

Health Care and Data Management System using Blockchain and Machine Learning Techniques.

Prof. Srinath G M

Assistant Professor

*Department of Computer Science
and Engineering*

S J C Institute of Technology

Chickaballapura,

Srinathgms88@gmail.com

Manjesh Kumar K P

*Department of Computer Science
and Engineering*

S J C Institute of Technology

Chickaballapura,

manjeshkumarkp@gmail.com

Vipul Kumar

*Department of Computer Science
and Engineering*

S J C Institute of Technology

Chickballapur,,

vipulkumargpj@gmail.com

Gajula Sambasivarao

*Department of Computer Science
and Engineering*

S J C Institute of Technology

Chickaballapura,

Sambasivaraogajula9@gmail.com

Harsh Kumar

*Department of Computer Science
and Engineering*

S J C Institute of Technology

Chickaballapur,

harshvardhan6611@gmail.com

Abstract— Over the beyond century, disruptions with the biomedical and clinical studies fields have brought about dramatic modifications in healthcare statistics control systems. This leads to a step forward in scientific statistics protection. This is a chief trouble inside the healthcare industry. The ability of Blockchain is to maintain an incorruptible, decentralized and obvious log of all affected person statistics makes it a generation rife for protection applications. In this project Blockchain technology is used for it's major gain of being transparent. Since it's far private, concealing the identification of any man or woman with complicated and secure codes which could shield the sensitivity of scientific statistics is achieved. The decentralized nature of this generation additionally lets in patients, medical doctors and healthcare vendors to share the equal records fast and safely. Extracting the applicable records from the statistics is feasible with the aid of using making use of KNN Machine Learning algorithm

shapes the inspiration of a localized medicative service stage shared by the patients and suppliers, acting as AN interface to the patient's record. Blockchain could be a cryptographically secured, immutable, write once, browse anyplace sort information structure. It consists of blocks and these blocks area unit coupled along mistreatment an unmodifiable key referencing mechanism.

The Blockchain data structure consists of the following components:

- The Blockchain network has secured list of blocks which contains the useful information.
- A peer-to-peer network which contains identical examples of the Blockchain data structure
- A consensus mechanism which secures the harmonized growth of Blockchain.
- A security mechanism that ensures that the data stored in the Blockchain network is immutable. client who orders that product and help them to identify if the product is authenticated or counterfeited.

I. INTRODUCTION

In Blockchain sort of a distributed ledger, singular transactions area unit encrypted into blocks by the applicable encoding, supplementary to the ledger and ne'er deleted. the data in Blockchain is verified essentially by a coupled list of encoded exchanges that utilizes a hash. The hash operate generates a hash by encrypting the data fed in Blockchain. It

Background:

A. BLOCKCHAIN OVERVIEW:

Blockchain is a decentralized gadget. It refers back to the collective renovation of a technical solution that maintains a Continuous document document as a dependable database thru decentralization. It become to start with used drastically on bitcoin the block era method of blockchain is to gather and

verify the records and then generate a brand new block via. We first describe the blockchain consensus mechanism the use of bitcoin as an example, its blockchain consensus mechanism is a proof of work algorithm (poor or worse). Every node competes based on their respective computing energy to remedy a SHA256 math problem this is complex to solve but easy to verify. The first node that solves this hassle will get the new block accounting right. Blockchain facts is stored on every node, then the nodes exchange data with each different over the community. Every node maintains a whole blockchain records. The node will verify the received transactions and encompass them in the new block based on its own blockchain information, and try to achieve the accounting rights of the brand new block within the above manner.

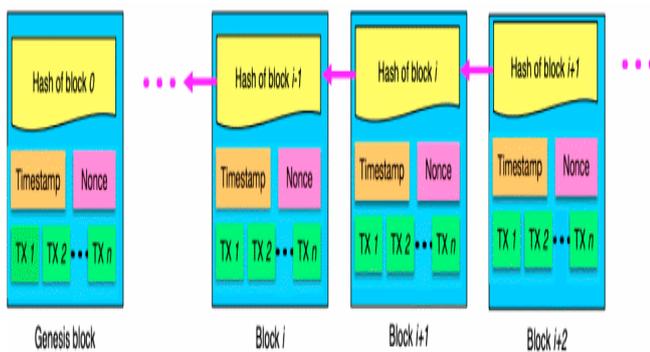


Figure 1. Connections Between Blocks In Blockchain

B. BLOCKCHAIN FEATURES:

In these day’s social machine, a large part of the economic conduct of individuals relies upon on believe wherein frequently facets interact with a third birthday celebration, as a consequence forming a trust relationship. Generally, there is a mutual non-consider between those two parties which have lengthy been primarily based on believe ensures supplied with the aid of 1/3 events, consequently it is critical to take observe of the characteristics of blockchain technology that assist subvert the inspiration of human transactions that have been performed for thousands of years.

