ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

Implement a High Level Secure Network to Maintain Crime Details Using Blockchain Technology

Budumuru Narendrakumar[1], Dr. K. Venkata Ramana[2]

Department of Computer Science & System Engineering, Andhra University College of Engineering (A), Visakhapatnam, India

ABSTRACT: Block chain is time stamped series of immutable records of a data that is operated by a group of computers not owned by a single entity. Each of these blocks of data is secured and bounded to each other using cryptographic principles. In this paper, we built a network with administrator and clients. Administrator will maintain crime data in IPFS. Depends on the client request administrator provides the reference case. Here we use SHA 256 to generate the hash transaction to create a relationship between administrator and client. So that trust can be built between the smart contract system.

KEYWORDS: Blockchain, IPFS, SHA 256, Smart-contract.

I. INTRODUCTION

Blockchain is a technology emerged to facilitate exchange transactions and eliminate the need for a trusted third party to notarize and verify such transactions as well as protects data security and privacy. A new structure of Blockchain has been designed to accommodate the need for this technology such as Law enforcement. In the Law Enforcement every registered criminal case maintains a data base. Mainly the project is used to reduce the investigation time of any case.

Blockchain is a decentralized network system, and highly provide security for a data. It is a growing list of records for every transaction, called blocks, which are linked using cryptography. Each block contains a Cryptographic hash of the previous block, a timestamp, and transaction data. Blockchain technology runs on Ethereum platform, and it is implemented by using solidity language. Not only in solidity, the serpent influenced by python and LLL influenced by lisp also implanted Blockchain technology. But the solidity language is most popular to implement Blockchain technology. The data base is stored in IPFS this is one type of online data store place.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

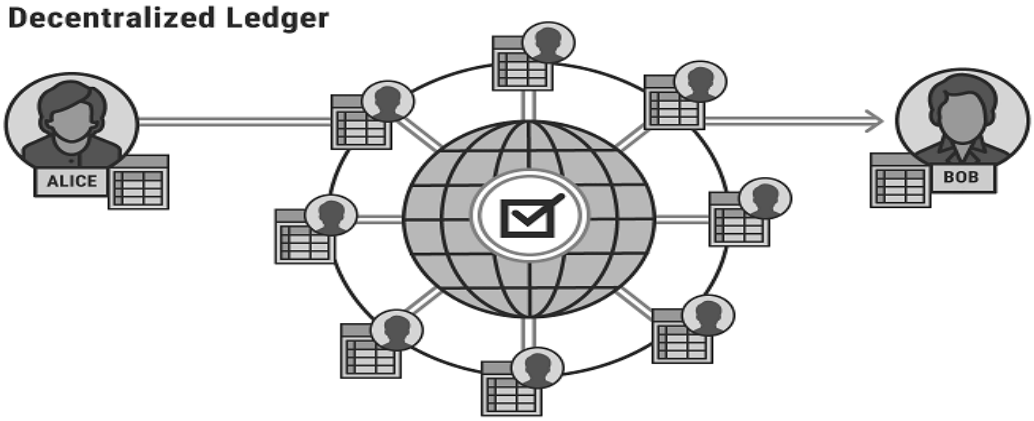

Fig.1. Decentralized Network

Block Chain model is cropped in two ways:

Permission less Blockchain:

Permissionless Blockchain is nothing but we don't need any permission to be a part of block chain network or block chain. The data or the transaction details stored in this permission less Blockchain, these are validated by the public present in that network or block chain.

Permission Blockchain:

Permission Blockchain is also called as Private Blockchain. In this Blockchain, we should require permissions to be a part of network because everyone may not be a part of a network.

Some of the key characteristics of a Permission and Permission Less system:

- Decentralization
- Transparency
- Anonymity
- Governance
- Tokens
- Scalability and performance.

In this paper we are using permission Blockchain, because of admin gives permission to client for access data from IPFS.

Today's network is inefficient and expensive, centralized, limiting opportunity. Those are disadvantages of present web. One thing is overcome by all the disadvantages of network i.e., IPFS. The IPFS is nothing but a distributed web. It is mainly use to share large files in online and maintain very large amount of database. In IPFS we can store all type of data like text and photos and video also IPFS provides hash value for every individual files or records. Files and records can be shared based on the hash value. The hash value must contain 46 bit length and starting two letters are 'Q' and 'm'. Otherwise the hash values is not valid.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

A smart contract may well be a computer protocol meant to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Wise contracts allow the performance of credible transactions where as not third parties. These transactions are unit traceable and irreversible. Proponents of wise contracts claim that many kinds of understanding clauses may even be created half or completely self-executing, self-enforcing, or both. The aim of wise contracts is to provide security that is superior to ancient law and to chop back totally different dealings costs associated with catching. Varied crypto currencies have enforced forms of wise contracts.

In Blockchain technology SHA-256(secure hash algorithm) algorithm is used for encryption and decryption data. The SHA256 algorithm is generate the 256-bit code for any data.

