
2. Akl E, Maroun N, Klocke R, *et al.* Electronic mail was not better than postal mail for surveying residents and faculty. *J Clin Epidemiol* 2005; 58 (4): 425–9.
3. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. *J Am Med Inform Assoc* 2017; 24 (6): 1211–20.
4. Buterin V. A next-generation smart contract and decentralized application platform. *White Paper* 2014; 3: 37.
5. The Linux Foundation. Hyperledger Architecture, Volume II: Smart Contracts. 2018. https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf. Accessed March 9, 2022.
6. Mettler M, ed. Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE; 2016; Munich, Germany.
7. Ekblaw A, Azaria A, Halamka JD, Lippman A, eds. 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. New York City, NY: IEEE; 2016.
8. Li MM, Kuo T-T. Previewable contract-based on-chain X-ray image sharing framework for clinical research. *Int J Med Inform* 2021; 156: 104599.
9. Kuo T-T, Bath T, Ma S, *et al.* Benchmarking blockchain-based gene-drug interaction data sharing methods: a case study from the iDASH 2019 secure genome analysis competition blockchain track. *Int J Med Inform* 2021; 154: 104559.

10. O2 T. *Towards a Sustainable Commons: The Role of Blockchain Technology*. https://public.nihdatacommons.us/. NIH; 2019. Accessed March 9, 2022.
11. Kuo T-T, Gabriel R, Ohno-Machado L. Fair compute loads enabled by blockchain: sharing models by alternating client and server roles. *J Am Med Inform Assoc* 2019; 26 (5): 392–403.
12. Kuo T-T, Kim J, Gabriel R. Privacy-preserving model learning on a blockchain network-of-networks. *J Am Med Inform Assoc* 2020; 27 (3): 343–54.
13. Kuo T-T, Gabriel R, Cidambi K, Ohno-Machado L. EXpectation Propagation LOgistic REgRession on permissioned blockCHAIN (ExplorerChain): decentralized online healthcare/genomics predictive model learning. *J Am Med Inform Assoc* 2020; 27 (5): 747–56.
14. Kuo T-T. The anatomy of a distributed predictive modeling framework: online learning, blockchain network, and consensus algorithm. *JAMIA Open* 2020; 3 (2): 201–8.
15. Turkanović M, Hölbl M, Košič K, *et al.* EduCTX: a blockchain-based higher education credit platform. *IEEE Access* 2018; 6: 5112–27.
16. Cheng J-C, Lee N-Y, Chi C, *et al.* Blockchain and smart contract for digital certificate. In: 2018 IEEE International Conference on Applied System Invention. New York City, NY: IEEE.
17. Endurthi A, Khare A. Certificate management system using blockchain. In: International Conference on Soft Computing and Pattern Recognition. Springer, Cham; 2019; Hyderabad, India.
18. Xie R, Wang Y, Tan M, *et al.* Ethereum-blockchain-based technology of decentralized smart contract certificate system. *IEEE Internet Things M* 2020; 3 (2): 44–50.
19. Liu L, Zhou Y, Han M, *et al.* E^2 C-Chain: a two-stage incentive education employment and skill certification blockchain. In: 2019 IEEE International Conference on Blockchain (Blockchain). IEEE; 2019; Atlanta, GA.
20. Castro-Iragorri C, Lopez-Gomez F, Giraldo O. Academic certification using blockchain: permissioned versus permissionless solutions. *J Br Blockchain Assoc* 2020; 3 (2): 1–8.
21. Kuo T-T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. *J Am Med Inform Assoc* 2019; 26 (5): 462–78.
22. Yu H, Sun H, Wu D, *et al.* Comparison of Smart Contract Blockchains for Healthcare Applications. In: Amia Annual Symposium Proceedings. Bethesda, MD: AMIA; 2019.
23. Ethash wiki. Version 23. 2021. https://eth.wiki/en/concepts/ethash/ethash. Accessed August 19, 2021.
24. Solidity Documentation. https://solidity.readthedocs.io/en/latest/. Accessed March 9, 2022.
25. Go-Ethereum Source Code. https://github.com/ethereum/go-ethereum/blob/6a33954731658667056466bf7573ed1c397f4750/core/tx_pool.go#L570. Accessed March 9, 2022.
26. Spring Boot Home Page; 2020. https://spring.io/projects/spring-boot. Accessed March 9, 2022.
27. Labs W. Web3j Home Page; 2020. http://web3j.io/. Accessed March 9, 2022.
28. UCSD Campus AWS. https://blink.ucsd.edu/technology/cloud/index.html. Accessed March 9, 2022.
29. Kuo T-T, Jiang X, Tang H, *et al.* iDASH secure genome analysis competition 2018: blockchain genomic data access logging, homomorphic encryption on GWAS, and DNA segment searching. *BMC Med Genomics* 2020; 13 (Suppl 7): 98.
30. Ropsten Testnet Source Code. https://github.com/ethereum/ropsten. Accessed March 9, 2022.
31. Solana Home Page; 2022. https://solana.com/. Accessed March 9, 2022.
32. Hyperledger Fabric Home Page.. https://www.hyperledger.org/use/fabric. Accessed March 9, 2022.
33. De Angelis S, Aniello L, Baldoni R, *et al.* PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. In: Italian Conference on Cyber Security, Milan. 2018.
34. Gupta D. Ethereum goes to "proof of stake": understand everything about this revolution in cryptocurrencies. 2021. https://techunwrapped.com. Accessed March 9, 2022.
35. OpenZeppelin Team. Proof of Authority. OpenZeppelin Forum. August 2, 2020. https://forum.openzeppelin.com/t/proof-of-authority/3577. Accessed August 19, 2021.
36. Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. *Appl Health Econ Health Policy* 2018; 16 (5): 583–90.