The use of blockchain you’ll create a information report device that does not rely on a trusted third party as a transaction middleman, and that is overtly shared and reliable at the identical time. The traits of blockchain technology are defined in detail beneath.

There are few basic properties of blockchain

1. **Decentralization:** Inside the conventional centralized machine, a trusted authority is required to validate each taking place transaction within the network. But, the decentralized surroundings do not support any governing authority or single entity to manipulate the entire network. All of the nodes in the network collectively control the community, i.e., decentralized

governance. The transaction in blockchain can consequently be finished among 2 friends (p2p) without the approval of a valuable enterprise.

2. **Security and Privacy:** SHA– 256 cryptography set of rules is used for hashing. Further fixed-duration has output value is generated regardless of the input facts length. This makes it hard to hack. Additionally, the components that go into block generation increase the difficulty degree for hacking. Immutability is every other factor including securing information. Thus the systemic thing of BCT inherently affords security.
3. **Untraceability:** After a block has been determined in the Blockchain, it cannot be tampered with. Due to the following circumstances, once a block in the Blockchain is altered, it will be immediately detected and rejected by other nodes.
4. **Transparency:** The shape of peer to peer community allows equality among the nodes. Even supposing the shape will become slightly altered, the members can inspect the kingdom of any transaction, while it’s far in the system. Therefore a consensus is given by using anode with full focus. Similarly, the peers have replicated shared ledgers. Consequently, any interest or transaction in a blockchain is facilitated with full transparency.
5. **Flexibility:** The technology of blockchain is open supply and all of us can use it to regulate it into our very own version. There are already several flexible blockchain platforms available, and users can also redevelop a new blockchain platform if they desire to. Blockchain is a limitless generation which means that customers can create more than one

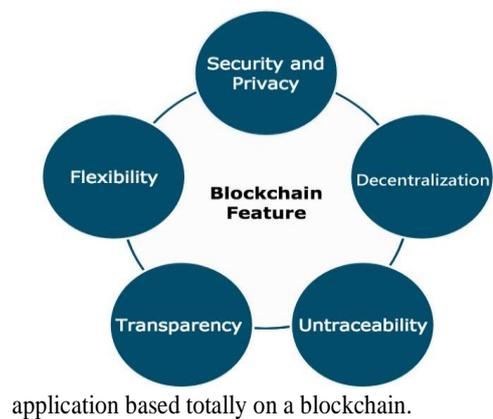


Figure2. Characteristics of Blockchain.

SHA-256 Algorithm

Secure Hashing Algorithm (SHA) - 256 is the hash capacity and mining calculation of the Bitcoin convention, alluding to the cryptographic hash work that yields a 256 pieces in length esteem. It directs the creation and the executives of addresses, and is likewise utilized for exchange check. Bitcoin utilizes twofold SHA-256, implying that it applies the hash capacities two times.

The calculation is a variation of the SHA-2 (Secure Hash Algorithm 2), created by the National Security Agency (NSA). SHA-256 is likewise utilized in well known encryption conventions, for example, SSL, TLS, SSH and open source working frameworks like Unix/Linux.

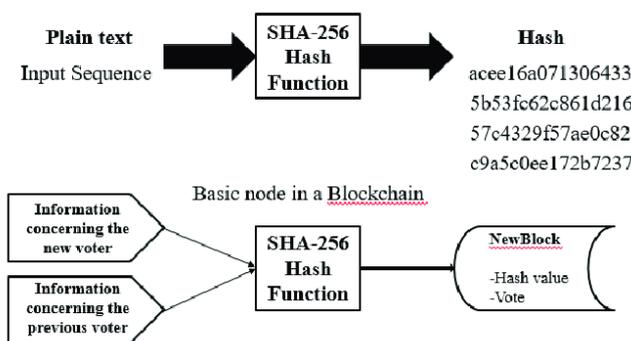


Figure 3 Usage of SHA-256 Algorithm in Blockchain

The hash calculation is very secure and its functions aren't known in the public area. It's utilized by the United States government to safeguard touchy data, because of its capacity to confirm a substance of information without uncovering it because of the utilization of computerized marks. Moreover, it is likewise used for secret phrase check, since it helpfully doesn't need the capacity of precise passwords, as the hash values can be put away and coordinated with the client section to confirm on the off chance that it's right or not.

As a matter of fact, it is almost difficult to uncover the underlying information from a hash esteem itself. In addition, a savage power assault is incredibly improbable to succeed on account of the galactic number of possible blends. Furthermore, it's additionally seriously impossible that two information values (known as impact) have a similar hash.

