Fine-grained Authorized Medical Data Management

Chunmiao Li[1,3], Yang Cao[2], Zhenjiang Hu[1,3,4], Masatoshi Yoshikawa[2]

[1] National Institute of Informatics, Japan [2] Kyoto University, Japan
[3] SOKENDAI (The Graduate University for Advanced Studies), Japan [4] University of Tokyo, Japan

***Abstract*—Electronic Medical data sharing between stakeholders, such as patients, doctors and researchers, can promote more effective medical treatment collaboratively. These sensitive and private data could only be accessed by authorized users. Given a total medical data, users may care parts of them and other unrelated information might interfere the user-interested data search and increase the risk of exposure. Besides accessing these data, users may want to update them and propagate to other sharing peers so that all peers keep identical data after each update. To satisfy these requirements, in this paper we propose a medical data sharing architecture that addresses the permission control using smart contracts on blockchain and splits data into fined-grained pieces shared with different peers then synchronize complete data and these pieces with bidirectional transformations. Medical data reside on each user's local database and permission-related data are stored on smart contracts. Only all peers have gained the newest shared data after updates can they start to do next operations on it, which are enforced by smart contracts. Blockchain-based immutable shared ledge enable users to trace data updates history. This paper can provide a new perspective to view complete medical data as different slices to be shared with various peers but consistency after updates between them are still promised, which can protect privacy and improve data search efficiency.**

***Index Terms*—medical data, authorization, update, distributed, bidirectional transformations**

I. Introduction

Now a lot of medical data are digitalized so as to be stored and accessed conveniently. A medical record is produced after a patient go to see doctor and often resides on the hospital's database. Medical records contain highly sensitive information about patient privacy. HIPPA Privacy Rule [1] in the U.S. regulates the use and disclosure of personally identifiable health information to protect patients' privacy. However, it hard to make sure that all medical institutes would follow these rules and they may expose patient privacy deliberately or for profit. Moreover, a patient might visit many hospitals and leave his records scattered [2] in different places, which make it hard for him to manage his records efficiently. So patient should be provided a platform to manage and review his historical medical data in case of exposure or being tampered. What's more, better communication between patients and doctors can contribute to patient adherence [3] and improved health [4]. In addition to provide data to doctor, patients tend to share their medical data with health experts to help understand some complex statistics. Many researches has been done to study how medical specialists with different expertise collaborate with each other [5]. Researchers can identify public hearth risks and then develop a better treatments by analyzing existing medical data [6]. As presented in [7], patients and experts can exchange information to develop better plans to satisfy individual routines. Sharing medical data under some constraints could benefit all relating stakeholders such as patients, researchers and doctors.

To be shared by multiple parties, medical data could reside in encrypted formats on a trusted cloud storage server. Only authorized stakeholders can access the shared data. Centralized access control might lead to single point of failure and become the bottleneck of sharing system. Some medical data sharing systems [8]–[10] are proposed to manage authentication based on blockchain [11] technology. Being a immutable shared ledger, blockchain can achieve consensus among distributed nodes via proof of work. Encoding the access control logic of medical data into smart contracts [8] or Chaincode [12] can prevent unauthorized party to access medical data, which will guarantee data security. Anyone who want to access medical data should be verified permission from blockchain side and their access process will be recorded on blockchain.

We identified that there are still other requirements on data sharing and ignored by current works.

Firstly, generally different stakeholders may have different focus on the same medical records. For example, doctors might be more concerned with the clinical data and researchers are interested in mechanism of action, whereas patients care more about the medicine dosage standard. Moreover, doctors may add some terminologies on records which might put patients in confusion and fear. Also, some statistics about hospital internal facilities should not be exposed to patients for privacy protection. To reduce the size of shared data to improve access efficiency and avoid additional data interference, the complete medical data (data source) might be split into lots of smaller data pieces (data views) which are shared by different peers. Each view can be regenerated from the source. Source and view should satisfy predefined consistency relationship. Different views from one source might have overlapped data. Moreover, each party will have a local complete data and different fine-grained data pieces to share with others. In this way, shared data are distributed among sharing parties.

