A Blockchain-based Ledger for tw-DRG Claim Auditing

Lie-Jane Kao[1]**, Ben-Chang Shia**[2]

Kainan University, Taoyuan, Taiwan

Taipei Medical University, Taipei, Taiwan

Abstract

In this paper we describe a solution based on a permissioned blockchain to facilitate the auditing of tw-DRG inpatients' claims so that the DRG creep cases can be decreased. Two smart contracts will be designed to cover scenarios in tw-DRG inpatients' claim process and be deployed on the permissioned blockchain, they are the Patient-Provider Service Contract (PPS) and the Coder Classification Contract (CCC), respectively. The PPS would log all the medical services provided by healthcare providers with the providers' encrypted signatures during an inpatient's stay in a hospital. The CCC will audit the coder's tw-DRG classification based on an artificial intelligent (AI) system. Once approved by the AI system, the coder submits the tw-DRG classification and his/her encrypted signature to the blockchain's distributed ledger so the insurer can share all the information that is required to audit the inpatient's claim. By leveraging the distributed, irreversible, and incorruptible nature of a blockchain, it is hoped that a platform where tw-DRG inpatient's claims can be audited more effectively to reduce the DRG creep cases is developed.

Keywords. *Permissioned blockchain, DRG creep, Smart contract, Encrypted signatures, Artificial intelligent, tw-DRG inpatient.*

1. Introduction

Medical insurance fraud claims are causing billions of dollars losses around the world. In US, medical fraud claims cost tax payers over US$80 billion a year [1]. In Taiwan, the total amount of medical fraud claims submitted to Taiwan's Health Insurance Bureau exceeds US$70 million in the year 2015 alone [2]. A broad array of scenarios constitutes medical insurance fraud claims, one of the scenario is DRG manipulations or DRG creep. Here DRG (Diagnosis Related Group) is a system to classify hospital stay cases of similar resource use into groups, which is based on diagnosis and procedure coding using the International Classification of Diseases (ICD) [3], and other important information such as age, gender, weight at admission, length of stay (LOS), discharge status, co-morbidity, complication, and hospital expenditure of individual patient admissions. In Taiwan, Phase I and II of tw-DRG started in 2010 and 2014, respectively, and the Phase III tw-DRG, based on ICD-10, is scheduled to start in March, 2016. However, due to the ambiguity of the DRG coding system, DRG manipulations or DRG creep by hospitals or physicians had been widely documented [4]. These DRG manipulations often do not focus on patients' needs but rather manipulate diagnostic coding to maximize reimbursements.

According to Pongpirul and Robinson [4], DRG creep is categorized into three kinds of practices: corporate, clinical, and coding practices. Corporate DRG creep practice includes manipulations directly related to hospital management, administration, or finance by the executive board or the hospital's director. Clinical DRG creep practice is due to clinical activities by health care professionals, which includes: premature discharge, dump high-cost patients [5], reporting signs or symptoms that patients did not have [6]. In a survey by Wynia et al. [7], 39% of 1,124 US physicians reported making exaggeration of patient clinical conditions sometimes or more often. Decreasing inpatients' length of stay is also a common reported DRG creep [8]. Coding DRG creep practice usually refers to upcoding by a hospital coder, in which patients are misclassified from lower-paying DRGs into higher-paying DRGs to receive higher reimbursements [8]. Upcoding can happen if the coding process starts after a patient's discharge and the coder challenges the physician by switching between the primary and secondary diagnosis [9],[10]. Another type of upcoding is exaggeration of codes by coders with more secondary diagnosis without supportive medical records by the physician [9],[10]. For a review, see [4].

Traditional medical insurance fraud detection is based on the rules established by experts to identify fraudulent cases [11]. In US, as electronic medical records (EMR) is mandated in 2014 by the American Recovery and Reinvestment Act, data-driven approaches for medical insurance fraud detection based on claimants' behavior trajectory big data and machine learning techniques have emerged. However, EMRs are not designed to manage patients' life-time medical records [12], [13]. The healthcare system is a complex ecosystem with multiple stakeholders, which leads to challenges in operational efficiencies. At the same time, to account for data security and privacy, ownership and trusted access to medical data must be considered. Due to these complex granularities, data-driven medical insurance fraud detection approaches have the difficulties in access to the life-time medical records [14], [15]. In this regard, interoperability or data sharing between patients, different healthcare providers as well as insurers pose great challenges to effective medical insurance fraud detection. Interoperability is also a critical component supporting Patient Centered Outcomes Research (PCOR), which helps patients and their care providers communicate and make informed healthcare decisions, allowing their voices to be heard in assessing the value of healthcare options [16].

