*International Journal of Research in Engineering and Science (IJRES)*
*ISSN (Online): 2320-9364, ISSN (Print): 2320-9356*
*www.ijres.org Volume 10 Issue 7 ǁ July 2022 ǁ PP. 914-924*

# A Patient-Centric Health Information Exchange Framework Using Blockchain Technology

Dr.SYED SALIM [1] , Apeksha G[2] , H MKavya [2] , Spoorthi D[2] , Syeda Yusra Asgar[2]

[1] *Associate Professor at Department of CSE, Vidya Vikas Institute of Engineering and Technology, Mysuru-570028, India*

[2] *Final year students of Department of CSE, Vidya Vikas Institute of Engineering and Technology, Mysuru-570028, India*

***Abstract*—*Health Information Exchange (HIE) exhibits remarkable benefits for patient care such as improving healthcare quality and expediting coordinated care. The Office of the National Coordinator (ONC) for Health Information Technology is seeking patient-centric HIE designs that shift data ownership from providers to patients. There are multiple barriers to patient-centric HIE in the current system, such as security and privacy concerns, data inconsistency, timely access to the right records across multiple healthcare facilities. After investigating the current workflow of HIE, this paper provides a feasible solution to these challenges by utilizing the unique features of blockchain, a distributed ledger technology which is considered "unhackable". Utilizing the smart-contract feature, which is a programmable self- executing protocol running on a blockchain, we developed a blockchain model to protect data security and patients' privacy, ensure data provenance, and provide patients full control of their health records. By personalizing data segmentation and an "allowed list" for clinicians to access their data, this design achieves patient-centric HIE. We conducted a large-scale simulation of this patient-centric HIE process and quantitatively evaluated the model's feasibility, stability, security, and robustness.***

***Index Terms*—*SHA algorithm,AES Rijandel algorithm,Block chain technology***

---

Date of Submission: 15-07-2022 Date of acceptance: 29-07-2022

---

This research is supported in part by the Emerging Technologies for Data-Driven Discovery Initiatives of the University of Missouri, the Ministry of Science and Technology through Pervasive Artificial Intelligence Research (PAIR) Labs, Taiwan under the grants MOST 108-2634-F-468-001 and MOST 108-2511-H-468-002.

Yan Zhuang is with the Institute for Data Science and Informatics, University of Missouri, Columbia, MO 65211 USA (e-mail: yznm9@mail.missouri.edu).

Lincoln R. Sheets, MD, Ph.D., is with the Institute for Data Science & Informatics, Health Management & Informatics Department, Missouri Telehealth Network, and School of Medicine, University of Missouri, Columbia, MO 65211 USA (e-mail: sheetslr@health.missouri.edu).

Yin-Wu Chen, Ph.D., and Zon-Yin Shae, Ph.D., are with the Artificial Intelligence Research Lab, Asia University, Taichung 41354, Taiwan (e- mail: yin94087@yahoo.com; zshae1@asia.edu.tw).

Jeffrey J.P. Tsai, Ph.D., is with the Department of Bioinformatics and Biomedical Engineering, Asia University, Taichung 41354, Taiwan (e- mail: jjptsai@gmail.com).

Chi-Ren Shyu, Ph.D., the corresponding author, is with the Institute for Data Science and Informatics, Department of Electrical Engineering and Computer Science, and School of Medicine, University of Missouri, Columbia, MO 65211 USA (e-mail: shyuc@missouri.edu).

## I. INTRODUCTION

ELECTRONIC health record (EHR) systems are widely used worldwide [1] with a more than 96% adoption rate among non-federal acute care hospitals in the USA [2]. Timely Health Information Exchange (HIE) across healthcare systems exhibits tremendous benefits in reducing health care costs, improving quality of care, and reinforcing disease surveillance [3]. The Office of the National Coordinator (ONC) for Health Information Technology has spent billions of dollars to achieve meaningful use of EHR and facilitate the development of HIE systems [4]. There has been some success in achieving HIE among business entities such as state-wide hospital systems in the same collaborative association [5, 6]. However, various forms of HIE, listed in Table I, pose challenges related to data quality [7], data security, patient privacy [8, 9], and patient engagement [10]. In addition, there are recent signs of shifting to patient-centered interoperability [5, 11]. Although one of the three existing HIE forms, consumer-mediated exchange, allows patient to access and

manage their health information online, to achieve a true patient-centric HIE, the patients should have a full control of their data, such as authoring healthcare facilities' data access, determining sharable information, acknowledging the data use [12], and approving the life cycle of the shared data.

TABLE I THREE FORMS OF HEALTH INFORMATION EXCHANGE

| HIE forms | Definitions |
|---|---|
| Directed Exchange | Allowing pairs of care providers to share the patients' information used for coordinated care |
| Query-based Exchange | Giving providers the ability to collect a specific patient's records from among different providers often used for unplanned/ emergency care |
| Consumer-mediated Exchange | Letting patients control the sharing of their own electronic health information to assist coordinated care and unplanned care. |

There are various conceptual models for different HIE forms:

(1) centralized model using a central repository to store and manage all patient's health information, (2) federated model consists a state-wide central HIE patient registry or record locator service (RLS) contains a combination of patients' identifiers to match the patients across multiple regional authorities which maintain the ownership and control over the regional healthcare facilities' records, and (3) hybrid model combines the centralized and federated models using a centralized data repository as the national central authority or RLS to locate patient's records from different healthcare facilities [13, 14]. The existing models have achieved a certain degree of success of three existing forms of HIE. However, to provide patients a robust and interoperable patient-centric HIE system, the existing HIE models have shown multiple challenges such as security and privacy concerns caused by central repository storage of data or patients identifiers [15], data ownership still controlled by authorities [16], mismatching of patients using RLS [17], and data breach caused by external cyberattacks and the threat of internal fraud [18]. Emerging technologies, such as blockchain, may provide potential solutions for the need function in the patient-centric HIE system to tackle the aforementioned challenges.

