International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

Secure Health Care Data using Blockchain - A Survey

Swathi S[1], Sujithra K[1], Sowmya R[1], Madhumathi C S[2]

[1]UG Students, KPR Institute of Engineering and Technology, Arasur, Coimbatore, Tamilnadu
[2]Assitant Professor, Dept. of Computer Science Engineering, KPR Institute of Engineering and Technology, Tamilnadu, India

---

Abstract – *A blockchain is just a chain and list of blocks. Each block in a blockchain will have its own digital signature, contain digital signature of the previous block, and have some data. Each block doesn't just contain the hash of a block before it, but its own hash is in part, calculated from the previous hash. If the previous block's data is changed then the previous block's hash will change in turn affecting all the hashes of the blocks there after. Calculating and comparing the hashes allow us to see if the blockchain is invalid. We create a blockchain for each patient for storing their medical information's. Details like Health insurance, doctor, lab results medicine details etc. If patient visit different hospital they identified patients previous details using patient key. Healthcare insurance and pharmacy also know patient details. Secure the transfer of the funds, by using a digital signature algorithm to prove ownership. And finally allows the users to make transactions on blockchain. We create system that allows users to create wallets and provides wallets with public and private keys using Elliptic-Curve cryptography. It secures the transfer of funds, by using a digital signature algorithm to prove ownership. And finally allows the users to make transactions on your blockchain.*

Key Words: blockchain technology, bitcoin mining, sha-256, decentralized distributer, health care.

1. INTRODUCTION

It is a very exciting time for health care and the information technology (IT). Due to the improvements in genetic research and the advancement of precision medicine, health care is witnessing an innovative approach to the disease prevention and treatment that incorporates an individual patient's genetic makeup, lifestyle and the environment. Simultaneously, the IT advancement has produced large databases of health information, provided tools to track the health data and engaged individuals more in their own health care. Combining these advancements in health care and the information technology would foster transformative change in the field of health IT.

The American Recovery and Reinvestment Act required all the public and private health care providers to adopt electronic medical records (EMR) by January 1, 2014, in order to maintain their existing Medicaid and Medicare reimbursement levels. This EMR mandate spurred significant growth in availability and utilization of EMRs. However, the vast majority of these systems do not have a capacity to share their health data.

Blockchain technology has a potential to address the interoperability challenges currently present in the health IT systems and to be the technical standard that enables individuals, health care providers, health care entities and the medical researchers to securely share electronic health data.

2. UNDERLYING FUNDAMENTALS OF BLOCKHAIN TCHNOLOGY

Blockchain is a peer-to-peer (P2P) distributed ledger technology for the new generation of transactional applications that establish transparency and trust. Blockchain is an underlying fabric for Bitcoin and is a design pattern consisting of three main components: distributed network, shared ledger and digital transactions.

2.1 Distributed Network

Blockchain is a decentralized P2P architecture with nodes consisting of the network participants. Each member in network stores an identical copy of blockchain and contributes to the collective process of validating, certifying digital transactions for the network.

2.2 Shared Ledger

Members in a distributed network record digital transactions into a shared ledger. To add transactions, the members in the network run algorithms to evaluate and verify a proposed transaction. If majority of the members in network agree that the transaction is valid, the new transaction is added to a shared ledger. Changes to the shared ledger are reflected in all copies of blockchain in minutes or, in some cases seconds. After a transaction is added it is immutable cannot be changed or removed. Since all members in a network have a complete copy of blockchain no single member has the power to tamper and alter data.

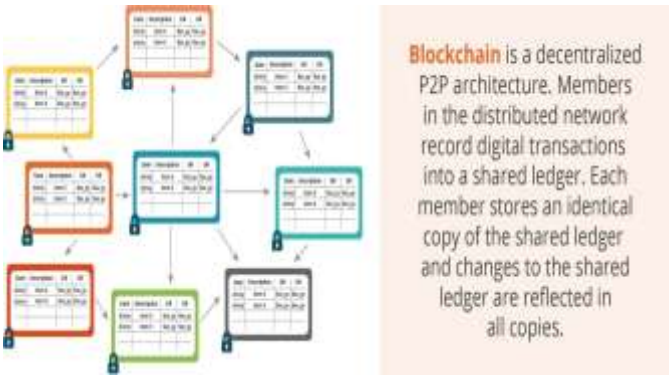

Fig-1: Shared Ledger

2.3 Digital Transactions

Any type of information and digital asset can be stored in a blockchain, and the network implementing a blockchain defines the type of the information contained in a transaction. Information is encrypted and signed digitally to guarantee authenticity and accuracy. Transactions are structured into blocks and each block contains a cryptographic hash to the prior block in a blockchain. Blocks are added in a chronological, linear order.

