NOTE : ADD THE SNAPSHOT OF APPROVAL MAIL OF YOUR GUIDE FOR THE REPORT HERE. CONTENT STARTS FROM NEXT PAGE. REMOVE THE TEXT IN THE RED FONT COLOR IN THE TABLE OF CONTENTS, IT IS AN INSTRUCTION TO PREPARE THE DOCUMENT.

B.M.S College of Engineering

P.O. Box No.: 1908, Bull Temple Road,

Bangalore-560 019

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

Technical Seminar

19IS4SRSMI

AY 2019-20

Implementation of Blockchain to Secure Medical Records of Patients

Submitted to – M.K Nalini

(Assistant professor)

Submitted by -

1BM18IS024	B.SHRIKARA VARNA
1BM18IS034	GAGANDEEP. M
1BM18IS039	GOWRISHANKAR. G

CONTENTS

ABSTRACT

The study gives an insight of the method to implement a peer to peer blockchain mechanism. A blockchain is a chain of blocks where each block contains data of value without any central supervision. Aim of the study is to develop a mechanism without any central supervision to store medical data. therefore blockchain is used as the base for this study. The study introduces methods wherein the admin can enter the data into the blocks,the peer to peer network ensures that the user will have access to the blockchain and can view the required information when verified through a consensus algorithm .This makes the mechanism tamper proof. The introduction of blockchain will be able to solve the problems related to notorious scandals, privacy violations, data control, and content relevance. Blockchain technology will allow banks to reduce excessive bureaucracy, conduct faster transactions at lower costs, and improve its secrecy. Hacking attempts on IOT devices will be minimized upon using blockchain technology.

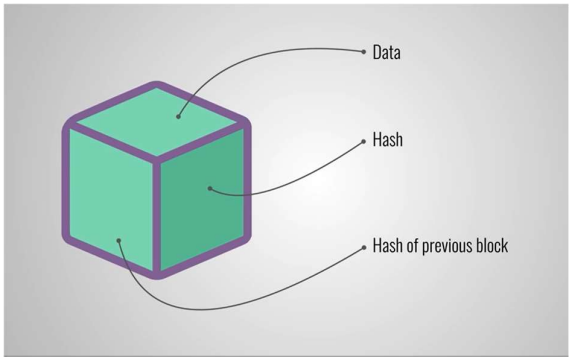
A fundamental open problem in the area of blockchain protocols is whether the Bitcoin protocol is the only solution for building a secure transaction ledger. Given the pseudonymous nature of Blockchain transactions, coupled with ease of moving valuables, the risk of misuse of the system is high. therefore the cryptocurrency-based technology is either in the downward slope of inflated expectations or in trough of disillusionment.

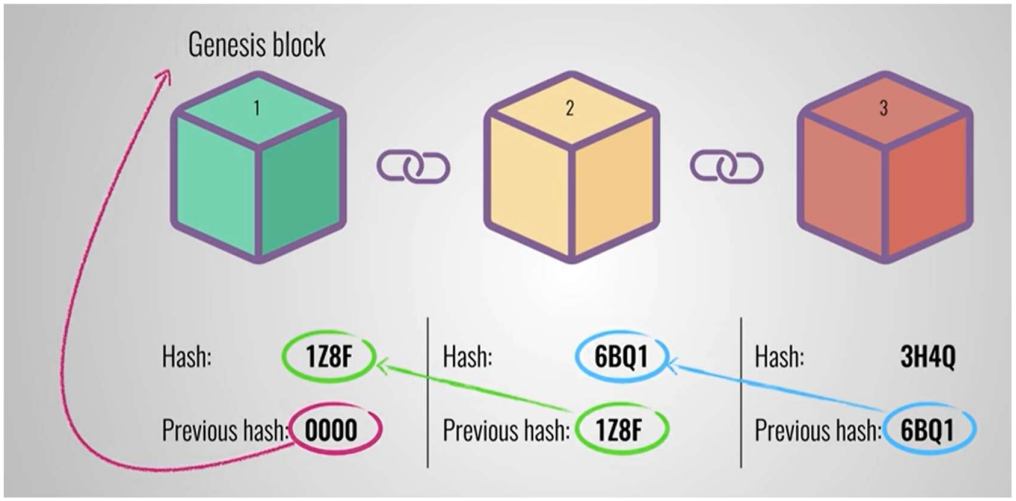
CHAPTER 1

1.1 Introduction to Domain

A blockchain is a chain of blocks where each block contains data of value without any central supervision.

