A Security Provisioned Blockchain Architecture for Multi-Purpose Health Information

Article · July 2018

DOI: 10.14257/ijast.2018.116.13

4 authors, including:

Rahul Saha
Lovely Professional University
24 PUBLICATIONS **27** CITATIONS

SEE PROFILE

Gulshan Kumar
Lovely Professional University
34 PUBLICATIONS **33** CITATIONS

SEE PROFILE

Mritunjay Kumar Rai
Lovely Professional University
54 PUBLICATIONS **150** CITATIONS

SEE PROFILE

International Journal of Advanced Science and Technology
Vol.116 (2018), pp.141-150
http://dx.doi.org/10.14257/ijast.2018.116.13

A Security Provisioned Blockchain Architecture for Multi-Purpose Health Information

Rahul Saha[1], Gulshan Kumar[2*], Mritunjay Kumar Rai[3] and Hye-Jin Kim[4]

[1,2]School of Computer Science and Engineering,
Lovely Professional University, India
[3]School of Electronics and Communication Engineering,
Lovely Professional University, India
[4]Business Administration Research Institute, Sungshin W. University,
2 Bomun-ro 34da gil, Seongbuk-gu, Seoul, Republic of Korea
**gulshan3971@gmail.com*

Abstract

Blockchain is a distributed technology used with the series of users in peer-to-peer transactions to utilize the usability properties of the immutable data records. Block chains are the new domain of research and has proved its strong existence in the field of Bitcoins [1, 2]. To use this emerging technology in other fields of network based computing sciences, we have chosen the field of medical data applications as these data needs to be privacy preserving and confidentiality along with its research value. Different medical researches use such data without any predefined framework based upon cloud applications. Several health clouds are also suggested so far. In this paper, we have tried to explore the possibility of the block chain in healthcare information and medical data which will have a transparency in the usage of medical information of the patients and their further analysis.

Keywords*: Block chain, health, privacy, confidentiality, authentication*

1. Introduction

Technology progression always gives the advancement of the devices and methods of applications. Along with this peoples' health and medical problems are also now handshaking with the technology advancements. In old times, people had to go by walk to call on a doctor or to get medicine. But, now doctors or medicine both are available at our doors just for a call. To strengthen the effect more, the analysis of critical diagnosis has been started online by consulting doctors and physicians from around the globe.

Patients aliased consumers play an increasingly important decision-making role in the healthcare market, particularly regarding decisions related to healthcare coverage and treatments. Also, many healthy consumers are taking an active role in maintaining their health and well-being by using smartphones and wearables to track their diets, exercise records and their vital signs; or to read reviews of doctors and care facilities. This increasing consumer participation is in turn driving the need for healthcare provider systems that offer more convenient access and facilitate greater interaction. Cloud computing enables consumers to identify and use best-of-breed health services [3, 4,5] from a range of providers but their security provisions are yet not confirmed.

Though the health organizations are excited about the usage of health clouds but they do not confirm regarding the security provisions of those electronic medical records.

Received (February 16, 2018), Review Result (May 10, 2018), Accepted (May 17, 2018)
* Corresponding Author

ISSN: 2005-4238 IJAST

Therefore, in this paper, we have shown a security provisioned blockchain approach to converge the use of healthcare information on the global platform. The rest of the paper has been organized as following. Section 2 describes some underlying fundamentals of basic block chain technology. Section 3 proposes a system model for the feasible blockchain application in medical and healthcare. Section 4 explains the advantages and limitations of the proposed system model and Section 5 concludes the paper.

2. Underlying Fundamentals of Block Chain Technology

Block chain is transitive logical chaining process in a peer-to-peer (P2P) distributed ledger technology for a brand new generation of transactional applications that establishes transparency and trust. It is considered as the primitive component of crypto currency such as Bitcoin but the underlying pattern of the constituents of the block chain including distributed network, shared ledger and digital transactions is to be used in any transactional process. We have described each of the components briefly in the following.