The following scenario illustrates the barriers of the current HIE process to provide patient-centric services: A patient lived in Los Angeles, California between 2000 and 2015 and moved to Columbia, Missouri, where he is a resident currently. He has a medical history of congestive heart failure since 2010 (well managed on medications), and a prior history of alcohol dependency (in continuous remission since 2005). While visiting New York City, he is admitted to an emergency department for shortness of breath. It is critical for the clinicians at the healthcare facility in New York City to access his prior records from providers in Los Angeles, California, and Columbia, Missouri. The patient selected to share only cardiology data but did not want other providers to know his history of substance abuse for reasons of privacy, concerns about provider bias, and recent assurances from his current primary-care physician that his remote history of alcohol dependency has no current relevance for the management of his congestive heart failure. As of today, for the traditional HIE process, this health information exchange will start with a request to the Hartland Regional Health Information Organization (RHIO) and then connect to Western and Midwest RHIOs to access EHR data from California and Missouri, respectively, through Regional Gateway Connections.

Patient-centric exchange is needed because there are two major barriers for this information exchange to happen: (1) the time required for the RHIOs to locate the patient's prior records without knowing the patient's protected health information (PHI) from the remote healthcare facilities where the patient visited previously [15]; and (2) the vulnerability of the patient's history of substance abuse being accessible to the provider against the patient's will [12, 15, 19]. However, there are three challenges to patient-centric exchange across institutions: (1) security and privacy concerns that may result in appalling financial and legal consequences [20-22]; (2) data breaches caused by unauthorized access of the patients' health records [23]; and (3) data inconsistency between the remote provider's EHR data and the recipient's data [24, 25].

## II. RATIONALE USING BLOCKCHAIN MODEL FOR PATIENT- CENTRIC HIE APPLICATIONS

Blockchain is an open-source distributed ledger technology that was first applied in the financial sector [26]. The most popular application of blockchain is the Bitcoin cryptocurrency which has proven that blockchain technology is stable, secure, and robust [27]. There are already prominent applications applying blockchain in the healthcare area such as the pharmaceutical supply chain [28], clinical trial management [29, 30], and medical record management [31, 32]; however, most blockchain applications in the healthcare area are still in the early stages of implementation [33].

Based on these barriers and challenges, disruptive technologies such as blockchain may provide feasible solutions by utilizing blockchain features, as shown in Table II. Blockchain is a chain of blocks which contain all the transactions. Blockchain is considered to be an "unhackable" system that can protect data security and patients' privacy [34]. All users are anonymous and use unique pairs of public and private keys to represent their identities which can be used to map the patient across multiple healthcare facilities [35]. The public key is similar to a user account and the private key is similar to a user password. When patients use blockchain to give permission to clinicians to access prior records, they need to sign this transaction using a private key. This can be done through mobile devices and biometric verifications.

TABLE II
BLOCKCHAIN SOLUTIONS FOR PATIENT-CENTRIC HIE CHALLENGES

| HIE Challenges | Blockchain Solutions |
|---|---|
| 1. The difficulty of timely matching a patient across different healthcare facilities | Public/ private key pair can be used to represent patients' identities |
| 2. Potential data inconsistency concerns due to integrity loss during transmission | Immutability feature can ensure data consistency |
| 3. Locating healthcare facilities to collect the patient-agreeable information | Smart contract can be utilized to store touchpoints for clinicians to quickly select |
| 4. Potential security and privacy concerns specified as data breaches caused by unauthorized access to health information | "Unhackable" peer-to-peer network ensures every transaction needs patient's authorization |

Blockchain is an immutable system. Any transaction written into a blockchain is unchangeable and can be checked at any time. This feature keeps all data consistent and eliminates any chance of tamper the data [36].

A new feature called "smart contracts" [37] – a self- executing protocol coded using Solidity, which is a Turing- complete language that provides the ability to solve any computational problem was added to the Ethereum blockchain [38]. All the transactions, which refer to permission granting, data requests, and data exchanges in the HIE setting will automatically follow smart contracts' regulations with mutual consent from all users in the blockchain. Using smart contracts can strengthen the feasibility of applying blockchain for patient-centric HIE. For example, some previous blockchain models used smart contracts to ensure all the transactions are following the different policies and all the data are in the same interoperability standard instantaneously [35, 39-42]. In our scenario, smart contracts can store touchpoints, which contain brief information such as primary diagnosis and treatments for each visit. Clinicians can select from the touchpoint list to request appropriate data for the current visit instead of filtering information after receiving all the patient's previous records. Patients can also perform personalized segmentations on the touchpoints to select the information they would like to keep confidential.

