Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017)
IEEE Xplore Compliant - Part Number:CFP17M19-ART, ISBN:978-1-5386-1959-9

HealthSense:

A Medical Use Case of Internet of Things and Blockchain

Tushar Dey
Information Technology Department
DJ Sanghvi College of Engineering
Mumbai,India
dey.tushar@yahoo.com

Shweta Sunderkrishnan
Computer Department
DJ Sanghvi College of Engineering
Mumbai,India
shwetaskrishnan@gmail.com

Shaurya Jaiswal
Information Technology Department
DJ Sanghvi College of Engineering
Mumbai,India
Jaiswal06@gmail.com

Prof. Neha Katre
Assistant Processor, Information Technology Department, D. J. Sanghvi College of Engineering,
Mumbai, India
neha.mendjoge@djsce.ac.in

***Abstract*- Blockchain and Internet of things are the most promising and upcoming technologies. Blockchain is a distributed, peer to peer database forming a chain between multiple blocks of data. The internet of things works on a similar paradigm where multiple devices are connected to the internet forming a network of networks. Combined together they offer solutions for various problems, especially in the field of healthcare where quick reporting of data or results is of utmost importance. Recent studies have proven that delays in providing healthcare are directly linked to patient confidence and chances of recovery. An unreliable storage of health records has only aggravated the problem. Our paper aims to provide a solution for these issues by proposing a Blockchain-Internet of things model where a bio-sensor measures and collects real time data with respect to a patient's medical status and stores it in the blockchain. In this way quick reporting and tamper proof storage of data occurs. By deploying a smart contract the final hospital bill can be calculated along with insurance coverage. This would negate the need of third party providers and create a transparent system. Our paper also proposes the use of Inter planetary file system to store discharged patients records thus reducing the load on the actual blockchain. Overall this will surely benefit patients and doctors alike by creating a safe and transparent environment along with quick response to a patient's need.**

Keywords— BlockchInternet of Things; InterPlanetary File System; MQTT; Representational State Transfer.

I. INTRODUCTION

In the very recent years of technological advancement, Blockchain and IoT have become a household terms. These two fields are in fledging state and scope and application in these fields is expected to be vast. In our paper, we review the proposal of combining these completely different fields with help of the third party application like BigChainDB or IPFS to serve a common purpose. It can be used in medical and transportation field.

Blockchain is a technology enabler which allows the exchange of digital assets or tokens directly between two parties without the need of a central authority for trust or mediation.

It essentially is a public, decentralized database which is used to store records or transactions between the nodes of a peer-to-peer network. It stores transaction records in units known as blocks which are stored in a chronological order as part of a public ledger. This ledger can be viewed by all the participating nodes of the network. The advantage of blockchain is that the database does not need to be maintained or verified by a central authority and the records of the blockchain are immutable making it impossible to be misused.

The paper is structured as follows. Section II introduces blockchain and its working along with

its advantages and applications. In Section III, IPFS and IoT have been described. MQTT and REST have been further described as protocols of IOT. Section IV throws light on the problem of current IoT model and to ameliorate those problems, the proposed solution using all the protocols mentioned in Section III are discussed. Further scope of development has been mentioned in Section V and paper ends with conclusion in Section VI.

II. BLOCKCHAIN

A. Working of Blockchain

Blockchain basically works as a distributed and open public ledger of transactions which can accessed by all participants of the network and the blockchain is maintained by the nodes of the peer-to-peer network themselves using mutual consensus. The ledger works in an append-only fashion.

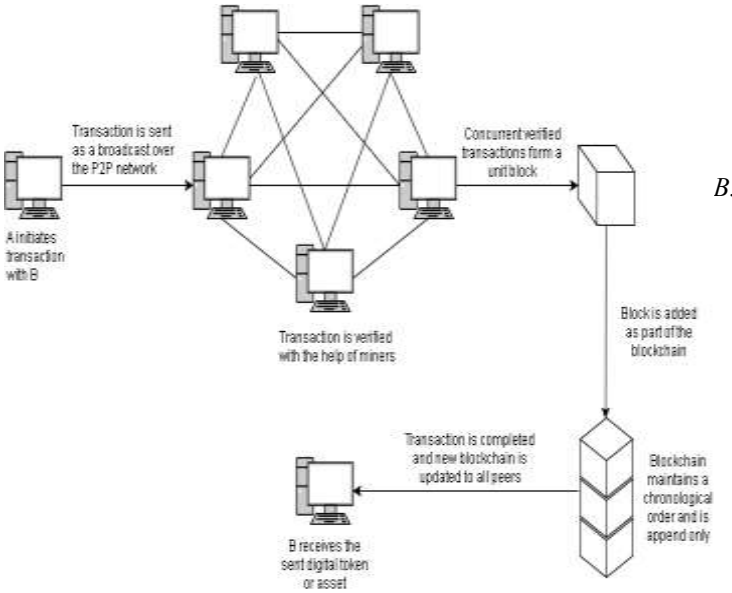


Figure 1

A transaction is recorded in the blockchain by the following steps [1]:

