

Application of Blockchain in Healthcare in Saudi Arabia

¹Asma A. Alsufyani, ²Mohammed A. AlZain, ³Ben Soh, ⁴Mehedi Masud, ⁵Jehad Al-Amri

^{1,2,4,5}College of Computers and Information Technology, Taif University, Saudi Arabia

³La Trobe University, Bundoora, Australia

Abstract

Blockchain is a new and an attractive concept in a few recent years. It makes a tangible change in a person's life in many domains and it is expected to change their life in more domains in a next couple of years. It is introduced to improve the reliability and comfortability of dealing between people. It has some applications such as Bitcoin and a smart contract, which cover many fields. Blockchain should be facing its challenges to do its task, these challenges come from it is a new concept. One of the domains the blockchain covers is healthcare and it still needs more search and development. We have a mini proposal about healthcare blockchain in Saudi Arabia.

Keywords

Security; Blockchain; Hash Function; Bitcoin; Smart Contract, Ethereum, Hyperledger; Merkle Tree; Proof of Work; Proof of Stack.

I. Introduction

Blockchain is a data structure or a distributed database [1] or a list of nodes, which all these blocks relate to each other using a cryptography algorithm through the internet [2-4]. It has inherent resistance to data modification [5]. In first time, it was developed alongside the cryptographic Bitcoin currency by Satoshi Nakamoto, then it is used for various applications [6-7].

It was created to save time, save money and to be more secure by a decentralized system which does not need to recourse to any trusted third party [8]. The reason of why it does not need a trusted third party is the consensus between the nodes to decide which information is right and which is wrong and to coordinate the nodes [9], this responsibility of deciding and coordinating is to the node [10]. It is resistant and adjustable, which means the modification of blocks is very complicated for security purposes. It provides the availability of a system and an information to the user. Each block in this data structure contains a cryptographic hash of transaction information, cryptographic hash of the previous block, nonce and timestamp. Blockchain allows to store information and run applications with a high level of availability and reliability by using consensus protocols such as (proof of stack protocol) and (proof of work protocol) [6].

Although the blockchain is a new concept, there are many fields to use it such as in cryptocurrencies, smart contract and video game [11]. It is used in financial services, healthcare, government organizations and so on. In healthcare for example, there is a case study that suggests that blockchain can store the sensitive data of a patient and he can share his data with the other under his control (like: which data, how much of it and for how). This service allows a patient to record their data only once and use it in different places [12-13]. It will expand more and more in many domains in the future. This paper focuses on the issues related to the blockchain and suggests a proposal about healthcare blockchain in Saudi Arabia. It pursues to apply a MedRec system in Saudi healthcare organization to enhance the medical field.

While the blockchain has many advantages like it is a distributed system, unchangeable and does not need to a trust third party, it too has disadvantages. The 51% attack is one of the drawbacks of the blockchain, which means if the one of the nodes has a control of hashing for more than 50% of all nodes, then it can deliberately crush the blockchain by removing or resequencing the transactions. The 51% attack threatens the immutable characteristic [14]. The immutable characteristic of blockchain is an advantage and a disadvantage in the same time, which the change or addition to the data in the blockchain is too hard. Each user in the blockchain has a public key and private key for the public key cryptography process, if the user loses his private key, he may lose a real money. It consumes a large amount of energy and storage capacity.

The remainder of this paper is organized as follows. Second section displays some blockchain concepts. The third section is an overview of related work of blockchain. Fourth section presents applications of blockchain. The fifth section is dedicated to explaining the structure of the Blockchain. Sixth section analyses the challenges that faced the blockchain. Seventh and last section discusses a proposal about healthcare blockchain in Saudi Arabia.

II. Blockchain Concept

A. Main Characteristics of Blockchain

There are 6 main characteristics of blockchain, which are decentralized, transparent, open Source, autonomy, immutable and anonymity [14]:

- 1. Decentralized:** not need to center node to manage its operations. Each node deals with its operations by itself.
- 2. Transparent:** all blocks in public blockchain are displayed to anyone.
- 3. Open Source:** open to all, to check and use it in their applications.
- 4. Autonomy:** based on consensus concept.
- 5. Immutable:** the block is unchangeable, unless there is a user has control of more than 51% of all nodes.
- 6. Anonymity:** the identity of the node can be anonymous. The operation depends on the node's address.