2.1. Distributed Network

Blockchain is depending upon a distributed network where each node is having equal advantages. No priority or weightage is to be provided to any particular node. This is to be considered as an extended peer-to-peernetwork design. Every node in the network stores a current copy of the block chain and also contributes to the cumulative method of verifying and certifying digital transactions for the network.

2.2. Shared Ledger

All the nodes in the network maintains a shared record of transactions known as ledger. This process makes the overall blockchaining as a trusted and transparent method of implementation. The nodes run algorithms to measure the validity of an initiated transaction of a digital record and verify the planned dealing. If a majority of the nodes within the network agree about the validity of the transaction, then the new transaction of the digital data is included in the block chain, recorded in the ledger and broadcast in the network for update. As the update decision is a group decision, therefore any particular node will not be able to tamper the record or ledger data at any point of time and therefore the openness of the process eventually provides the integrity of the shared ledger.

2.3. Digital Transactions

Any form of data or digital quality is keep during a block chain, and therefore the network implementing the block chain defines the kind of data contained within the group action. Data is encrypted and digitally signed to ensure legitimacy and accuracy. Transactions are structured into blocks and every block contains a cryptologic hash to the previous block within the block chain. Blocks are other during a linear, written account order.

3. Proposed system

In the proposed system model, we have considered each health organization that are willing to access any Electronic Medical Report (EMR) need to be registered with the block chaining process with their details of the organization. Once they are registered, they need to apply for wallet assignment process (Figure-1). This wallet assignment process is nothing but a generation of public-private key combination so that each organization can use those keys as per the cryptographic applications' requirement. Moreover, each wallet will also have wallet id (W_ID) to identify the corresponding health organization.

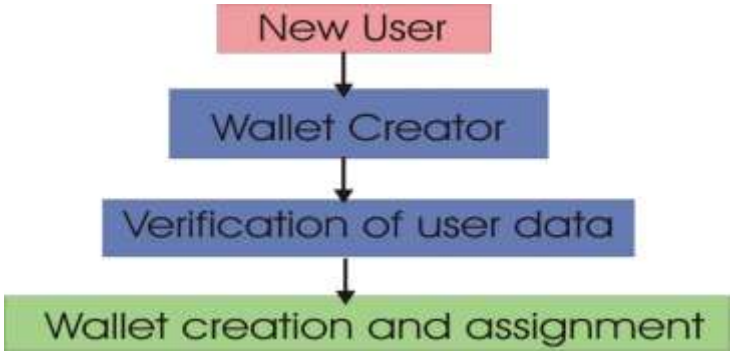

Figure 1. Steps for Wallet Assignment

Therefore, as per the model, the wallet consists: {W_ID, U_i_PUB, U_i_PR}, where U_i_PUB and U_i_PR is the public and private key respectively of the user U_i.

The overall process of healthcare EMR in proposed blockchaining model is summarized below.