1. A transaction can be initiated by any node of the network to a receiver node of the same P2P network.
2. Using the private key of the sender node the transaction is encrypted before sending it to the network.
3. The transaction is sent as a broadcast to all peers of the network.
4. The nodes on the network then verify the transaction using the public key of the sender node.
5. Few nodes of the P2P network function as miners i.e. these nodes are responsible for the verification of the transaction.[13] A great deal of computing power is required for this verification; hence these miners are given incentive as a small percentage of the transaction.
6. Concurrent transactions which have been verified are compiled into a unit known as a block, which is then added to the blockchain. The new blockchain is then updated to all the other nodes of the network.
7. A block along with the transaction records contains the hash of the previous and the next block forming a structure similar to a list. It also contains a random identifier known as nonce along with a timestamp.
8. Once the a block is added to the blockchain it becomes immutable and no further changes can be made to that particular block or to the sequence of the chain.

B. Advantages of Blockchain

- Records are immutable hence cannot be altered with. The history of all transactions is also available.
- It is cheaper as no central authority is required to maintain data at high costs. Only cost associated are the transaction charges to the miners.
- Safety is improved as compared to potential data leaks from central authority. All data in the blockchain is encrypted and the identities remain anonymous as only the public address is required for a transaction.
- Modifying a block requires a great deal of computing power and would also need to alter all the subsequent blocks of the chain; hence it is immune to attacks or alterations.
- The transactions can occur anytime 24/7.

C. Applications of Blockchain

- Cryptocurrency – A virtual currency can be created using blockchain with would be an agreed mode of transfer of monetary services between the participating peers of the network. It allows peers to exchange money without the need of a central

authority like a bank for confirmation of payments.Concurrently, it makes the process of transferring money much faster in a matter of minutes rather than days. [2]

- Smart contracts – These are predefined & programmable contracts between two nodes in the network which enables performing particular actions depending on the conditions met according to the contract. [3]

III. WORKING OF OTHER PROTOCOLS

A. IPFS

InterPlanetary File System commonly known as IPFS is hypermedia distribution protocol which not only gives a permanent and decentralized method of storing and sharing file, but also make web faster, safer and more open at the same time. In this each nodes of IPFS together creates a distributed file system which connects devices with same system of files. IPFS can be considered as single bittorrent swarm which is exchanging git objects. [5]

At the HTTP layer, IPFS uses the method of content addressing in which the address is defined by the content of the file. All the files are securely hashed using cryptography. Each hash is unique and used to identity the file. IPFS is a peer-to-peer network which is run using the IPFS object. This object is a data structure with Data and Links as its fields. Data is a blob of binary data which is not structured and has size less than 256 KB, whereas Links is an array of Link Structure. This link structure has three data fields that is the name, hash that is generated and total size of linked IPFS objects. Generally, IPFS objects are identified by their Base58 encoded hash.

Following are the advantages of having IPFS

1. Node in IPFS only stores those contents, like common indexing information, that are important.

2. Since each file in network is been assigned its own unique hash, it can recognise the redundant file and delete them as useless data.

3. It can stores huge amount of data and then place the immutable links of IPFS into blockchain. This way the content is secure even without putting in the blockchain directly.