B. Some Concepts

There are some concepts we should define to more understanding:

- 1. Node:** is the user or computer that is part from blockchain.
- 2. Block:** is the file contains the data about transaction and data that allow to connect between the it and the previous block and between it and a new block.
- 3. Transaction:** is a main data that stored in a block and we seek to protect it [15].
- 4. Ledger:** is a list of transactions used to record the transactions among the blockchain to prevent any attempting to modify or alter [9].
- 5. Mining:** is the annexation of transaction to the ledger, this concept related to Bitcoin more than any other application

of blockchain.

6. **Miners:** is the users of blockchain which they seek to do something required by system to accomplish the mining process.

III. Related Work

Several papers studied and analyzed blockchain technology, in this section we will present some of it. Stuart Haber and W. Scott Stornetta in 1990 introduce a proposal of timestamped a digital documents to prevent any modification in it [16]. Their timestamp model must meet two conditions: timestamp must be on all document's bits and its time and date should be forgeable. Their proposal has two solutions based on hash function: linking scheme and distributed trust scheme. Linking solution purpose involve some bits of previous user request in a certificate of current request to save the sequence of requests, then submitted to a centralized timestamp service (TSS). Distributed trust solution allows to each user to sign the documented using a pseudorandom generator algorithm. In March 1992 Stuart Haber, W. Scott Stornetta and Dave Bayer improve this proposal by adding trees in its design [17].

Bitcoin appeared before the blockchain technique. In 2008, Satoshi Nakamoto proposes a digital payment scheme through peer to peer network without depending on a trusted third party called bitcoin [6]. It is also designed to prevent a double spending problem. Bitcoin based into: digital signature using a hash function, does not rely on financial institution as a trusted third party, and proof-of-work protocol. Their paper was a first white paper in blockchain.

Arshdeep Bahga, Vijay K. Madiseti present a Blockchain Platform for Industrial Internet of Things (BPIIoT) platform, which is a decentralized platform of an internet of things (IoT) [7]. This platform allows for owners of services sale offer their manufacturing services directly through the blockchain network to the users and allows to the users to buy these services using bitcoin cryptocurrency.

Patrick McCorry, Siamak F. Shahandashti and Feng Hao wrote a paper called "A Smart Contract for Boardroom Voting with Maximum Voter Privacy" propose a distributed voting protocol through the internet with high privacy for the voter and it was implemented in the blockchain network [18]. It is a first protocol which does not depend on a trusted third party to use in boardroom elections. It is a smart contract runs on Ethereum, which is based on a consensus mechanism in its implementation.

IV. Blockchain Applications

A. Bitcoin

Bitcoin was invented in 2008 by Satoshi Nakamoto before the blockchain technology [19-20]. Easy and fast way to exchange payment, cheaper than online payment and useless to steal are the reasons of why people are using the bitcoin [6]. Bitcoin is a most popular application used blockchain to do its functions, it has all characteristics of blockchain. Bitcoin is a digital currency or a cryptocurrency, people can use it to buy services and products, but it does not accept in all places in the world. Three ways to obtain a bitcoin: buying it by using real money, selling products and allowing to the buyer to paying you with bitcoin and it also can be generated.

B. Smart Contract

Smart contract is a protocol of a digital contract developed by Nick Szabo in 1994 [21], which used to exchange a valuable thing in a fast and effective way [17], such as money or holding. It is a computer code used to direct connect between two nodes through the decentralize blockchain without need to know each other or trust in each other because the contract will be canceled when one of the requirements does not complete. This agreement code exists on each node to do predefined and specific task like exchange shares or in payment completion or in content rights management. Because it is an application of blockchain, so it has the blockchain properties.

The Ethereum is an open source code and a public network platform to implement the smart contract [22]. It run the contract through an Ethereum Virtual Machine (EVM). It was programmed by Vitalik Buterin using a special programming language of Ethereum [21]. Ether is a digital cryptocurrency, like the coin in bitcoin, used in buying and selling nodes and services in Ethereum. It can be used in many fields e.g. healthcare[23-25], philanthropy or decentralized finance.

C. Hyperledger

Hyperledger project is publicly available platform of blockchain-related decentralized ledgers under the Linux Foundation begin in December 2015. It designed to support transactions of global businesses, to achieve high efficiency and confidentiality. Its goal is to provide number of protocols to building a blockchain [14]. It has five sub-projects: fabric, sawtooth, indy, burrow, and iroha. Each of sub-projects use the Hyperledger open source to deal with special case.

