International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

Patient Record Monitoring in a Notary Service Blockchain

Rini PL[1]

[1]*Research Analyst, KAS Innovative, Chennai, India*

Abstract – *Patient records were observed through the IoT sensor devices and stored in blockchain, in order to secure the healthcare information and to provide the complete access control to the patient. Data mobility in IoT causes data hackers to access and alter data in healthcare system. Blockchain with Corda, a permissioned platform provides transfer of data in real time to improve performance secure patient's health records and provides permission only to the validated nodes to access the records. Immutable data generated by using blockchain provides unaltered data. The Global ledger is encrypted in order to verify any changes or modification in each block of transactions. Raft based notary service is used as a consensus algorithm for cryptographic hashing. Complement to cloud servers, edge and cloud computing integrates and forms edgecloud computing to avoid security issues and provides access to data even during offline.*

Key Words: Corda, Raft, Notary, Health data, Immutable, edgecloud computing

1.INTRODUCTION

Blockchain is a shared, immutable ledger that enables the procedure of recording transactions and monitoring property in a commercial enterprise community. An asset may be tangible (a house, car, cash, land) or intangible (highbrow property, patents, copyrights, branding). Virtually something of price may be tracked and traded on a blockchain community, decreasing hazard and slicing prices for all involved. Why blockchain is important: Business runs on data. The quicker it's obtained and the extra correct it is, the higher. Blockchain is right for turning in that data as it gives immediate, shared and absolutely obvious data saved on an immutable ledger that may be accessed most effective via way of means of permissioned community individuals. A blockchain community can song orders, payments, accounts, manufacturing and lots extra. And due to the fact individuals percentage an unmarried view of the truth, you could see all info of a transaction end-to-end, supplying you with more confidence, in addition to new efficiencies and opportunities. What desires to change: Operations frequently waste attempt on replica report preserving and third-celebration validations. Record-preserving structures may be at risk of fraud and cyber-attacks. Limited transparency can gradual statistics verification. And with the appearance of IoT, transaction volumes have exploded. All of this slows commercial enterprise, drains the lowest line — and way we want a higher way.

1.1 Blockchain Benefits

Greater trust

With blockchain, as a member of an individuals-most effective community, you could relaxation confident which you are receiving correct and well-timed statistics, and that your personal blockchain data might be shared most effective with community individuals to whom you've got mainly granted access.

Greater security

Consensus on statistics accuracy is needed from all community individuals, and all verified transactions are immutable due to the fact they're recorded permanently. No one, now no longer even a machine administrator, can delete a transaction.

More efficiencies

With a dispensed ledger this is shared amongst individuals of a community, time-losing report reconciliations are eliminated. And to hurry transactions, a fixed of rules — referred to as a clever contract — may be saved at the blockchain and performed automatically.

1.2 Key factors

Distributed ledger technology

All community members have get right of entry to the disbursed ledger and its immutable file of transactions. With this shared ledger, transactions are recorded the best once, disposing of the duplication of attempt that's normal of conventional commercial enterprise networks.

Immutable records

No player can alternate or tamper with a transaction after it's been recorded to the shared ledger. If a transaction file consists of an error, a brand-new transaction ought to be brought to opposite the error, and all transactions are then visible.

Smart contracts

To velocity transactions, a hard and fast of rules — referred to as a clever agreement — is saved at the blockchain and achieved automatically. A clever agreement can outline situations for company bond transfers, encompass phrases for tour coverage to be paid and lots more

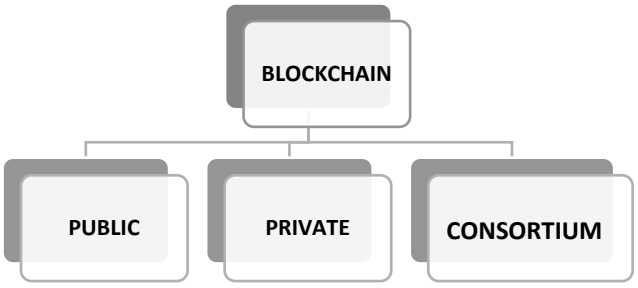

Fig -1: Types of Blockchain

2. LITERATURE REVIEW

Corda, designed especially for the finance enterprise tackles the problems of privateers and scalability however attaining a consensus at the individuals concerned with inside the transaction stage and now no longer with inside the disbursed ledger stage making it higher applicable for the Financial enterprise.[5]. Send the encrypted personal user information to the institutional user node [1]. Sensor device placed on patient's body collects health data and transmits data packets through nearest radio access point [2].Introduce classes of security problems in Ethereum Smart contracts [3].The integration of blockchain with 5G and healthcare system can be a "cure" for 2 and 4 healthcare pain points [4]. To ensure the privacy of records, it can be encrypted by the hospital using the public key of the patients. However, Public Key Infrastructure-based key sharing is not feasible because of various factors such as cost and a digital certificate for every patient [6].

