Cluster Based Approach in Ethereum Architecture for Blockchain Technology

Amani Al Qarni

Department of Computer Science, College of Engineering & Computer Science, Jazan University, Saudi Arabia, Email: aalqarni@jazanu.edu.sa

Blockchain technologies have been an emerging trend in areas such as Financial Sectors, Health Management Records, Internet of Things, Supply Chain Management etc. In this paper, we have proposed a clustered based approach protocol in Healthcare Application in order to strengthen the security standards within the hospital network. The emergence of the blockchain technologies have proved to be a secured approach, therefore we have incorporated this technology in the Healthcare Management System. Since the usage of Hash values have been incorporated in the blockchain technologies and it is also observed that the hash values have been an irreversible feature in terms of security. In our paper, we have highlighted how miners are efficiently tampering the public blockchain and computing the hash values by creating their private block chains. Therefore, we have studied the ethereum architecture with our proposed system that can enhance the security of the blockchain by considering a clustered based approach in which the execution time is reduced and we have also discussed the attackers from manipulating any timestamps that are integrated with a transaction in the Healthcare Management System.

Keywords: Timestamps, Blockchain, Timestamp servicing, Distributed transaction Ledger, bitcoins

1. Introduction

Blockchain technology is an emerging technology that has proven to attain definite security. “Blockchain” first appeared in a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” published by a group known as “Satoshi Nakamoto” in 2008 [9]. The blockchain technology is a distributed ledger system that has the ability to store information digitally in the form of centralized database system [3]. The way the data is stored is based on the timestamps that helps in following up the sequence of events that have occurred for a particular transaction. This data is immutable and readily available for the public with a proper protocol of entrusted policy. Blockchain has gained popularity in areas such as Financial Sectors, Health Management Records, Internet of Things [1], Supply Chain Management etc. However the

blockchain technologies when fused with digital forensic tools are proven to be advantageous as the hash values for every transaction is been uniquely identified.

The term Blockchain refers to blocks that has features like:

- Security- Data stored is highly secured as it is connected to a pool of computers that have a centralized a database
- Immutability- The data remains unchanged and unaltered
- Distributed ledgers- a database that is maintained across various geographical locations in order to expanse the network
- Transparent log – stores information in a way that it cannot be altered without making records in all computers
- Irreversible data storage- Once a block is written in a blockchain, it cannot be altered instead it gets overwritten and stored as a new block.

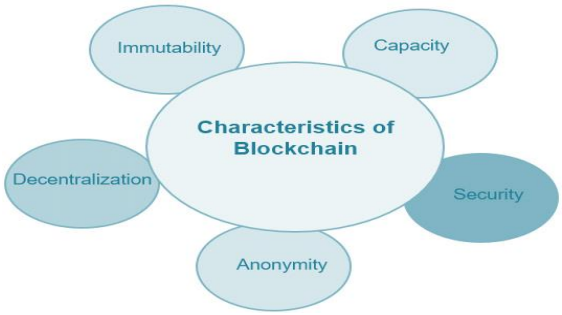


Fig. 1. Blockchain Characteristics

The strongest and concrete reason for implementing Blockchain Technology is due to its highest degree of decentralization and transparency. These are the major areas of transactions that a banking sector can possibly face in terms of payments, bank to bank transfers [4]. A detailed explanation of the decentralization and Transparency has been explained.

a. Blockchain Decentralization: It is a process that builds and stores data unlike the traditional database system. In this system, the blocks are distributed throughout the network and each machine on the network is called as “node”. Each node is then been familiarized by specific rules pertaining to the policies of the organization. These rules are then applied among all the nodes of the network henceforth making it a unified database that attains uniformity and authenticity. This database is famously called as Transaction Ledger that maintains similar data related to the same transaction. Whenever there is an update in the transaction, the ledger continuously updates the transaction list called as “blocks” and these blocks are remarkably encrypted using the Hash technologies that helps in maintaining the integrity and confidentiality of the data.

b. Blockchains Transparency: This feature of transparency in Blockchain confirms to the entrusted policies and high security of blocks by allowing the users to view the historical data, transactions and timestamps. The deletion or updation in the block is only made possible if all the users related to the transaction agree and apply the hash function process in uniformity.