In this paper we describe a solution based on the blockchain technology to facilitate the auditing of tw-DRG inpatients' claims so that the DRG creep cases can be decreased. The solution would log all the medical services provided by the healthcare providers during an inpatient's stay in a hospital. These logs need encrypted digital signatures by the healthcare providers as well as the inpatient. To be able to start the claim process of the inpatient's stay, a threshold amount of services with encrypted digital signatures is required. Later on, the logs are stored on the blockchain's ledger and the coder is notified, who needs to classify the inpatient's DRG category based on the logs and the other information of the inpatient. The coder's DRG classification needs to be audited by an artificial intelligent system. Once approved by the artificial intelligent system, the coder submits the DRG classification with his/her encrypted digital signature to the blockchain's distributed ledger to be shared with the insurer. By leveraging the distributed, irreversible, and incorruptible nature of a blockchain that serves as a repository of information, it is hoped that a platform where tw-DRG inpatient's claims can be audited more effectively to reduce DRG creep cases can be developed.

2. Background

In healthcare industry, research is seeking to apply blockchain's distributed ledger and decentralized database solutions to the critical issues of interoperability, as well as data security and privacy. Figure 1 illustrates the scenario of using blockchain in the healthcare information system. Blockchain was first introduced by bitcoin [17], but its practical uses extend far beyond cryptocurrency exchanges. The blockchain network is a distributed, decentralized peer-to-peer network, among which a group of peers validate transactions, which are governed by the terms of a smart contract, through a consensus protocol [18],[19]. A smart contract consists of a program code that runs on the blockchain by all nodes, a storage file, and an account balance, agreed by two or more transacting parties [20],[21]. By extending blockchain's smart contracts to network management or connecting myriad medical devices, blockchain technology will drive innovation in healthcare services and administration [22].

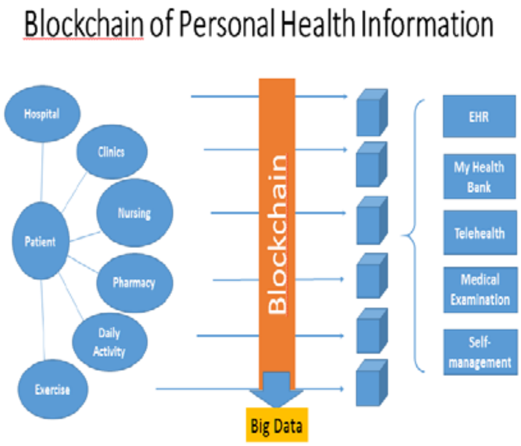

Figure 1. When a health care provider (hospotal, clinics, nursing, pharmacy) creates a medical record, the record is encrypted and a digital signature would be created to register the record in the blockchain. At the same time, the patient is notified that health data was added to his blockchain.

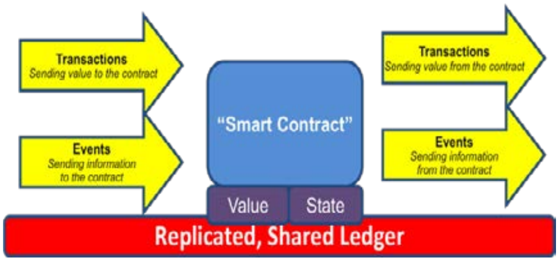
Transactions
Sending value to the contract
Events
Sending information to the contract
"Smart Contract"
Value
State
Transactions
Sending value from the contract
Events
Sending information from the contract
Replicated, Shared Ledger

Figure 2. The information flow of a smart contract (Source: [23])

Once deployed to the blockchain, the contract's code is invoked and executed automatically whenever it receives a message, either from a user or from another contract. While executing its code, the contract may read from or write to its storage file, and pass a return value back to the sender. Figure 2 illustrates the information flow of a smart contract. Ensuing invocation(s) are ordered by a leading node and broadcast to validating peers for consensus. Following validation, transactions are recorded to the ledger in blocks. The ledger is then distributed to all network nodes through replication.

