Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials

Yan Zhuang, BS[1], Lincoln Sheets, MD, PhD[1,2], Zonyin Shae, PhD[3], Jeffrey J. P. Tsai, PhD[3], Chi-Ren Shyu, PhD[1,2,3]

[1]Informatics Institute, [2]School of Medicine, University of Missouri, Columbia, MO, USA

[3]Artifical Intelligence Research Lab, Asia University, Taichung, Taiwan

Abstract

"Blockchain" is a distributed ledger technology originally applied in the financial sector. This technology ensures the integrity of transactions without third-party validation. Its functions of decentralized transaction validation, data provenance, data sharing, and data integration are a good fit for the needs of health information exchange and clinical trials. We investigated the current workflow of Health Information Exchange and clinical trials; conducted design thinking processes with clinicians, trial managers, informaticians, and blockchain professionals; and implemented a private blockchain model to tackle known issues. We used coded Smart Contract regulations to simulate several scenarios in healthcare processes. This proof-of-concept work provides a feasible simulation for potential solutions to monitor clinical trials across different census regions persistently. Various levels of data access privileges have been designed to utilize a suite of customized Smart Contract settings. These settings emulate the workflow protocols for the monitoring entities, trial sponsors, clinical sponsors and participating subjects.

Keywords: Blockchain, Smart Contract, Health Information Exchange, Clinical Trial, Persistent Monitoring.

Introduction

Health Information Exchange (HIE) is a process of sharing patients' Electronic Health Records (EHR) or Electronic Medical Records (EMR) among healthcare providers and patients[1]. Timely HIE could have multiple benefits for patients' healthcare, such as decreasing rates of readmission, avoiding medication errors, improving diagnoses, and decreasing duplicate testing[2]. There are several systems designed for HIE, including Community Health Management Information Systems (CHMIS) and Regional Health Information Organizations (RHIO)[1]. However, there are persistent challenges surrounding HIE: poor clinical efficiency, threats to patient privacy, data insecurity, poor integration of disparate data sources, and dependency on centralized data storage. The latter issue has caused, in some instances, ongoing disagreement between competing providers[1]. Another challenge is the high cost of maintaining and operating these systems. Most systems are designed for healthcare providers, and therefore patients lack personal access and cannot get their data, which means patients cannot benefit from HIE when they visit hospitals outside their home systems[3].

Data sharing issues also exist in the current clinical trial system. Data inconsistency in clinical trials results in the infamous "imprecision medicine" problem[4]. It is a challenging issue because the Food and Drug Administration (FDA) only receives aggregated reports from clinical trial sponsors, without an auditing process to detect potential data quality issues. Data falsification and human entry errors could happen between trial sites and trial sponsors or between trial sponsors and the FDA. Under the current clinical system, it is difficult to perform the timely detection of anomalies. If the system featured real-time collection and analysis of EHR update logs, it would allow sponsors and the FDA to continuously monitor the quality and legitimacy of the data. Because the process is complex, it is difficult to audit every clinical trial from each clinical site frequently (daily or even weekly). Instead, the FDA only receives information from sponsors with aggregated outcomes. A robust system that could ensure data accuracy with analytic capability would allow the FDA to play a more proactive role during the trial process.

Blockchain is a distributed ledger technology which keeps all transactions synchronized among users[5]. All the transactions can be audited publicly by all the users inside the blockchain. Once a transaction occurs, the information can never be erased or changed. A widely known application of blockchain technology is the Bitcoin cryptocurrency[6]. The success of Bitcoin shows the stability, robustness, and security of the blockchain system. Another reason for its success is the anonymity of all users in the blockchain system, which protects user privacy. All user information is recorded as account addresses and does not link with personal information[6]. The features of decentralized transaction validation, insurance of data provenance, data sharing, and data integration are perfect fits for the needs of HIE[5, 7]. In the healthcare community, other prominent applications using blockchain include pharmaceutical research[8].

Because patients are seen and recorded by different healthcare providers, data heterogeneity is expected. Legacy Electronic Data Capture (EDC) platforms need manual data entry. These processes are prone to data inaccuracy[9]. There is a coded self-executing computer protocol on blockchain systems with agreements between requester and receiver called "Smart Contract". Smart Contract could ensure data provenance and create immutable audit trails. We have used Smart Contracts to regulates the transactions in our system. Since each transaction's source is recorded inside the transaction, Smart Contract would only accept transactions sent directly from clinical sites, and other transactions would be declined. This would ensure the accuracy of the data. If the data were falsified outside Smart Contract during the transition, every subsequent user in the blockchain could detect that the data was not sent directly from a clinical site. The transaction would not be accepted due to a high chance of falsification[8].