V. Structure

Blockchain is a peer-to-peer network, which each computer in this network called node. The nodes can send and receive data between them. A single node can upload the data and then resend it to the connected nodes and these nodes resend the data to the other connected nodes too and so on to distribute the data [7]. Every block comprising: main data and hashing of a previous block, timestamp, hashing of transaction information and nonce in a header of the block as shown in Fig. 1.

A hash is a function compress random-length string of number and letters in the input to become fixed-length string in the output. The reason of why we use hash function in blockchain, it is so difficult process to find the value of the input from the output and change one bit in the input leads to completely change in output, so it is secure and no probability of modification or alteration and that what we need [26]. A hash of the previous block is to connect the blocks to each other and to assure that block did not change. The timestamp is a time of creating the block. The nonce is a random string of numbers used only once in the hashing process of the block. Merkl tree is a hash tree, where is hashing the hashed blocks. It is to quick movements between blocks and quick verification of the chain of blocks [14].

Consensus is a set of rules specify if all nodes in the blockchain agree to add a new block to a chain or not. Each node can transfer and update data under this agreement. Consensus is applied by using some protocols such as proof of work protocol and proof of stack protocol. These two protocols have the same goal, but the difference between them is in the approach of each one.

A. Proof of Work

It is a consensus protocol, which the miners try hard to solve difficult mathematical puzzle to mining some blocks to the blockchain. First miner who finds the answer to this puzzle takes a block reward. This process needs to high electronic power and high computational power so the miner who has a higher computational power has a higher probability to mining the block [27].

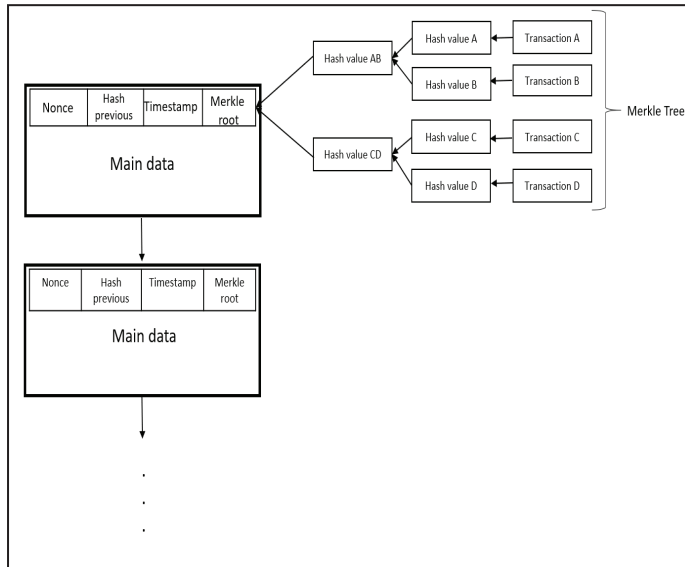


Fig. 1: Adapted from Arshdeep Bahga, Vijay K. Madiseti [4], Iuon-Chang Lin and Tzu-Chun Liao[14].

