

eHealth Block-Chain

Nitin Kamble
iNurture, Bangalore

Monali Bachhav
iNurture, Bangalore

Rohini Deshmane
iNurture, Bangalore

ABSTRACT

This paper describes block-chain architecture as a new solution to provide a new age reliable mechanism for exchanging medical records very securely and efficiently. The Advanced Block-Chain architecture was designed to meet the demands in growing healthcare systems as well as in the new form of social interactive norms. It is going to reform the e-Health industry with countless proficiency by eradicating many of the intermediators known to world today.

Keywords

eHealth, security, block-chain, audit and tracking

1. INTRODUCTION

The purpose of eHealth research program is to develop next generation healthcare digital service solutions to improve patient results, reduction in the cost. It also focuses on the complexity of challenging eHealth problems in terms of security, reliability, efficiency and flexibility. As demands of healthcare spending outgrow many countries' GDPs, there is necessity to adapt the eHealth technological services to meet the demands not only in numbers but also in improvement of social collaborative standards. Latest developments in eHealth research [1] have empowered interoperable and scalable networking, applications, and services for effective sharing of electronic health records, flexible data representation including semantic metadata, and more efficient services that access such health data.

The unified view of worldwide care results, over-prescriptions and billing integrity cannot be easily addressed by the traditional e-Health design solutions as they are more focused on the needs of clinical/hospital/lab usages. To improve the culpability of the e-Health usage data, a new solution direction is necessary to improve inventory access of eHealth data while complementing it with government directives in privacy and security.

The novel approach in this paper is to discover the Advanced Block-Chain paradigm [2] for eHealth record keeping and while addressing the exceptional necessities of patient privacy. As people are moving in the direction of peer networking and on-line practices, we are going to syndicate the best parts of two worlds in both the healthcare regulation and the technology revolution.

2. E-HEALTH DESIGN

There is rapid change in eHealth high-tech solution for interconnection services. While the fundamental Digital Health Care architecture [3] was originated from the Service Layer solution over networked eHealth systems, the detail design have evolved from network interoperability solutions and eHealth security framework, to cloud-computing as well as fast development platforms [4,5,6]. Among the many functions of a continuously scalable universal exchange for current and future eHealth with data originating from diverse sources in multiple formats, advanced processing methods are required for monitoring and sustaining data integrity, security, privacy and reliability also providing trustworthy patient identification and

authentication and access control protocols along with maintaining sensitivity to cultural, legal and ethical issues associated with universally accessible eHealth data.

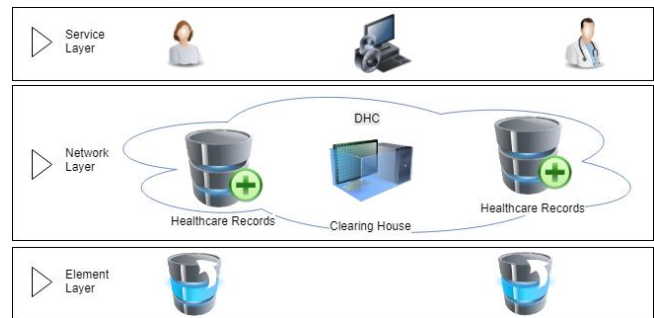


Fig. 1: Interconnections of eHealth System

One example of advanced architecture development is in Smart and Connected eHealth Service [7]. It was designed with context-aware networking capability allowing that any application-oriented services will push the security policies down to the network layer. The access devices and their adaptor gateways are regulated with the e-Health security scheme to facilitate dynamic fork/join of the e-Health network flows. Cross-layer management further provisions with centralized security service management to guarantee the cross-layer performance as well as security assurance.

Another major architecture advancement is the BDeHS [8, 9] approach for big data eHealth model that provided trustworthy patient identification and authentication and access control protocols, maintaining the sensitivity to the legal, cultural and ethical issues associated with universally accessible e-Health data of variety of types like structured, semi-structured and unstructured from variable data sources, including

- HL7 (Health Level 7) well-structured messaging [10,11]
- NCPDP (National Council for Prescription Drug Program) prescription insurance claims and NCPDP SCRIPT for electronic prescription messaging [12]
- DICOM (Digital Imaging and Communications in Medicine) semi-structured data for radiology image exchanges over IP networks [13]
- ISO/IEEE suite of protocols and messaging standards for digital health monitoring and diagnostics devices [14]
- HIPAA transactions for insurance claims and other privacy and security regulation standards [15,16]
- Internal e-Health system logging and security audit records with semi-structured data as far as end-to-end system flows are concerned
- Operational data including security events and usage accounting/charging functions.