We have implemented a private blockchain system to simulate scenarios in Health Information Exchange. Since blockchain technology utilizes distributed databases to store all transactions[10], our system is designed to connect multiple EHR databases from different clinical sites and respond to the data requester directly without the need to store the data during a transition. To accomplish this, we have developed an Application Program Interface (API) on a Remote Procedure Call (RPC) server which communicates with the blockchain system to physically and securely transfer health data outside the blockchain.

Blockchain

Blockchain is an open source platform to allow all users to make transactions without a mediating party. It reduces the cost of transactions and time of working with third parties. The entirety of the transaction and validation processes are performed by users inside the blockchain. When a user makes a transaction, all of the information from this transaction is encrypted using cryptographic algorithms and broadcast to every user in the blockchain network for validation[6].

The validation processes contain two parts. The first part is the validation of the user's key pair; the second part is validation that the user's account balance is sufficient to make the transaction[6]. Each user has a unique key pair consisting of a public key and a private key. The public key is similar to proxy user ID in the blockchain system so that no blockchain node is able to know patient's identification. The private key is similar to a user's signature. Each transaction is sent to the receiver's public key and digitally signed by the sender's private key. The receiver needs to validate the identity of the sender by checking whether or not the public key matches the sender's digital signature. Since we use Smart Contract to regulate all transactions executed in the blockchain, transactions only need to be validated through confirmation of sender's identity. If there is a consensus of most users in the system, this transaction is written into the new block. All validated transactions occurring after a previously created block are recorded in the next block. All transactions are secure, trusted, auditable, and immutable. When patients desire to see their personal data or grant other physicians to access to their health data, hospitals need to validate the patients' identities. Blockchain could help hospitals to validate whether or not their public keys and private keys are matched. Using similar concepts, when a clinical trial sponsor or the FDA wants to access subjects' data for persistent monitoring, the same validation process is required.

Blockchain can be set up as a "public chain" or a "private chain." A public chain is also known as "permissionless" chain, which means anyone can join this chain and see all the transactions which have occurred since its beginning[11]. They can also participate in the validation and consensus process. The Bitcoin cryptocurrency uses a public blockchain. A public chain is a fully distributed chain, which means that all transactions are dependent on a consensus decision of all nodes. The stability of blockchain depends on a mass of participating nodes; they contribute computing power to ensure the reliability of the consensus. A private chain is also known as "permissioned chain"[11]. Users must get permission to join the private chain. Each node installs the specific "genesis block" of a private chain in order to join the system. The private chain is not fully decentralized since the creator of a private chain decides who has permission to join this chain[12]. The great benefit of private chains versus public chains is it is easy to regulate the users and transactions in order to ensure privacy, scalability, and security. For EHR data, making transactions visible only to authorized users is ideal. In this work, we utilize a private blockchain system for more security and ease of regulation. Each clinical trial could have different regulations based on their protocols, and each hospital could have different regulations based on their policies. Therefore, a private chain is better than a public chain to offer customized functionality for HIE and clinical trial settings.

Every blockchain will start with a genesis block which is the first block in the chain. We can set up multiple parameters in the genesis block which determine the characteristics of the private chain. A parameter called the "gas limit" restricts the transaction size. In the Ethereum blockchain system, each bytecode inside a transaction has a pre-defined "gas amount". When users deploy Smart Contract in a system, they must pay a "gas fee" for the deployment. If the gas fee

exceeds the gas limit, the transaction will be declined. In our implementation, which does not focus on financial aspects of blockchains, we have assigned a sufficient balance for each user inside the private chain so that every user will be able to send transactions at any time. We have also set up a maximum value of the "gas limit" in case some clinical information is too large to be sent through the blockchain. Another important parameter is called "difficulty", which determines the "block generating rate"[12]. Private chains can set up a high generating speed which can support real-time transactions. In HIE, a transaction can be validated and executed in seconds. Private chains can also build "proof of stake" models to validate transactions, instead of using extensive computing resources[13]. Therefore, private chains are more sustainable than public chains in our applications. In addition, private chains also have Smart Contract protocols to regulate transactions and validate users' identities through coding the policies of different clinical sites and the protocols under different scenarios.

Since we can use Application Program Interface (API) on a Remote Procedure Call (RPC) server to communicate with blockchain systems, all the users inside a blockchain system can use any network terminal device to access the system. An RPC server could also connect EHR databases at clinical sites. Our blockchain system uses an RPC server as a bridge to connect clinical sites databases to perform information exchange. The private chain allows only authorized users to join the system and all transactions are regulated by Smart Contract. Any authorized user can join the system without extra charges for software. Clinical sites need to maintain their local databases as usual and provide at least one node to join the blockchain system. Ideally, each site should provide adequate computing power for its shared transaction activities.