The shared ledger is the single source of truth with the entire history of validated transactions on the blockchain network. The ledger's integrity is checked whenever a new transaction is added and a consensus process is carried out by trusted peers. Any discrepancies in the shared ledger are resolved through consensus. The shared ledger is tamper-proof as time-stamped cryptographic signatures are used to prove that the right participants have added the right transactions at a specific time. For the above characteristics, one often leverages blockchain technology to establish a shared ledger with one or more owners that enables real-time claim adjudication, transparent agreements between stakeholders. In summary, such a distributed ledger may offer major benefits as follows:

1) Reconciliation through consensus. Healthcare providers and the health insurance companies, currently send messages to each other to pass on details of the claims, and then update their own ledgers separately. There is no reliable way to ensure that these separate copies match. Blockchain can solve this by reaching to a consensus state of the ledger through a protocol, and sharing the same reconciliation copy of the ledger to all the parties,
2) Access control. Blockchain technology uses keys and signatures to control who can access the ledger with a specific privilege. For example, a payer may have a 'view key' that allows him to audit a provider's transactions.
3) Transparency and privacy. The decentralized nature of the blockchain has a high degree of transparency since all members in the network have a complete copy of the ledger. At the same time, a distributed ledger combined with cryptographic signatures ensure that an adversary cannot learn anything from the shared ledger as only hashed pointers and encrypted information are contained within the transactions.
4) Tamper-proof to facilitate external auditing. A transaction is incorporated into the blockchain using a public and private key, which provides a timestamped record so that the integrity and authenticity of the transaction at a specific time point can be independently verified. Any changes made to the original transaction generated different public and private keys indicating that transaction had been altered.

In the following, we consider a permissioned blockchain that restricts participants of a blockchain's network [24]. The structure of the proposed permissioned blockchain's network is given.

3. Solution Architecture

The solution is a platform that leverages a permissioned blockchain to enable transparent transactions between stakeholders. Four types of stakeholder groups form the consortium of participants in the blockchain network, they are: tw-DRG inpatients, healthcare providers, coders, and insurers. The permissioned blockchain network has an enrollment authority that requires stakeholders to register for long-term identity credentials. Together the wallet service, with which the end-users store their key material to submit their digital private signatures to the network, the enrollment authority is in charge of stakeholders' transaction certifications in the network.

Smart contracts that would automate the stakeholders' transactions will be deployed to the permissioned blockchain. Smart contracts are applications designed to be decentralized, autonomous, and pseudonymously running on the blockchain at graduated stages of increasing automation and complexity [18],[19],[20]. Thus, the blockchain could be one potential path to artificial intelligence (AI). Transparency and interoperability of theses transactions to the consortium can be guaranteed due to the distributed nature of the blockchain network.

Due to the complexity of the auditing of tw-DRG inpatients' claim process, two smart contracts will be designed to cover all scenarios and be deployed on the permissioned blockchain, they are the Patient-Provider Service Contract and the Coder Classification Contract, respectively. Due to the cost, only data that is needed for the smart contracts to be executed can be added to the blockchain. Additional detailed clinical information would be stored as a reference URL associated to applicable transaction in the blockchain. In this way, the amount of data shared by the nodes is minimized and interoperability is maintained.

3.1 Smart Contract: Patient-Provider Service Contract (PPS)

Patient-Provider Service (PPS) Contract is a smart contract with stipulations regarding tw-DRG clauses of medical treatments to be provided and hardcoded into the program beforehand. With a multi-signature authorization scheme, each of the healthcare providers as well as the inpatient has a digital private key needed to submit encrypted signatures to the contract. Upon arriving at an inpatient's ward with a sensor connected to the blockchain network, the provider's timestamped encrypted signature for the medical service provided is sent using his/her smartphone or any network connected device to the smart contract. In this way, an auditable history of medical interactions between inpatients and healthcare providers are logged, and a tamper resistant check-in device to keep track of the pieces of services by the healthcare providers that are relevant for the tw-DRG is provided.