Since blockchain is a fully distributed peer-to-peer network conducting transactions without third-party intervention, the transaction will be broadcasted to all the users (patients and clinicians in the healthcare facilities within the blockchain system) to audit whether the "signed" private key matches the sender's public key [26]. The auditing process runs automatically through blockchain's validation process and keeps the private key invisible to all the users. The data inside the transaction (authorization of the data access in this case) are only accessible to the sender and the receiver. This auditing mechanism saves the time and cost of working with a third- party organization, keeps users anonymous and ensures all transactions have the senders' authorizations.

This work demonstrates the feasibility of applying blockchain for HIE with unique settings using the principle that patients should have ownership of their EHR data to achieve patient-centric HIE. We have also conducted a large-scale patient-centric HIE simulation from granting permission by patients to receiving data by clinicians.

## III. METHODS

To utilize the unique technological capabilities of blockchain for patient-centric HIE, we have implemented a private Ethereum blockchain system with multiple smart-contract functions. A private blockchain is also called a "permissioned blockchain" which limits access to certain users. The system architecture, shown in Fig. 1, contains two modules: (1) the *Linkage module*: a system administrator from each

healthcare facility will create a touchpoint for each patient's visit after the EHR is ready and input the related primary information into a smart contract for future indexing (as shown in Fig. 2), (2) the *Request module*: patients grant clinicians permission to access their data by adding clinicians to the "allowed list" in the smart contract. Clinicians can select records through the touchpoints after being granted access to the patient's records without identifying the hospitals storing those records. The subsequent exchange of data among the involved remote healthcare facilities will include data encryption and use of the blockchain system to send and retrieve decryption keys (as shown in Fig.3).

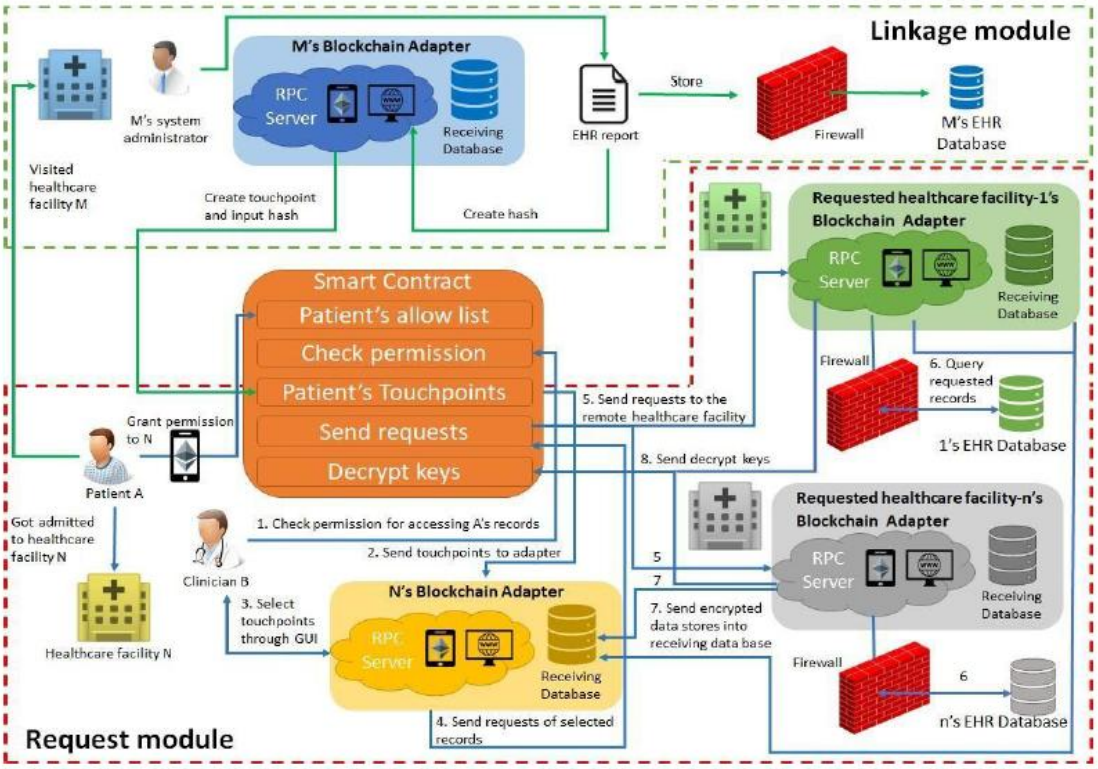


Fig. 1. System architecture with two modules (the Linkage module links the EHR databases with the blockchain by creating touchpoints to index the records in the future; the Request module allows patients to give permission to clinicians to access their data through blockchain and to request records by selecting touchpoints through the blockchain adapter).

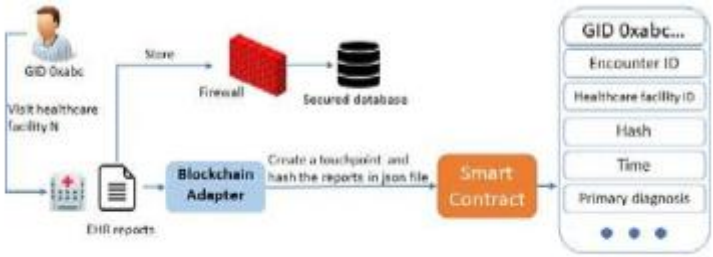


Fig. 2. The blockchain adapter extracts metadata and hashes the EHR reports in JSON format, stores this information in a smart contract, and stores the EHR data in the secure database.