There is a debate regarding private chain versus databases since a private chain is not a fully distributed system[14]. Shared databases could share "read" permissions with multiple authorized users without any issues. However, when users get shared "write" permissions, they can easily modify the master file which could result in unrecoverable errors[15]. Private blockchains provide more secure identity validation and a higher level of error checking than regular shared databases. Private chains can code any permission level for any user. When there is a conflict between users' requests and protocols, Smart Contract uses cryptographic algorithms to ensure that invalid transactions are not added to the blockchain. Even if a hostile attack on a user's account sends fraudulent requests, each user keeps a copy of the transaction history and can recover the system from any given timestamp[16]. Private chains can create peer-to-peer networks; any authorized party inside the private blockchain can query transactions from another party without changing the original data.

Smart Contract

Smart Contract is an agreed computing protocol on top of blockchain, used especially in the Ethereum blockchain system. It was first proposed by Nick Szabo in 1994 to allow distributed ledger systems to regulate contracts[17]. These contracts could be coded as computing protocols, stored inside blockchain systems, and self-executed. Ethereum is a distributed ledger that runs Smart Contract[12]. Smart Contract is written using Solidity, which is a Turing-complete language that can encode all rules needed for HIE. It can also encode data exchange policies from clinical sites.

Smart Contract is compiled using a Solidity compiler residing on a blockchain. After deploying Smart Contracts to the blockchain, the system returns an address[18]. Users who want to use other Smart Contract functions must use the application binary interface (ABI) of the Smart Contract and the Smart Contract address. Users can only check the ABIs for a different Smart Contract. The source code is totally anonymous and is believed to be unhackable[19].

Smart Contract is a coded consensus protocol: all the users in a blockchain system must follow the protocols to make transactions. Figure 1 is an example Smart Contract from our blockchain design, showing how transactions follow the Smart Contract regulations and how different permission levels are set up for different users.

```
pragma solidity ^0.4.13;

contract Ownable {
  address public owner = msg.sender;
  /// @notice check if the caller is the owner of the contract

  modifier onlyOwner {
    require (msg.sender == owner) ;
    _;
  }
  address[] pharmas;
  function Add_pharmas(address[] pharmas_) public
  onlyOwner
  {
      for (uint i = 0; i < pharmas_.length; i++) {
        pharmas.push(pharmas_[i]);
      }
  }

  mapping (address => uint) perms;
  function set_permission() public{
       for (uint i=0;i<subjects.length;i++)
       {
           perms[subjects[i]]=3;
       }
       for (i=0;i<pharmas.length;i++)
       {
           perms[pharmas[i]]=2;
       }
       perms[owner]=1;
       //1 is highest, 2 is high, 3 is low
  }
```

Figure 1 A Smart Contract example demonstrating ownership and permission levels of different roles in the blockchain system.

The contract is deployed by its owner. In our system, we hypothetically assign the FDA as the owner of the Smart Contract. As shown in Figure 1, the "onlyOwner" modifier (line 7) ensures that functions with this modifier can only be executed by the owner. The "Add_pharmas" function (lines 12-18) with the "onlyOwner" modifier ensures that only the owner can add clinical sponsors; executions of this function from other users would be declined automatically. Different roles in the system have different privileges to execute different functions. The "set_permission" function (lines 21-32) is a public function: any user in the system can call this function to initialize their own permissions. There is a pre-defined permission level giving the FDA the highest privilege.

RPC server

To move actual health data around the participating clinical sites, we rely on Remote Procedure Call (RPC) servers connected to different clinical sites' EHRs, since blockchain is not designed to communicate with databases outside the blockchain system[20]. Programs on an RPC server can engage with the Smart Contract within a blockchain. After receiving a request from the Smart Contract, the RPC server queries data from different EHR databases and pushes the required data back to Smart Contract. The whole process is automatically performed after each request.

RPC is a client-server interaction function. After clients from different IP addresses send requests to the server, the RPC server executes functions automatically. The RPC server is the connection between the blockchain system and the clinical sites' databases. The API is built on this server with all pre-defined functions coded in. Authorized users can execute functions from Smart Contract through the API, which can also interact with a PHP Hypertext Preprocessor (PHP) environment so that, after validating a user's identity and permission levels, the server could use PHP to query the proper level of EHR access from the distributed databases.

System Implementation

Overview: We have implemented a private blockchain for HIE and persistent monitoring of clinical trials. Participating clinical sites and clinical trial sponsors can be added to the private chain. Clinical sites provide computing resources as "miners" to perform automatic validation of blockchain integrity. Using Smart Contract in private chains also prevents "51% attacks," in which one miner or pool of miners gains control of 51% of the computing power and is able to manipulate the blockchain[21]. Clinical trial contracts can be structured to reward the contribution of blockchain mining resources. All health records are structured by HL7 standards[22]. All users inside the private blockchain can audit all transactions in the system. Any falsification of a transaction will change the sender of the transaction and will be seen by all other users in the private blockchain.