In our paper, we have discussed the following:

Sec II , discusses about the types of blockchain network that are applicable in various sectors. In Sec III, we have discussed the history of bitcoin and its development. In Sec IV, we have discussed how a transaction is processed using the blockchain technology, followed by examples of Blockchain applications in the next section.

We have also compared in Sec VI, the traditional banking system with the Bitcoin Technology.

Various applications of Blockchain Systems have been discussed briefly in Sec VII. The Timestamping procedures have been highlighted in Sec VIII, followed by the Ethereum Architecture and its Transaction Management System has been discussed. At the end of the paper, we have discussed our proposed ethereum based medical data management architecture in Sec X. In conclusion, we have presented the results and analysis.

2. TYPES OF BLOCKCHAIN NETWORK

Every organization, be it a finance sector or education sector or health sector typically maintains three types of Blockchain namely: Pubic, Private and Consortium. Every type has its own criteria of accepting and operating its function by its own unique procedure.

a. Public Blockchain: It's a chain of blocks that is purely constructed in a decentralized nature that can be accessible by all the devices that are interconnected to each other. In this type of blockchain, every user has the liberty to open or create a new transaction without the need of a governing authority in order to make use of the network. This procedure is carried out by "tokens" concept.

b. Private Blockchain: In this type of procedure, a specific authority is been assigned to grant permission to have access to the transaction in order to view, update or delete.

c. Consortium Blockchain: It's a procedure where the network grants permission to only specific group of authorities in a network.

3. BITCOIN AND ITS DEVELOPMENT

Worldwide, there was a global financial crisis in the year 2007-08. It was considered as the worst financial crisis the world had ever experienced which led to a loss of $2 Trillion of the global economy . This crisis slowly moved into a global economic shock that resulted in many bank failures. Considering the situation of the world crisis of the financial sector, Satoshi Nakamoto created a paper-like object and along with the paper he developed a protocol to be followed for performing monetary transactions digitally that was based on cryptography or cryptocurrency, a situation where the currency is encrypted in order to be sent to another location digitally. This currency that was implemented was known as "Bitcoin"[2] . The protocol was developed in such a way that people across the world established a stronger trust and performed transactions without the involvement of a third party. This introduced the concept of Peer-to-Peer transactions and the technology that is used in this bitcoin is refered to as Blockchain. All the transactions are not stored centralized way rather they are distributed across a globally accessible ledger that makes use of the highest degree of cryptography.

4. HOW A TRANSACTION IS PROCESSED USING THE BC TECHNOLOGY?

The term "transaction" refers to an operation in the form of add/delete/update that is done to a customer's account, in case of banking system. All information related to the customer is maintained in the form of a table called "database". A blockchain is a type of database that holds clusters of information in the form of blocks. When these blocks are filled a chain of data in the form of blocks are formed. Therefore as and when any new transaction is performed, the blocks keep adding and the chain is formed with different hash values.

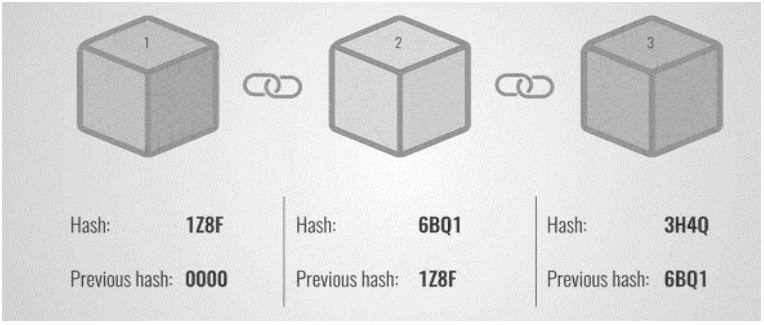


Fig. 2 Blocks with different hash values

All participants approve the transaction and each transaction is added as a block and henceforth creates a transparent and permanent record over the network.

Block Description: A block is a structure that stores transactions history right from the time it is created. If the block is to be studied in detailed, its structure comprises of:

- Block size
- Block header
- Transaction counter
- Transactions

Miners: Miners are people who constantly keep track of all transactions that are occurring in a blockchain[16]. The data is openly available and accessible for the public. If there is any malicious content that is performed on the block is still available to view by the public.