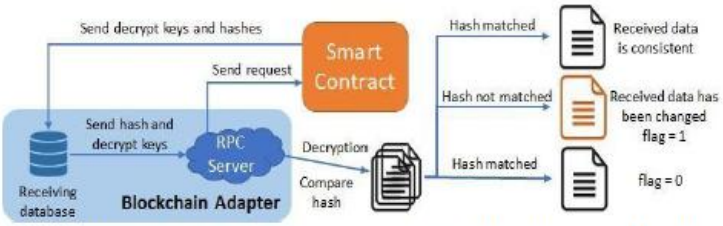


Fig. 3. The blockchain adapter retrieves decryption keys and hashes from a smart contract to decrypt the received EHR data, then hash the data using the preinstalled hashing function and compare it with the original hash; any mismatched records will be marked.

***A. Environment setup***

To join the blockchain system, each healthcare facility is required to provide at least one node, which can be any computer or a mobile phone; there is no special hardware required for the node. These nodes need to take the following steps to build a "blockchain adapter" to communicate with the system: (1) deploy the correct "Genesis block" (the starting block of the blockchain), which is a JSON file containing the blockchain's unique characteristics, and add the starting node as a peer node; (2) build a remote procedure call server which can communicate with servers outside the adapter and secure EHR databases inside the healthcare facility's firewall; and (3) build a receiving database outside the firewall to store data received from all other healthcare facilities' blockchain adapters. These steps are embedded into an installation file that can automatically convert a node into a blockchain adapter.

Once the healthcare facility has built a blockchain adapter, the adapter will generate a blockchain account which is a hash of the user's public key for the system administrator, who is responsible for creating accounts for clinicians and patients and inputting touchpoints to the smart contract (as shown in Fig. 2) [43]. When a patient opts into the system for the first time, the healthcare facility's administrator registers a blockchain account for the patient and automatically generates a global ID based on the blockchain account. Then the PHI from the healthcare facility is associated with the global ID which will be used for patient indexing. The patient must add biometric information to the blockchain account for future identification. When patients later visit additional healthcare facilities, they can prove the identity of the blockchain account by using biometric information. Then the system administrator links the PHI from that healthcare facility to the global ID. Accurate patient matching is a challenge for providers, payers, HIE organizations, and others as there is no standard mapping information across all healthcare facilities because of multiple regulations [44]. The master patient index (MPI), which contains basic demographic information such as name, race, and gender, is used to identify patients across different healthcare facilities [17]. However, mismatches still occur frequently due to the lack of unified standards, missing values, or data input errors [45]. Using blockchain to solve the patient matching problem could avoid mismatching. Patients will have blockchain-generated global IDs which securely map to different patient IDs with the patients' consent after validating their identities. Patients own the information about which healthcare facilities they have visited before and what their patient IDs are at each facility; other users will only see the global IDs without revealing their real identities in the system. This approach provides a more secure and efficient solution for the patient matching task (Challenge 1 of Table II) than the current MPI-matching mechanism. When administrators create accounts for clinicians, the server assigns a unique proxy clinician ID to each clinician used for granting clinician access.

***B. Linkage Module***

When the EHR data is ready for a patient's visit, the healthcare facility's adapter will hash the entire visit record in a JSON file and store the hashing value in the smart contract along with the touchpoint before the EHR data is stored in the secure database. The hashing value will be used for verifying data consistency in the data decryption step. Any modification of the data, even initiated from the healthcare facility adapter, intentionally or unintentionally, will result in unmatched hashes and security alerts after final decryption (Challenge 2 of Table II).

Once the smart contract is deployed into the blockchain, the blockchain returns a smart-contract address and an application binary interface (ABI); this, rather than the smart-contract code or the data stored inside the smart contract, is viewable by all users. Using the smart contract to store the touchpoints can keep the touchpoints secure, immutable, anonymous, and easily searched bythe patients and the authenticated clinicians. Fig. 4 shows the source code for the inputting touchpoint function and its ABI in the smart contract.

```
function Input_touchpoints(
                        string _GID,
                        string _Encounter_ID,
                        string _facility_ID,
                        string _hash,
                        string _time,
                        string _PD
                        ) public {
    records memory record;
    record.GID=_GID;
    record.Encounter_ID=_Encounter_ID;
    record.facility_ID=_facility_ID;
    record.hash=_hash;
    record.time=_time;
    record.PD=_PD;
    patient_EHR[GID[_GID]].push(record);
}
```

```
{"constant": false,
    "inputs": [
        {"name": "_GID",
            "type": "string"},
        {"name": "_Encounter_ID",
            "type": "string"},
        {"name": "_facility_ID",
            "type": "string"},
        {"name": "_hash",
            "type": "string"},
        {"name": "_time",
            "type": "string"},
        {"name": "_PD",
            "type": "string"}
    ],
    "name": "input_touchpoints",
    "outputs": [],
    "payable": false,
    "type": "function",
    "stateMutability": "nonpayable"}
```

Fig. 4. The source code of inputting touchpoint function is coded in Solidity which shows on the left; the ABI of this function, which only contains structure information, is shown on the right.