II LITERATURE SURVEY

A literature survey could be a text of a erudite paper, which incorporates the present knowledge as well as substantive findings, similarly as theoretical and method contributions to a specific topic. Literature reviews use secondary sources, and do not report new or original experimental work. most frequently related to academic-oriented literature, like a thesis, thesis or a peer-reviewed journal article, a literature review

usually precedes the methodology and results sectional tho' this is often not forever the case. Literature reviews are common in are search proposal or prospectus (the document that is approved before a student formally begins a thesis or thesis). Its main goals are to situate the present study among the body of literature and to produce context for the particular reader.

Existing system:

- a) Meditab, a code company, claims itself collectively of the foremost electronic medical records code creators for medical establishments. The corporate includes electronic faxes and this can be technique continues to be used considerably to share patient knowledge to different knowledge seekers. however this technique of sharing knowledge has evidenced to be insecure and reliable creating terribly less preferred.
- b) Spider Silk, a Dubai-based cybersecurity firm, had a fax server, that was running associate Elastic search info including not but six million health care records .The server didn't even had passwords for security, that indirectly granted access to everybody and therefore anyone may browse the transmitted faxes in period .The fax that were sent consisted of the many recognizable data concerning patients like their case history, treatment undertaken within the past, their social security numbers and different records

III PROPOSED METHODS FOR HEALTH CARE USING BLOCKCHAIN

There is no proper solution before tackling this issue. As patient ID can be easily copied it is also not a guarantee system, nor a Proper solution to differentiate counterfeit Medical Field from originals Data. Blockchain technology is one of the promising technologies emerging in recent years that can help solve such a problem. Blockchain technology can be used to monitor and regulate the data of Patients in the Data Base of Hospital so that users (Patients) can only obtain original records. The main goal of the project was to provide people's Data in term of Medical field and help Patients identify whether data is safe or not using blockchain technology. The prototype of the system will be a distributed application (DApp) with a supporting blockchain network. The network will be developed on hyper-ledger fabric which is an open-source Blockchain development tool and uses the default DPoS/PBFT consensus algorithm.

The basic module of our system;

- Data Preprocessing: The Dataset is described, we will use scalar functions to remove the non filled data.
- We are passing raw data set to the input we are using sum, average, standard deviation mathematical approaches to fill the missing values and removing the repeated data.
- Training model: We are using the KNN- classifier to

- train the dataset.
- In this module the given dataset will get divided into train set and test set and train using fit().
- Trained model will saved in pickle file.

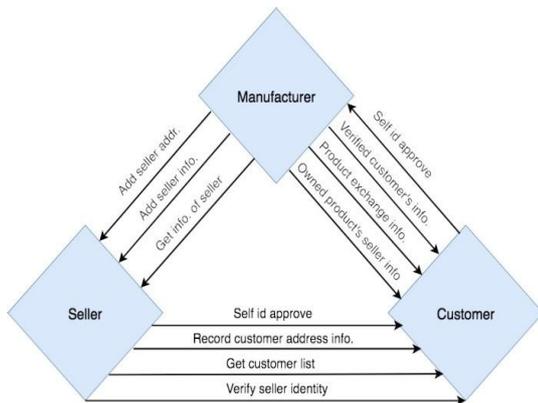


Figure 3 Modules and dataflow in Blockchain.

IMPLEMENTATION

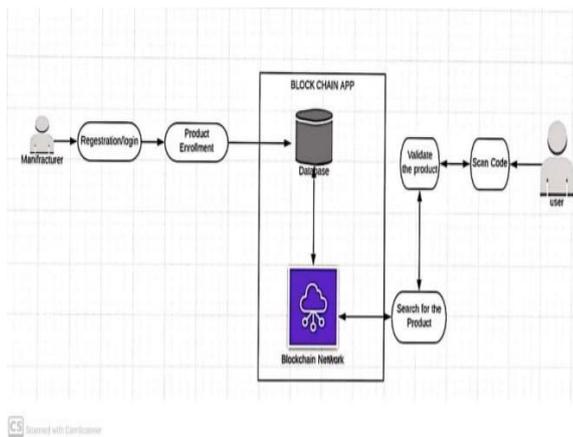


Figure 4 System Architecture of Dapp

1)Login process: Before establishing a connection to the system, the user must choose which account to log into. The user's accounts are linked to the accounts in Geth, as long as Geth is started, the user can choose the account which is also linked to the serial number of the list of accounts in Geth. Next, the user has to type the Keystore file, which is an encrypted file that contains the private key. Finally, the user can type the contract address and click the save button to set the basic information.

2)Public information about the contract: With the aim of disclosure of information, information about the patients/doctors is completely public. Our system provides smart contract data search functions, which can return the list of Patients, the list of Doctors, all information about the safe.