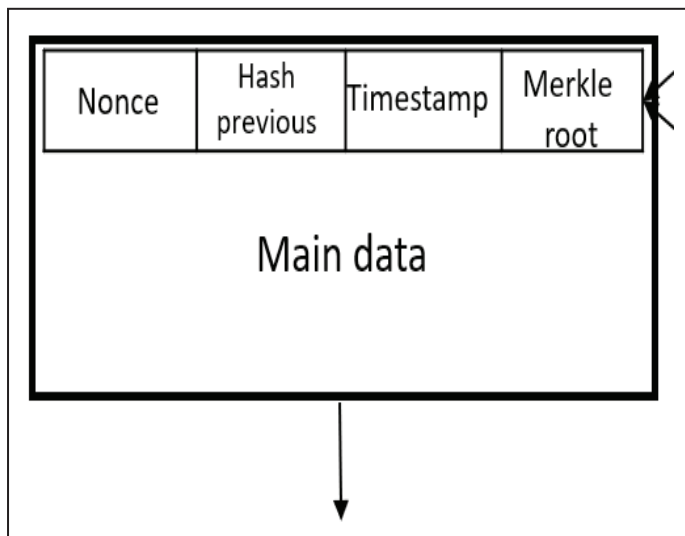


Fig. 1(a): Structure of a Block

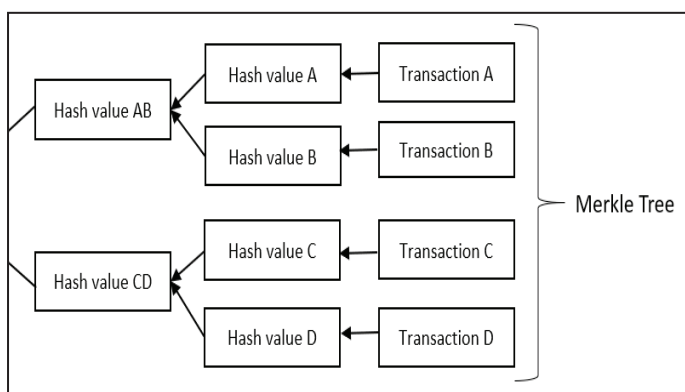


Fig. 1(b): Merkle Tree

B. Proof of Stack

The resources are giving the miner an ability to mine a new block based on random and various criteria such as holding or wealth. For example, if a miner in bitcoin system has 4% of the bitcoin, then he can mine 4% of the all blocks [14, 28]. The miner takes the block reward based on some predefined rules. This protocol comes after proof of work protocol to solve its drawback.

The blockchain works as the following: at the beginning the node receives a new transaction and broadcasting it into the blockchain network. Then the blocks in a network, check if the broadcasting block suitable to join in the network or not by using proof-of-work protocol. After that the block will be a part in the blockchain when the result of consensus algorithm is true [14].

VI. Blockchain Challenges

Blockchain is new concept designed to solve many problems in many fields. While it has strong points, it also has weak points that need to protect.

A. 51% Attack

It is also called majority attack. The power of mining a block relies on the efforts of the miners, that from the meaning of the proof of work protocol, this is a motive to miners to working together in a mining pool to mining as much as possible of blocks. If one block has control of 51% or more than of the blockchain blocks, then this block has the control of all blockchain [29-30]. The one who control more than 50% of all blockchain can access to the value of nonce faster than the others. And then this one can decide which the block can join to the blockchain or it cannot.

The 51% attack can lead to tampering with the transaction information, prevent the verification process of the blocks or pause mining process. The improvement in the block reward and the mining techniques reduce the probability of the 51% attack [14] [31].

B. Fork Issues

Fork issues occur when a blockchain software version for some nodes differs from a blockchain software version for other nodes. When a blockchain software version update, then the consensus protocols also update and consequently the agreement standards change for blocks. So, the blocks of blockchain separate into two kind: old blocks and new blocks. Some cases of how the old blocks handle with the new blocks: the new blocks receive a transaction from the old blocks and agree the transaction of it, the new blocks receive a transaction from the old blocks and does not agree the transaction of it, the old blocks receive a transaction from the new blocks and agree the transaction of it or the old blocks receive a transaction from the new blocks and does not agree the transaction of it. Based in these situations, there are two types of fork problem: hard fork and soft fork. The new blocks have a different computing power from old blocks [14].

1. Hard Fork

Hard fork happens when the blockchain version update with its consensus protocols and the new version did not suitable with the old version, the old blocks cannot agree mining with the recent blocks. The new blocks have a stronger computing power than old blocks and that lead to dividing the only one chain into two chains, one of them will keep on the old block chain unless the old blocks upgrade the agreement. Fig. 2 and 3 display the concept of hard fork problem [14].