B. IOT

The Internet-of-Things is a global network of connected devices. They are connected to each other and to the internet. Each physical device originally operating on different protocols connects by means of interfacing with others or registering at a common address. At the basic level each sensor or physical device works by measuring and collecting data i.e. by sensing the changes in the environment. The protocols used for forming this internetwork of devices at the lowest level can be 6LowPAN, IPv4/IPv6 (Internet protocol), RPL (Routing protocol). They provide end-to-end datagram transmission across multiple IP networks. Various discovery protocols like HyperCat, m-DNS can also be used when devices wish to find each other or a gateway. For example HyperCat is an open, lightweight JSON-based hypermedia catalogue format for exposing collections of URIs. This gets broadcasted all over the network and helps in forming connections. All the devices together sense the changes in the environment and this is then passed onto the next higher level as data. The data layer works with protocols like MQTT, CoAP. There is a topic or address where the client also known as device, registers, and at the same topic a client on the other side registers too. The data published on one end is received at the other. To further connect to the platform, semantic protocols like JSON-LD, Web Thing Model can be used. They are linked Data standards for describing the Internet of Things. Thus in this way a multilayer frame work is formed. [6]

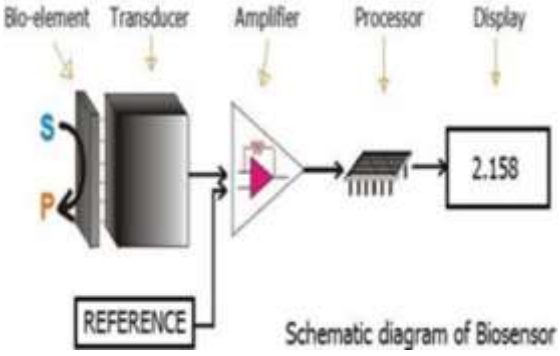


Figure 2[7]

Each bio-sensor measures the changes in the human body based on certain selected parameters. The preferred biological material, selected as the parameter to be measured is in contact with the transducer. To produce a bound analyte, the analyte binds to the biological material which produces the electrical response to be measured. This response is recorded and displayed.

C. MQTT

MQ Telemetry Transport is an open source protocol which is used for device with constrained and low power. It is Publish/Subscribe message

transport protocol that is lightweight and is used to connect the smart devices used in IoT. Facebook Messenger, Amazon Web Services and Microsoft Azure IOT use it.

IoT networks use MQTT protocol due to some specific reasons. The first reason is that it reduces the amount of packets being sent to internet, as the central broker in MQTT functions as server to do so. Also, with help of TLS\SSL internet security, data is encrypted either partially or completely to mitigate the use of TCP, which is not secured. The 3 QoS available in MQTT are At Most Once, At Least Once and Exactly Once, depending upon the repetitiveness of the message in that environment. There are 2 special features that are Last Will and retained message. Last Will lets us know about the availability of the particular client which avoids waiting for improbable situation and saves the power. Retained message ensures that even those messages from long back are received by subscribers. Finally, Clients are able to subscribe to all the topics based on particular pattern which makes it flexible in subscription pattern. [9] MQTT-S which uses UDP protocol instead of TCP is a possible alternative.

D. *REST*

REpresentational State Transfer (REST) is a recent architectural style introduced in 2000 as a light weight and simpler alternative to the XML based SOAP. It simply functions as a messenger between two APIs or web services to allow exchange of textual data available in the internet. [10] Data could be in the format of CSV, XML, JSON, HTML files. In comparison to SOAP it is much more flexible while being easier to use as well. REST works as a stateless protocol which uses the standard functions available in HTTP protocol.

IV. OUR PROPOSED MODEL AND IT'S NEED

A. *Problem with current model of IOT*

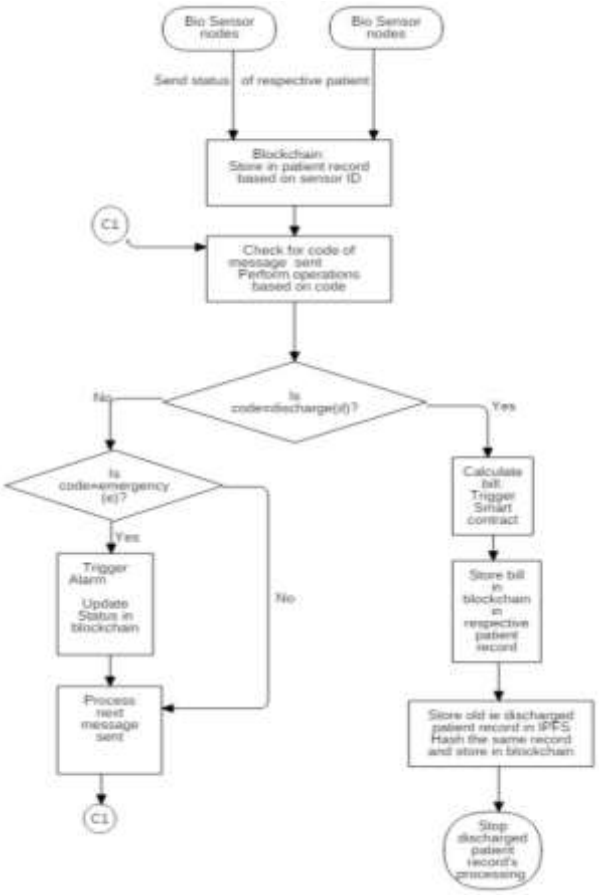
The Server/Client model is generally used for current IOT devices, which is a centralized model. So Cloud server plays an important role for IoT to work efficiently as it registers and updates those devices. There is a huge pressure put on these servers in terms of storage and computing. So in nearby future, when there will be a vast amount of these devices, IoT will not only be expensive but also a single point of failure due to central cloud servers [11]