3) Adding new patients and number of patients: In our system, manufacturers can check patients information, including adding new patients addresses and also the number of patients that can be sold by a specific patients. The program in the smart contract will first check if the function setter is the producer. If correct, the program will build a patients structure and set the maximum number of details that can be sold for patients, this amount can also be changed later.

4) Exchange provision for specific user product details: as customers provide proof of identity and the address to send the product to. The manufacturer will initially check if the identity is correct and then determine if the consumer's product information is in the smart contract, then proceed to change the product status to exchange status. As an observation, this function will check if the setter is the producer. Otherwise, the function will return without setting the value.

5) Smart Contract: When the transaction between patients and consumer is established, the patients will add the consumer's address in the smart contract. Each patients has a details structure in the patients structure, the patients enters the details addresses in the details so field. Also, the access rights of the patients field can only be set by the patients

6) Identity Verification: Identity Verification is one of the most important components of our system. Users of our system can use their addresses as their representation. The address is defined within the last 20 bits of the user's public key. Whenever a user wants to make a change to the current status of the Ethereum contract, the user must sign the transaction with his or her private key to perform a digital signature. As long as the user's private key is secure, there will be no other means to change the user's identity

Result and discussion:

The system enhanced security, the system provides decentralization, it provides transparency and it protects the data which we are given to the system it gives privacy and it increased efficiency.

V CONCLUSION

There area unit innovative applications of Blockchain in health care thanks to inherent encoding and spread. It enhances the protection of patients' electronic medical records, promotes the monetization of health information, improves ability among health care organisations, and helps counterfeit combat medicines. totally different health care fields will change with Blockchain technology; areas like health care, digital agreements allowed by intelligent contracts represent one among Block-chain's most important applications. By removing intermediaries from the payment chain, intelligent contracts can minimise prices. The Blockchain potential in

health care depends considerably on the adoption of associated advanced technologies within the scheme. It includes system pursuit, healthcare insurance, medicines tracing, and clinical trials. Hospitals will chart their services employing a Blockchain framework, even over the whole life cycle, exploitation device pursuit. Blockchain technology will preferably be used to improve patient history management, particularly pursuit and also the insurance mediation method, thereby accelerate clinical actions with optimised information maintenance. Overall, this technology would considerably enhance and eventually revolutionise however patients and physicians treat and use clinical records and improve health care services.

Future work:

Blockchain technology may additionally progressively support financial transitions between patient and care center, particularly at the amount of small payments. The new value-based attention models may see the compensation of the services provided by the suppliers supported the well-being created, instead of on the number. "Doing the proper thing" may become the target to be rewarded with incentives, maybe provided through a universal and easy-to-use blockchain platform of small payments. This platform may well be used each to reward patients' efforts to pursue correct behavior and to change the sharing of health prices. There are already various samples of pilot applications that aim to use blockchain to permit the validation of health information (as genomics) by users. World Health Organization plan to create them offered for public health or analysis functions. The target is, during this case, to beat the issues coupled to the particular consent needed for the secondary use of information, through the remuneration of patients. World Health Organization plan to share their anonymized information, for instance for applications within the field of preciseness medication.

VI REFERENCES

[1] Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework", *Journal of Medical Systems*, vol.43, no. 5, 2018. [2] G.Magyar, Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management, Budapest, Hungary, 24-25 Nov. 2017. [3] Aimee O'Driscoll (2019, July), "The biggest medical data breaches in history", [Online]. Available: <https://www.comparitech.com/blog/vpn-privacy/biggest-medical-data-breaches/> [4] HIPAA JOURNAL (2018, March), "Healthcare Data Breach Statistics.", a.[Online]. Available: "https://www.hipaajournal.com/healthcare-data-breach-statistics/" [5] Zaheer Merchant (2019, April), "Health department of northern state exposed data of

12.5 million pregnant women.", [Online]. Available: <https://www.medianama.com/2019/04/223-health-department-indian-state-pregnant-women-data-leak/> [6] "Medicalchain Whitepaper - 2.1" [Online]. Available: <https://medicalchain.com/en/whitepaper/> [7] Zack Whittaker (2019, March), "A huge trove of medical records and prescriptions found exposed.", a.[Online]. Available: <https://techcrunch.com/2019/03/17/medical-health-data-leak/> [8] Shuai Wang, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han and Fei-Yue Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, pp.2266-2277 [9] Shuai Wang, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han and Fei-Yue Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, pp.2266-2277 [10] Laura Ricci, Damiano Di Francesco Maesa, Alfredo Favenza and Enrico Ferro, "Blockchains for COVID-19 Contact Tracing and Vaccine Support: A Systematic Review", *IEEE* 2021, pp.37936 - 37950.