Secondly, not only limited to access data, patients or doctors may want to update existing shared data. Although some works [8] claimed to allow updates on shared medical data, they did not propose any concrete scheme to implement updates and details about how to synchronize all sharing peers to keep them still have same shared data after updates.

In this paper, we aim to solve these two issues on distributed shared medical data as stated above. Each participant

may have multiple fine-grained shared data[1] with different peers and keep this shared ones consistent with complete medical records. We apply bidirectional transformations [13] to synchronize them after updates on either one side. For example, we can invoke *put* direction of a BX program to reflect modifications on shared data to complete data and *get* to produce shared data from complete data. Moreover, any operations on the shared data should be conducted after the peer has been authorized. Permission related data are encoded into smart contracts. Any modifications on the existing shared data should be updated to all sharing peers immediately. We store the sharing peers' identity not pointers to the raw data into smart contracts in case of private data leakage. Each sharing peer will receive the notification from smart contracts after updates on shared data are verified. Then each peer will request the newest data from updater and then use it to update his local complete data. Smart contracts will refuse any further operations on shared data before all sharing peers have pulled the newest data to their local database.

Our contribution are as follow.

1) We proposed to partition complete medical records to a more fine-grained data pieces shared with different peers and apply bidirectional transformations to synchronize a record and multiple pieces.
2) We designed a decentralized medical data sharing architecture where data reside on user's local database and metadata are stored on smart contracts of blockchain to control permission for managing data.
3) We sketched procedures for data management (i.e., Create, Read, Update, Delete) operations on shared data.

The remainder are organized like this. Section II gives some preliminaries about blockchain and bidirectional transformations. Section III sketches our system design and provides a implementation architecture. Section IV discusses identified threats and proposes countermeasures. Section V compares our work with existing ones to clarify our improvement over them. Section VI concludes and directs our future work.

II. Preliminaries

A. Blockchain

Proposed with Bitcoin [11] in 2008, blockchain technology has been widely used in many fields. Blockchain provides a solution for data storage, data transfer and consensus protocol in a distributed and decentralized environment. Generally speaking, blockchain is a shared ledger and replicated by all nodes on a distributed network, which records the historical valid transactions in a chronologically chained blocks. The nodes who generate new blocks by solving a computational puzzle (the proof-of-work problem) are called miners.

Not only can support the platform of cryptocurrency, blockchain can also be applied to other scenes. Ethereum [14] extend blockchain with additions such as a built-in Turing-complete programming language so that one can use this scripts (i.e., Ethereum Virtual Machine (EVM) byte codes) to write programs (i.e., smart contracts[2]) on blockchain. We can just write Solidity[3] programs and then compile it to EVM code. Besides the user accounts controlled by private keys like in Bitcoin, the accounts for smart contracts are allowed in Ethereum. Anyone can build decentralized applications which consist of a collection of smart contracts. Once a transaction involving smart contract creation gets confirmed, an address is generated for the contract and later anyone can send transactions to this address to execute the programs on it. A smart contract transaction is enforced when a miner includes it in a new produced block. Other nodes will validate it and re-run contracts if it is valid.

B. Bidirectional transformations

Maintaining consistency between different data representations having overlapping contents is important [15]. For example, in databases, a view table can be produced by querying a base source table; this view table can be modified, in which case we will want to "restore consistency", i.e., we need to change the source such that the modified view coincides with the result of the query on the changed source — this is the well-known view update problem [16]. To achieve this, one may consider providing two separate programs to represent the two directions to propagate updates from one side to the other. But it is hard to prove that the source and view can still be kept consistent after updates. Bidirectional transformations (BXs) were proposed [17] to solve this.