5. EXAMPLES OF BLOCKCHAIN APPLICATIONS

a. Reduction in Scams

Exposure of banks to attacks is a challenging scenario that can be faced by the bank authorities. It's a known fact about database that is maintained centrally in any organization is always vulnerable to hackers and attacks in the entire network. Constant attack force work is been ensured in order to compromise the security protocol of a network due to the digital revolution, henceforth, it is always recommended to keep aligned with the upcoming trends in order to combat the unpredictable cyber-attacks [5]. Blockchain technology helps organizations to minimize threats and processing overheads, also saves the time and cost.

b. Entrepreneurship Platform

Since the records are readily available and transparency is maintained at top most priority, it becomes much easier for the entrepreneurs to view the historic records of the various commodities and assets available for any transaction.

c. Monetary Transactions

Using this technology has helped to perform payments at a faster speed and by not depending upon the various payment schemes that certain organizations have adapted. The entire process is available 24 hours a day unlike the system that was implemented in the 1970s and the 80s.Some of the major disadvantages that exist within this system is that of the "privacy". The data that belongs to the customer can be mitigated due to the use of permissioned blockchains. Another major issue to be resolved is the scalability of the transaction. The speed of the transaction, the verification and limitations to the data size have also been a part of the challenged involved.

6. TRADITIONAL BANK SYSTEM VS. BITCOIN

a. Service availability: Traditional banks offer services in a limited time, weekdays 9 – 5 working hours whereas the Bitcoin technology is open 24 hours a day.

b. Monetary fees: Traditional banking services offer a nominal fees as it greatly involves international banks services too whereas the bit coin technology have a minute amount of transaction fee.

c. Monetary speed: A span of 24 hours is observed in traditional banking whereas less than 15 minutes are observed in bitcoin transactions.

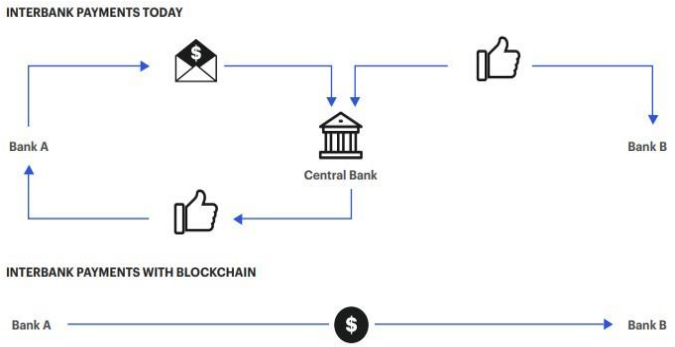


Fig. 3 Traditional Vs. Blockchain Technology

7. APPLICATIONS OF BLOCKCHAIN SYSTEMS

Following are the lists of sectors that have successfully been implementing the blockchain technology. They include:

i. Internet of Things

ii. Government Services

iii. Supply Chain

iv. Financial Transactions

v. Robotics control in Healthcare

vi. Intellectual property privacy

8. TIMESTAMPING

Every block in a transaction has a timestamp as it involves audit records of various timestamps[11]. First its important to understand the concept of hash value. It's a value that is computed by a mathematical computation, which takes input of any type of file, it can be a character, a text, an image or picture, a webpage etc. using a function called "Hashing function". The output obtained is irreversible and does not allow to trace back the original file. Hashing takes in input of arbitrary length and produces length of a fixed value. This value of hash when stored in a blockchain is referred to as a "Timestamp", So basically, timestamp is considered as a birth certificate of a transaction.

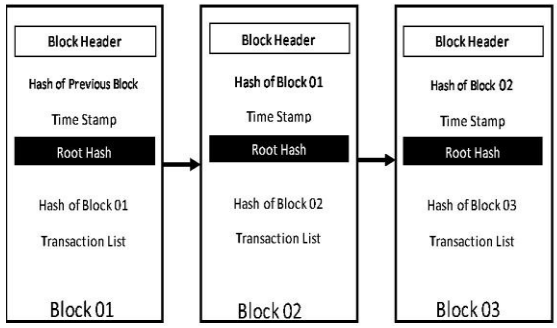


Fig. 4 Timestamps in blockchain

9. ETHEREUM

Ethereum is a first public blockchain that supports smart contracts. It was first introduced in the year 2015 and the emergence of this concept was to create a platform on the basis of smart contract which is open source and has the capability of integrating and embedding programming codes. Because of this dynamic feature of smart contracts, it opens doors for any type of customized coding based on the structural requirements of an enterprise. Therefore, smart contracts are based on language called as Solidity, which is the most striking feature of Ethereum (fig 5).