- Hash: Every block in the chain contains a unique value called hash. If any data in a block is changed, then correspondingly the block's hash value changes.
- Chain formation: By storing the hash of the previous block in the current block.
- Decentralized: There is no central authority supervising anything.
- Consensus Mechanism: A P2P link exists between all users for a certain blockchain. Now, when one of them tries to add a new block, an agreement/consensus by every other node is required in order to add the new block to the chain.





1.2 Problem Definition

Use blockchain technology to implement a secure portal for transfer and viewing of medical reports between doctor and patients.

1.3 Objective

- Implementing a secure blockchain.
- Create a network of patients and doctors who have access to the blockchain.
- Allow transfer of data and reports between patients and doctors.
- Thus, create a discretionary and digitized healthcare system

Chapter 2

2.1 Literature Survey

1. BlocHIE: a blockchain-based platform for Healthcare Information Exchange

- Mingyu Derek Ma, Shan Jiang, Yanni Yang

- First, we analyze the different requirements for sharing healthcare data from different sources. Based on the analysis, we employ two loosely-coupled Blockchains to handle different kinds of healthcare data.
- Second, we combine off-chain storage and on-chain verification to satisfy the requirements of both privacy and authenticity.
- Third, we propose two fairness-based packing algorithms to improve the system throughput and the fairness among users jointly.

To demonstrate the practicability and effectiveness of BlocHIE, we implement BlocHIE in a minimal-viable-product way and evaluate the proposed packing algorithms extensively.

2. Blockchain in healthcare and health sciences - A scoping review

- Anton Hasselgrena, Katina Kralevskab, Danilo Gligoroskib, Sindre A. Pedersenc, Arild Faxvaaga

A key attribute of blockchain is decentralization.It is practically impossible to delete entries after being accepted onto the blockchain due to the distributed ledger, stored across multiple nodes. Blockchains make audit and traceability possible by linking a new block to the previous by including the hash of the latter, and in this way forming a chain of blocks.

The transactions in the blocks are formed in a Merkle tree where each leaf value (transaction) can be verified to the known root. This enables the tree structure to verify the integrity of the data by only storing the root of the tree on the blockchain.

A transaction is validated by a consensus algorithm. Proof of work is a consensus protocol where miners try to find the hash of the proposed block with a value lower than a predetermined one,using brute force. Proof of Stake (PoS), the selection of an approving node is determined by the stake each node has in the blockchain.the stake is represented by the balance one possesses of a given currency.

In Practical Byzantine Fault Tolerance (PBFT), all nodes need to beknown to the network, which limits the usage of this consensus protocol in a public blockchain.

The purpose of this study was to systematically review, assess and synthesize peer-reviewed publications utilizing/proposing to utilize blockchain to improve processes and services in healthcare health sciences. In the global healthcare industrial sector, where the blockchain technology market is expected to cross $500 million by 2022.

3. On Trees, Chains and Fast Transactions in the Blockchain

- Aggelos Kiayias and Giorgos Panagiota kos School of Informatics, University of Edinburgh

A fundamental open problem in the area of blockchain protocols is whether the Bitcoin protocol is the only solution for building a secure transaction ledger.

A recently proposed and widely considered alternative is the GHOST protocol which is touted as offering superior performance compared to Bitcoin (potentially offering block production speed up by a factor of more than 40) without a security loss.

We introduce a new formal framework for the analysis of blockchain protocols that relies on trees (rather than chains). We showcase the power of the framework by providing a unified description of the GHOST and Bitcoin protocols, the former of which we extract and formally describe. We then prove that GHOST implements a “robust transaction ledger”.

3. Blockchain Technology: Beyond Bitcoin

- Michael Crosby, Nachiappan , Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman

Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. As far as the technology is concerned, the cryptocurrency-based technology is either in the downward slope of inflated expectations or disillusionment.

We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. Scaling of the current nascent services based on Blockchain presents a challenge since, while executing a BlockChain transaction for the first time the entire set of existing blockchains

must be downloaded and validated before the first transaction.