BX programs[4] can be invoked in two ways as forward and backward transformations. A forward transformation (denoted as *get*) extracts some information from the source to build an abstract view, and the backward transformation (denoted as *put*[5]) embeds information of the view back into the source and produces an updated source. This pair of transformations should satisfy the *round-tripping* laws (also referred to as *well-behaveness*) called *PutGet* and *GetPut*.

$$get(put(\textbf{source}, \textbf{view})) = \textbf{view} \qquad (\textit{PutGet})$$

$$put(\textbf{source}, get(\textbf{source})) = \textbf{source} \qquad (\textit{GetPut})$$

Intuitively, *GetPut* states that no update should be performed on the source when there is no change on the view, while *PutGet* hints that *put* should take all updates on the view into account so that the view can be regenerated from the updated source by *get*. The most distinguished point of BX is that a view can contain only a part of a source. With respect to some consistency between a source and a view, BX programs can synchronize the source and view, and their well-behavedness guarantees that the source and view are kept consistent after updates on either side. There are some

[1]Our work assume that the initialization of shared data has been finished. We only consider management on existing shared data.

[2]Hyperledger and others still provide platforms to write smart contracts.

[3]https://solidity.readthedocs.io/en/v0.5.2/

[4]The BXs we refer to in this paper are asymmetric lenses [18], one of the synchronization models studied by the BX community.

[5]*put* is not a simple inverse of *get*. Instead, it accepts the view and the original source as input and produces an updated source as output.

languages for constructing well-behaved BX programs, such as Boomerang [19], BiGUL [20] and HOBiT [21].

III. System Architecture

We are ready to illustrate our system architecture.

To simplify our expression next, we adopt nodes and users to denote devices connecting to blockchain network and stakeholders (doctors, patients, etc.) in medical scenarios respectively. Users sharing data are called sharing peers.

A. Fine-grained shared data

Shared data[6] can exist in different peers, as shown in Fig. 1. Suppose there are three users: patient Alice, researcher Charlie and doctor Bob. Each user have their own complete base table which is named as D1, D2, D3 respectively and different shared data with other users. For example, Bob and Charlie share some data which are stored in D32 on Bob side and D23 on Charlie side respectively. D32 and D23 should contain same contents, which means either one is updated and the other one need be modified to become identical with it again. Similarly, Alice and Bob share same contents that stored in D13 and D31 separately in their sides. Notably, the formats and contents of shared data are predefined by sharing peers.

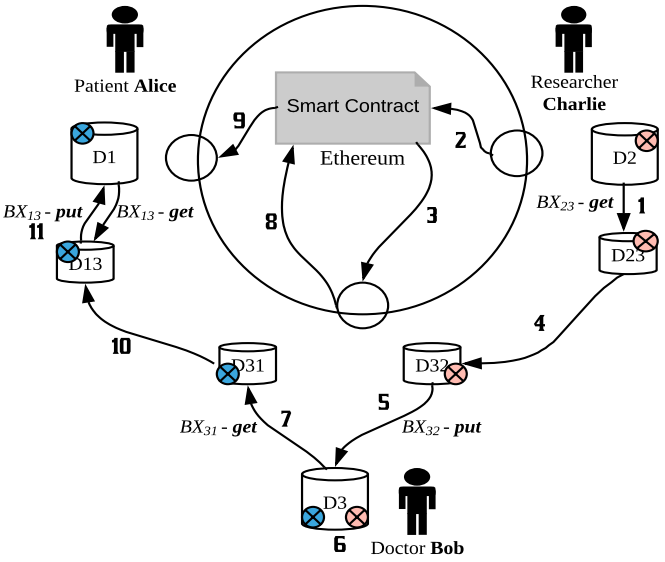

Fig. 1. A workflow for updating data fields of shared data

Figure 2 presents a concrete example with statistics to illustrate this structure. Each user stores a complete medical record and different shared data pieces on their local database. As we said before, BX programs are used to synchronize the complete data and shared data. Shared data can be seen as views which can be produced from complete records named as sources. For example, Table D13 is shared by Alice and Bob and can be produced from D1 by BX_{13}-*get* (i.e., applying get direction of the BX program between D1 and D13). If D13 is

[6]In our prototype, medical data are entered directly by users. Later we may consider using the data from wearable devices.