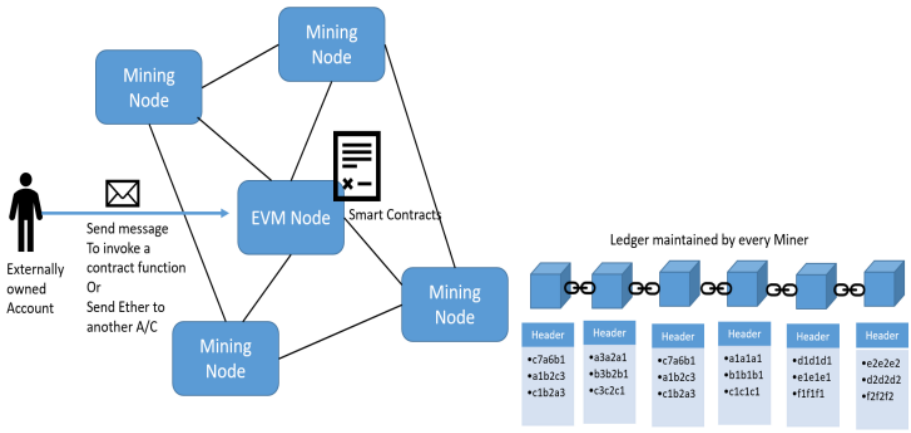


Fig. 5 Ethereum Architecture

Transaction Management System:

All transactions in an ethereum architecture, can be intervened by any external user in order to update the existing records or the database of the information system.

When a smart contract is deployed in ethereum blockchain , it assures the management of data and relationships between various components, for instance, patients, doctors, medicines etc[12].

Ethereum blockchain network:

An Ethereum transaction contains following elements :

- From (message sender) Address of 20-bytes
- To (message recipient)
- Value - the fund amount transferred from sender to recipient
- Data (optional) - contains the message that is being sent to the recipient.
- Gas – Whenever a transaction is made in ethereum network, a limited fee is incurred which is called as “Gas”.
- Gas Price: the maximum capacity that the sender can pay.
- Gas Limit: maximum gas that could be paid for this transaction.

A. SMART CONTRACTS

In the world of ethereum, Smart Contract [6] is a scripted text that is flexible to be customized according to the requirements of the components. Whenever a transaction is executed, the script is executed too. Its execution is directly run on the blockchain network and so it is secured from any type of tampering and alterations. Since its flexible to be scripted and rescripted, the programmers compile the code using the virtual machine of ethereum, specifically termed as EVM. Upon successful execution, its deployed over the

Ethereum blockchain. The various programming languages used in the scripting is:

- JavaScript
- Python

These languages are integrated with the solidity language[13].

B. ETHEREUM VIRTUAL MACHINE (EVM)

The virtual machine of Ethereum is designed in a way that offers users a flexible choice of customizing [14] the script based on the requirements of their network architecture. The commonly used application in this machine is termed as DApps, i.e. Distributed Applilcations, that offers an efficient platform to run the customized applications. These applications are embedded with smart contracts, that contain scripted coding.That code is deployed and executed using the Ethereum Virtual Machine (EVM).

10. PROPOSED ETHEREUM BASED MEDICAL DATA MANAGEMENT ARCHITECTURE.

Head Timestamp Manager (HTM)

The HTM is the main source for regulating the timestamps in the blockchain. It regulates by accepting transactions and assigns timestamps and generates blocks.

In this section, we have discussed, how the patient's data is appended to the ethereum architecture.