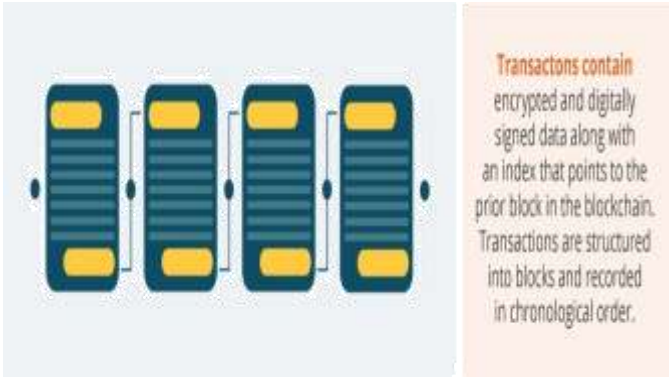

Fig-2: Digital Transactions

3. Proposal

Our proposal involves the use of public blockchain as an access-control manager to health records that are stored off blockchain. There are no open standards currently or implementations of the blockchain that utilize this approach but the research supports feasibility of the proposed solution. Bitcoin has already been demonstrated that trusted, auditable computing is the possible using distributed network accompanied by a shared ledger. Additionally, technologies for the data storage, security and encryption exist and are in use today. This paper has borrowed heavily from the Massachusetts Institute of Technology's published research on using public blockchain to manage and control the access to personal data.

4. BITCOIN AND PRIVATE BLOCKCHAIN LIMITATIONS FHE HEALTH CARE APPLICATION

Bitcoin is based on the open-source cryptographic protocols and it has proven to be a very safe platform for the crypto-currency exchange. While the identities behind some of the Bitcoin transactions remain unknown, the platform provides transparency as anyone can access blockchain and see the balances and transactions for any Bitcoin address.

Lack of data privacy and absence of the robust security make Bitcoin public blockchain unsuitable for health blockchain that requires privacy and controlled, auditable access. Additionally, Bitcoin standard for block size and maximum number of transactions per second present scalability concerns for the large-scale and widely used blockchain applications. Private and consortium led blockchains would address privacy, security and scalability concerns. However, these blockchains would be able to pose different challenges as they run the risk of not being vendor neutral and do not use open standards.

5. A BLOCKCHAIN MODEL FOR HEALTH CARE

Any blockchain for the health care would need to be public and would also include the technological solutions for three key elements: scalability, access security and data privacy.

5.1 Scalability

A distributed blockchain that contains health records, documents, images would have the data storage implications and data throughput limitations. If it is modeled after the Bitcoin blockchain, every member in distributed network of the health care blockchain will have a copy of every health record for every individual in U.S. and this would not be practical from data storage perspective. Because health data is dynamic and expansive, replicating all the health records to every member in a network would be bandwidth intensive, wasteful on the network resources and pose data throughput concerns. For health care to realize the benefits from blockchain, blockchain would need to function as an access-control manager for the health records and data.

b. Access Security and Data Privacy

The user would have a full access to his data and control over how his data would be shared. The user would assign the set of access permissions and designate who can query and write the data to his blockchain. A mobile dashboard application would allow a user to see who has permission to access his blockchain. User would also be able to view an audit log of who accessed his blockchain, including when and what data has been accessed. Same dashboard would allow the user to give, revoke access permissions to any of the individual who has a unique identifier.

VI. TECHNICAL ADVANTAGES OF A HEALTH CARE BLOCKCHAIN

Blockchain technology offers many advantages for the health care IT. Blockchain is based on the open-source software, commodity hardware, and Open API's. These components facilitate faster, easier interoperability between the systems and can efficiently scale to handle large volume of data and more blockchain users. The architecture has the built-in fault tolerance and disaster recovery, and data encryption, cryptography technologies are widely used and accepted as the industry standards. The health blockchain will develop as open-source software. Open-source software is peer-reviewed software developed by the skillful experts. It is reliable and robust under the fast-changing conditions that cannot be matched by closed, proprietary software. Open-source solutions also drive the innovations in applications market. Health providers and individuals would be benefited from the wide range of application choices and could select the options that matched their specific requirements and needs.