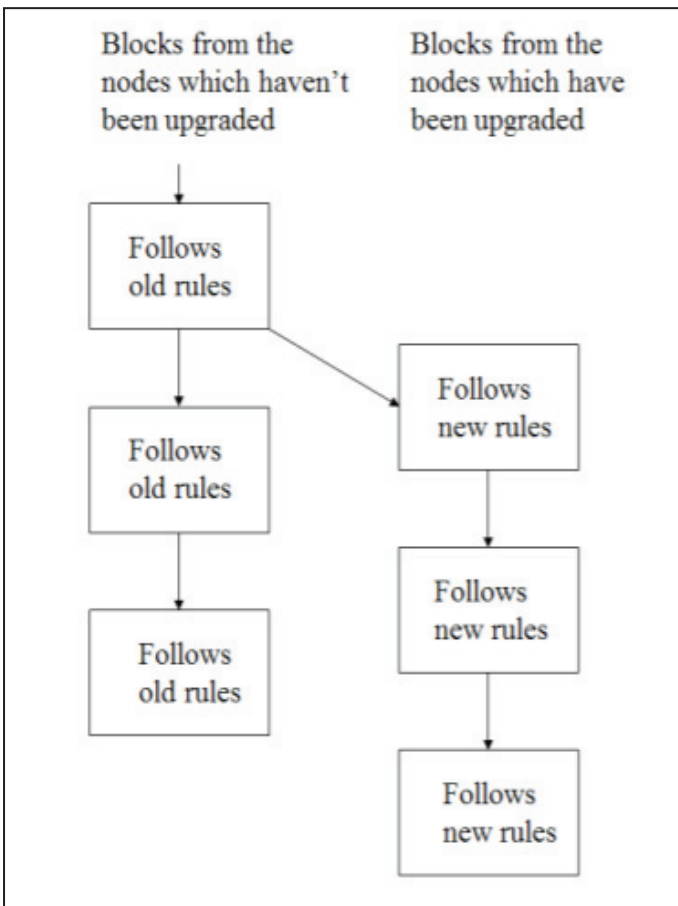


Fig. 2: Hard Fork, Adapted from Iuon-Chang Lin and Tzu-Chun Liao [14].

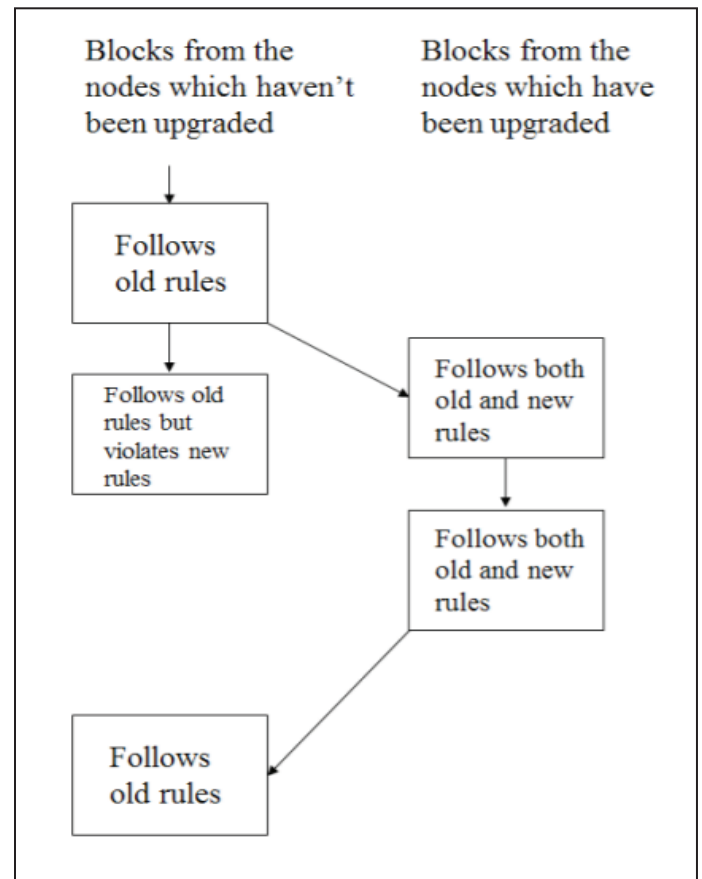


Fig. 4: Soft Fork, Adapted from Iuon-Chang Lin and Tzu-Chun Liao [14].

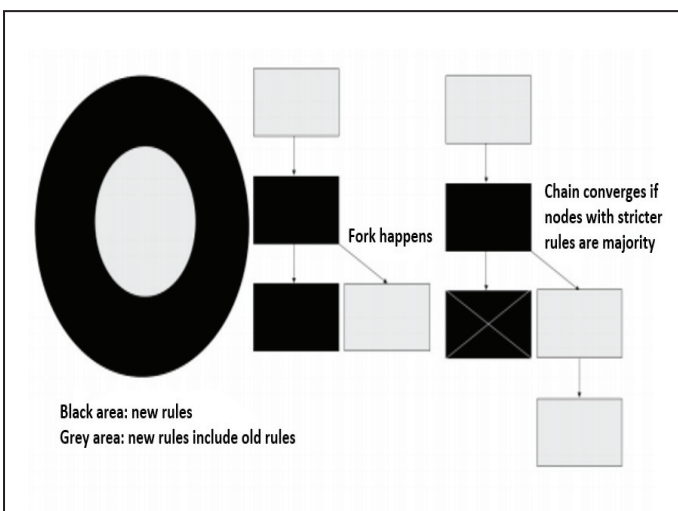


Fig. 3: Hard Fork, Adapted from Iuon-Chang Lin and Tzu-Chun Liao [14].