Append data: To append patient's data to the ethereum architecture, the request is sent to the ethereum architecture. The request includes Patients ID, Hospital ID and the timestamp. This request is hashed by a Hash Function and this value is encrypted using the private key from where the block is generated

This text obtained after encryption is considered as a digital signature of that specific block. Now we have 2 units, one the encrypted text and the other is the timestamp of the block. These units are stored in the HTM (Head Timestamp Manager).All transactions likewise are accumulated in a node and a block is generated. Since a block has limited storage, the HTM, then performs a Hash Function collectively on the block and this hash function is propagated to the remaining nodes. The TM or the timestamp manager verifies the transaction to check its availability and validity.

The TM then decrypts the transaction using a public key in order to obtain a hash value. This will allow the TM to compare hashes of encryption and decryption and if this value is matched then the security component of Data integrity is assured.

Security Analysis and its solution

Any Management Information System is vulnerable to attackers and often face a compromised network policy. In our proposed paper, we make use of a hospital management dataset that uses blockchain method for a promising secured policy. Online Payments, Monetary transactions, Insurance companies applications are the most common transactions that occur

in any Hospital Management system, due to which all transactions must be updated in the Hospital Management System. Due to this reason utmost confidentiality and scalability must be maintained in the Transaction Ledgers of a centralized database and also ensure strict monitoring of any malicious activity. In this paper we have proposed a system that ensures all timestamps are free from any intrusions and if any intrusions do occur how they can be identified, detected and analysed with the help of our model that accepts transactions with a different ID and how data is fused and visualized. Transaction fusion is a concept of merging or updating transactions based on timestamps from various parties and henceforth afford precise and significant evidence. Main goal underlying behind this procedure is about transaction updating with varied timestamps service and to create successful blocks in which the same data is fragmented into smaller modules and yet accurate information for a better analysis. The dataset belongs to renowned nationalized hospital dataset in the Middle East. A Forensic Toolkit is also been administered to implement the appended transactions in the blockchain. From this blockchain, the transactions are mined by miners and further studied for updating timestamps.Since our study involves the timestamps service ,a dataset [10] is used with features that idealize the timestamps based data. Timestamp Service is considered as a required feature in the field of information security as a basis of investigation for the network forensics team. Ever since online medical consultations have been revolutionized, attacks over the network have grown immensely henceforth, third party hindrance must be eliminated . Due to this reason, a decentralized timestamp system was proposed in the year 2008.The data is first collected in the files. And the investigation tool summarizes the following:

A. Timestamp Analysis

Each block that is created for a particular transaction is updated and appended to the blocks and must encompass the following:

- Transactions gathered in the form of a dataset
- Information of Updated transaction ID
- Updated blockchain.

The Transaction ID term implies to the blocks that have updated information about the transactions that were carried out. As per the requirement of the case study, few attributes are laid out that can also display the malicious activities with updated timestamps. Categorization of the data is based on:

B. Phase I Analysis

In this phase, the timestamps are updated along with the transaction IDs. In the first stage of "Timestamp Analysis" the data is first formatted into a common format. The formatted data is then compared and further processed since the same data is been placed in different blocks and different procedures are applied with a varied hash value. The timestamps are gathered and is recorded in the following format:

- Timestamp Data
- Hash value
- Transaction Details

During the categorization, significant values are noted from the blockchain to form the basis of gathered data.

Timestamps recorded from various blocks possess different types of hash values and transaction details. If the network traffic is analyzed, it records more of the hash values appropriately than from the network address that it originates from. If timestamp, hash value and data are changed, then it concludes that the block has to be added and linked together.

C. Phase II Analysis

In this phase, multiple correlations are observed amongst the blocks.

D. Final Phase Analysis

All procedures are carried out in MS-Excel, however if the data is run on MATLAB, it can give significant pictorial mapping of the various changes in the data. The following operations are performed:

- Searching for similar transaction IDs: When each node of the input data competes with each node of output data the units are matched and those weights are considered.
- Hash value monitoring: Upon successful matching of values, every node of the network is moved to the next input layer.

The variations in the hash values are treated as Input pattern in SOM. This step is iterated to a fixed value of number until the values of each block are completed. The results obtained are represented in a rigid structured format, making it difficult for any changes to occur in the block. The results help in ensuring all possible hash values are entered and no similarity is observed in between each unit (pictorial representation of blocks).