***C. Request Module***

After a patient is admitted to a healthcare facility, it is unrealistic for patients to authorize each of the clinicians in some situations, such as an emergency room visit when many clinicians are involved during the patient's care. The healthcare facility will be assigned an umbrella account in the blockchain that links to all clinicians involved in the care. All the clinicians could access the patient's records with one-time authentication (adding the shared account into the "allowed list") from the patient. The access history will be recorded to the blockchain and the auditing of individual clinician'saccess to the patient's record will be managed by the local access control within the healthcare facility. The patient can add the facility's umbrella ID to the "allowed list" through biometric authentication or a web-based graphical user interface (GUI), as shown in Fig. 5. The clinician's proxy ID should be automatically populated into the GUI after the patient and the clinician provide biometric information to authenticate the system. Only the clinicians under this umbrella ID can access the patient's data through the GUI for clinicians, as shown in Fig.6.

After the patient's consent is recorded in the blockchain, the HIE process takes the following steps (as enumerated in Fig. 1):

(1) the clinician confirms that his/her clinician ID has been added to the patient's allowed list; (2) the clinician receives the touchpoint list from the smart contract; (3) the clinician selects the touchpoints related to this visit through the GUI; (4) the touchpoint selections are sent to the smart contract through the healthcare facility's blockchain adapter; (5) the smart contract uses the recipient's healthcare facility's adapter to request the selected records chosen from the remote healthcare facilities' adapters; (6) the remote healthcare facilities query the records inside their EHR systems; (7) all selected EHR data is dynamically encrypted by the remote healthcare facilities' adapters and temporarily stored outside the clinician's facility's firewall; the encrypted data's locations and hash values are sent to the receiving database in the adapter of the clinician's facility; and (8) the remote healthcare facilities' adapters will automatically encrypt the decryption keys with the recipient's public key and send the encrypted decryption key to the smart contract. The recipients' private keys will be stored at the home hospital's adapters and protected by the hospital's security policy.


Fig. 5. GUI for patients to grant clinician permission, check personal EHR reports, and check who has accessed their records in the past (showing the transaction ID of the accessing clinician ID, and the date); patients can personalize the data segmentation after retrieving their health records.

Selecting touchpoints saved into blockchain from each visit, the clinician can quickly check the records related to the visit instead of browsing all the historical data. This function offers efficient information retrieval for the clinician in order to have a better sense of the patient's medical history (Challenge 3 of Table II).

Two layers of data security are implemented, at both smart contract level and user application level, to the original hashing algorithm of the Ethereum blockchain. The smart contract level defines multiple modifiers on smart contract functions, meaning that only selected roles can execute certain functions. For example, after the recipient's blockchain adapter automatically retrieves the decryption keys from the smart contract and the encrypted data, only the clinicians in the "allowed list" can retrieve the decryption keys. The decryption process will then automatically run on the recipient's healthcare facility's adapter using the clinician's private key to decrypt the decryption keys. This process then decrypts the data using a predefined encryption algorithm and a

preinstalled hashing algorithm to hash each decrypted visit. The adapter automatically compares the hashing value with the original hash that has been retrieved from the touchpoint. Any modification of the data from the original source, or in the transition, will result in a mismatch of the hash and the record will send an alert in red font. For example, as shown in Fig. 6, we falsified patient #3853's single record in the database (by changing the patient's value for the race from "2" to "1") after the touchpoint and hash were stored in the smart contract, which resulted in a flag showing "False" even when the encrypted data was decrypted.

In our scenario, the patient does not want to show his history of substance abuse and can choose to hide this information from the touchpoints, but the hidden records will not be removed from their records. Patients can always recover the original list after data segmentation. After the decryption process, the recipient's healthcare facility's adapter will hide the information from the decrypted data and will not show it to the clinician.

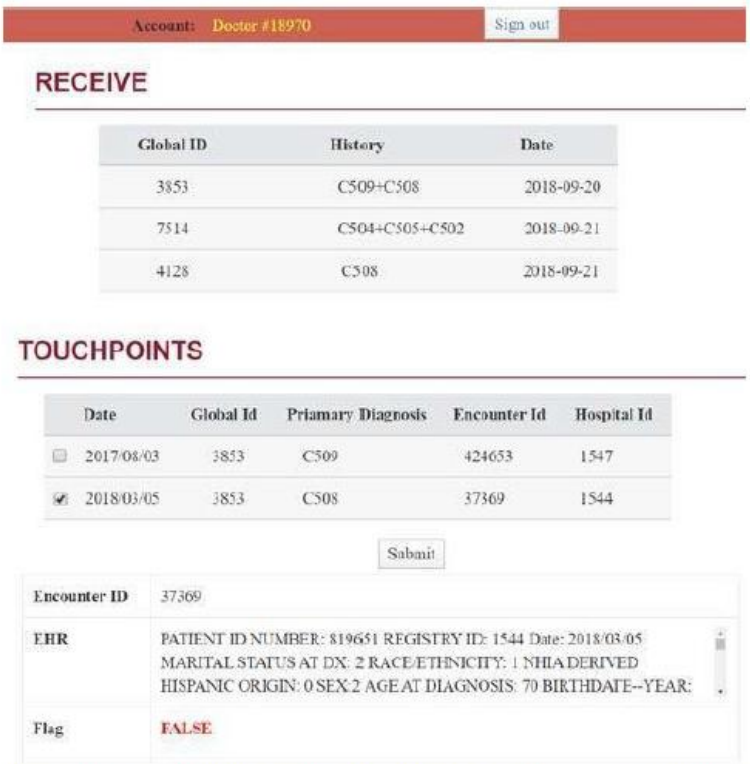


Fig. 6. GUI for clinicians to check received patient records, showing a summary of EHR record for patient #3853 after selecting the exact visit; the flag shows "False" because the hash values don't match since we have intentionally modified the data.