To get the contract executed, a threshold amount of medical treatments signed by the healthcare providers must be achieved. Finally, the encrypted signature of the inpatient is also required to get the contract executed. Once executed, a transaction with all the logs of inpatient's medical services during his/her stay in a hospital is submitted to the blockchain. In this way, conspiracy must take place in order for abuse to be undertaken, as no single individual has the unilateral ability to abuse a system [25]. If the required signatures can not be obtained before certain amount of time, the PPS would follow some predefined termination based on an nLockTime clause.

3.2 Smart Contract: Coder Classification Contract

Upon the discharge of the inpatient from the hospital, and the PPS contract submits the transaction to the blockchain network with all the digital signatures of the healthcare providers and the inpatient. Once the transaction is added to the blockchain's ledger, a signal that gives the coder a notification is issued. The coder then starts the Coder Classification Contract (CCC). At this stage, the CCC coder issues a query request with a data pointer to the provider's database to return the inpatient's data. The query string is affixed with the hash of the inpatient's data to guarantee that data have not been altered at the source. With the inpatient's data, the coder classifies the inpatient's category. Once the coder classifies the inpatient's category, artificial intelligence (AI) and data analytics layer, which integrates with provider's database and the National Health Insurance Research (NHIR) database of Taiwan, is invoked to further automate the auditing of the classification by the coder. The coder's classification needs to pass the auditing of the AI and data analytics layers. Once passed, the coder sends his digital signature, and the CCC contract gets executed to submit a transaction with a tw-DRG classification for the inpatient claim. At the same time, a signal that gives the issurer a notification is issued. Figure 3 illustrates the backend implementation of the solution platform.

4. Conclusion

This study proposes a platform though which a consortium would share medical information to drive interoperability, and the auditing of the healthcare providers' services as well as the coder's classification. The platform uses smart contracts to orchestrate a tw-DRG inpatient's claim process, in which authentication logs of medical services are recorded to facilitate care auditability and data sharing. The objective is to leverage the blockchain technology to drastically reduce DRG creep due to either clinical activities or coding practices.

Not only that, the potential uses of blockchain technology in healthcare are multiple and varied. Recently, due to the concerns in privacy, Google's DeepMind has adopted a blockchain protocol in the deal with Royal Free London Stream to build an application that distinguishes kidney issues for hospital patients. It can be expected the blockchain technology and artificial intelligence using machine learning are having more and more interlaced relationships in healthcare.

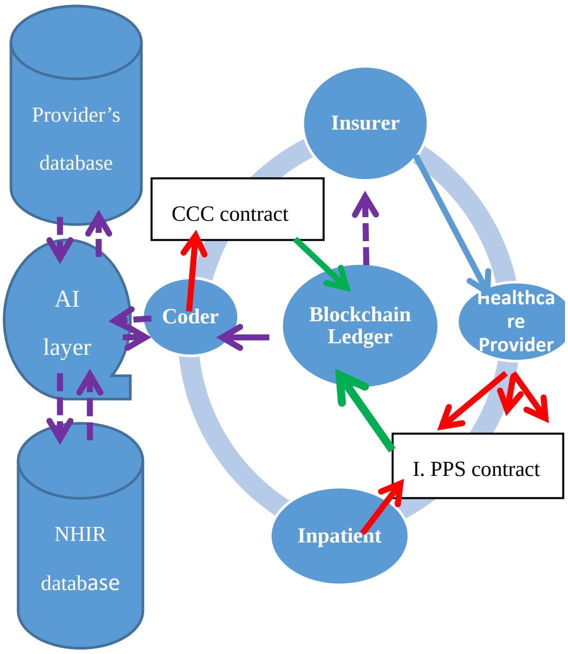

Figure 3 The structure and the workflow of the blockchain network. Four types of nodes on the network: the insurer, healthcare providers, inpatients, and coders. The workflow starts from the Patient-Provider Service (PPS) Contract. After the execution of the PPS, the coder is notified and the Coder Classification Contract (CCC) is invoked. The coder's node is connected to an AI layer, which integrates with provider's database and the National Health Insurance Research (NHIR) database to audit the coder's classification.

References

[1] Aldrich, N., J. Crowder, and B. Benson. 2014. How much does medicare lose due to fraud and improper payments each year? The Sentinel.