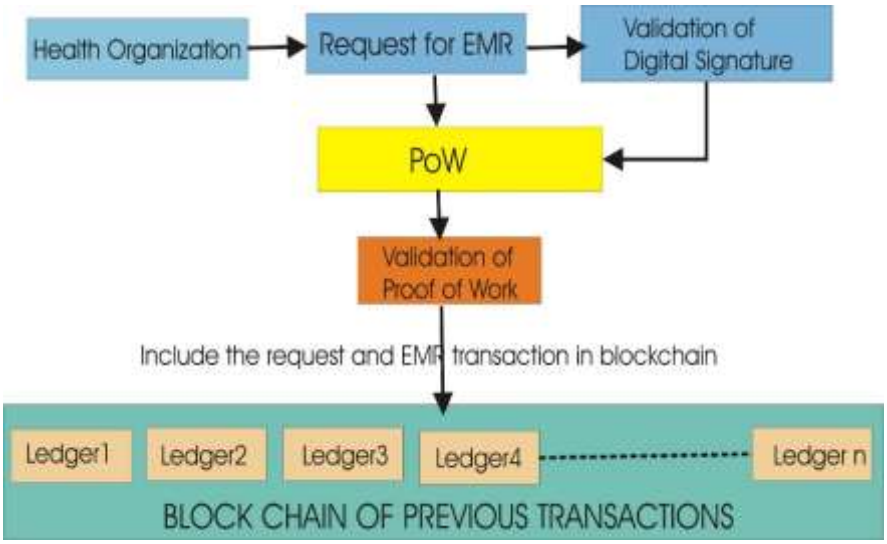

Figure 2. Blockchaining Process for EMR Request

Step 1: A user (health organization who wants the EMR) joins the medical blockchaining network by providing the digital signature and request for an EMR.

Step 2: Once the request has been made and authentication has been proved, the user has been provided a Proof-of-Work (PoW) system. Proof of work is like solving a puzzle such as identifying two same cryptographic hash or prime factorizing a large prime number.

Step 3: Once PoW is solved, the requested transaction has been validated by all the block chain members and the record is added in the ledger.

Step 4: All the members in the block chain network update their own ledgers accordingly and broadcast in the network.

The overall blockchaining process is shown in Figure-2.

4. Feasibility of the Proposed Block Chain Model in EMR Transactions

Any block chain for health care must be open and public without any hindrance to properly analyse the usage of the EMRs. This additionally requires to provide three key security services for: measurability, access control and confidentiality.

Measurability

A distributed block chain that contains health records, documents or pictures would have information storage implications and information output limitations. It is not possible that every member is having a replicated pool of EMRs as it will exhaust the resources of he distributed networks and update of any information is also make it a complex process. Rather, we can see from the block chain previous transactions that whether a requested EMR is already requested previously. If yes, then we can directly send the EMR request to that organization. This will greatly reduce the network overloading. Measurability will also have the effect on the EMR request counts so that unnecessarily requests can be avoided. Though this part is not in scope of the discussion at the present time.

The information contained in this projected health block chain would be an associate in nursing index, an inventory of all the user's health records and health information. The index is analogous to a library catalog in an exceedingly library. The cardboard catalog contains data concerning the book and a location wherever the book will be found. The health block chain would work an equivalent manner. Transactions within the blocks would contain a user's distinctive identity through its wallets ID. Once the PoW is validated, the health record and a timestamp is o be created to boost information access potency, the dealing would contain the sort of information contained within the health record and the other data that may facilitate of times used queries (the data might be intercalary as tags). The health block chain would contain a whole indexed history of all medical information, together with formal medical records moreover as health information from mobile applications and wearable medical kits in real time basis and is to be followed a personal user throughout the life.

All medical information [10,11] would be keep off block chain in an exceedingly information repository known as a health pool. Health poolsare extendable and should store a various type of information, from pictures to documents to key-value stores. This is a valuable tool for health analysis and is to be used for a spread of study together with mining for factors that impact outcomes, determinative optimum treatment choices supported genetic markers and distinguishing components that influence preventative medication. Health pool must also support interactive queries, text mining, text analytics and machine learning for request response applications in real time manner. All info keep within the health pool would be encrypted and digitally signed to ensure privacy and legitimacy of the data. Figure 3 represents a health pool showing the various components.