Our proposed procedure makes a possibility to display, analyze and observe hash values of blocks and the following logic is applied to the Timestamping Service:

1. Regularize

hashvalue = Transaction_ID (p)

2. If hashvalue ∈ blockchain

Then

write “New_Timestamp(“ ”)

Else if tid ∉ blockchain

Then write “failed tid”

Else no Timestamp Updation

Exit

3. Timestamp updated

4. Observe Event_date, Event_time, Transaction_ID, Timestamp onto the

Transaction Ledger

5. End.

In a single repository, various TIDs are maintained which are privately available to the Hospital Management Information System. The primary TID is compared with the block data and If the TID observed in the block is similar to the database, the system will allow the block to be updated and further carried out if any transactions have to reoccur.

The data set is processed using MATLAB 9.7. The time taken to process and iterations are set by the network administrator due to the limitless stages of operations to a specific block. Each data set is run on the tool to visualize the existence of blockchains and any blockchain with discolored unit is observed, is considered as an attempt to tamper the data by a hacker. The hacker simply creates his own private blockchain and creates a similar transaction ID making it easier to compute the hash values and merge with the original blockchain.

Our proposed architecture also has the capability of handling malicious attempts like denial of service attack. An attempt can be made by an attacker even in robotic controlled based systems that can jeopardize the transactions by creating fake blocks or forged blocks. The denial of service attack can hinder in providing services to the organization. In our proposed architecture, the HTM is responsible for handling transactions so that HTM is the primary source to detect attacks.

Upon detection the HTM can maintain a separate block comprising of unidentified sources, which can be used for future reference. Since HTM have the immutability property of the blockchain, so any type of malicious activity is not possible in blockchain.

Performance analysis

We have analysed and compared the proposed architecture with the ethereum architecture. We simulated the ethereum architecture and our proposed architecture using CISCO packet tracer Ver_8.0.0.0212 simulator. Several nodes that are ready to be simulated are connected likewise fashion of a etheurem architecture. And these nodes are arranged in the form of clusters and each cluster is supervised by a HTM. The same fashion is implemented in other clusters as well. In order to avoid overburdened network, we form clusters in the form of 50 nodes forming 1 cluster.

In an ethereum architecture, since the information is decentralized and the code inside each node is scripted, there is no possibility of any third party intervention. Also because our data is encrypted with hash functions and also decrypted and served as a digital signature. Since there is no intervention of third party here, the additional costs incurred are also curbed off. The coding is applied in the solidity compiler and the basic code for solidity is when the smart contract is defined as follows:

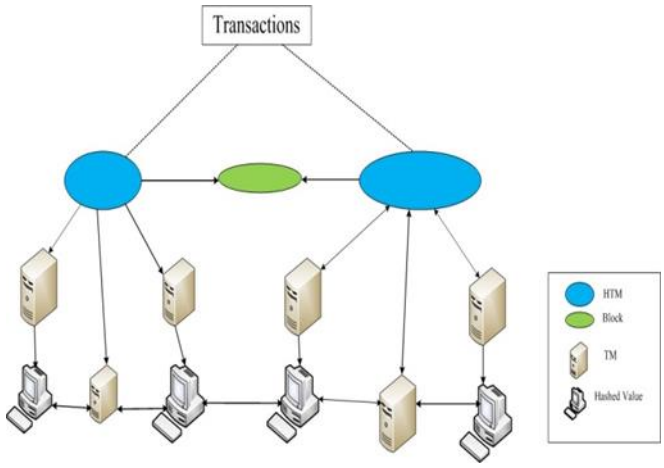
```
contract SimpleStorage {
  uint storedData;
function set(uint x) public {
      storedData = x;
   }
```

```
    function get() public view returns (uint) {
        return storedData;
    }
}
```

We can evaluate the ethereum architecture and a proposed architecture on the basis of the increment in the nodes.

Nodes are restricted to 50 with an increment to the number of blocks from 5 to 25 with the time difference of 0.5 seconds. In order to calculate the total amount of data been transfered in the ethereum network, 5 blocks of 1 MB each generated by network nodes is broadcasted to 49 other nodes of the network to update the ledger of each node[15]. All the 50 nodes are clustered in 10 pairs with an intervention of HTM for simulation. The number of hops required are 2 in order to trigger the smart contract to execute a node and total amount of data transmitted is calculated.