The current structures have sure flaws in its control and protection making it liable to protection assaults and making exclusive affected person facts at a completely excessive risk. Keeping this in mind, authors attempt to clear up this trouble with the aid of using introducing the concept of blockchain and clever settlement gadget which makes use of encryption and decentralized nodes in its method to offer protection.

3. CORDA

3.1 R3 Corda Language

The code in Corda is written in the usage of Kotlin, a programming language from JetBeans that goals the JVM and JavaScript. The principal cause for choosing Kotlin is the excessive stage of integration. Due to the JVM, any associated programming paradigm may be used.

Corda has 'pluggable' uniqueness services. This is to decorate privateers, scalability, prison-tool compatibility and algorithmic agility. A single provider may be composed of many on the identical time non-trusting nodes coordinating via a Byzantine fault tolerant algorithm, or may be very simple, like a single tool. In some cases, like whilst evolving a state requires the signatures of all relevant sports, there may be no need for a uniqueness provider at all.

These uniqueness services are required handiest to attest whether or not or now no longer or now not the states fed on thru manner of manner of a given transaction have previously been fed on; they will be now no longer required to attest as to the validity of the transaction itself, that is an trouble for the sports to the transaction. This approach that the distinctiveness services are not required to (and, with within the famous case, will now no longer) see the complete contents of any transactions, appreciably improving privateers and scalability of the tool in assessment with possibility allotted ledger and blockchain designs. This format preference represents an essential desire as to the proper trade-offs in shared ledger architectures.

3.2 Scalability and Privacy

The pluggable uniqueness provider in Corda and using shared cryptographic hashes to ensure restrictive viewing of transactions cope with the scalability and privateers issues.

Corda commenced as an international ledger. In case whilst the transaction entails a small subgroup of events, corda strives to maintain the applicable records in basic terms in the subgroup.

The basis item is a kingdom item that statistics the existence, content material and present day kingdom of a settlement among or extra events. It is meant to be shared most effective with the ones who've a valid purpose to look it. To make sure consistency in an international, shared machine wherein now no longer all records is seen to all participants, Corda is predicated closely on secured cryptographic hashes to become aware of events and records. The ledger is described as a hard and fast of immutable kingdom objects.

The modularity and interoperability of Corda permits establishments to combine already present setup, consisting of databases, into the Corda network.

3.3 Governance

Corda is a permissioned blockchain which gives the manipulate of Governance to R3 and the organizations taking detail with within the transaction.

3.4 Smart Contract

Corda allows smart contracts. Smart contracts in Corda are agreement whose execution is every automatable thru manner of manner of laptop code taking walks with human input and manipulate, and whose rights and obligations, as expressed in a prison prose, are legally enforceable. The smart agreement links organization now not unusual place revel in and organization statistics to an associated prison prose to ensure that the economic agreements on the platform are rooted firmly in law and can be enforced with within the event of ambiguity, uncertainty or dispute.

Corda enforces organization now not unusual place revel in via smart agreement code, it honestly is constructed as an herbal function that each accepts or rejects a transaction, and which can be composed of simpler, reusable functions.

Contracts define a part of the economic organization now not unusual place revel in on the ledger, and they will be mobile: Nodes will down load and run contracts indoors a

sandbox without any assessment in some deployments, regardless of the reality that Corda envisages using signed code for Corda deployments with within the regulated sphere.

The virtual tool determined on for agreement execution and validation is the Java Virtual Machine. However, virtual tool has been augmented with a custom sandbox that is significantly more restrictive than the everyday JVM sandbox, and it enforces now no longer handiest protection requirements but moreover deterministic execution.

3.5 Consensus

In Corda, there are elements of consensus:

· **Transaction validity**: sports can gather fact that a proposed possibility transaction defining output states is valid thru manner of manner of checking that the associated agreement code runs efficaciously and has all of the required signatures; and that any transactions to which this transaction refers are also valid.

· **Transaction uniqueness:** sports can gather fact that the transaction in question is the suitable customer of all its input states. That is: there exists no precise transaction, consensus have been reached (validity and uniqueness), that consumes any of the identical states.