Patient ID	Medication Name	Clinical Data	Address	Dosage
188	Ibuprofen	CliD1	Sapporo	one tablet every 4h

D1 (Patient **Alice**)

Patient ID	Medication Name	Clinical Data	Mechanism of Action	Dosage
188	Ibuprofen	CliD1	MeA1	one tablet every 4h
189	Wellbutrin	CliD2	MeA2	100 mg twice daily

D3 (Doctor **Bob**)

Patient ID	Medication Name	Clinical Data	Dosage
188	Ibuprofen	CliD1	one tablet every 4h

D13 (also D31)

Medication Name	Mechanism of Action
Ibuprofen	MeA1
Wellbutrin	MeA2

D23 (also D32)

Medication Name	Mechanism of Action	Mode of Action
Ibuprofen	MeA1	MoA1
Wellbutrin	MeA2	MoA2

D2 (Researcher **Charlie**)

Fig. 2. Data distribution

modified, then D1 need to be updated from original D1 and D13 by using BX_{13}-*put*(i.e., invoking put direction of the BX program between D1 and D13) to ensure that the modified D13 can be regenerated from the updated D1.

In our design, shared data between any two peers are not exposed to the third party, which can keep data privacy between them in some degree. For example, any operations on D23 or D32 can only be known by Charlie and Bob and Alice have no information about this. However, after the change on D32 are reflected to D3, since D3 has been modified, D31 might need to be regenerated by using BX_{31}-*get* on D3.

B. Permission on data management

Figure 3 presents an metadata collection table which dictates the update permission on each attribute of the shared data. These kind of tables reside in smart contracts on blockchain. Each metadata entry corresponds to a shared table. For example, the entry for D13 or D31 declares that it is shared by Alice and Bob and Bob can update all attributes value but Alice can only change the clinical data. The "Latest Update Time" shows when the metadata was modified most recently. The value on "Authority to Change Permission" delegates Bob to change other peers' (here just Alice) authority. For instance, for D13 and D31, Bob can change the permission to update "Dosage" to "Bob, Alice" so that Patient Alice can also update the "Dosage" later.

If users want to share data, they need to form agreement on the structure of shared table and register the corresponding

Metadata ID	Sharing peers	Authorized Update Peer			Last Update Time	Authority to change permission
D13 & D31	Alice, Bob	Medication Name	Dosage	Clinical Data	2018.12.22	Bob
		Bob	Bob	Alice, Bob		
D23 & D32	Bob, Charlie	Medication Name		Mechanism of Action	2018.12.23	Bob
		Bob, Charlie		Charlie		

Fig. 3. Metadata collection in smart contract

metadata on smart contracts. Suppose doctor Bob initiates the data sharing with patient Alice. According to their agreement, he will deploy a smart contract on blockchain which stipulates the metadata about the shared data, such as sharing peers (i.e., Alice and Bob) and so on.

C. Data Management

In Fig. 4, we briefly sketch the procedures for CRUD (i.e., Create, Read, Update, Delete) operations on shared data considering entry level or table level respectively. For Read operation, since shared data just stay in users' local databases, they can just execute query to get the shared data. Notably, we describe the workflow for updating an item on Section III-D.

	Entry Level	Table Level
Create, Update, Delete	1. A user try to execute operation locally and send request (transaction) to smart contract 2. Smart contract verify permission 3. If user is authorized then do following 4 (If permission denied, then this request failed) 4. Smart contract notify sharing peers of modification 5. Sharing peers fetch this update on shared data 6. Update metadata on contract 7. Sharing peers conduct BX programs to reflect change on shared data to comlete data	
Read	Query local database directly	

Fig. 4. CRUD operations on shared data

D. Case analysis for Updating shared data

Figure 1 depicts an scenario where researcher initiates the update the shared data. We use the same notation such as D1 in III-A. The numbers indicates the corresponding operations sequence. The red and blue circles with wrong sign indicate the updated places. Step 1 - 5 and Step 7 - 11 achieve procedures for an operation on Fig. 4. Notably, step 6 check whether D32 and D31 have some dependencies.