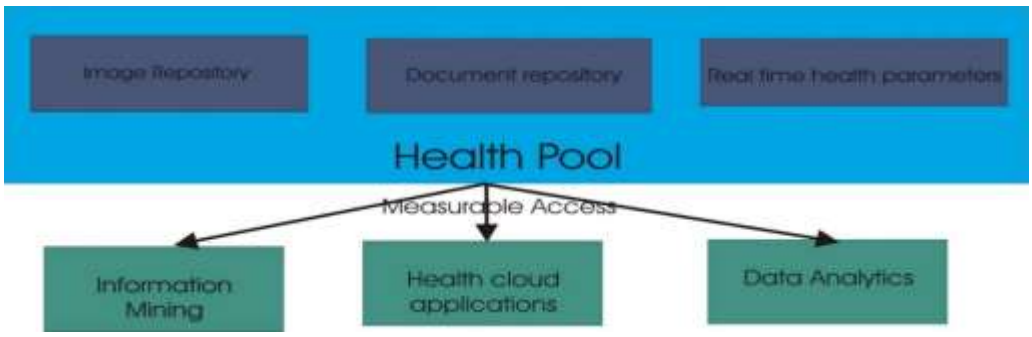

Figure-3. Proposed Concept of Healthpool

Access Security and Information Privacy

The block chain is distributed and open, therefore the information access must be having some condition. The user who are sharing the information will have full access to his information and management in what manner its information are to be shared. The user would assign a collection of access permissions while writing to its own block chain. The user would even be ready to read associate degree audit log of the users that who are accessing his block chain, as well as once and what information was accessed. The permission of the information access will only be given after verifying the digital signature (such as Digital Signature Standard with SHA-256 or SHA-512) of he requested user from the wallet user.

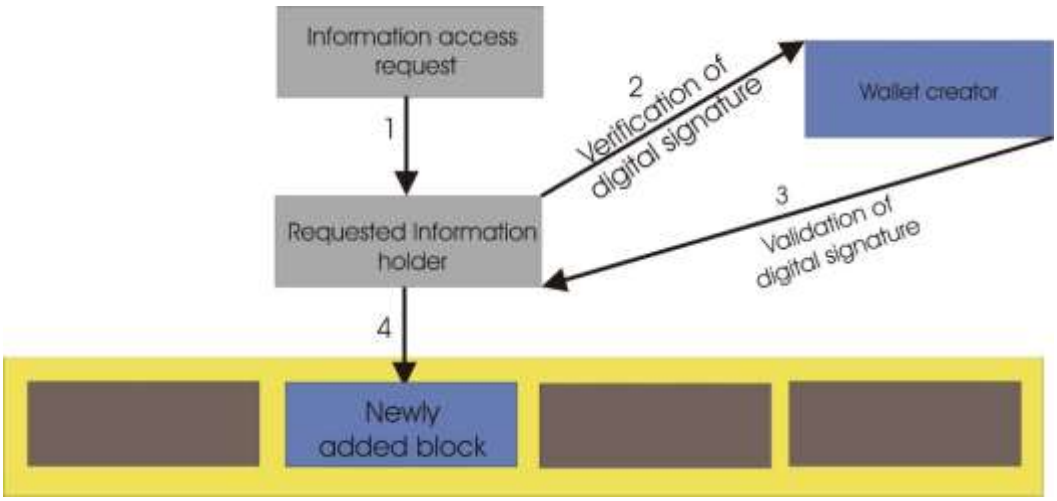

Figure 4. Access Permission Process

Access management permissions would be versatile and would handle over "all-or-nothing" permissions. The user would setup specific, elaborate transactions regarding which user has access, the assigned time-frame for access and therefore the specific forms of information which will be accessed. At any given time the user could alter the set of permissions. Access management policies would even be firmly keep on a block chain and solely the user would be allowed to vary them. This provides associate degree setting of transparency and permits the user to create all choices regarding what information is collected and the way the info are often shared. After a health care supplier is granted access to a user's health info, he queries the block chain for the user's information and utilizes the digital signature to use the information. The health care supplier might utilize a tailor-made best-of-breed application to research the health information. The process is shown below in Figure 4.