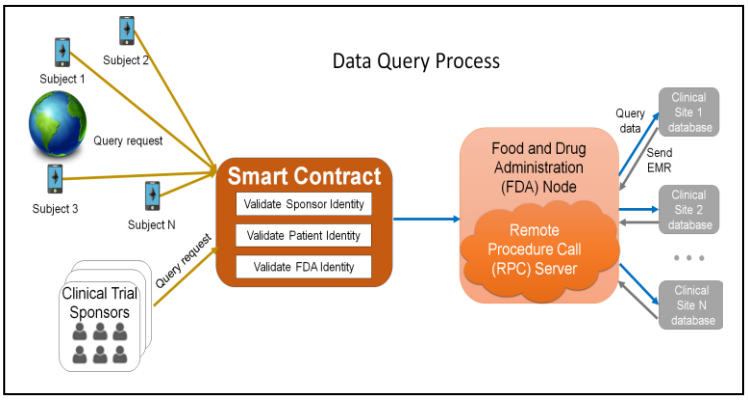

Figure 2. Data Query Workflow between users and clinical sites.

The greatest benefit of using blockchain technology for clinical trials communication is that the FDA could receive raw data from different healthcare providers in real time without barriers or data corruption. Blockchains would ensure immutable audit trails and reliable data provenance. After querying patient records from the trial subjects, the RPC server would push data back to the Smart Contract for further requests. This feature is particularly powerful for a Phase IV clinical trial after new drugs are approved and widely used in practice. This phase may not require recruitment of new patients but does need adverse event updates from patients who have been taking the new drug or treatment[23]. The Smart Contract creates automatic requests after a given time period, so the FDA and clinical trial sponsors can use the system to perform persistent monitoring with a timely decision for potential recalls. The data query process for clinical trials is shown in Figure 2.

We have set up a scenario for HIE process as shown in Figure 3. The patient is admitted to the Emergency Department of Hospital X, where the patient has never visited before. The patient has his medical records stored in both Hospital 1 and Hospital 2. The ER physician needs the patient's records to provide timely treatment. Assume all the hospitals (1, 2 and X) are part of the private blockchain and have set up the blockchain environment with accounts for all patients and physicians in the system. When the patient authenticates the physician to access his/her data using a traditional web-based system or a biometrics-enabled mobile app, the request first goes to the Smart Contract. The Smart Contract validates the patient's identity and the physician's identity prior to sending a request to Hospital 1 and

2, where the patient visited previously. The RPC servers in Hospital 1 and 2 will connect to their own EHR databases and query the patient's records. Then the RPC servers will encrypt the patient's data and send the encrypted data to the RPC server in hospital X. Meanwhile, the RPC servers will also send the encrypted key to the Smart Contract. The Smart Contract will then generate the decrypt key and send it to the RPC server in hospital X. This process will protect from data tampering in the middle of an exchange between the RPC servers. The physician can use the RPC server to decrypt the data using the decrypt key recorded in the blockchain. The physician can access the data with one click, and all the decryption will be performed from the backend automatically.

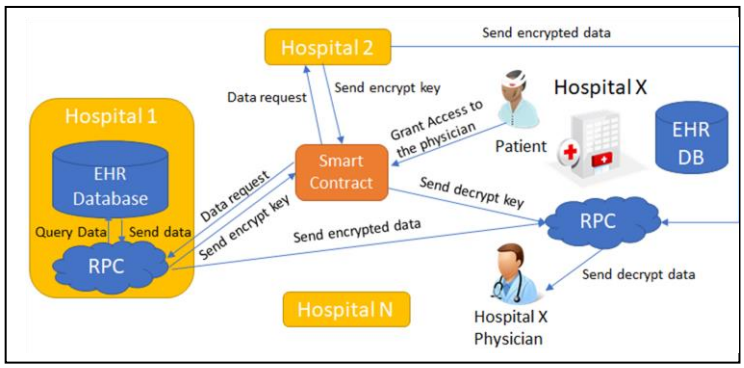

Figure 3 An HIE scenario for an ER visit in Hospital X, with data requests simultaneously sent to multiple clinical sites (Hospitals 1 -N) using a Smart Contract through the private blockchain.

Blockchain: We have created our private blockchain with unique hashing parameters inside the genesis block to ensure privacy. We have also set up a maximum gas limit, which ensures that all transactions can be executed without gas limit issues. Our private chain is set to a low "difficulty" value, so the new block generated speed is around 2 seconds. All participating nodes for this blockchain system must install the genesis block and add an FDA public key as a peer member to finish the installation.