Let's try to describe this work flow using the data on Fig. 2. After update the "MeA1" on D2, the researcher Charlie wants to propagate the update to the shared data D23 so he uses the BX_{23}-*get* to regenerate D23 (step 1). Then he will call a smart contract via a node connected to Ethereum by sending the request for updates to the D23 (step 2). Note that the smart contract on Fig. 3 records all permission info about that D23. The smart contract will be executed until all nodes form consensus on this update request, which means Charlie is permitted to update D23. Each node will conduct the smart contract locally. The entry relating D23 & D32 of the contract are modified and the doctor Bob will receive notification that D32 need to modified (step 3). Then he will request data from Charlie by sending a message based on some encrypted communication protocol and get the newest shared data to refresh D32 (step 4). After that, Bob will use BX_{32}-*put* to reflect the change on D32 to D3, i.e., update the "MeA1" to a new name. (step 5). Since Bob shared some data (D31) with patient Alice, he need to check whether D31 need to be reproduced (step 6). (If there is no need to reproduce, step 6 - 11 will not happen.) For example, Bob may want to modify the "Dosage" on D31. He will use BX_{31}-*get* to regenerate D31 (step 7) and request smart contract for permission to update D13 (step 8). Once allowed, Alice will receive a notification about the change on "Dosage" (D31) (step 9) and ask Bob to send the updated D31. After Alice get the modified D31 (step 10), he will use this to update D1 via *put* (step 11).

E. System architecture

To achieve our idea, our system will contain four parts, which can be seen from Fig. 5.

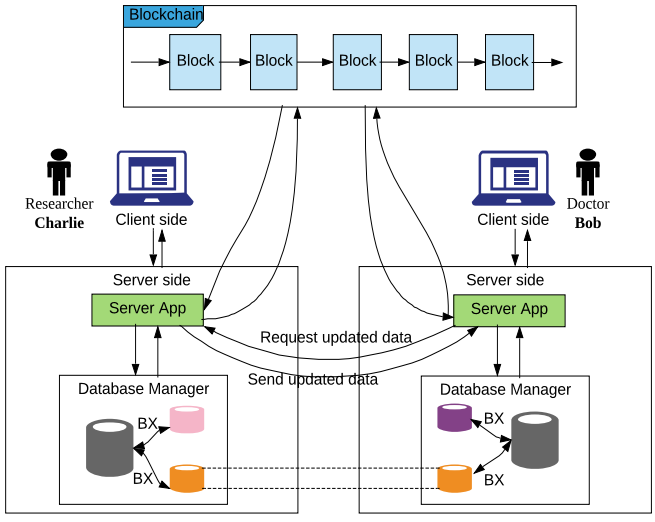

Fig. 5. System Architecture

- Client side: control the interaction between users and other components.
- Blockchain: keep the manage permission of shared data on smart contracts and notify sharing peers the change on them.

- Database manager: disposes the synchronization between shared data and local data according to consistency logic relations. These synchronization are implemented by executing BX programs.
- Database: each user has an complete database and many data pieces shared with other users. The latter (seen as a view) can always be reproduced from the former (seen as a source).

Next, we discuss more details about this architecture.

Firstly, Raw medical data always stay in each peer's local database and data transfer only exist between sharing peers, which avoid data being leaked to the third party so as to keep shared data security. The data can not only be provided by doctors. Instead, each node can be a shared data provider. As referred in [7], many clinics encourage patients to collect data by themselves that are supposed to be gathered by doctors and expect to increase clinic efficiency and promote patient awareness.

Moreover, blockchain's consensus protocol scheme keep the shared data between sharing peers are same after updates since each peer will receive the notification from contracts and request new shared data from other sharing peers. Additionally, any modification on shared data can be recorded on blockchain. Blockchain properties such as immutability, auditablility and transparency enable nodes to check and review update history on shared data. Still, simultaneously updates to the same shared data by multiple peers are forbidden. Smart contracts dispose the updates according to received requests in chronological order. If a transaction for updates on shared data has been included in a block, then other requests on this shared data will not be accepted, i.e., one block can contain one transaction at most on some shared data at one time. This can promise that only when all sharing peers have had newest shared data can they execute further operations.

Lastly, this system architecture can also be applied to other data sharing scenarios.