Parties can agree on transaction validity thru manner of manner of independently strolling the identical agreement code and validation now not unusual place revel in.

4. NOTARY

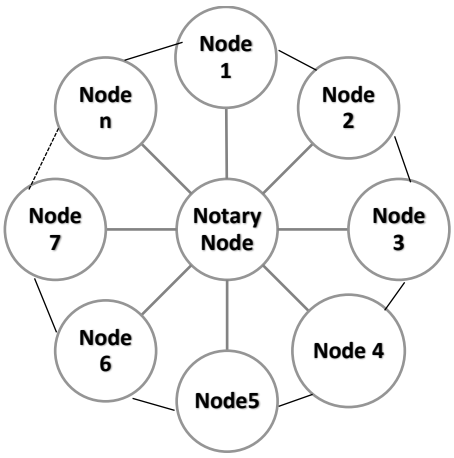

Fig -2: Notary Node

A notary is a network provider supplying uniqueness consensus for a given transaction. Notary offers the element of finality with within the tool. Parties can't make certain that a similarly valid, but conflicting transaction is appeared as a valid, attempt to spend the given input state until the notary signature is obtained. Each state has an appointed notary, and the notary will handiest notarize the transaction if it's far the appointed notary of all of the transaction's input states.

Notary service is a part of a node on the Corda network that turns a regular node into a notary node. A notary is an authority in the Corda platform with the aim to provide consensus.

Notary clusters prevent "double-spends" and provides time stamping authorities.

4.1 Duties of a notary encompass the following:

• Identifying fraud

• Affirming the kingdom of thoughts of collaborating parties

• Verifying and recording the identity of settlement participants

• Completing notarial certificates on all documents

• Bearing witness to documents/objects in a secure deposit box

• Maintaining a notary journal

• Administering oaths

• Taking affidavits and statutory declarations

• Handling mortgage documents, contracts, marriage certificates, and different criminal documents

5. BLOCK

In Blockchain blocks are recorded in chronological order. Once the data is recorded, it cannot be changed or altered by hackers. A block is a record book which contains the details of transaction data. Block consist of four details:
Each blocks holds the hash value of previous block. Genesis block doesn't contain previous hash value since it's the first block in the blockchain. Transaction data contains the details of several transactions. Nonce is a random value, and Hash is an alphanumeric value which is used to identify a block.

- Hash of Previous Block
- Transaction data
- Nonce
- Hash

Every block consists of a hash of the preceding block (determine block) besides or a Genesis block. Imagine a string of blocks with hashes of determine blocks. If the statistics in this kind of blocks is changed, it impacts all different chain blocks. However, because the community grows, converting hashes throughout all of the blocks will become nearly impossible. Therefore, the hashing system is vital for the blockchain, making sure the individuality and originality of every detail of the system.
Immutable and truthful statistics is one of the blockchain's center properties, making it treasured and giving gigantic capacity to the blockchain.

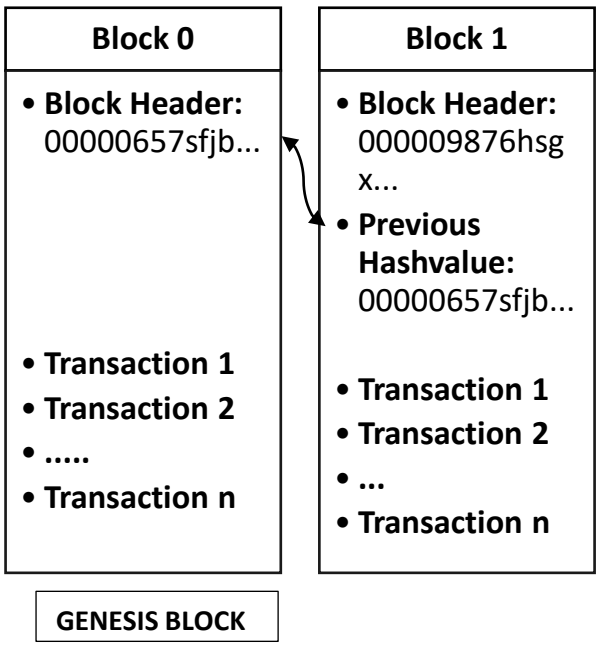

Fig -3: Block contents

6. MINING

Mining is a "guessing game". Guessing a random number to secure a block using hashing. Powerful computer user wins the game.