The architecture that we have proposed for the node is generated by the HTM. Supplementary each node that is propagated also conveys the hashes and data transmitted that were calculated by both public and private keys.



Fig, 6 Proposed architecture

The size of the hash is 512 because we have used sha512 structure. Therefore the amount of data propagated in our architecture is calculated by adding the data transferred during the propagation of the nodes hash value and data. The calculations of time is simulated in the network and all processing times are observed and recorded and simultaneously applied in the log book

In a similar fashion, if the number of nodes are increased with varied intervals and if the nodes are clustered and calculated, then the amount of data transferred and the time required for processing the data shall improve. When compared with the ethereum virtual machine and our proposed architecture, the amount of data increases and hence leads to increase in computational and traffic overheads. When compared between both approaches the EVM is

higher than our proposed architecture. This improved performance is because of clustering approach [8] that we proposed in our architecture. Where the data is propagated only on HTM as compared to EVM which propagates data on all nodes which requires more processing time[7].

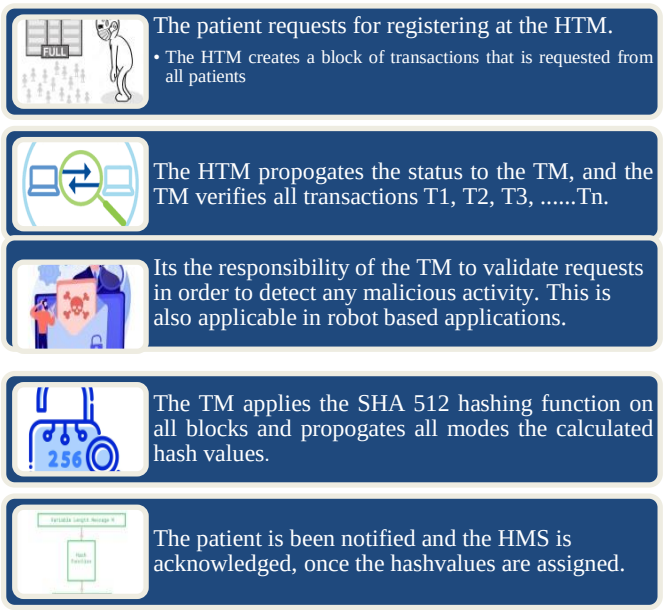


Fig 7 Hospital data Management System

In order to analyze and calculate the processing time required, we have made simulation of the network, we had broadcast the blocks with our proposed architecture as well with ethereum network. We have calculated the total processing time for the successful data replication and update of the ledger during the simulation.

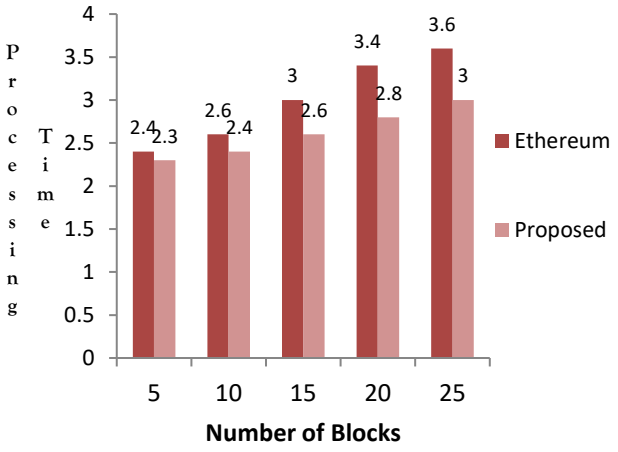


Fig 8. Comparitive analysis of Ethereum & proposed architecture

In the above graph, we have compared the ethereum architecture with our proposed algorithm, that illustrates the processing time with the increase of block numbers. It shows that using the proposed architecture, it consumes less time to propagate the transactions within the blocks. This is because of the clustering approach in our architecture which eliminates data replication on all the nodes. On average when the number of blocks increases, the ethereum network takes 1.04 to 1.21 times more time to replicate the data compared to our proposed architecture.

The difference between the processing times with both approaches increases when the number of blocks in the network increases.