IV. Threats and countermeasures

In this section, we identify some threats to our system and propose relating countermeasures.

1) Throughput: We employ smart contracts to control access to shared data. As we all known that the block creation time is approximately 12 seconds on Ethereum. We argue that this time interval is acceptable since nodes may choose to collect a lot of updates then send requests to contracts. Usually it is not so urgent for a patient or doctor get the immediate updated shared data.

2) Correctness of smart contracts : Smart contracts might be inconsistent with specifications. We may apply some theorem prover such as Coq [22] to prove or verify the correctness of smart contracts to prevent these attacks.

3) Public blockchain: Once deployed to the public Ethereum blockchain, transactions relating to our systems might not be chosen into a block by miners. So a private blockchain might be a better choice for our system.

4) Incentive: Like in [23], we don't include any incentive for mining beyond the use of our system. We presume that all nodes on the blockchain already have incentives to keep medical data from being tampered and illegal access or updates.

V. Related work

In this section we review existing blockchain-based research on medical data sharing field and state advantages of our system compared with them.

Zyskind et al. suggested using blockchain for access control in [24] where encrypted data reside on the third party storage. But data might be exposed by this "trusted" third party so that data privacy are violated.

The idea of introducing Blockchain technology to healthcare was presented firstly in [25] where they use blockchain for data storage to guarantee medical data can not be modified by anyone. Also, they designed a Healthcare Data Gateway (HDG) to control access of the shared data. However, medical data size can become huge so that become a burden for blockchain nodes' storage since each node have the same copy of blockchain. Usually, the size of metadata is smaller than data. (It also depends on the the structure of metadata and data.) We store metadata on smart contracts so as to reduce the storage pressure for each blockchain node.

MedRec [8] choose to store raw medical data on providers' database and patients can download the data from it after authorized by smart contract on blockchain. They aimed to enable patient to engage in their healthcare. Whereas in our system, all parties, such as doctors, patients, and researchers can benefit from sharing data with others. MedRec recognized that not all provider data such as physician intellectual property can be exposed to patients [26], [27] so that they don't claim to manage contents automatically from physician's output. In our work, instead we allow each node share a piece of medical data not total but still keep consistency between them after the updates to the shared ones. Additionally, any modifications on data shared by two nodes will not be disclosed to the third party which keep the consistency only exists in sharing peers. Moreover, since all shared data with others can be a part of each nodes' local total databases, we can decide whether one shared data have some influence on the other shared pieces and then propagate this change to the third party.

Dubovitskaya at al. gave an architecture to mange and share medical data for cancer patient care [12]. They stored encrypted categorized shared data on cloud and relating metadata in blockchain and implemented the prototype on Hyperledger [28]. The access control policy are defined in the chaincode Logic by patients. Whereas we think that each data provider not just patients can use smart contracts to encode the control policy when they deploy them to Ethereum.

Notably, previous three works and others [9], [10], [23], [29], [30] mostly targeted to the access problem on shared data but did not pay much attention to updates on the them. Additionally, they presumed that different parties can share the same data. Unlike them, we aims to solve the updates issues on the shared data and allow one party can split total

data into multiple pieces (i.e, views) which are shared with different parties but still keep consistency between source and views.

VI. Conclusion

Medical data sharing are necessary and important, which allow stakeholders on medical scenarios to contribute their knowledge to better the medical treatment. Users may have different interest on the same complete medical record. Some peers might update some values of fields in the existing data. This updates need to be propagated to sharing peers. Our architecture divides a record into pieces that shared with different users separately, which can protect data privacy by limiting essential data between two peers and reduce the unrelated data interference. Any updates on data pieces can be synchronized to complete records by bidirectional transformations. Moreover, based on smart contracts on blockchain, we can promise that only authorized users can update the existing shared data and only when all peers have updated to the newest data contents they can continue the operations on shared data.

We are still developing the prototype to implement our idea. In the future, we will use the real patient data to do experiment but use some de-identification technology to protect patient data from being exposed.

References

[1] H. Centers for Medicare & Medicaid Services *et al.*, "Hipaa administrative simplification: standard unique health identifier for health care providers. final rule." *Federal register*, vol. 69, no. 15, p. 3433, 2004.