6.1 Types of Mining

The system of mining can get certainly complicated and an everyday laptop or PC can't reduce it. Hence, it calls for a completely unique set of hardware and software program that works properly for the consumer. It enables to have a custom set unique to mining sure blocks.

The mining system task may be divided into 3 categories:

Individual Mining

When mining is completed via way of means of an individual, consumer register as a miner. As quickly as a transaction takes place, a mathematical hassle is given to all of the unmarried customers within side the blockchain community to resolve. The first one to resolve it receives rewarded.

Once the answer is found, all of the different miners within side the blockchain community will validate the decrypted fee after which upload it to the blockchain and hence confirm transaction.

Pool Mining

In pool mining, a collection of customers works collectively to approve the transaction. Sometimes, the complexity of the records encrypted within side the blocks makes it tough for a consumer to decrypt the encoded records alone. So, a collection of miners works as a crew to resolve it. After the validation of the result, the praise is then cut up among all customers.

Cloud Mining

Cloud mining removes the want for pc hardware and software program. It's a hassle-unfastened approach to extract blocks. With cloud mining, managing all of the machinery, order timings, or promoting earnings is not a regular worry.

Blockchain era have become the maximum influential improvements of the beyond century that decided the destiny improvement of technologies. Hashing is a cryptographic feature that empowered this era. It's important to recognize what's hashing and the essence of era to mining in a blockchain and earn on it.

Hashing is the plaintext stored in the form of message digest. The Output of the hashed value will be 256 bits and contains the nonce value at the starting of the hash value. Nonce is a randomized set of digits used to vary the value of hash.

Hash generated from the record + last hash, so each entry depends on the previous record. Nonce number is added at the end of each record. Nonce is the number used only once.

7. COMPUTATION

Edge computing are group of local micro data centres that take some of the burden off the cloud. Regional office handles local computing tasks instead of sending it to a central data center which is thousands of miles away.
Edge gadgets can make a contribution to a cloud, if the garage and computing talents furnished via way of means of the ones gadgets on the endpoints of a community are abstracted, pooled, and shared throughout a community—basically turning into a part of a bigger cloud infrastructure.
Edge computing isn't always a part of a cloud. What makes aspect computing so beneficial is that its miles purposefully cut loose clouds and cloud computing.
Edge computing is break away clouds for two essential reasons:
Time sensitivity. The fee at which a selection desires to be made doesn't permit for the lag that might typically take location as facts is amassed via way of means of an aspect tool, transferred to a vital cloud with out modification, after which processed earlier than a selection is despatched returned to the threshold tool for execution.
Data quantity. The sheer quantity of facts amassed is an excessive amount of to send—unaltered—to a cloud.

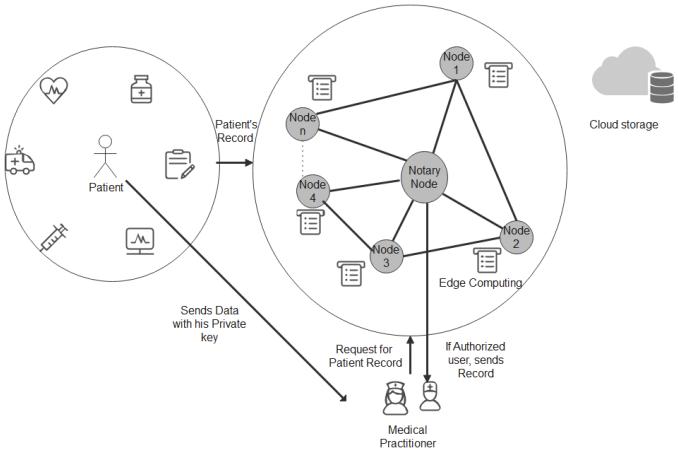

Fig -4: Record access process

Fig -4 explains how the patient records stored in the blockchain based on the notary based service, where the notary node is elected on voting the node by all the nodes in the network. The notary node ensures whether the node is an authorized user. Everyone in the network has a copy of the Blockchain, which is used for ensuring that the data remains untampered. Even one of the node got corrupted can be known by other nodes and can be rectified as soon as possible. The patient have the full control over his record. If any medical practitioner needs patient previous health records, which stored in blockchain. The user should send his private key to the doctor, now the doctor using the patient's private key along with his private key can only access his records for a particular period of time. Therefore, patient's data will become secured and the patients have the privacy of his own records.