11. CONCLUSION

In the advanced technology of Healthcare Management System, Blockchains have an integral role to enhance the security of the data. Bitcoin architecture addresses several issues, but its expensive and execution time is more. However, Ethereum is a better approach for blockchain technologies. In this paper, we have analysed the ethereum architecture and proposed our architecture which uses clustering technology in ethereum. Significant results have been achieved in our proposed architecture for healthcare management system. Initially we have discussed how the smart contract is scripted in Solidity compiler with the hashvalues and how timestamping of each transaction is performed. The results show that ethereum architecture takes on an average of 1.04 to 1.21 times more time to process no of blocks in comparison to our clustered based approach architecture.

We have discussed how a patient registers at the Hospital Management System and how the Time Manger (TM) propagates transactions of patients in the block. The TM is also significantly identifying for any malicious activities in the transactions. For each transaction that is generated, a Cryptographic algorithm namely SHA 512 structure is applied on the blocks. Henceforth generating irreversible hash values. This helps in creating a separate TID for every transaction. Once a hashvalue is assigned the patient is been notified of its request.

In future work, we will integrate our proposed architecture with cloud computing technology, which concentrates on utilization models of resources.

References

1. S. Fu, Q. Fan, Y. Tang, H. Zhang, X. Jian, and X. Zeng, “Cooperative computing in integrated blockchain-based internet of things,” IEEE Internet Things J., vol. 7, no. 3, pp. 1603–1612, 2019.
2. A. Urquhart, “Under the Hood of the Ethereum Blockchain,” Financ. Res. Lett., p. 102628, 2021.
3. E. A. Opare and K. Kim, “A compendium of practices for central bank digital currencies for Multinational financial infrastructures,” IEEE Access, vol. 8, pp. 110810–110847, 2020.
4. Tobias Adrian, Martin Muhleisen, Maurice Obstfeld, Casting light oncentral bank digital currencies, Staff Discussion Notes 2018 008 (2018)A001.
5. H. Chen, M. Pendleton, L. Njilla, S. Xu, A survey on Ethereum systems security:Vulnerabilities, attacks, and defenses, ACM Computing Surveys (CSUR) 53 (3)(2020) 1–43.

6. Simon Joseph Aquilina, Fran Casino, Mark Vella, Joshua Ellul, Constantinos Patsakis,EtherClue: Digital investigation of attacks on Ethereum smart contracts,Blockchain: Research and Applications, 2021,100028,ISSN 2096-7209
7. Peter Robinson, Raghavendra Ramesh, Sandra Johnson, Atomic Crosschain Transactions for Ethereum Private Sidechains, Blockchain: Research and Applications, 2021, 100030, ISSN 2096-7209.
8. Jung Yoon Song, Woojin Chang, Jae Wook Song, Cluster analysis on the structure of the cryptocurrency market via Bitcoin–Ethereum filtering, Physica A: Statistical Mechanics and its Applications, Volume 527, 2019,121339, ISSN 0378-4371
9. Nakamoto,S.(2009).Bitcoin: A Peer-to-Peer Electronic Cash System Bitcoin.
10. D. L. Hall, and J. Llinas. An introduction to Multisensor data fusion. In Proceedings of the IEEE, vol. 85, n° 1, pp. 6-23, 1997.
11. B.Gipp, N.Meuschke and A.Gernandt. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. In Proceedings of the iConference 2015,Newport Beach,CA,USA,Mar 24-27, 2015
12. Andrian Tudor & Vasile Manta, "Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network" 2018, Taylor and Francis Online.
13. Dannen C. (2017) Solidity Programming. In: Introducing Ethereum and Solidity. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2535-6_4
14. Gabriel Estevam, Lucas M. Palma, Luan R. Silva, Jean E. Martina, Martín Vigil, Accurate and decentralized timestamping using smart contracts on the Ethereum blockchain,Information Processing & Management,Volume 58, Issue 3, 2021
15. Lin Liu, Wei-Tek Tsai, Md. Zakirul Alam Bhuiyan, Hao Peng, Mingsheng Liu, Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum,Future Generation Computer Systems,Volume 128,2022,Pages 158-166,ISSN 0167-739X
16. Runkai Yang, Xiaolin Chang, Jelena Mišić, Vojislav B. Mišić, "Assessing blockchain selfish mining in an imperfect network: Honest and selfish miner views",Computers & Security, Volume 97,2020,101956, ISSN 0167-4048.