Smart Contract: There are multiple Smart Contracts instances for different clinical trial protocols. The FDA has the highest privilege in a private chain system and registers a list of the clinical trial sponsor's public keys for a clinical trial. Only the FDA has the privilege to add, delete or alter sponsors. When there is a change in sponsor staff, the sponsor needs to contact the FDA to modify the list. Clinical trial sponsors will receive a Smart Contract address from the FDA through the blockchain after the FDA registration. They can use the Smart Contract function to add trial subjects' public keys. Then the Smart Contract generates a unique subject ID for each subject using a hashing algorithm. Registered subjects receive the Smart Contract address at this point. They need the unique subject ID to log in the system. They must input the hospital at which they are currently enrolled. They can input multiple hospitals if appropriate. The patients' subject IDs will map to their real patient IDs from each clinical site. However, only the subject ID is visible to all the users in the blockchain system. The whole process is encrypted. All the public keys are stored inside the private chain. Only the FDA and clinical trial sponsors can check the address list. Clinical trial sponsors and the FDA can check a specific subject's data or all subjects' data; subjects can only query their own data through the Smart Contract. Any request beyond these privileges is automatically declined by the Smart Contract.

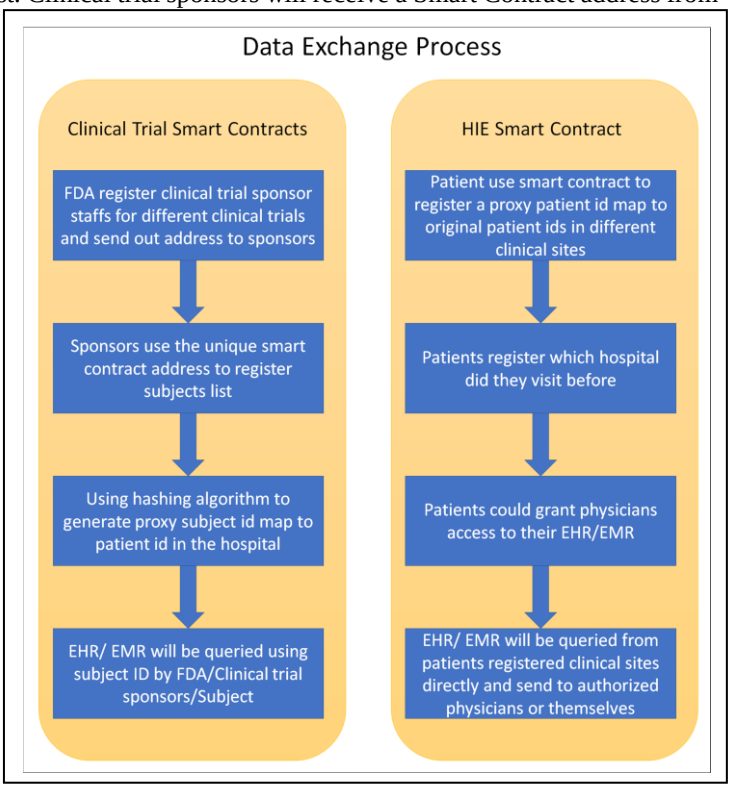

Figure 4. Data Exchange Process using Smart Contract

We have also created an automatic daily or monthly data request function inside the Smart Contract because phase IV clinical trials need a persistent monitoring process. Under this setting, the FDA and clinical sponsors do not

need to send frequent manual requests. After the FDA calls the persistent monitoring function, all the subjects' data will be queried automatically. They only need to check subject data for major adverse events during a given period.

We also developed Smart Contracts to simulate HIE activities. Different from multiple Smart Contracts in charge of different clinical trials, there is only one Smart Contract in charge of HIE process. Users can call the functions in this Smart Contract directly through an API using mobile apps or traditional web-based systems. The API registers a proxy patient ID using a hashing algorithm. The Smart Contract stores the hospitals visited previously and the corresponding patient IDs from those hospitals. Using proxy patient IDs protects patient privacy because users in the system need to validate whether they are querying their own EHR. They can also grant healthcare providers access privileges to their data through the system's calling the access function and feeding the physician's public key. The physician can check the patient's data through the system's calling a function inside the Smart Contract.

Application Program Interface: We have built a web-based Graphical User Interface (GUI) on the RPC server to demonstrate the workflow of the HIE and persistent monitoring of clinical trial processes, using the web3.js library. The RPC server connects to the back-end private chain system. Users can access the blockchain system using their public keys and private keys. Ideally, users should have all keys stored in their portable devices, such as mobile phones, and the authentication process should be straightforward without manually entering keys. Different users have different GUIs to execute dedicated functions of the Smart Contract. After executing functions through the GUI, the blockchain sends a pre-defined command in Structured Query Language (SQL) through a PHP Hypertext Preprocessor (PHP) to query the requested EHR data from a participating hospital's database.