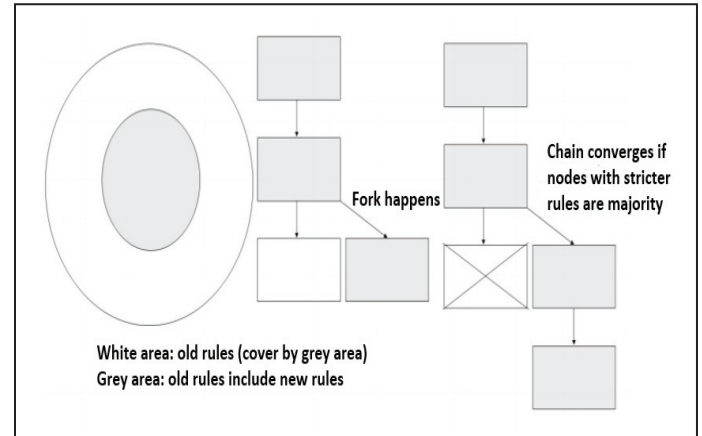


Fig. 5: Soft Fork, Adapted from Iuon-Chang Lin and Tzu-Chun Liao [14].

2. Soft Fork

Soft fork occurs when the blockchain version update with its consensus protocols and the new version did not suitable with the old version, the old blocks cannot agree mining with the recent blocks. The new blocks have a stronger computing power than old blocks, but this difference in a computing power did not effect in the performance of the work. The old and new blocks adapt with the new situation and develops gradually. Fig. 4 and 5 explain the soft fork problem [14].

C. Sybil Attack

The attacker can have the control of most blocks in the blockchain network by trying to fill this network with valid blocks. After that he can use his privileges to sabotage the system [9].

D. Blockchain Scale

The blockchain size is increasing more and more over a time and that require more of store and computing power. The increase in the size of data with the same system capability may lead to problems [32-34]. There is a payment technology that's designed to reduce the need of high computing power and to high storage capability by dealing only with the header of single block instead of recovering all blockchain data, it is a Simplified Payment Verification (SPV) [14].

E. Blockchain time Verification

The time required to confirm blockchain transaction is much better the time that required to confirm the same transaction in the traditional systems, but still need to reduce it [14].

F. Other Challenges

The blockchain policies may be incompatible with the government's policies, and this requires government intervention to amend its policies commensurate with the blockchain policies.

Blockchain as a new technology need to spend a lot of time and money to change the old systems to new systems that suitable to use with blockchain.

VII. Blockchain Types

Blockchain has three types: public blockchain, private blockchain and hybrid blockchain.

A. Public

It is available to everyone to access to the transaction, confirm it and be a part in consensus process. The most popular examples of this type are Ethereum and bitcoin [14].

B. Private

Based on the use, sometimes we need to use a private blockchain. It limits the ability of blocks that can access to the transaction and confirm it [14].

C. Hybrid

It is a mixed of the above two types. It is a blockchain which complains the features of public blockchain and private blockchain. It is available for all sometimes and limited to some blocks at the other times [14].

VIII. Proposal about Blockchain and Healthcare in Saudi Arabia

The use of blockchain in healthcare domains is the most discussed topic of the blockchain uses. The main characteristic of blockchain such autonomy, immutable and anonymity, that encouraged to use blockchain in healthcare domains. We can build a secure and an unchangeable databases of healthcare information. Based on decentralized and peer-to-peer properties of blockchain network, we can share healthcare information in the same time in all node of the network.

We suggest implementing "MedRec" prototype in Saudi allied health professionals [12]. MedRec applied blockchain technology to Electronic Health Records (HERs) to solve four problems. The first problem that MedRec addressed is a data fragmented, which means the patient's information is saved in different health organizations' databases based on the traditional ways, which is the separated health organizations does not exchange the information between them[23]. This fragmented of data making the access to the previous data difficult and late, this delay on access to health data is a second problem addressed by MedRec.

The lack of exchanging and management the medical data between health organizations is coming from the data fragmented concept and lead to challenges in access and share of data between the patient and the service provider [34-35]. This was a third challenge addressed by MedRec. The last problem MedRec concern with it is patient agency, which the patient is not a part in the therapeutic

process and does not have an enough access to his medical information.

