CRIMINAL RECORD KEEPING WITH BLOCKCHAIN

[1] Purvi Makwana, [2] Dr.Priyanka Sharma

[1] Post Graduation, Cyber Security, M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India

[2] Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

For any infrastructure, database are highly conserved information. With the growing digitalization, the database are also need to manage digitally. Simultaneously attacks are also raising, therefor it's hard to manage database. Blockchain is best solution for database management. Blockchain with decentralized nature gives an integrity, authenticity and transparency of data. This research paper explained about where block chain technology can applicable for criminal record management cities. Which is help to authorities (court of law, government bodies) can easily access the data. Moreover this paper evaluate the crime chart based on criminal record. Using block chain technology time, cost, and paper work and also corruption will decrease.

KEYWORDS: blockchain, criminal record, recordkeeping, blockchain record management

INTRODUCTION:

An important function of government is to maintain trusted information about individuals, organizations, assets, and activities. Local, regional, and national agencies are charged with maintaining records that include, for instance, birth and death dates or information about marital status, business licensing, property transfers, or criminal activity. Managing and using these data can be complicated, even for advanced governments. Some records exist only in paper form, and if changes need to be made in official registries, citizens often must appear in person to do so. And, of course, these data must be protected against unauthorized access or manipulation, with no room for error.

There are many ways to verify the authenticity of paper documents, including watermarks, signatures and embossed seals. But there is also a drawback as paper can be misplace, hard to store and finding a particular record, take time for copying and editing, hard to share, and major was security of data. Therefore, digital records are introduce. Documents in digital form can be modified and copied with no one being the wiser. Also data process speed is increased and reduce the possibility of error in data. There are many products and services that provide secure and verified document management, but they can be expensive and often require the involvement of a third party. A Central database can be hacked by many attacks which may effect on security and integrity of data. Any organization or systems core part is database. Every system laid on database. So database or record are important part of any system or process or organization. SQL injection attacks have become more common in recent days [1]. SQL injection is a highly destructive attack in which hackers try to access information stored in a database [1].

BLOCKCHAIN LOG KEEPING SOLUTION:

Blockchain is an important technology for records management professionals to understand because it has broad implications for securing and authenticating data at lower cost and higher efficiency. It does this by embedding authentication into the document itself and using a closed loop tracking system to protect against tampering or modification. If you've ever used a synchronized file-sharing system like Drop Box or Microsoft One Drive, you know basically how the process works. Those services enable people to share files and retain local copies by synchronizing the files between everyone who shares them. If one person changes a document, the new version is automatically copied to everyone else's local folder.

Blockchain works the same way, but it adds a layer of code called a block to the process. A block is just a sequence of unique letters and numbers protected by a highly secure form of encryption called public key. The use of public key encryption is important because it enables the owner of the information to control it without giving up personal information like names or Social Security numbers. Every party in a blockchain network gets a "golden copy" of the document containing the embedded block. If the document changes, a new block is added and the revised file is synchronized throughout the network, a process that usually takes just seconds. As more changes are made, new blocks are added, forming a chain. That blockchain is both an audit trail and a version tracking system. Each block represents an earlier version of the document, enabling anyone to backtrack to see what was changed.

WHY IT MATTERS:

Here are some reasons records management professionals should become familiar with blockchain.

Cost savings - This is the most obvious benefit. Because blockchain transactions don't require intermediaries, processes can be made more efficient and less expensive. There's no need for auditors or legal professionals to validate the authenticity of information, so those costs come out of the process.

Efficiency - Fewer people means faster turnaround. Transactions that might take days waiting for multiple sign-offs can be concluded in seconds.

Security - The fewer participants there are in a transaction, less risk there is that something could go wrong. Handoff points are a prime vulnerability, and blockchain effectively eliminates them.

Flexibility – Any digital asset can use blockchain, including difficult-to-protect items like multimedia and email records.

Competitive advantage - Companies in the intellectual property space – such as law firms and stock photo agencies – can consider using blockchain to offer new services that benefit both buyers and content creators.

TYPES OF BLOCKCHAIN:

1. Public blockchain: It means everyone can check and verify the transaction also can participate in it. For ex. Bitcoin and Ethereum are both Public Blockchain.
2. Consortium blockchain: It means the node that had authority can be choose in advance, usually has partnerships like business to business, the data in blockchain can be open or private, can be seen as Partly Decentralized. For ex. hyper ledger and R3CEV are both consortium blockchain.
3. Private Blockchain: the node is restricted only authorized can access and participate in it.

Hyper Ledger Fabric Platform:

You can make building for your own blockchain applications using hyper ledger Fabric. It makes different from other known blockchain systems in case of private and permissioned. Before participants can be part of the network, all contributors must be enrolled through a trusted Membership Service Provider (MSP) [8].

Without verification of participant no transaction is permitted. There is no need for proof-of-work or other protocols that are used in Bitcoin or Ethereum, when all participants are known. A participant in permissioned network can be allowed invoke smart contract, but not allowed to deploy a new one. A separate channel can be created for private, confidential transactions. Participants of the channel can only view the data. Distributed ledger is shared between all nodes.

It is contain two data structures-: transaction log and world state.

The transaction log cannot be replaceable and is built in. New world state is agreed and written after accepting new block with transactions. World state describes the end state of sequential transactions [8].