This may take hours or longer as the number of blocks increases exponentially. Given the pseudonymous nature of Blockchain transactions, coupled with ease of moving valuables, the risk of misuse of the system is high.

5. Blockchain Technology in Healthcare:A Systematic Review

-Cornelius C. Agbo *, Qusay H. Mahmoud and J. Mikael Eklund

Participants in a blockchain network are represented as nodes and each node uses public key infrastructure (PKI) to create and propose transactions. Each participant possesses a pair of public and private keys. The public key serves as the public address of the user while the a private key is used to authenticate the user.

When a transaction is created, the public key of the user, the transaction message and public key of the receiver is included. All of these are bundled together and cryptographically signed using the
user's private key and subsequently broadcast to the other nodes in the blockchain network.

When this is done, the user is said to have proposed a transaction. Special nodes in the blockchain network run the consensus algorithm to validate the transaction, these are called miners. the miner proceeds to check if the transaction is valid. Validated transactions are included into a block. After a period (or block) of time, the new block of validated transactions is linked (or chained) to the previous blocks, creating a chain of blocks, known as blockchain.

Chapter 3

3.1 Methodology/Algorithm/Techniques

The system architecture of BlocHIE is presented in *fig.3*. BlocHIE is envisioned for storing and sharing healthcare data from medical institutions and individuals. There are mainly three components in BlocHIE. The first component is the Blockchain network. The Blockchain network is responsible for storing and sharing the collected healthcare data. Anyone who is willing to contribute to this platform can join the network. The medical institutions, e.g., hospitals and clinics, act as the second component. When there are new patients in a hospital, their diagnostic records will be submitted to the Blockchain network and shared with other hospitals and clinics. The third component consists of all the individuals who are willing to store and share their daily healthcare data. In a smart home, numerous healthcare data are generated by the IoT devices, e.g., smart watch, smart thermometer, and smart sphygmomanometer. These devices can automatically submit the generated data to the Blockchain network through the procedure described in *fig.2*.

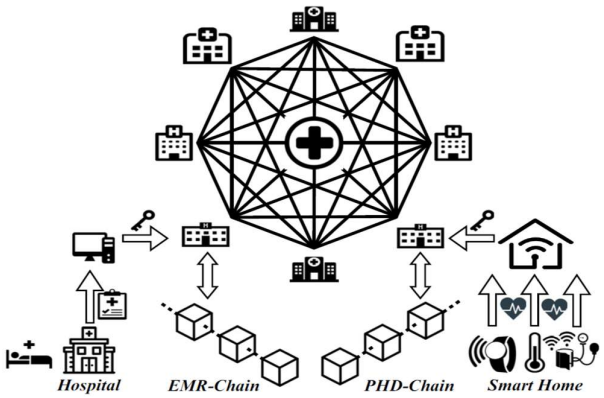


Fig. 3. BlocHIE system architecture

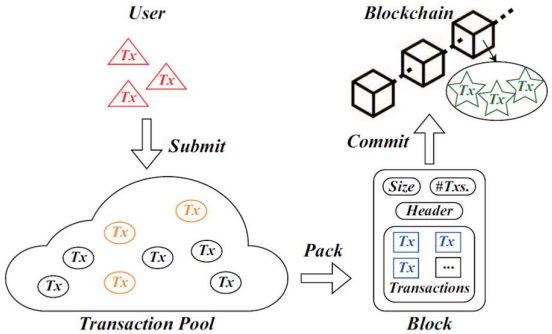


Fig. 2. The procedure for commiting transactions

In the following parts, they abbreviate the data generated by medical institutions and individuals as critical data (EMR) and personal healthcare data (PHD) respectively.

TABLE I
REQUIREMENTS TO PUBLISH AND SHARE HEALTHCARE DATA

Requirement	EMR	PHD
privacy	high	moderate
authenticability	high	no
throughput	moderate	high
latency	moderate	moderate
fairness	moderate	moderate

The requirements to publish and share EMRs and PHD are summarized in *Tab. I*. As we can see from the summarization, their requirements are significantly different. Hence, we propose to store and share EMR and PHD with two loosely coupled Blockchains, namely EMR-Chain and PHD-Chain as shown in *fig.5*.