The content of block in MedRec related to two types of data: the viewership privileges and the ownership data. MedRec uses smart contract in private and peer-to-peer blockchain network to control the transactions, which runs on an Ethereum. To satisfy the integrity in our blockchain, we use a hash function cryptography on the medical record. Any update in a state of a medical record in specific party, this party receives a notification about this update before it occurs, and this party can accept or reject the update, this makes the parties knowing and sharing in the record changing process. The update we mentioned in the last sentence may be an adding a new data from the provider or may be a record sharing by the patient with the providers.

The MedRec system achieves a confidentiality of the identity by using asymmetric key cryptography[36] and domain name system (DNS), an example of a DNS is a using an identity form that accepted around the world and pre-existing such as a name or a specific kind of numbers. The MedRec is an easy to use, easy to access and easy to learn system. It allows for the patient and for the provider to know all evolution of the health record.

IX. Conclusion

The blockchain needs to time to proof its effect in person's life. It can be a part in several fields and enhance it. It is designed to more secure and to save a time and a money by using many techniques like cryptography. It has a complicated concept and structure, but it is useful, we still should be careful when we use it.

In this paper we introduce a survey about the blockchain and a proposal to use this technology in healthcare in Saudi healthcare organization. We present some works related with the blockchain, explain the blockchain structure, present a blockchain applications, display a number of challenges that faced the blockchain.

References

- [1] T. Nugent, D. Upton, M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, Vol. 5, 2016.
- [2] O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, Vol. 7, pp. 4184-4194, 2018.
- [3] M. A. AlZain, J. F. Al-Amri, "Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform," *International Journal of Applied Engineering Research*, Vol. 13, pp. 6380-6387, 2018.
- [4] M. A. AlZain, "Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition," *International Journal of Advanced Computer Science and Applications*, Vol. 9, pp. 196-200, 2018.
- [5] C. Cachin, "Architecture of the hyperledger blockchain fabric," In *Workshop on distributed cryptocurrencies and consensus ledgers*, pp. 4, 2016.
- [6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [7] A. Bahga, V. K. Madiseti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, Vol. 9, pp. 533, 2016.

- [8] A. Lovejoy, "The great chain of being: A study of the history of an idea: Routledge", 2017.
- [9] N. Prusty, *Building Blockchain Projects*: Packt Publishing Ltd, 2017.
- [10] T. Biscontini, "Blockchain (technology)," Salem Press, 2019.
- [11] T. Felin, K. Lakhani, "What problems will you solve with blockchain?," MIT Sloan Management Review, Vol. 60, pp. 32-38, 2018.
- [12] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data," In Proceedings of IEEE open & big data conference, pp. 13, 2016.
- [13] K. D. Mandl, D. Markwell, R. MacDonald, P. Szolovits, I. S. Kohane, "Public standards and patients' control: How to keep electronic medical records accessible but private," *Bmj*, Vol. 322, pp. 283-287, 2001.
- [14] I.-C. Lin, T.-C. Liao, "A Survey of Blockchain Security Issues and Challenges," *IJ Network Security*, Vol. 19, pp. 653-659, 2017.
- [15] D. E. Dillenberger, G. Su, "Parallel execution of blockchain transactions," Google Patents, 2019.
- [16] S. Haber, W. S. Stornetta, "How to time-stamp a digital document," In Conference on the Theory and Application of Cryptography, pp. 437-455, 1990.
- [17] D. Bayer, S. Haber, W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II*: Springer, 1993, pp. 329-334.
- [18] P. McCorry, S. F. Shahandashti, F. Hao, "A smart contract for boardroom voting with maximum voter privacy," In International Conference on Financial Cryptography and Data Security, pp. 357-375, 2017.
- [19] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," In International Conference on Financial Cryptography and Data Security, pp. 34-51, 2013.
- [20] L. P. Nian, D. L. K. Chuen, "Introduction to bitcoin," In *Handbook of Digital Currency*: Elsevier, pp. 5-30, 2015.
- [21] R. Casado-Vara, A. González-Briones, J. Prieto, J. M. Corchado, "Smart contract for monitoring and control of logistics activities: Pharmaceutical utilities case study," In *The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications*, pp. 509-517, 2018.
- [22] C. Dannen, *Introducing Ethereum and Solidity*: Springer, 2017.
- [23] H. Samra, A. Li, B. Soh, M. Al Zain, "Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems," *Health Information Management Journal*, p. 1833358319847120, 2019.
- [24] H. E. Samra, A. S. Li, B. Soh, M. A. AlZain, "A Conceptual Model for Cloud-Based E-Training in Nursing Education," In *Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth*: IGI Global, 2019, pp. 295-310.
- [25] H. E. Samra, B. Soh, M. A. Alzain, "A Conceptual Model for an Intelligent Simulation-Based Learning Management System Using a Data Mining Agent in Clinical Skills Education," In *2016 4th International Conference on Enterprise Systems (ES)*, 2016, pp. 81-88.
- [26] S. S. Gupta, *Blockchain*: John Wiley & Sons, Inc, 2017.
- [27] A. Kiayias, E. Koutsoupias, M. Kyropoulou, Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, 2016, pp. 365-382.
- [28] S. King, S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, Vol. 19, 2012.
- [29] N. T. Courtois, L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," arXiv preprint arXiv:1402.1718, 2014.
- [30] I. Eyal, E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, Vol. 61, pp. 95-102, 2018.
- [31] A. Gervais, H. Ritzdorf, G. O. Karame, S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 692-705, 2015.
- [32] G. Karame, "On the security and scalability of bitcoin's blockchain," In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 1861-1862, 2016.
- [33] M. A. AlZain, E. Pardede, B. Soh, J. A. Thom, "Cloud computing security: from single to multi-clouds," In *2012 45th Hawaii International Conference on System Sciences*, pp. 5490-5499, 2012.
- [34] M. A. AlZain, A. S. Li, B. Soh, M. Masud, "Byzantine Fault-Tolerant Architecture in Cloud Data Management," *International Journal of Knowledge Society Research (IJKSR)*, Vol. 7, pp. 86-98, 2016.
- [35] M. A. AlZain, B. Soh, E. Pardede, "Mcdcb: using multi-clouds to ensure security in cloud computing," In *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, pp. 784-791, 2011.
- [36] G. K. Sodhi, G. S. Gaba, L. Kansal, E. Babulak, M. AlZain, S. K. Arora, M. Masud, "Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code," *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 12, pp. 1297-1304, 2018.