Given this model, the user has singular management over his information and also the power to grant access to specific health care suppliers and/or health care entities for communication and collaboration in malady treatment and hindrance. The suburbanized nature of the block chain combined with digitally signed transactions make sure that any third party in between of transaction cannot create any obscurity because the user or corrupt the network as that might imply the individual solid a digital signature or gained management over the bulk of the network's resources. Furthermore, the information in the newly created block will be encrypted therefore, the information containment in the block will only be visible after a key exchange process with the information holder. For this purpose, we can use Diffie-Hellman Key Exchange algorithm [18].

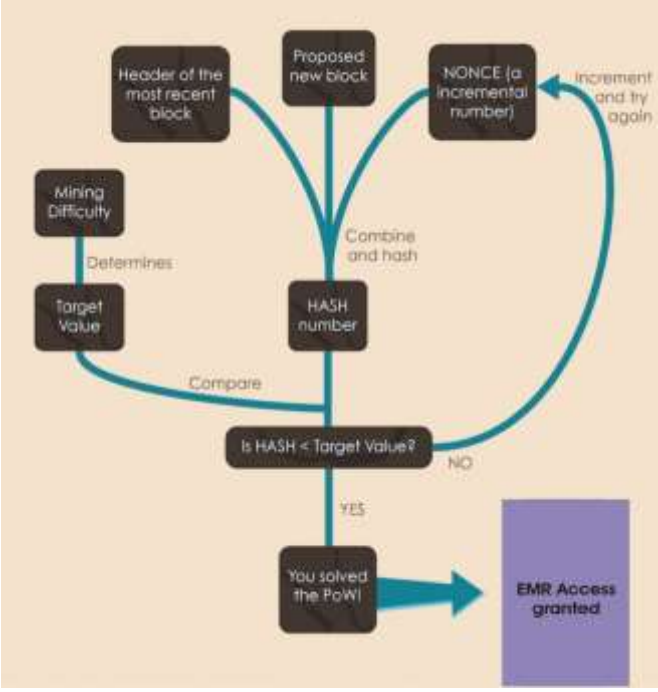

Figure 5. Process of PoW [19]

For the proof-of-work (PoW) we can use different prime factorization problems, optimization problems, random number generation, matching of two random number and many more. The main objective to process with PoW is to check the efficiency and need of a particular EMR by different parties. At the beginning, the PoW puzzle can be kept minimal but when the number of participants increases, PoW also increases its complexity. The working of PoW is shown in Figure 5.

5. Technical benefits of a Health Care Block Chain

Block chain technology offers several benefits for health care applications such as medication analysis, distributed diagnosis EMRs, emergency consultancy of group of doctors and obviously research purpose and identifying new symptoms or medicines for a health problem. Block chain relies on ASCII text file software package, trade goods hardware, and Open API's. These parts facilitate quicker and easier ability between systems and might with efficiency scale to handle larger volumes of knowledge and a lot of block chain users. The design has inbuilt fault tolerance and disaster recovery, and also the cryptography technologies for providing security services such as authentication and confidentiality are wide used and accepted as business standards.

The health block chain would be developed as ASCII text file software package. ASCII text file software package is peer-reviewed software package developed by skilful consultants. It's reliable and sturdy underneath fast-changing conditions that can't be matched by closed, proprietary software package. ASCII text file solutions conjointly drive innovations within the applications market. Health suppliers and people would enjoy the wide {selection big selection} of application selections and will select choices that matched their specific necessities and desires.

Block chain would run on wide used and reliable trade goods hardware. Trade goods hardware provides the best quantity of helpful computation at low price. The hardware relies on open standards and made by multiple vendors. It's the foremost price effective and economical design for health and genomic analysis. Excess block chain hardware

capability might be shared with health researchers and facilitate quicker discovery of recent medicine and coverings.

Block chain technology conjointly addresses the ability challenges inside the health IT system. Health IT systems would use Open API's to integrate and exchange information with the health block chain. Open API's are supported business best practices. They are simple to figure with and would eliminate the necessity for development of advanced point-to-point information integrations between the various systems.