The user application level is defined by the smart contract based on each role, such as the future access mechanism for clinicians. While intuitively the remote site could choose to store all exchanged data**,** in our design, a policy is required for each healthcare facility's blockchain adapter to either delete, partially keep, or set a life cycle of the shared data in the local facility based on patients' permission. This mechanism ensures that all of the exchanged information should be only used with the patient's consent which could be granted for future use (permanently stored in the EHR of the remote facility) or one- time use (immediately revoked after care is completed and updates are sent back to the home facility). Furthermore, we have set up a trigger for the local databases in all the adapters; once the encrypted data is queried from the database for decryption, the decryption key and encrypted data will be deleted from the database to prevent future data access without patients' consent and to clear storage space for future transactions. The smart contract will monitor the process in each blockchain adapter to enforce the policy, in order to minimize the data breach problem (Challenge 4 of Table II). Patients can also revoke permission through the GUI if they have mistakenly input a clinician's ID or an umbrella healthcare facility ID by removing the ID from the "allowed" list.

## IV. SIMULATION

To conduct the system simulation, we made the following assumptions: (1) each healthcare facility provides at least one node that has been converted to the blockchain adapter in the system; (2) patients have

opted in to our system through healthcare facilities and their patient IDs have been mapped to a global ID; and (3) each healthcare facility has administrators to operate the system.

We set up five computing nodes representing five different healthcare facilities. Each node was installed on an Ubuntu 16.04 system and Apache HTTP Server. The starting node initialized the blockchain and the smart contract was deployed. The other four nodes joined the blockchain by going through the setup procedure described previously. We created 20,000 patient accounts in total and 100 clinician accounts for each healthcare facility node. The simulation randomly selects patients to grant clinician access data for multiple healthcare facilities based on patient preferences.

We used the Surveillance, Epidemiology, and End Results (SEER) dataset [46] for the simulation. We selected 80,000 records with 133 attributes from the original dataset and generated a PHI (date of birth and email address), visit date, healthcare facility ID and patient ID to be added to each record. These data were distributed and stored in four nodes depending on the healthcare facility ID. We created these scripts to simulate the whole HIE process: (1) load the touchpoints into the blockchain from different adapters depending on the visit location; (2) randomly select five patients to respectively grant access to five different clinicians from different healthcare facilities; (3) randomly select several patient's records from the touchpoints list and request these records by authorized clinicians from their healthcare facilities' adapters; (4) query the requested records by each selected remote healthcare facility's adapters; and (5) encrypt all the queried records in the adapters and send the encrypted data to the smart contract locations as URL pointers and decryption keys. Scripts #2 and #3 were run every five seconds to balance the memory load for running scripts on each blockchain node. Script #4 was run twice per second to detect the requests. These steps not only simulate the process of patient-centric HIE, but also test the stability of the system.

The adapters at the simulated recipients' healthcare facilities retrieved the data locations and decryption keys from the smart contract, and another script decrypted the data and hashed each record to compare with the original hashes; but because these steps were performed off the blockchain, statistical summaries were not completed for them. We manually falsified several records to test the data integrity function (as shown in Fig. 4).

In order to test the robustness of the system, we also randomly stopped nodes during the simulation. The other nodes continued to work, but all the requests sent to the stopped node's adapter could not be executed. The result was that the affected transactions were still approved and stored in the blockchain, but the recipients' healthcare facility could not receive data from the remote healthcare facility simulated by the stopped node. After restoring the node to service, the adapter automatically found the previous peers and synchronized itself with the blockchain for the missing period within seconds. The blockchain will only stop working if all of its supporting nodes stop working simultaneously.

## V. RESULTS

We simulated 1,553,635 data request transactions in four months by running the scripts continuously. One hundred percent of the transactions were successfully approved, and their encrypted queried data was stored in the requesting facilities' databases. The box plots in Fig. 7 report the total processing times for clinicians to receive (1) permissions after being added to the "allowed list" by patients and (2) the decryption keys provided by different remote healthcare facilities involved in the HIE process. If a clinician requests the patient's records from all four other healthcare facilities, the clinician would receive four separate decryption keys sent by all healthcare facilities. Table III lists the statistics of the processing time of HIE procedures after patients grant clinicians permissions to access the records. On average, clinicians received permissions as well as the metadata lists in 20.398 seconds and retrieved the encrypted data's locations with their decryption keys in 23.844 seconds.

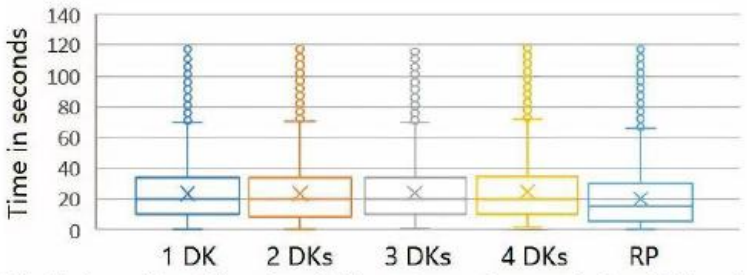


Fig. 7. Box plots of time for clinicians to receive permission (RP) and time to receive decryption keys (DK) from different facilities.