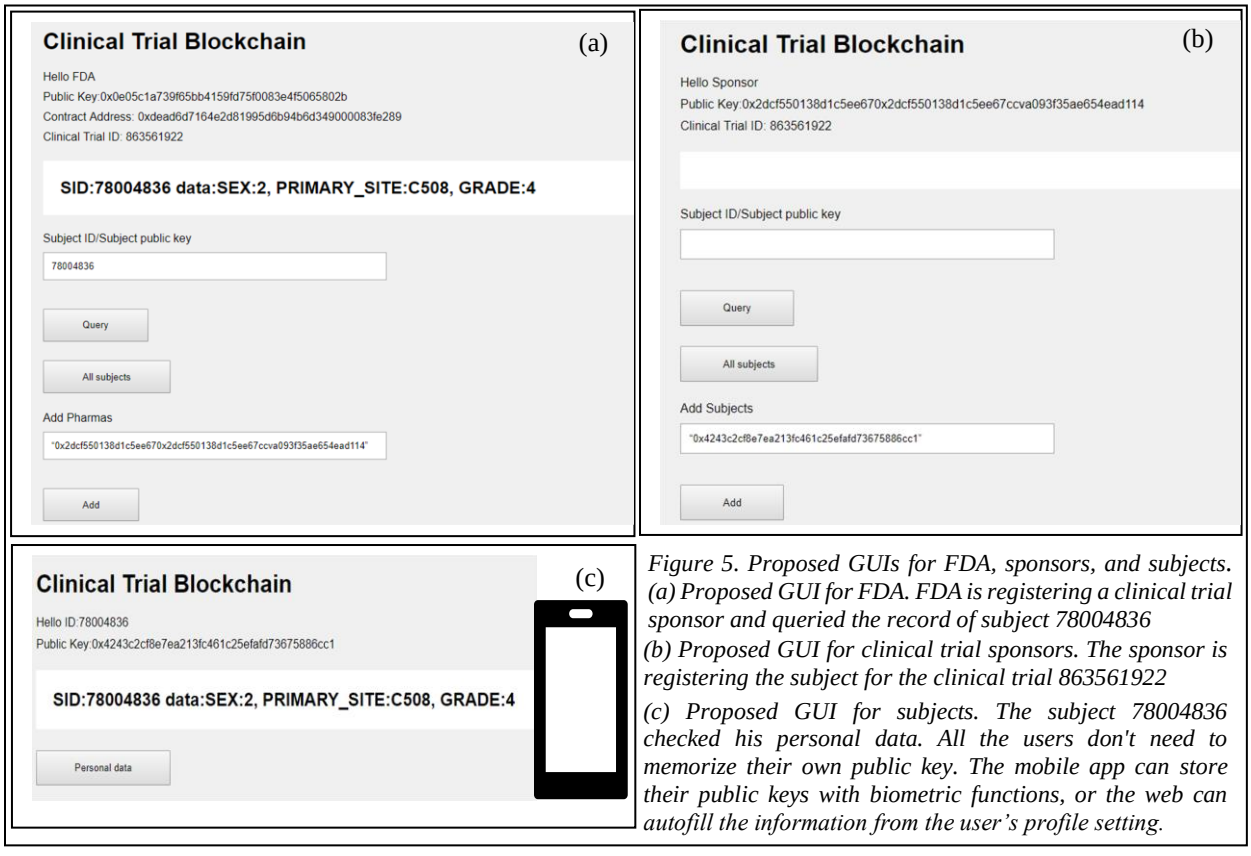

Figure 5. Proposed GUIs for FDA, sponsors, and subjects. (a) Proposed GUI for FDA. FDA is registering a clinical trial sponsor and queried the record of subject 78004836
(b) Proposed GUI for clinical trial sponsors. The sponsor is registering the subject for the clinical trial 863561922
(c) Proposed GUI for subjects. The subject 78004836 checked his personal data. All the users don't need to memorize their own public key. The mobile app can store their public keys with biometric functions, or the web can autofill the information from the user's profile setting.

As shown in Figure 5, after users log into the system, they will have different GUIs based on their roles and privileges. The FDA will see the current contract address and current clinical trial ID. Each clinical trial has a unique Smart Contract. In our proposed setting, the FDA can check specific subjects' data using the subject ID. It can also check all the subjects' data (Figure 5(a)). Another function is registering the list of sponsors. This will give that account the privilege as clinical trial sponsor. GUI for clinical trial sponsors will show the public key and the clinical trial ID on the top, as shown in Figure 5(b). Sponsors can also query all the subjects' records and add subject lists from authorized trials approved by the FDA, as shown in Figure 5(b). For patients/subjects, the GUI will show their subject ID. Their only privilege is checking their own data, as shown in Figure 5(c).