[2] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[3] K. B. H. Zolnierek and M. R. DiMatteo, "Physician communication and patient adherence to treatment: a meta-analysis," *Medical care*, vol. 47, no. 8, p. 826, 2009.

[4] R. L. Street Jr, G. Makoul, N. K. Arora, and R. M. Epstein, "How does communication heal? pathways linking clinician–patient communication to health outcomes," *Patient education and counseling*, vol. 74, no. 3, pp. 295–301, 2009.

[5] G. Fitzpatrick and G. Ellingsen, "A review of 25 years of cscw research in healthcare: contributions, challenges and future agendas," *Computer Supported Cooperative Work (CSCW)*, vol. 22, no. 4-6, pp. 609–665, 2013.

[6] O. of the National Coordinator for Health Information Technology, "Report to congress: Report on health information blocking," 2015.

[7] C.-F. Chung, "Using personal informatics data in collaboration among people with different expertise," Ph.D. dissertation, 2018.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[9] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 136, 2018.

[10] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[12] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA Annual Symposium Proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[13] Z. Hu, H. Pacheco, and S. Fischer, "Validity checking of putback transformations in bidirectional programming." in *FM*, 2014, pp. 1–15.

[14] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger."

[15] F. Abou-Saleh, J. Cheney, J. Gibbons, J. McKinna, and P. Stevens, "Introduction to bidirectional transformations," in *Bidirectional Transformations*. Springer, 2018, pp. 1–28.

[16] F. Bancilhon and N. Spyratos, "Update semantics of relational views," *ACM Transactions on Database Systems (TODS)*, vol. 6, no. 4, pp. 557–575, 1981.

[17] K. Czarnecki, J. N. Foster, Z. Hu, R. Lämmel, A. Schürr, and J. F. Terwilliger, "Bidirectional transformations: A cross-discipline perspective," in *International Conference on Theory and Practice of Model Transformations*. Springer, 2009, pp. 260–283.

[18] J. N. Foster, M. B. Greenwald, J. T. Moore, B. C. Pierce, and A. Schmitt, "Combinators for bidirectional tree transformations: A linguistic approach to the view-update problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 29, no. 3, p. 17, 2007.

[19] A. Bohannon, J. N. Foster, B. C. Pierce, A. Pilkiewicz, and A. Schmitt, "Boomerang: resourceful lenses for string data," in *ACM SIGPLAN Notices*, vol. 43, no. 1. ACM, 2008, pp. 407–419.

[20] H.-S. Ko, T. Zan, and Z. Hu, "BiGUL: A formally verified core language for putback-based bidirectional programming," in *Proceedings of the 2016 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation*, ser. PEPM '16. New York, NY, USA: ACM, 2016, pp. 61–72. [Online]. Available: http://doi.acm.org/10.1145/2847538.2847544

[21] K. Matsuda and M. Wang, "Hobit: Programming lenses without using lens combinators," in *European Symposium on Programming*. Springer, 2018, pp. 31–59.

[22] G. Huet, G. Kahn, and C. Paulin-Mohring, "The coq proof assistant a tutorial," *Rapport Technique*, vol. 178, 2004.

[23] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[24] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

[25] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[26] U. D. of Health, H. Services *et al.*, "Individuals' right under hipaa to access their health information 45 cfr 164.524," 2017.

[27] C. Grossman, W. A. Goolsby, L. Olsen, and J. M. McGinnis, "Clinical data as the basic staple of health learning: creating and protecting a public good," *Washington, DC: Institute of Medicine*, 2011.

[28] Hyperledger, "Hyperledger," 2017.

[29] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "Bpds: A blockchain based privacy-preserving data sharing for electronic medical records," *arXiv preprint arXiv:1811.03223*, 2018.

[30] S. Amofa, E. B. Sifah, O.-B. Kwame, S. Abla, Q. Xia, J. C. Gee, and J. Gao, "A blockchain-based architecture framework for secure sharing of personal health data," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*. IEEE, 2018, pp. 1–6.