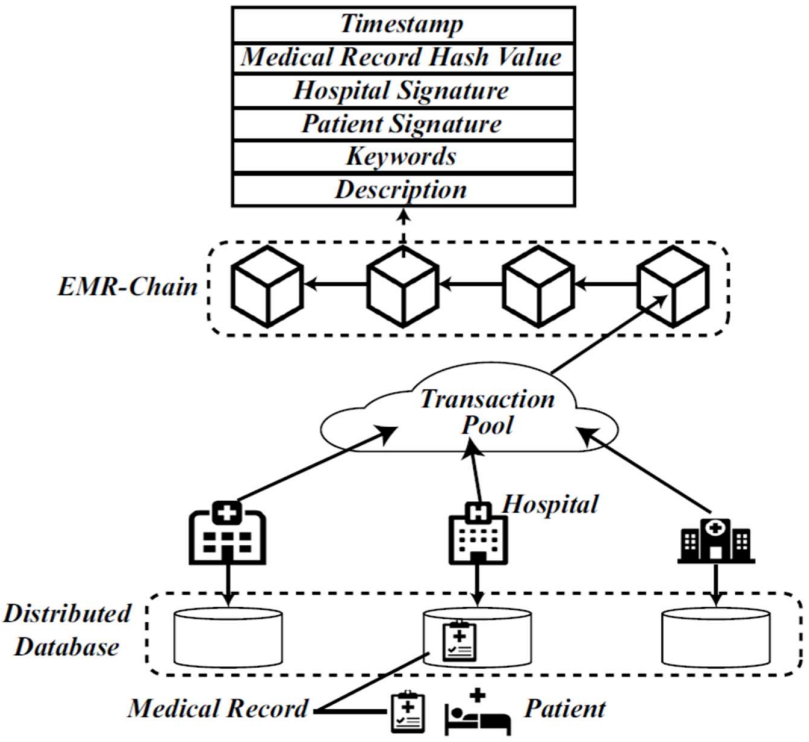


Fig. 5. The mechanism and structure of EMR-Chain

Chapter 4

4.1 Tools identified for domain/ types of inputs

REQUIREMENTS:

Cyphers for hashing
Ethereum
Cryptography
Eclipse for Java/ Codeblocks for C++

INPUTS:

Data of medical records of patients

4.2 Possible Outcome

Our system of securing data of patients into two chains, for further discrimination of electronic health record and personal data, is the next step in digitalization of health care system of a country.

We expect the system to handle tons of data and secure them properly with transparency and the highest level of security.

We integrate the techniques of off-chain storage and on-chain verification to take good care of privacy and authentic ability. Moreover, we use two transaction packing algorithms to enhance the system throughput and the fairness among users.