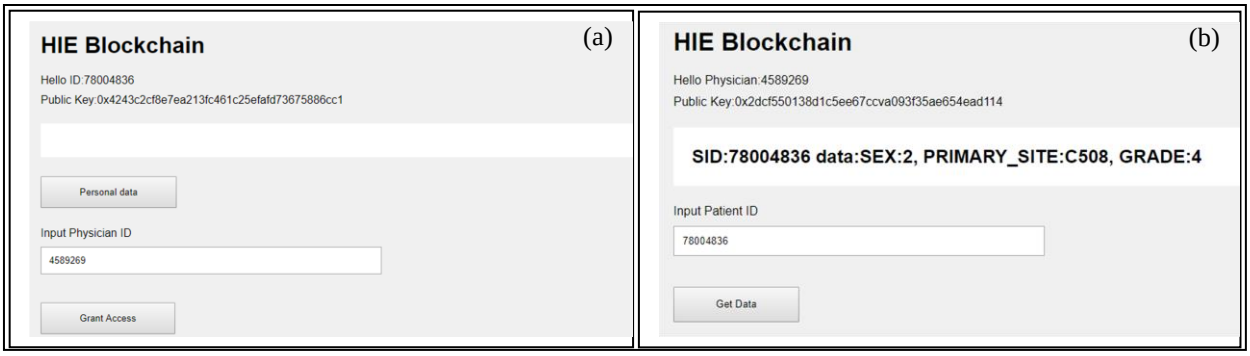

Figure 6. Proposed GUIs for HIE process. (a) GUI for patients. The patient authenticates the physician 4589269 to access his/her data, (b) GUI for physicians. The physician 4589269 can access the patient 78004836's data after his/her authentication.

As for the HIE process, the patient must authorize physicians in the treatment team to access his/her data from remote sites through a web-based GUI or a biometric-enabled mobile app by passing keys to the blockchain system (Figure 6(a)). The physicians in the treatment team will be authenticated via their local EHR system and automatically receive access to the blockchain. The Smart Contract will verify whether the physician has the access to the patient's data. The GUI will show an alert if the request fails the validation process. After the patient authenticates the physician using the physician ID, if the physician is registered in the system, the system will show a confirmation when this transaction is successfully recorded in the blockchain. If the physician is not registered or the public key is not valid, the transaction will be declined and not recorded in the blockchain. The patient's data will be automatically queried from databases from remote clinical sites where he/she visited previously. The necessary data will be sent to the physician progressively through the RPC servers (Figure 6(b)).

Discussion

Blockchain is a disruptive technology to ensure HIE security by tackling several key issues in the current clinical trials workflow. The validation process is automatically executed without any intermediate parties. Current HIE systems have many challenges including costly investment and maintenance by participating clinical sites. In some cases, participating sites not only need to purchase special software, but they may also need to purchase dedicated hardware for the system. Blockchain is an open source platform that requires general computing infrastructure. The private chain we have implemented for the HIE process provides authorization means for users in different applications without a requirement of specialized hardware. There is no third party in the validation process of the blockchain system. This saves costs and time to work with intermediate parties.

Moreover, issues with current clinical trials include patient privacy, data security, data integration, and agreement between competing healthcare providers if a centralized database is used. Blockchain technology addresses these problems effectively. All users in a blockchain system utilize a public key and a private key to validate their identities. These keys will link to their personal information in the hospital's RPC servers rather than the blockchain system. In the clinical trial setting, only the FDA knows the role of each address: either trial sponsor or trial subject. All data in the blockchain system are encrypted using hashing algorithms. Under Smart Contracts regulations, all transactions follow rigorous protocols under secure conditions. Merkle-tree structures inside the blockchain make the system secure, stable, and efficient to search[24].

Competing healthcare providers may have concerns about showing their data to others and storing all data in a centralized database. Blockchain systems mainly focus on identity validation and data encryption. Clinical sites still maintain their own databases and blockchain systems do not require changes to data storage settings. All queries and data analytics are performed on a distributed database. Since blockchain is a distributed ledger technology, it doesn't store any healthcare data inside the blockchain. However, the blockchain system still needs permissions to access clinical sites' databases.

Our blockchain system provides a platform for advanced data analytics using artificial intelligence (AI) methods[23]. Since different hospitals currently use different data management systems, their EHR data formats differ. Data analytics tools play a critical role in the persistent monitoring process which provides the FDA and clinical trial sponsors with real-time alerts for unexpected clusters of adverse events. This novel surveillance feature may change the paradigm of clinical trial processes.