The security in the current IoT model is lax as it is used mostly for simple device with no security features. The main concern is the reliable and secure storage of identities, digital rights and the properties of the system itself. Blockchain solves this problem with immutability feature. Due to this, as long as the original data inserted is correct, the data is secure. This immutability and Proof of Work/Stake also prevents IP spoofing as there is no scope of injecting the fake signatures by system anonymously. Use of hashes to retrieve data makes it difficult to do unauthorized access. [12] So basically a Blockchain plus Iot model which is decentralized is the need of the hour

B. *Proposed Model and Architecture for Medical Application*

A sensor is connected to each patient's bed that measures the patient's vitals and state in a real time manner. This response is recorded and displayed. These bio sensors being IoT devices lack processing power or any computing power. They can't mine the blockchain to add their block of data. Thus in order to register as a sensor and communicate with block chain, the address of the smart contract needs to publicly be announced along with the ABI, the Application Binary Interface, of the contract. The ABI connects the Iot platform on one end to the device program or application on the other. This enables bio-sensors to know where the contract is and what functions are available to interact with. This would allow IoT devices to autonomously find other devices and begin trading data, both with each other and the platform. Multiple sensors can also connect to a hub. The hub would know the smart contract address and thus connect to the blockchain.

A Device Management Agent is connected to each device to initiate and aid in device registration and initialization. It also takes care of the device's battery status i.e. the awake and sleep cycle. Multiple devices are connected to a hub which then connects to the IoT platform using MQTT protocol. In MQTT protocol the initials of the device are sent in the payload. There are separate codes for different situations, like initialization, registration accepted, registration rejected etc...Each device is identified by a device ID which it then sends to the IoT platform in the payload of MQTT protocol. The IoT platform connects to the co-located blockchain using rest API and rest protocol [13] Using the obtained device ID a hash is generated which is then mapped to the chaincode of a blockchain.Thus initial registration is done. Later when the device sends the current status of the patient, the data is sent to the IoT platform which is then communicated to the blockchain using rest API. The rest API contains methods for create,



read, and update blockchain data. In the blockchain, the records of each patient measured and collected by its respective sensor, can be stored as a block, thus remaining tamper proof. Each patient or doctor can access his/her record via a dashboard connected to the DM/ blockchain server via rest API. This API runs select queries only, update queries can be run only by doctors thus ensuring access control at the respective levels. All transaction logs in terms of treatment given, medicines, cost is stored in the chain. A smart contract can be coded and written on the blockchain to use information stored on the block. This then calculates the total bill and current status of the patient. Once treatment is complete the contract is invoked and record of the patient is updated by sending the total bill to the respective record. One can also link IPFS to the file system. This has several advantages:

The historic blocks are linked to its hash values due to the DAG structure of the blockchain. IPFS solves the problem faced in duplication of data in blockchain structure. Instead of storing every single transaction, as done in traditional blockchain, IPFS blockchain only stores the changes between two blocks which is known as state entries. This method allows easier block access, performance gain from deduplication and a data structure which can be maintained with more ease.

Thus, old records of discharged patients can be stored on the IPFS, which can be linked to the blockchain with a hash value. Thus, the hash value of that data is stored on the chain. Each data item has a tag saying on chain or off chain. If the data is off chain then the content is stored in IPFS but its hash is on the chain. Similarly IPFS is used to communicate data between smart contract and IPFS.