Asma Abbad, received the Bachelor's degree in computer science from the Computer Science Department, Taif University, Saudi Arabia. She is currently doing a Master's degree in Cybersecurity at Taif University. Her areas of scientific interests include computer science, information systems, information security, and machine learning.



Mohammed A. AlZain has achieved his PhD degree from the Department of Computer Science and Engineering at La Trobe University, Melbourne, Australia in Sept 2014. Dr. AlZain's PhD research is in Cloud Computing Security. His thesis title was "Data security, Data management, Performance evaluation for a multi-cloud computing model". He has received his Bachelor degree in Computer Science from King Abdulaziz University, Saudi Arabia

in 2004, and then achieved his Master's degree in Information Technology from La Trobe University in 2010. Currently, Dr. AlZain is Associate professor in the College of Computers and Information Technology at Taif University in Saudi Arabia. His area of interest includes Cloud Computing Security, Information Security, and Distributed Systems.



BEN SOH (S'89–M'92–SM'03) received the Ph.D. degree in computer science and engineering from La Trobe University, Melbourne, Australia, in 1995. He is currently an Associate Professor with the Department of Computer Science and Computer Engineering, La Trobe University. He had numerous successful Ph.D. graduates. He has authored more than 150 peer-reviewed research papers.

He has made significant contributions in various research areas, including fault-tolerant and secure computing, and Web service



Mehedi Masud is a Full Professor in the Department of Computer Science at the Taif University, Taif, KSA. Dr. Mehedi Masud received his Ph.D. in Computer Science from the University of Ottawa, Canada. His research interests include cloud computing, distributed algorithms, data security, data interoperability, formal methods, cloud and multimedia for healthcare. He has authored and coauthored around 50 publications

including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as a technical program committee member in different international conferences. He is a recipient of a number of awards including, the Research in Excellence Award from Taif University. He is on the Associate Editorial Board of IEEE Access, International Journal of Knowledge Society Research (IJKSR), and editorial board member of Journal of Software. He also served as a guest editor of ComSIS Journal and Journal of Universal Computer Science (JUCS). Dr. Mehedi is a Senior Member of IEEE, a member of ACM.



Jihad Faisal Al Amri is a assistant professor in Computer Informatics. He graduated from the Centre for Computing and Social Responsibility at De Montfort University June - 2013. The thesis title is "An Analysis of the Influence of Cultural Backgrounds of Individuals upon their Perspective towards Privacy within Internet Activities". Currently, he is a lecturer at the Faculty of Computers and

Information Technology at Taif University, Saudi Arabia.