We have conducted simulations of persistent monitoring in a clinical trial, based on new drug testing across different census regions. Various levels of data access privileges have been designed to utilize a suite of customized Smart Contract settings, emulating the workflow protocols for the monitoring institution (the FDA), clinical trial sponsors (pharmaceutical companies), healthcare providers (physicians), and study subjects (patients). The time between sending the request and receiving the data is usually in seconds.

Conclusion and Future Work

Our proof-of-concept work provides the informatics community with a prototype system that goes beyond planning and high-level discussions of blockchain in healthcare. We have shown that blockchain technology is able to facilitate an automatic validation process for HIE and clinical trials without third-party involvement. Using Smart Contracts, blockchain could perform HIE from distributed databases in a secure environment. It could also ensure data provenance and data security. Our future plans include adding artificial intelligence component for real-time detection of anomalies and significant adverse events within certain patient populations. We plan to integrate data analytics tools with Smart Contracts to analyze distributed data, which could improve decision-support efficiency. We also plan to integrate patient-generated Internet of Things (IoT) data, such as self-management sensors and homecare devices.

Acknowledgement

This research is supported in part by the Shumaker Endowment of Biomedical Informatics (YZ and CRS) of University of Missouri, and the Ministry of Science and Technology under the grants MOST 106-2632-E-468-002 and MOST 106-2632-E-468-003 (ZS and JT).

References

1. Vest JR, Gamm LD. Health information exchange: persistent challenges and new strategies. Journal of the American Medical Informatics Association. 2010;17(3):288-94.
2. HealthIT.gov. Health Information Exchange [Available from: https://www.healthit.gov/providers-professionals/health-information-exchange/what-hie].
3. Fontaine P, Ross SE, Zink T, Schilling LM. Systematic review of health information exchange in primary care practices. The Journal of the American Board of Family Medicine. 2010;23(5):655-70.
4. Schork NJ. Personalized medicine: time for one-person trials. Nature. 2015;520(7549):609-11.
5. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017;24(6):1211-20.
6. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.
7. Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. ONC/NIST Use of Blockchain for Healthcare and Research Workshop Gaithersburg, Maryland, United States: ONC/NIST; 2016.
8. Sylim P LF, Marcelo A, Fontelo P. Blockchain Technology for Detecting Falsified and Substandard Drugs in the Pharmaceuticals Distribution System. JMIR Preprints. 2018;16/02/2018:10163.
9. Harris PA, Taylor R, Thielke R, Payne J, Gonzalez N, Conde JG. Research electronic data capture (REDCap)—a metadata-driven methodology and workflow process for providing translational research informatics support. Journal of biomedical informatics. 2009;42(2):377-81.
10. Underwood S. Blockchain beyond bitcoin. Communications of the ACM. 2016;59(11):15-7.
11. Shrier D, Wu W, Pentland A. Blockchain & infrastructure (identity, data security). MIT Connection Science. 2016:1-18.
12. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014;151:1-32.
13. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]. ACM SIGMETRICS Performance Evaluation Review. 2014;42(3):34-7.
14. Greenspan G. Private Blockchains are More Than 'Just' Shared Databases 2015 [Available from: http://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/].
15. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access. 2016;4:2292-303.
16. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (SoK). International Conference on Principles of Security and Trust; 2017: Springer.
17. Szabo N. Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16). 1996.

18. Luu L, Chu D-H, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016: ACM.
19. Delmolino K, Arnett M, Kosba A, Miller A, Shi E. A programmer's guide to ethereum and serpent. URL: https://mc2-umd github io/ethereumlab/docs/serpent_tutorial pdf(2015)(Accessed May 06, 2016). 2015.
20. McConaghy T, Marques R, Müller A, De Jonghe D, McConaghy T, McMullen G, et al. BigchainDB: a scalable blockchain database. white paper, BigChainDB. 2016.
21. Bradbury D. The problem with Bitcoin. Computer Fraud & Security. 2013;2013(11):5-8.
22. Dolin RH, Alschuler L, Boyer S, Beebe C, Behlen FM, Biron PV, et al. HL7 clinical document architecture, release 2. Journal of the American Medical Informatics Association. 2006;13(1):30-9.
23. Braun J, Kästner P, Flaxenberg P, Währisch J, Hanke P, Demary W, et al. Comparison of the clinical efficacy and safety of subcutaneous versus oral administration of methotrexate in patients with active rheumatoid arthritis: Results of a six-month, multicenter, randomized, double-blind, controlled, phase IV trial. Arthritis & Rheumatology. 2008;58(1):73-81.
24. Buterin V. A next-generation smart contract and decentralized application platform. white paper. 2014.