Block chain would enable patients, the health care community and researchers to access one shared information supply to get timely, correct and comprehensive patient health information. Blockchain information structures combined with information lakes will support a large form of health information sources together with information from patients' mobile applications, wearable sensors, EMR's, documents and pictures. the info structures are versatile, long and would be ready to accommodate the unforeseen information that may be accessible within the future.

Data from low-cost mobile devices Associate in nursing wearable sensors is growing at an exponential rate. Distributed architectures supported trade goods hardware give price economical high measurability. As a lot of health information is accessorial to the block chain price economical trade goods hardware will be simply accessorial to handle the hyperbolic load. Another advantage of block chains distributed design is inbuilt fault tolerance and disaster recovery. Information is distributed across several servers in many alternative locations. There's no single purpose of failure and it's unlikely a disaster would impact all locations at an equivalent time.

Blockchain works with commonplace algorithms and protocols for cryptography and encryption. These technologies are heavily analysed and accepted as secure and are wide used across all industries and plenty of government agencies.

6. Health Care Benefits of Health Care Blockchain

Blockchain technology offers several benefits to medical researchers, health care suppliers, care givers and people. Creation of one storage location for all health information, following personalised information in period and also the security to line information access permissions at a granular level would serve a time-efficient, location efficient process for medical issue discussions.

Health researchers need broad and comprehensive information sets so as to advance the understanding of malady, accelerate medicine discovery, means the event of medicine and style bespoke individual treatment plans supported patient biology, lifecycle and surroundings. The shared information surroundings provided by Blockchain would deliver a broad numerous information set by together with patients from completely different ethnic and socio-economic backgrounds and from numerous geographical environments. As block chain collects health information across a patient's lifespan, it offers information ideal for longitudinal studies.

Blockchain information structures would work well for gathering information from wearable sensor devices and mobile applications and, thus, would contribute important data on the risks and thresholds versus edges of treatments also as patient reported outcomes. moreover, combining health information from mobile applications and wearable sensors with information from ancient EMR's and genetic science can provide medical researchers hyperbolic capabilities to classify people into subpopulations that respond well to a selected treatment. Daily, personalised health information can possibly interact with a patient for a lot of his ownself of health care and improve patient compliance. Moreover, the power for physicians to get a lot of frequent information (i.e., daily blood pressures or blood glucose levels versus only if a patient seems for Associate in Nursing appointment) would improve personal care with specialised treatment plans supported outcomes/treatment efficaciousness.

Blockchain would guarantee continuous convenience and access to period information. Period access to information would improve clinical care coordination and improve clinical care in emergency medical things. Period information would conjointly enable researchers and public health resources to speedily notice, isolate and drive modification for environmental conditions that impact public health. as an example, epidemics might be detected earlier and contained.

The period convenience of mobile application and wearable detector information from the blockchain would facilitate continuous, twenty-four hour-a-day watching of high risk patients and drive the innovation of "smart" applications that might advise care givers and health suppliers if a patient reached a crucial threshold for action. Care groups may reach intent on the patient and coordinate treatment choices for early intervention.

A health care block chain would possible promote the event of a brand new breed of "smart" applications for health suppliers that might mine the most recent medical analysis and develop personalised treatment ways. The health supplier and patient would have access to an equivalent data and would be ready to interact in a very cooperative, educated discussion regarding the best-case treatment choices supported analysis instead of intuition.

While block chaining is having its advantages for accessing information, the retrieval of information from the block chain possess a concern of data privacy. Data privacy deals with the confirmation that a particular data cannot be reused by any other party without acknowledging or permission access. But the problem lies at the point where data privacy is relative rather than quantitative. Therefore, policies and regulations need to be variant to incorporate the Blockchain health information. Along with this, the key usage in the process and the notification of the information retrieval at the user level makes it a transparent and trustworthy approach.