Blockchain would run on widely used, reliable commodity hardware. Commodity hardware provides a great amount of useful computation at low cost. The hardware is based on the open standards and manufactured by multiple vendors. It is most cost effective and efficient architecture for health, genomic research. Excess blockchain hardware capacity could be shared with the health researchers and facilitate faster discovery of the new drugs and treatments. Blockchain technology would also address the interoperability challenges within the health IT ecosystem. The health IT systems would use Open API's to integrate, exchange data with the health blockchain. Open API's are based on the industry best practices. They are easy to work with and also it would eliminate the need for development of the complex point-to-point data integrations between the different systems.

Blockchain would allow the patients, the health care community and researchers to access one shared data source to obtain timely, accurate, comprehensive patient health data. Blockchain data structures that is combined with data lakes can support a wide variety of the health data sources including data from patients, mobile applications, wearable sensors, EMR's, documents and the images. The data structures are also flexible, extendable and would be able to accommodate unforeseen data that will be available in the future. Data from a cheap mobile device and wearable sensor is growing at an exponential rate. Distributed architectures based on the commodity hardware provide cost efficient high scalability. As more health data is added to blockchain, cost efficient commodity hardware can be easily added to handle the increased load. Another advantage of the blockchains distributed architecture is a built-in fault tolerance and disaster recovery. Data is distributed across many servers in many of the different locations. There is no single point of failure. It is unlikely that a disaster would impact all locations at the same time.

Blockchain works with the standard algorithms and protocols for cryptography and data encryption. These technologies have been heavily analyzed and accepted as secure and it is widely used across all industries and many government agencies.

7. HEALTH CARE ADVANTAGES OF HEALTHCARE BLOCKCHAIN

Blockchain technology offers many advantages to the medical researchers, health care providers and individuals. Creation of single storage location for all health data, tracking personalized data in real-time and security to set data access permissions at a granular level would serve research as well as personalized medicine. Health researchers require a broad and comprehensive data sets in order to advance the understanding of the disease, accelerate biomedical discovery, fast track the development of drugs and the design customized individual treatment plans based on the patient genetics, lifecycle and environment. Shared data environment provided by Blockchain would deliver a broad diverse data set by including patients from different ethnic and also socio-economic background and from various geographical environments. Blockchain collects health data across a patient's lifetime, it also offers data ideal for longitudinal studies.

A health care blockchain would expand acquisition of the health data to include data from populations of people who are currently under-served by medical community or who don't typically participate in a research. The shared data environment provided by the Blockchain makes it easier to engage "hard-to-reach" populations and develop the results more representative of the general public. Blockchain data structures would work well to gather data from wearable sensors and mobile applications and, thus would contribute significant information on risks versus benefits of treatment as well as patient reported outcomes. Furthermore, combining health data from the mobile applications and wearable sensors with data from the traditional EMR's and genomics will offer the medical researchers increased capabilities to classify individuals into subpopulations that respond well to an specific treatment or who are more susceptible to particular diseases. Daily, personalized health data will likely engage a patient more in his/her own health care and improve the patient compliance. Moreover, the ability for physicians to obtain more frequent data (i.e., daily blood pressure or blood sugar level versus only when a patient appears for an appointment) would improve individualized care with specialized treatment plans based on the outcomes/treatment efficacy.

Blockchain would ensure a continuous availability and access to real-time data. Real-time access to the data would

improve clinical care coordination and improve clinical care in emergency medical situation. Real-time data would also allow researchers and public health resources to rapidly detect, isolate and drive the change for environmental conditions that impact public health. For example, epidemics could be detected earlier and also contained. The real-time availability of the mobile application and wearable sensor data from the blockchain would facilitate continuous, 24 hour per day monitoring of high risk patients and drive the innovation of "smart" applications that would notify the care givers and health providers if a patient reaches a critical threshold for action. Care teams could reach out to a patient and coordinate the treatment options for early intervention.

A health care blockchain would likely promote a development of the new breed of "smart" applications for health providers that would mine the latest medical researches and develop personalized treatment paths. Health provider and the patient would have access to the same information and would be able to engage in an collaborative, educated discussion about the best-case treatment options based on the research rather than intuition.