When the patient is about to be discharged the smart contract is triggered which then calculates the bill and amount covered by insurance. The Latest software version of billing and insurance software can be stored on IPFS. Thus data can be communicated between Smart contract and IPFS using IPFS protocol. The hash of this software is stored in the smart contract. When the medical record device gives a discharge signal by sending a discharge code and its device ID, using MQTT protocol, the respective patient's record is accessed by mapping ID to hash of record. Since patient is still in hospital his/her record will be in the blockchain. The record is accessed and updated to indicate status of patient as discharged. This triggers the smart contract which in turn triggers IPFS to generate bill and coverage. In this manner real-time patient monitoring and processing of data is done.

V. SCOPE OF IMPROVEMENT OF THE MODEL

Despite all the advantages of the proposed model, there is still areas where this model can be inferior to the current model of IOT. Some of them are discussed below-

1) Mining – It is a process for achieving consensus between devices which doesn't trusts each other by reviewing each and every block present in the chain [14] Mining of data takes considerate resources and can be costly .But a form of incentive in terms of virtual token is generally given to device or party which is able to successfully mine the data. Generally IOT device like Raspberry Pi are low end device with very low CPU power. These devices are not good option for hashing unlike higher end device [15]

2) Consumption of energy-In our model by this term, we mean the energy consumed by the device which takes highest amount of energy which known as miner. The reason it takes such large

amount of energy is because it is responsible for all transaction taking place and for process of the encryption done by hashing. When compared to the present model, our model takes more energy [16]

3) Response Time- The time taken by IoT device of our model to do the required task can be a little more than current model.

VI. CONCLUSION

The scope of blockchain is still being widely explored after its advent in the use of Bitcoin in 2008[18]. Its applications are vast and still hasn't reached it potential. The scope of innovation using blockchain is beginning to explode in the past few years. It is being used in utility distribution, distributed file storage, digital identity management, IoT platform integration and many more use cases.

We propose a blockchain based IoT model for medical device transactions and communication as an alternative to the traditional IoT model. The traditional model has a major limitation in terms of use of a central server which can, not only be expensive but also a single point of failure. The data communication not being secure and the transaction being mutable can cause further aggravation to the system. Lastly, the computing power of the IoT devices is not being used to its potential in the traditional model.

The proposed model overcomes these drawbacks as the use of blockchain facilitates the system being decentralized and distributed. The transactions stored are immutable and the communication occurring between the devices is encrypted. These things are fundamental with respect to medical devices as all medical history should be available and it should be safe disallowing its modification or theft. Due to the distributed nature of our model, a central server isn't required and the computing is divided equally and efficiently between all participating nodes.

Although, the scope of our proposed model covers most of important points relevant to medical IoT devices, there are few things which could further improve the scope of our project in the future. With advancements in micro processing and smaller devices we hope the energy consumption of these devices will decline in the future, allowing cutting edge medical devices for more people at lower costs. Another improvement which could occur over a period of time is shorter latency of appending in the blockchain using faster, more efficient algorithms for encryption and compression complemented with faster processers.

REFERENCES

Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things."

[1]Croman K. et al. (2016) On Scaling Decentralized Blockchains. In: Clark J., Meiklejohn S., Ryan P., Wallach D., Brenner M., Rohloff K. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9604. Springer, Berlin, Heidelberg

[2]https://blockgeeks.com/guides/smart-contracts/

[3] http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[5] https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

[4]Pradip Kumar Sharma, Saurabh Singh, Young-Sik Jeong, Jong Hyuk Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks", *Communications Magazine IEEE*, vol. 55, pp. 78-85, 2017, ISSN 0163-6804.

[5] https://www.edgefx.in/biosensors-types-its-working-and-applications/

[6] http://ars.els-cdn.com/content/image/1-s2.0-S1319157816300799-gr5.jpg

[7] https://www.slideshare.net/paolopat/mqtt-iot-protocols-comparison

[8] https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228)scribd.com

[9] Can Blockchain Strengthen the Internet of Things?Nir Kshetri

[10] https://developer.ibm.com/blockchain/resources/rest-apis/

[11] https://console.bluemix.net/docs/services/IoT/blockchain/dev_blockchain.html#IoTblockchain_link

[12] http://www.blockchaintechnologies.com/blockchain-mining

[13] https://securityledger.com/2016/12/analysis-three-things-may-limit-blockchain-use-on-the-internet-of-things/

[14] A. Dorri, S. Kanhere and R. Jurdak. 2017. Blockchain for IoT security and privacy: The case study of a smart home, in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops

[15] M. Samaniego and R. Deters. 2016. Blockchain as a Service for IoT, in Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). DOI:https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

[16] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).