Nodes:

The system contains three types of nodes: peers, client and orderers. The client is the node that represents the end-user. Also it connects to peers and orderers for updating the data. SDK is provided in Java, JavaScript (Node.js) and Go. Chaincode means peer managing digital ledger data, transactions and runs smart contract.

The ledger consists of two components: • transaction log

• world state.

The transactions change the world state by using chaincode. Transaction considered as a deploying a new chaincode. The chaincode will be signed and system creates an unchangeable package of the chaincode[8].A separate Docker image is created with version tag and it is running as a separate machine. This will ensure that the peer will not crash without something happens within the chaincode. Peers will run the chaincode on a channel, a separate ledger, and one peer can run multiple channels. Hyperledger Fabric depends on certificates, the same ones used by HTTPS protocol. In certificates every move is signed, so there is no users in perspective of system. Advance certificates can be created, but for enterprise applications that would be too static, there for a separate service called Fabric CA is provided to dynamically generate certificates for users[8]. Persistence is provided by MySQL, PostgreSQL or LDAP server. Orderer is agreement service that purpose is to quarantine that for all participants, their all transactions would be same in order and it send them as a block to all peers, which will persist as a block to the ledger. There are multiple implementations supported, SOLO a single instance well-known distributed streaming platform for developing and Apache Kafka. Kafka used Apache ZooKeeper, well-known coordination service, for providing group services, distributed synchronizing and maintaining configuration information. The work of adding Simplified Byzantine Fault Tolerance is on the way. This is one of the strengths of the system, it is built modular and is possible can change the consensus service as needed. Each peer has a world state database kept in a key-value store LevelDB or document-oriented database called Apache CouchDB. Latter enables chaincode to execute complex queries on blockchain data[8].

Chaincode:

Chaincode known as a smart contract in Hyperledger Fabric. It is a program, written in Go, Node.js or Java language. The lifetime programming language developing vast libraries enable to use. Chaincode runs in an isolated Docker container. For that to use existing API and make the migration easier. Chaincode purpose is to be the business layer in software development. Deployment of new chaincode is two-step process. In the first step the code is deployed to all peers file system. Second step is called instantiate for new code and upgrade for upgrading existing chaincode. The second step is for actually deploying the code into production[8]. Deployment of chaincode going through the same process as transactions and requires that all peers sign the new chaincode. When deploying new chaincode, it is possible to assign policy, of which peers must sign transactions running this chaincode. Chaincode can be deployed via CLI or by using SDK. To implement permissioned ledgers, platform offers channels. Chaincode is running on the channel as a separate ledger. Same Chaincode can run on different channels, similar how same server software can run on different client environments. It is possible to invoke other chaincode and even chaincode in another channel[8]. Channels can be used to keep private data safe to other members. When channel is set up between subset of members, the blockchain data is physically available only to the participant's nodes. Hyperledger Fabric latest adds a possibility to encrypt part of data using built in functions. Use this built in functionality enables even querying the encrypted data. The safekeeping of encryption key is trusted to the client.

Processing of transactions, Transaction management is split between peers and orderers. This allows higher parallelism and concurrency for the network. Every transaction is executed in the peer using world state. If the transaction succeeds, it is signed with Peers certificate. Executing transactions before ordering allows each node to process multiple transaction at the same time. The orderer will not re execute the transaction, just order them and do not maintain ledger. This also enables the peers to trust all orderers and vice versa, so they can run independently. Peers are divided into endorsing peers (peers that contain specific chaincode and are part of the policy) and peers without the chaincode. Peers without the chaincode can still validate and commit the transaction to their ledger after receiving it from the endorsing peer [8].

CONCLUSION:

Government or public records are often tampered by various attacks and it effect are dangerous. Protect a record or data without third party, blockchain is the best solution. Criminal record is very crucial information. For its protection we create a web application using hyper ledger fabric. It is differ from other framework because of privacy issues, scalability, and an immutability of smart contract, storage issues, and unsustainable consensus algorithm. For uploading or accessing data digital signature confirm the authenticity of data. Furthermore encryption and pair of keys are used for securely storing the data in blockchain. All this are together provide a maximum security to criminal record. The data are stored in Ethereum platform therefore any authorized node or client can access it. So each criminal record can access by another city police. That can solve a timing issue and it is transparent so any client can track their complains.

REFERANCES:

1. M. S. R. Maisha Afrida Tasnim1 and M. Z. A. Bhuiyan3, “CRAB: Blockchain Based Criminal Record Management System,” *springer,* 2018.
2. J. Moubarak, E. Filiol and M. Chamoun, “On Blockchain Security and Relevant Attacks,” *IEEE,* 2018.
3. “From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues,” *IEEE,* 2018.
4. R. N. M. Auqib Hamid Lone, “Forensic-chain: Ethereum blockchain based digital forensics chain of custody,” *Scientific and practical cyber security journal | ISSN 2587-4667.*
5. K.-H. Y. Shi-Cho Cha, “An ISO/IEC 15408-2 Compliant Security Auditing System with Blockchain Technology,” *IEEE,* 2018.
6. Luciano García-Bañuelos Fredrik Milani, Blockchain Application - Case Study on Hyperledger Fabric,Tartu,2018