7. Conclusion

The most economical and effective approach for advancing the online nursing capability objectives would be to ascertain a national technology infrastructure for health IT supported open standards. Open API's supported business best practices are important and essential for addressing this ability. However, open API's are essential however not decent. A shared distributed infrastructure that has a comprehensive read of Associate in nursing individual's health information across a lifespan is Associate in nursing equally essential part of practical health IT systems. Blockchain technology relies on open standards, provides a shared distributed read of health information and can accomplish widespread acceptance and readying throughout all industries. Utilization of the projected health block chain represented during this paper has the potential to have interaction countless people, health care suppliers, health care entities and medical researchers to share amounts of genetic, diet, lifestyle, environmental and health information with warranted security and privacy protection. The acquisition, storage and sharing of this information would lay a scientific foundation for the advancement of medical analysis and preciseness medication, facilitate establish and develop new ways that to treat and stop malady and take a look at whether or not or not mobile devices interact people a lot of in their health take care of improved health and malady hindrance. Blockchain technology positively encompasses a place within the health IT system our technology progress for achieving a digital life is powerfully contemplated by making a base with their ability strategy on block chain.

References

[1] T. Alcorn, A. Eagle and E. Sherbondy, "Legitimizing Bitcoin: Policy Recommendations", MIT.
[2] Bitcoin. (n.d.). Retrieved from Bitcoin: https://bitcoin.org/en/.
[3] BitFury Group, "Digital Assets on Public Blockchains", BitFury Group Limited, **(2016)**.

[4] Blockchain. (n.d.). Retrieved 7 2016, from Wikipedia: https://en.wikipedia.org/wiki/Blockchain_(database).
[5] S. Fielder and J. Light, "Distributed consensus ledgers", Accenture, Accenture Payment Services. Accenture, Form a Vital Link. (n.d.). Retrieved 8 2016, from pcori: http://www.pcori.org/, **(2015)**.
[6] How does bitcoin work? (n.d.). Retrieved 7 2016, from Bitcoin: https://bitcoin.org/en/how-it-works.
[7] Hyperledger Project. (n.d.). Retrieved 7 2016, from GitHub: https://github.com/hyperledger.
[8] K. Scholer, "An Introduction to Bitcoin and Blockchain Technology", www.kayescholer.com, **(2016)**.
[9] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem", (S. International, Ed.) ACM Transaction on Programming Languages and Systems, **(1982)** July.
[10] M. A. Makary and M. Daniel, "Medical error - the third leading cause of death. BMJ", Monegro, J. (n.d.). The Blockchain Application Stack. Retrieved 7 2016, from Joel Monegro Blog: http://joel.mn/post/103546215249/the-blockchain-application-stack Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[11] Patient-Centered Health on the Blockchain with Chelsea Barabas, **(2015)**.
[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] J. Rodriguez, "Building an IOT Platform: Centralized vs. Decentralized Models", Retrieved from https://jrodthoughts.com/tag/enterprise-software/page/2, **(2015)** January 26.
[14] B. Rogers, "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-par0074-2-c1fa3bdfa848#.gbiei2jc6 Schwartz, D., Youngs, N., &Britto, A. (2014). The Ripple Protocol Consenus Algorithm. Ripple Labs Inc. Ripple Labs Inc, **(2015)** November.
[15] "Security and Compliance For Scale-Out Hadoop Data Lakes". EMC, **(2014)**.
[16] M. Shead, 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, **(2009)**.
[17] G. Zyskind O. Nathan, "Enigma: Decentralized Computation Platform with Guaranteed Privacy", MIT. MIT Media Lab, **(2015)**.
[18] G. Zyskind, O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data. MIT", MIT Media Lab.
[19] W. Diffie and M. Hellman, IEEE Transactions on Information Theory, doi:10.1109/TIT.1976.1055638, vol. 22, no. 6, **(1976)**, p. 644-654.
[20] https://www.bitcoinmining.com/what-is-proof-of-work/.