[2] Shi, G.I. Epoch Times, 2016. http://www.epochtimes.com/b5/16/11/22/n8517551.htm.

[3] International Classification of Diseases (ICD). World Health Organization. 2008. http://www.who.int/classifications/icd/en/

[4] Pongpirul, K. and C. Robinson. 2013. Hospital manipulations in the DRG system: a systematic scoping review Asian Biomedicine, V7, 3: 301-310.

[5] Malcomson JM. 2005. Supplier discretion over provision: Theory and an application to medical care. RAND Journal of Economics. 36:412-32.

[6] Silverman E, Skinner J. 2004. Medicare Upcoding and Hospital Ownership. Journal of Health Economics; 23:369-89.

[7] Wynia MK, DS. Cummins DS, JB. VanGeest, IB. Wilson. 2000. Physician manipulation of reimbursement rules for patients: between a rock and a hard place. JAMA. 283:1858-65.

[8] Dafny LS. 2003. How Do Hospitals Respond to Price Changes? In: National Bureau of Economic Research, Inc, NBER Working Papers: 9972.

[9] Serden L, Lindqvist R, Rosen M. 2003. Have DRG-based prospective payment systems influenced the number of secondary diagnoses in health care administrative data? Health Policy, 65:101-7.

[10] Steinbusch PJ, Oostenbrink JB, Zuurbier JJ, Schaepkens FJ. 2007. The risk of upcoding in casemix systems: a comparative study. Health Policy, 81:

289-99.

[11] Ngai, E., Y. Hu, Y.H. Wong, Y.J. Chen, and X. Sun. 2011. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems 50(3): 559–569.

[12] Mandl, K.D., D. Markwell, R. MacDonald, P. Szolovits, and I.S. Kohane. 2001. Public Standards and Patients' Control: how to keep electronic medical records accessible but private. *Bmj* 322, 7281: 283-287.

[13] Azaria A., A. Ekblaw, T. Vieira, and A. Lippman. 2016. MedRec: Using Blockchain for Medical Data Access and Permission Management, 2016 IEEE International Conference on Big Data.

[14] Musal, R. M. 2010. Two models to investigate medicare fraud within unsupervised databases. Expert Systems with Applications: An International Journal 37(12):8628–8633.

[15] Liu, J., E. Bier, A. Wilson, T. Honda, S. Kumar, L. Gilpin, J. Guerra-Gomez, and D. Davies. 2015. Graph analysis for detecting fraud, waste, and abuse in healthcare data. *IAAI-15*, 3912–3919.

[16] Shrier, A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J., and Riezen, R. 2016. Blockchain and Health IT: Algorithms, Privacy, and Data, Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services, https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf.

[17] Nakamoto, S. 2008, Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.com.

[18] Szabo, N. 1997. The idea of smart contracts, http://szabo.best.vwh.net/smart_contracts_idea. html

[19] Swanson T. 2014. Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management, eBook. https://www.amazon.com/Great-Chain-Numbers-Contracts-Management-ebook/dp/B00IRUBMXO.

[20] Ethereum, 2016. A next-generation smart contract and decentralized application platform. White Paper. https://github.com/ethereum/wiki/wiki/White-Paper.

[21] Wood, Gavin. 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.

[22] Linn, A., and M. Koo. 2016. Blockchain for health data and its potential use in health IT and health care related research, Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services, https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf.

[23] Brown, R. 2015. A simple model for smart contract, https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/

[24] Swanson T. 2015. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Creative Commons Attribution-ShareAlike 4.0 International License. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

[25] Szabo. N. 2001. trusted third parties are security holes, from http://nakamotoinstitute.org/trusted-third-parties/#selection-11.0-13.0

First Author. LieJane Kao is a professor of the Department of Banking and Finance, Kainan University, No.1 Kainan Road, Luzhu Shiang, Taoyuan 33857, Taiwan, phone: 886-3-341-2500, fax: 886-3-341-2558,

email：ljkao@mail.knu.edu.tw

Second Author. Ben-Chang Shia is the Chief of the Preparatory office in Big Data Research Center and the Dean of the School of Management, Taipei Medical University, 11 F., No. 172-1, Section 2, Keelung Rd., Taipei 110, Taiwan. fax: 886-2-6638-2736, email: stat1001@tmu.edu.tw