While most of these system architectures could be preserved for a block-chain environment, the external data links and communication format will be totally revamped into block-chains.

3. E-HEALTH BLOCK-CHAIN BASICS

In the framework of eHealth, a block-chain maintains a sequence of care records, lab activities, prescription dispense, insurance billings and other supporting activities involving patients, healthcare service providers and supporting organizations. Inside a continuously growing linked list of medical records, each block contains a timestamp and a link to a previous block. The first block-chain was invented by Satoshi Nakamoto in 2008 [2]. A block-chain can serve as an open, distributed ledger that can record transactions between two parties ably and in a certifiable and stable way. The ledger can also be automated to initiate transactions spontaneously.

After a successful implementation in the Bitcoin transactions, the design of a public ledger for all transactions has been the inspiration for other applications such as automatic legal services, insurance processing and even supply chain tracking. All need to resolve the security integrity problem without the use of a trusted authority or central server.

Before moving further, let us analyze some technical features [17, 18] of block-chain in the context of eHealth

3.1 eHealth Block Chain

The basic notion is an eHealth transaction which is redefined as any occurrence of healthcare record generation, submission and exchange. This broad concept can cover EMR (Electronic Medical Records), HER (Electronic Health Records), and e-Prescribe, a Lab request and report including simple blood test, as well as insurance billing and payment. The e-Health Block Chain constitutes all published care related transactions in the block format, each linking to the previous block and linked to by the next e-Health block.

3.2 Distributed Database

Everyone on a block-chain has right to use to the entire database and its complete history. After the eHealth data is posted and validated, no single party controls the data. Because the open access to the eHealth block-chains, correlations between records will overlay new ways for medical research and epidemic reporting.

3.3 Peer-to-Peer Transmission

Peers communicate directly with each other's instead through a central node. Each node stores and forwards information to all other nodes. In healthcare activities, the patients and service providers' records no longer have to be shuffled around via a huge admin center or insurance. Instead each party posts the activities involved to the eHealth block-chain. Once they are validated and agreed upon via the block-chain protocol, the admin center and insurance companies become a wholesome consumer of the original eHealth activity blocks. Of course, the insurance payments could form their own blocks outside the healthcare one which are the center of the next generation eHealth solution.

3.4 Transparency and auto tracking

Every single transaction along with its associated value are visible to anyone with access to the system. Each node, or user, on a block-chain has a unique 30-plus-character ID that identifies it. Users can decide on to stay anonymous or provide proof of their identity to others. Every party can authenticate the records of its transaction partners directly, without an intermediary. Audit of care services become realistic by all interested parties. Excessive cure procedures or abusive consumption of healthcare resources can be detected by constantly mining the public eHealth block-chains.

3.5 Irreversibility of Records

Block-chains are secure by its design and best example of a distributed computing system with high fault tolerance. Block-chains are intrinsically resilient to modification of the data, because the data in any given block cannot be altered without the alteration of all subsequent blocks. Once a transaction is entered within the database and therefore the accounts are updated, the records can't be altered, because they're coupled to each transaction record that came before them (so called as 'chain'). Various computational algorithms and approaches are deployed to make sure that the recording on the information is permanent, chronologically ordered, and out there to any or all others on the network.

4. E-HEALTH BLOCK-CHAIN DESIGN

Use of block-chain achieved decentralized consensus, which makes block-chains potentially suitable for the recording of medical records, treatment events, patient identity management and documenting provenance. However, there are additional hurdles to overcome when an eHealth application is riding directly on a classical block-chain implementation of care record distributions.

4.1 Protocol

These blocks can contain any subset and combinations of the existing HL7 messages, Lab LOINC codes, ICD codes, e-Prescribe as well as the block ID and corresponding signatures from the eHealth service providers and the patients acknowledging to the acceptance of care. Healthcare service providers apply digitization of fast eHealth resources and publish available records during transfer of ownership in handling patient cares, so cares can be conducted at a speed more in line with the pace of doing e-business. Through the use of IDs and permissions, patients can specify which eHealth record details they want others to be permitted to view. Permissions can be expanded for government agencies and auditors, who may need access to more healthcare detail.