SYSTEM IMPLEMENTATION AND EVALUATION

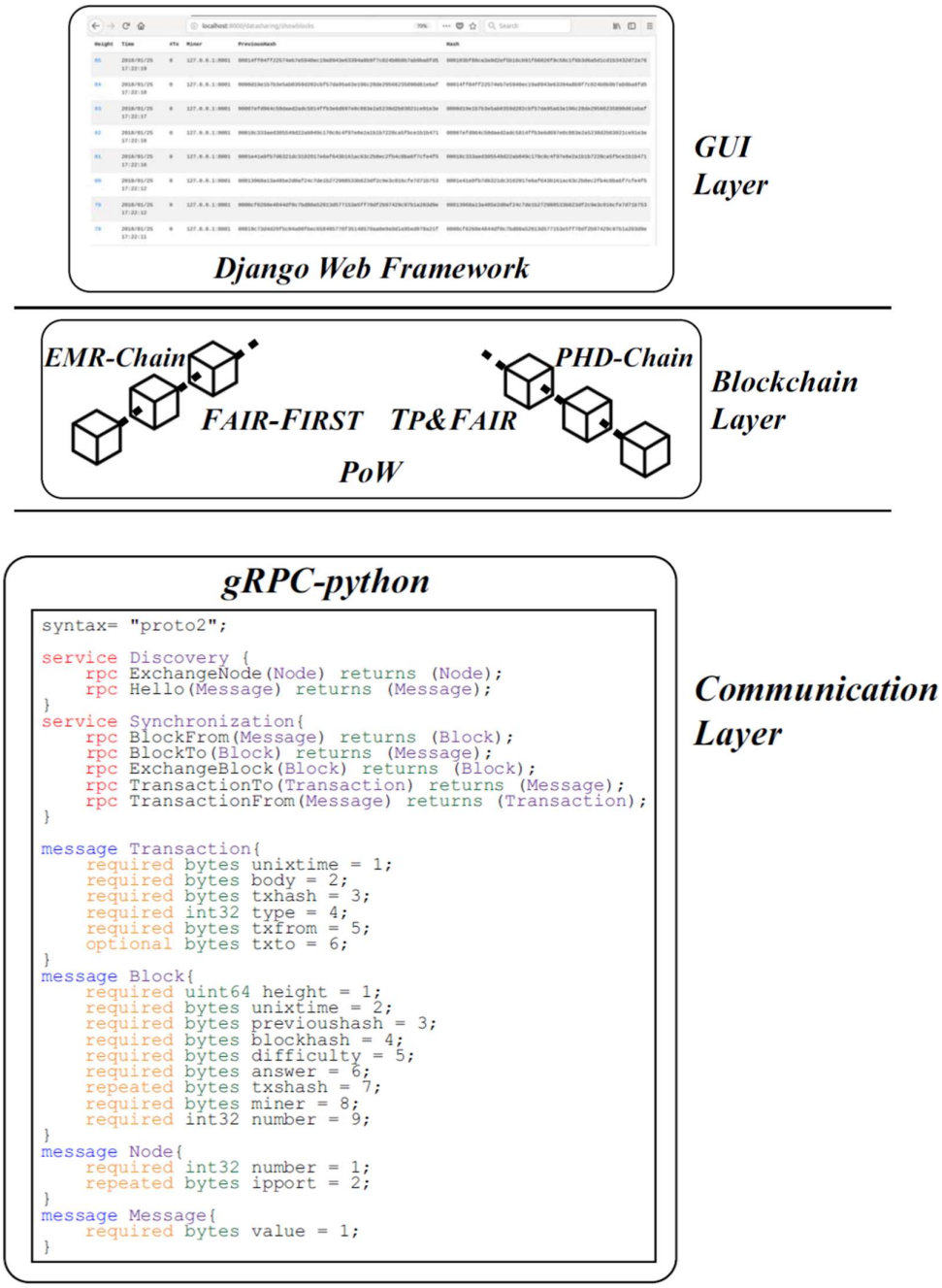


Fig. 7. Techniques for system implementation level by level

References

1. Anton Hasselgrena, Katina Kralevskab, Danilo Gligoroskib, Sindre A. Pedersenc, Arild Faxvaag – "Blockchain in healthcare and health sciences—A scoping review" NTNU-Norwegian University of Science and Technology, Trondheim, Norway Received 13 May 2019.

2. Aggelos Kiayias and Giorgos Panagiotakos – "On Trees, Chains and Fast Transactions in the Blockchain". School of Informatics, University of Edinburgh, 2015.

3. Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman – " BlockChain Technology: Beyond Bitcoin". Applied Innovation Review, Issue No. 2 June 2016.

4. Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei He – "BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange" - The Hong Kong Polytechnic University, Hong Kong, China. April 2018

5. Cornelius C. Agbo, Qusay H. Mahmoud and J. Mikael Eklund – "Blockchain Technology in Healthcare:A Systematic Review" Department of Electrical, Computer and Software Engineering, University of Ontario. Accepted: 28 March 2019; Published: 4 April 2019

6. derek.ma@connect.polyu.hk , jeffrey.he@huawei.com

7. https://blockgeeks.com/guides/blockchain-developer

8. https://www.pluralsight.com/courses/blockchain-fundamentals?clickid=2QuQyXzoRxyJUHZ0O7XQxx3QUknXhm2ddQ0kVs0&irgwc=1&mpid=1193463&utm_source=impactradius&utm_medium=digital_affiliate&utm_campaign=1193463&aid=7010a000001xAKZAA2

9. https://www.udemy.com/course/blockchain-theory-101/?LSNPUBID=JVFxdTr9V80&ranEAID=JVFxdTr9V80&ranMID=39197&ranSiteID=JVFxdTr9V80-2hLFP3pKrVnnOXy5Wgibaw

10. https://www.quora.com/How-do-I-get-training-to-develop-blockchain