TABLE III
RESULTS OF PROCESSING TIMES OF HIE PROCEDURES

| | Request # | Mean | Min | Max | Stdev |
|---|---|---|---|---|---|
| Receive permission | 1,533,620 | 20.398 s | < 0.01s | 122s | 22.217 |
| Receive encrypted data, decryption key | 1,533,620 | 23.844 s | < 0.01s | 121s | 19.2800 |

Most transactions were validated and written into a block in about 23 seconds. Receiving decryption keys from a different number of nodes did not significantly affect the receiving time. The access-granting process took insignificantly less time than retrieving decryption keys. Fig. 8 shows the distribution of time elapsed to generate blocks with different transaction volumes; most blocks required around 40 seconds. The maximum transactions occurring in one block was 274, with a validation time of 78.37 seconds. The longest validation time is 122.54 seconds with 77 transactions occurring in the block. Block generation times in our experiment were varying but reasonably stable.

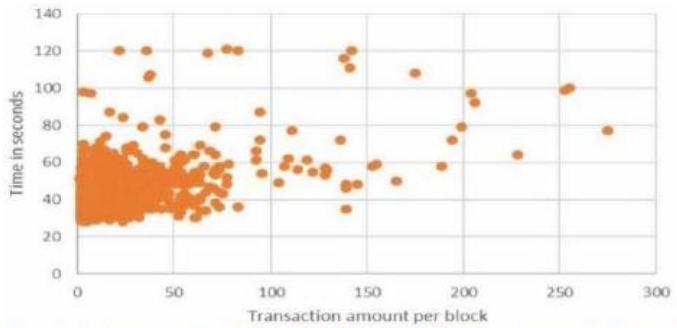


Fig. 8. Time to generate new blocks containing different numbers of transactions.

## VI. LIMITATIONS

The main limitation of our approach is the setup required at each healthcare facility. Each healthcare facility is required to provide at least one node to the blockchain and complete the process of converting servers into blockchain adapters. Secondary limitations include the dependence of the model's performance on the blockchain nodes' properties, the potential need for patients to provide blockchain nodes for data generated by Internet of Things (IoT) devices, and the need for facilities to agree on an interoperability standard such as Fast Healthcare Interoperability Resources (FHIR) [47].

Another limitation is scalability constraints from the blockchain protocol [48]. Ethereum can handle roughly 13-15 transactions per second as of today. At any moment, the total number of transactions, including permission granting, touchpoint selection, and decrypt key insertion/retrieval, may exceed the limit. Our simulation provides a partial solution to this limitation by spacing the transactions as queuing up the transactions by the adapters and control the speed of sending out the transactions to the blockchain and keeping the backlog in a transaction queue. For example, if five permission granting transactions per second are determined for the spacing setting, 300 simultaneous HIE requests can be handled within a 1- minute window at any moment. This spacing solution is to ensure the successful delivery of the requests under the intrinsic scalability constraint existing in the current blockchain protocol.

## VII. FUTURE WORK

Our blockchain model keeps all the log files so that patients can always review who has accessed their data. All clinicians can check the source of EHR data, which ensures data provenance. Clinicians are able to check only the data input by trusted healthcare facilities. System administrators can see how many clinicians have retrieved data from their healthcare facilities. We also kept log files in the smart contracts, which can improve health data management. Depending on their roles, users can simply call the smart contract functions to check different parts of the log file. For future simulations, we will add an artificial intelligence component to the blockchain adapters to allow researchers to retrospectively study HIE outcomes by analyzing log files [8], which cannot be accomplished in current HIE systems. Our future work will continue to evaluate the blockchain protocol to fundamentally solve the scalability issue by reengineering the time- and resource- consuming mining process of the private blockchain system.

Flexible business models could be created using blockchain. Smart contracts could include a credit mechanism to give users incentives to join the system. The healthcare facility could receive incentives for providing data to other facilities; patients could receive credits for providing their data to research projects; and credits could also be used to acquire data in return.

## VIII. DISCUSSIONS AND CONCLUSIONS

The unique contributions of this work include providing the following practical characteristics to the blockchain system to achieve patient-centric HIE: (1) blockchain adapter setup to communicate with blockchain, process the sending/receiving healthcare records, and provide graphical user interfaces for users to have a better visualization of the interaction with the blockchain system, and (2) two layers of security settings to ensure that only authorized users can execute certain smart contract functions and minimize the data breach problem, and (3) a hashing mechanism to ensure data consistency and (4) personalized data segmentation gives patients the ability to control of their records by choosing only the information they would like to share, and (5) touchpoint selection for clinicians to select the health records that related to the visit without browsing through entire records, and (6) a large-scale simulation using the implemented proposed model to evaluate the feasibility, stability, and robustness of the proposed blockchain model for the HIE application.

It is noteworthy to mention that blockchain technology is not the only solution for HIE. This paper demonstrates the feasibility and robustness of using the unique features of blockchain technology in HIE for the health IT community to consider applying the variations of the blockchain technology for HIE tasks, as well as to evaluate regulations and policies to adopt this emerging technology.

## REFERENCES


[1]. C. A. Pedersen, P. J. Schneider, and J. P. Santell, "ASHP national survey of pharmacy practice in hospital settings: prescribing and transcribing—2001," American Journal of Health-System Pharmacy, vol. 58, no. 23, pp. 2251-2266, 2001.

[2]. A. M. Heekin, J. Kontor, H. C. Sax, M. S. Keller, A. Wellington, and S. Weingarten, "Choosing Wisely clinical decision support adherence and associated inpatient outcomes," The American journal of managed care, vol. 24, no. 8, p. 361, 2018.