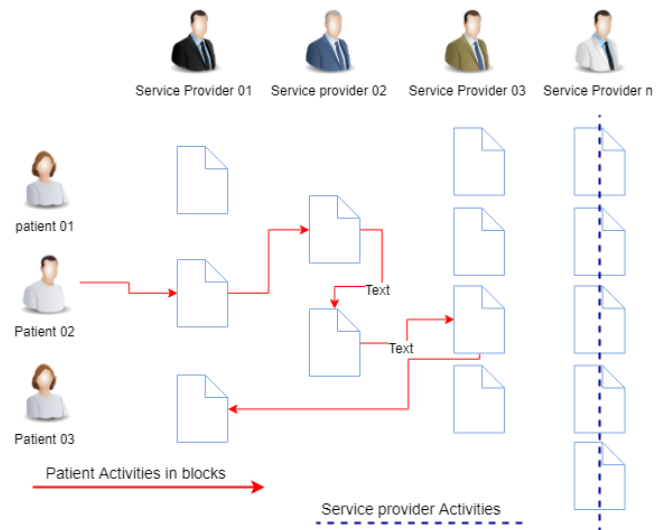


Fig. 2: block-chain design

In fig. 2 there are two dimensional processing threads for the eHealth block-chains. The patient initiated chains forms the information equivalent to the currently know EHR yet in a total different format. On the vertical processing threads are the eHealth blocks as processed by the service providers for their rendered treatment services. Each blocks have to be signed by all involving parties before posting. And they are validated by the eHealth block-chain protocol. Above figure only shows a

two-dimensional block-chain structure, a multiple dimensional block-chain are conceivable when we adds regulatory processing flows and other conformance requirements. Additional system level components will be shown on next page, after the key eHealth block-chain functions are described.

4.2 Certificate Authority

Before any party can participate in the block-chain, it has to be certified and be issued with an authenticated certificate. A security manager in the eHealth block-chain cloud will constantly monitoring the security with a predesignated domain. While the eHealth block-chain usually operate without intermediary intervention, a regulated operational authority can still be instituted. When there are any occasionally non-convergence in block-chain reconciliation as demonstrated in the 2014 Bitcoin, the e-Health services industry cannot simply rely on the faith of the underlying block-chain protocol to resolve. Since timing is the essence in most of eHealth services, especially in accurate care scenarios.

4.3 Regulatory Conformance

The eHealth block-chain enhances the privacy as required since HIPAA [15, 16] and facilitates regulatory conformance. Through the use of IDs and permissions, patients can specify which eHealth record details they want others to be permitted to view. Permissions can be expanded for government agencies and auditors, who may need access to more healthcare detail. Having a shared block-chain that serves as a single source of truth improves the ability to monitor security and audit the cares.

4.4 Block-Chain eHealth Engines

Unlike the passive adaptation gateways that mechanically translate with the e-Health block-chain protocols, the ABC eHealth engines provide health-specific logic to trigger smart transactions defined as a proven treatment procedure flows with maximize automation in mind. This is where the Artificial Intelligence and Machine Learnings are integrated with the block-chain technology for decision making and collaboration. The engine provides the essential supports to other functional blocks in:

- adaptation rules,
- orchestration of service logics,
- API abstraction virtual machine,
- decision rules and processing supports,
- Regulatory compliance rules to drive other additional services such as reporting, discovery and research.

4.5 Value Added Systems

Additional value-added service systems are derived from accessing to the SP-and-patient identities with voluntarily disclosure. For example, a supporting entity such as insurance may obtain identification information and extract and process the eHealth blocks as referenced by a billing block chain without the physicians to submit billing requests as in existing flows. These activities are in turn automatic because of the computational logic in e-Health blocks automatically trigger billing processing and payment transactions between nodes in insurance and in a doctor's office.

Besides the patients and service providers described earlier, additional participants on an eHealth block-chain network play a role in its operation. An eHealth block-chain regulator attends special permissions to oversee the records happening within the network. Block-chain developers create the eHealth application services and smart e-Health contracts that follow the healthcare flows. The eHealth block-chain operators have special monitor the block-chain network. Last but not least, the Certificate

authority issues and manages the different types of certificates required to run a permissioned block-chain either for block-chain users or to individual transactions.

5. BENEFITS & LIMITS

The key benefits of adopting Blocked-Chain eHealth architecture approach are in many folds. The opening of accountable treatment records and insurance billing records sets new cost-effective analysis and place them directly into the hands of the public. This provides auditable eHealth records while preserving patient privacy and security. Medical researchers are open to access the vast eHealth blocks, while government and regulatory agencies are given additional identifiers for audit and conformance purposes. The large number of developers as well as the high interest levels in the industry will eventually push the block-chain technology into a well-accepted mode of operation into the eHealth territory. Our solution is a good attempt to further improve efficiency and reliability as inherently derived from the nature of block-chains. With computational logics to be embedded to the eHealth block-chains, additional personalized medicine is enabled by the complete and consistent data blocks available for all service providers involved. The eHealth Block Chain engine stands ready for the embedded security audits, regulation compliance reporting, billing updates, alerts from lab results and medication events. Innovative healthcare flows with eHealth devices will eventually emerge from the new eHealth block-chain practices. The automation using Block-Chain architecture in turn creates more new types of eHealth professionals.