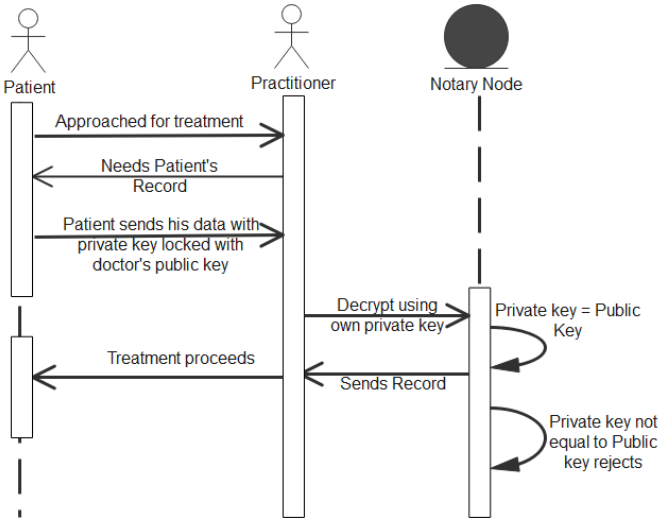

Fig-5 Patient record request

From figure 5, when patient approaches the Doctor for treatment, his report was already stored in blockchain. When the Doctor wants to refer his past records. It's not safe for the patient to carry his record everywhere to the hospital. The reports saved in the blockchain benefits the patient by not losing his reports and can be accessed whenever needed. Now the report in the blockchain was locked by the patient using his private key. When the doctor asks for the report he shares his data with his own private key to the doctor. Now Doctor decrypts the data with his private key and sends a request to the blockchain to deliver the report. If the Doctor is a valid user then the data will be sent, or else rejected. The privacy is given to the patient to control his own record.

8. CONCLUSION

Raft-based notary service used as a consensus algorithm because of high efficiency and simplicity. Corda Blockchain provides real-time processing with better performance. Raft-based notary service used as consensus mechanism to validate data. To avoid brittle in network during offline Edge-Cloud Computing is proposed.

REFERENCES

[1] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, ``Making smart contracts smarter,'' in Proc. ACMSIGSAC Conf. Comput. Commun. Security, Oct. 2016, pp. 254269.

[2] Kedir Mamo Beshar, Zareen Subah and Mohammed Zamshed Ali (2020). IoT Sensor Initiated Healthcare Data Security. IEEE Sensors Journal, Vol.21, No. 10, 2021.

[3] Michel Rwibasira, Dr. Suchithra R (2020). A Survey Paper On Consensus Algorithm Of Mobile-Healthcare In Blockchain Network. International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).

[4] Khalimjon Khujamatov, Ernazar Reypnazarov (2020). Blockchain for 5G Healthcare architecture. 2020 International Conference on Information Science and Communications Technologies (ICISCT).

[5] https://micobo. medium.com/technical-difference-between-ethereum-hyperledger-fabric-and-r3-corda-5a58d0a6e347

[6] S. Namasudra and G. C. Deka (eds.), Applications of Blockchain in Healthcare, Studies in Big Data 83, https://doi.org/10.1007/978-981-15-9547-9_5

[7] Wood, G. (2014). ETHEREUM: A secure decentralized transaction ledger. Yellow paper. Golang - The Go Programming Language. https://golang.org/.

[8] Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., & Zhang, X. (2017a). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), p. 44.

[9] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017b). MeDShare: Trustless medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757– 14767.

[10] Yip, K. (2016). BlockChain and alternative payment models. White paper, https://www.healthit.gov/sites/default/files/15-54-kyip_blockchainapms_080816.pdf. Last accessed 14 February 2018.

[11] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), Feb. 2017, pp. 492–496.

[12] RSS. IoT Explained—How Does an IoT System Actually Work? Accessed: Nov. 28, 2019. [Online]. Available: https://www.leverege. com/blogpost/iot-explained-how-does-an-iot-system-actually-work

[13] Wipro. IoT in Healthcare Industry: IoT Applications in Healthcare. Accessed: Nov. 28, 2019. [Online]. Available: https://www. wipro.com/en-US/business-process/what-can-iot-do-for-healthcare-/

[14] S. Sodagari, B. Bozorgchami, and H. Aghvami, "Technologies and challenges for cognitive radio enabled medical wireless body area networks," IEEE Access, vol. 6, pp. 29567–29586, 2018.

[15] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," IEEE Internet Things J., vol. 6, no. 1, pp. 410–420, Feb. 2019