[3]. N. Menachemi, S. Rahurkar, C. A. Harle, and J. R. Vest, "The benefits of health information exchange: an updated systematic review," Journal of the American Medical Informatics Association, vol. 25, no. 9, pp. 1259-1265, 2018.

[4]. D. Blumenthal, "Stimulating the adoption of health information technology," New England journal of medicine, vol. 360, no. 15, pp. 1477-1479, 2009.

[5]. S. Rahurkar, J. R. Vest, and N. Menachemi, "Despite the spread of health information exchange, there is little evidence of its impact on cost, use, and quality of care," *Health affairs*, vol. 34, no. 3, pp. 477-483, 2015.

[6]. K. S. Williams and S. J. Grannis, "Examining the Heartland Region Pilot: First Look at the Patient-Centered Data HomeTM Framework," in *AMIA*, 2018.

[7]. (2016). *Health Information Exchange: Opportunities and Challenges for Health Centers*.

[8]. R. S. Rudin, A. Motala, C. L. Goldzweig, and P. G. Shekelle, "Usage and effect of health information exchange: a systematic review," *Annals of internal medicine*, vol. 161, no. 11, pp. 803-811, 2014.

[9]. J. S. Ancker, M. Silver, M. C. Miller, and R. Kaushal, "Consumer experience with and attitudes toward health information technology: a nationwide survey," *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 152-156, 2013.

[10]. K.-Y. Wen, G. Kreps, F. Zhu, and S. Miller, "Consumers' perceptions about and use of the internet for personal health records and health information exchange: analysis of the 2007 Health Information National Trends Survey," *Journal of medical Internet research*, vol. 12, no. 4, p. e73, 2010.

[11]. C. Williams, F. Mostashari, K. Mertz, E. Hogin, and P. Atwal, "From the Office of the National Coordinator: the strategy for advancing the exchange of health information," *Health affairs*, vol. 31, no. 3, pp. 527-536, 2012.

[12]. J. J. Cimino, M. E. Frisse, J. Halamka, L. Sweeney, and W. Yasnoff, "Consumer-mediated health information exchanges: The 2012 ACMI debate," *Journal of biomedical informatics*, vol. 48, pp. 5-15, 2014.

[13]. D. B. McCarthy, K. Propp, A. Cohen, R. Sabharwal, A. A. Schachter, and A. L. Rein, "Learning from health information exchange technical architecture and implementation in seven beacon communities," *EGEMS*, vol. 2, no. 1, 2014.

[14]. L. Kolkman and B. Brown, "The Health Information Exchange Formation Guide: The Authoritative Guide for Planning and Forming an HIE in your State, Region or Community," 2011: HiMSS.

[15]. J. R. Vest and L. D. Gamm, "Health information exchange: persistent challenges and new strategies," *Journal of the American Medical Informatics Association*, vol. 17, no. 3, pp. 288-294, 2010.

[16]. H. Wu and E. M. LaRue, "Linking the health data system in the US: challenges to the benefits," *International journal of nursing sciences*, vol. 4, no. 4, pp. 410-417, 2017.

[17]. C. Feied and F. Iskandar, "Master patient index," ed: Google Patents, 2007.
[18]. J. D. Price, "Reducing the risk of a data breach using effective compliance programs," Walden University, 2014.
[19]. M. M. Goldstein, A. L. Rein, M. M. Heesters, P. P. Hughes, B. Williams, and S. A. Weinstein, "Data segmentation in electronic health information exchange: policy considerations and analysis," 2010.
[20]. M. Terry, "Medical identity theft and telemedicine security," *Telemedicine and e-Health*, vol. 15, no. 10, pp. 928-933, 2009.

**Jeffrey J. P. Tsai** (F'96) received his Ph. D. degree in Computer Science from Northwestern University, Evanston, Illinois. He is currently the President and the Chair Professor of Bioinformatics and Medical Engineering at Asia University, Taiwan. Dr. Tsai was a Professor of Computer Science and the Director of the Distributed Real-Time Intelligent Systems Laboratory at the University of Illinois, Chicago. He was also a Visiting Professor at Stanford University, a Visiting Scholar at the University of California at Berkeley, a Senior Research Fellow of IC2 at the University of Texas at Austin, and an Adjunct Professor at Tulane University. Tsai chaired the IEEE/CS Technical Committee on Multimedia Computing and served on the steering committee of the IEEE Transactions on Multimedia from 2000 to 2003. He was an Associate Editor of the IEEE Transactions on Knowledge and Data Engineering from 1994 to 1999, and an Associate Editor of the IEEE Transactions on Services Computing from 2008 to 2012. He is currently the Co-Editor-in-Chief of the International Journal on Artificial Intelligence Tools.

Dr. Tsai has served on the IEEE Distinguished Speaker program, U.S. DARPA ISAT working group, and on the review panel for U.S. NSF and NIH. He received Engineering Foundation Research Award from the IEEE and the U.S. Engineering Foundation Society, a University Scholar Award from the University of Illinois Foundation, an IEEE Technical Achievement Award and an IEEE Meritorious Service Award from the IEEE Computer Society, IETI Annual Scientific Award, Distinguished Alumnus Award and Outstanding Leadership Award from National Chiao Tung University. He is a Fellow of the AAAS, a Fellow of the IEEE, a Fellow of the SDPS, and a Distinguished Fellow of IETI.