6. BENEFITS & LIMITS

There are number of unknowns that still potentially limit the fact and wide spread of this approach. The first one is in the regulation of the public block-chain concerning uniform rollouts and leveling the fields. It is recommend that the regulators should keep up with the technological development advances and begin to address any conformance concerns. Second limitation is the cost of implementation in a wide rollout of this disruptive technology. This concern is alleviated with the understanding that the industry has pooled resources in creating reusable block-chain implementations. A number of developed nations and wealthy multi-national corporations can lead in the realization of the Block-Chain eHealth architecture solution.

Finally, how to migrate existing eHealth records into the new block structure is still an open problem that requires additional research and development. Future flows have to be migrated to the new Block-Chain paradigm and derive the inter-SP events using the Patients as center point. Even with these challenging limitations, with this direction of eHealth block-chain solution will show the feasibility and great potential in access, reliability and growth of new services. The most significance of this efforts is in the ultimate purpose of fulfilling the calls for digital health care priorities [19, 20, 21] around the global world.

7. REFERENCES

- [1] M. Braunstein and B. Todd, "Disruptive Technology in the Healthcare Space", GaTech Seminar on technology innovation in the healthcare space, Atlanta, Georgia, on February 10, 2016.
- [2] S. Nakamoto, "Bitcoin P2P e-Cash Paper". Originally published in The Cryptography Mailing List (Mailing list), on October 31, 2008.
- [3] W. Liu, "Digital Health Care (DHC) Information Technology Infrastructure Framework", IEEE Consumer

- Communications Network Conference, Las Vegas, January 2010.
- [4] W. Liu, E.K. Park and U. Krieger, “e-Health Interconnection Infrastructure Challenges and Solutions Overview”, IEEE HealthCom-2012, Beijing, China, October 2012.
- [5] W. Liu, T. Mundie, U. Krieger, E.K. Park and S.S. Zhu, “Rapid delivery e-Health service (RDeHS) platform”, Proceedings of HealthCom-2016, International Conference on e-Health Communications, Services and Applications, Munich, German, September 2016.
- [6] W. Liu, E.K. Park and S.S. Zhu, “e-Health PST (Privacy, Security and Trust)”, IEEE International Conference on Computer Communication Networks, ICCCN/PST Workshop, Shanghai, China, August 2014.
- [7] W. Liu, U. Krieger, E.K. Park and S. Zhu, “Smart and Connected e-Health R&D Platform: A Lab Approach for e-Health Research and Development”, Proceedings of HealthCom-2015, International Conference on e-Health Communications, Services and Applications, Boston, MA, October 2015.
- [8] Technology Association of Georgia, “Big Data in Healthcare”, <http://tagtvonline.com/tag-events/2013-big-data-in-healthcare>, Atlanta, GA, June 2013.
- [9] W. Liu and E.K. Park, “Big Data as an e-Health Service”, Proceedings of IEEE ICNC2014, International Conference on Computing, Networking and Communications, Honolulu, Hawaii, February 2014.
- [10] Health Level Seven International, <http://www.HL7.org/implement/standards>.
- [11] Health Level Seven International, <http://www.HL7.org/fhir>.
- [12] NCPDP, National Council for Prescription Drug Program, <http://www.ncdp.org>.
- [13] Digital Imaging and Communications in Medicine (DICOM)
- [14] ISO/IEEE11073, “Medical/Health Device Communication Standards”, 2004(base standards) to 2017(revisions).
- [15] US Congress, “Health Insurance Portability & accountability Act”, 1996.
- [16] US Committees on Energy and Commerce, Ways and Means, and Science and Technology, “Title IV - Health Information Technology for Economic and Clinical Health Act”, January 16, 2009.
- [17] M. Iansiti and K.R. Lakhani. "The Truth About Blockchain". In Harvard Business Review, issue of January–February 2017.
- [18] B. Yuan, W. Lin, and C. McDonnell, "Blockchains and electronic health records", available from mcdonnell.mit.edu. Cited March 2017.
- [19] J.P. Hu, “Informationization Strategy for Supporting Medical Reforms”, IEEE Healthcom 2012 Keynote Speech, October 11, 2012.
- [20] E.U., “European countries on their journey towards national eHealth infrastructures”, Europe Union, 2011.
- [21] US Department of HHS, www.hhs.gov 2009~2017.