8. CONCLUSIONS

The most efficient and effective approach to advance ONC's interoperability objectives would be to establish a national technology infrastructure for the health IT based on open standards. Open API's based on the industry best practices are vital and essential to addressing interoperability. However, the open API's are essential but not sufficient. A shared distributed infrastructure that provides comprehensive view of the individual's health data across a lifetime is an equally essential component of the interoperable health IT systems.

Blockchain technology addresses interoperability challenges and is based on open standards, provides a shared distributed view of the health data and will also achieve widespread acceptance and deployment throughout all industries. Utilization of the proposed health blockchain that is described in this paper has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share the vast amount of genetic, diet, lifestyle, environmental and health data with a guaranteed security and privacy protection. The acquisition, storage and sharing of the data would lay the scientific foundation for an advancement of the medical research and precision medicine, help identify and develop a new way to treat and prevent disease and test whether or not the mobile devices engage individuals more in their health care for improved health and disease prevention. Blockchain technology definitely has a place in health IT ecosystem, and the ONC should strongly consider basing their interoperability strategy on blockchain and also using blockchain to promote an advancement of precision medicine.

REFERENCES

1) Alcorn, T., Eagle, A., & Sherbondy, E. Legitimizing Bitcoin: Policy Recommendations. MIT.

2) Bitcoin. (n.d.). Retrieved from Bitcoin: https://bitcoin.org/en/

3) Bit Fury Group. (2016). Digital Assets on Public Blockchains. Bit Fury Group Limited.

4) Blockchain. (n.d.). Retrieved 7 2016, from Wikipedia: https://en.wikipedia.org/wiki/Blockchain(database) Fielder, S., & Light, J. (2015). Distributed consensus ledgers. Accenture, Accenture Payment Services. Accenture. Form a Vital Link. (n.d.). Retrieved 8 2016, from pcori: http://www.pcori.org/

5) How does bitcoin work? (n.d.). Retrieved 7 2016, from Bitcoin: https://bitcoin.org/en/how-it-works

6) Hyper ledger Project. (n.d.). Retrieved 7 2016, from Git Hub: https://github.com/hyperledger

7) Kaye Scholer. (2016). An Introduction to Bitcoin and Blockchain Technology. www.kayescholer.com.

8) Lamport, L., Shostak, R., & Pease, M. (1982, 7). The Byzantine Generals Problem. (S. International, Ed.) ACM Transaction on Programming Languages and Systems.

9) Makary, M. A., & Daniel, M. (2016). Medical error - the third leading cause of death. BMJ. Monegro, J. (n.d.). The Blockchain Application Stack. Retrieved 7 2016, from Joel Monegro Blog:
10) http://joel.mn/post/103546215249/the-blockchain-application-stack Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

11) (2015). Patient-Centered Health on the Blockchain with Chelsea Barabas.

12) Precision Medicine Initiative Cohort Program. (n.d.). Precision Medicine Initiative Cohort Program. Retrieved 7 2016, from National Institutes of Health: https://www.nih.gov/precision-medicine-initiative-cohort-program

13) Rodriguez, J. (2015, 1 26). Building an IOT Platform: Centralized vs. Decentralized Models. Retrieved from https://jrodthoughts.com/tag/enterprise-software/page/2/

14) Rogers, B. (2015, 11). How the Blockchain and VR Can Change the Music Industry (Part 1). Retrieved 7 2016, from https://medium.com/cuepoint/bc-a-fair-trade-music-format-virtual-reality-the-blockchain-76fc47699733#.q8lp7sxfl Rogers, B. (2016, 2 24). How the Blockchain Can Change the Music Industry (Part 2). Retrieved 7 2016, from https://medium.com/cuepoint/how-the-blockchain-can-change-the-music-industry-part-2-c1fa3bdfa848#.gbiei2jc6 Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple Protocol Consenus Algorithm. Ripple Labs Inc. Ripple Labs Inc.

15) (2014). Security and Compliance For Scale-Out Hadoop Data Lakes. EMC.

16) Shead, M. (2009). Retrieved 2016, from Productivity501: http://www.productivity501.com/digital-signatures-encryption/4710/ The Office of the National Coordinator for Health Information Technology. (2015). Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap.

17) Zyskind, G., & Nathan, O. (2015). Enigma: Decentralized Computation Platform with Guaranteed Privacy. MIT. MIT Media Lab.

18) Zyskind, G., Nathan, O., & Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. MIT. MIT Media Lab.