II. RELATED WORK

We have studied papers based on Blockchain technology and crime investigation process. Some of the papers describe how to provide security and security types for a network by using Blockchain technology, and also implement a private Blockchain and data transformation between peer to peer networks. Remaining papers describe how to start investigation process for a case, finding the proofs, how to solve a case with reference case and without reference case and also explore how to access the reference case if it is in centralized crime database.

"Wu Lifeng, Wang Yinao", the author proposed, **"Grey System Model of Criminal Investigation and Solving Cases",** in this paper, they introduce based on the principles of informational differences, non-uniqueness, minimal information, recognition base and acquiescence of the grey system theory, grey natures of the criminal investigation and solving cases are analyzed. Basic steps of building gray system model and designing relevant computer program of assistant criminal investigation and solving cases are put forward [1].**"Qiuhong Zheng,"** the author proposed, **"An innovative IPFS-Based Storage Model for Blockchain",** this paper proposed an IPFS-Based Blockchain data storage model to solve this problem. In this paper, the miners deposit the transaction data into the IPFS network and pack the returned IPFS hash of transaction into the block. Utilizing the characteristics of the IPFS network and features of IPFS hash, the block chain data is greatly reduced. The scheme is applied to the Bitcoin block chain. According to the experimental results, the compression ratio can reach 0.0817. According to the analysis, it also has good performance in terms of security and synchronization speed of new node [2].**"Raj Patel",** the author proposed, **"Blockchain – Future of Decentralized Systems",** this paper reviews the study of Blockchain technology and articulates the need and concept, which establishes it as a suitable alternative to conventional methods, its distinct types, the actors involved, the working of Blockchain and the execution of a transaction on the Blockchain. The main methods of finding consensus are explained. A brief comparison to centralized systems has been done and its strengths and weaknesses have been outlined. Furthermore, its applications in various domains are discussed in detail. An overview of currently live applications in these domains like bitcoin for crypto currency is made, and the role of Blockchain in these applications is discussed [3].**"Weiqin Zou, David Lo"**, the authors proposed**, "Smart Contract Development: Challenges and Opportunities"**, this paper focuses on the study of exclusively on this subset of smart contracts. Such smart contracts have increasingly been gaining ground, finding numerous important applications in the real world. In this paper, they performed an exploratory study to understand the current state and potential challenges developers are facing in developing smart contracts on Blockchains, with a focus on Ethereum[4].

III. SYSTEM DESIGN

Existing system:

Now a day's so many criminal cases or some other cases are in investigation state. Some cases are easily solved because those cases don't need any reference case. But some cases need reference case, those cases are waiting until find the reference case. The criminal data base is maintained by center police department in three levels of accessing any reference case. Local polices start investigation process, finds evidences and interrogate the accused person. If case is successfully completed then it is stored in a database. Otherwise the state police department needs reference case from central police department to follow below steps. The state police department request to a state government. The state government will pass this request to a central government. Finally central government passes order to central

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

police department, then the central police department find the reference case in data base. In case, reference case is find then provide to state police department, otherwise suggest how to solve the case.

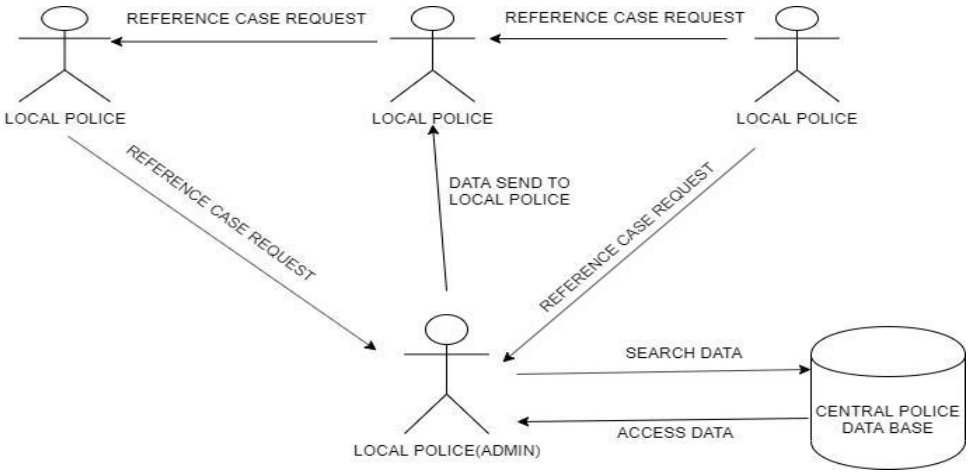

Fig 2: Existing system architecture

PROBLEM STATEMENT:

Implementing a Blockchain network to maintain crime and its details. This network plays a key role in any investigation process of a particular case. This network mainly provides a reference case based on the scenario. If the reference case is not available then suggest how to solve the case in easy manner.

PROPOSED SYSTEM:

Within next few years the pending cases are rapidly increasing. Because the maximum number of pending cases are still in the investigation process because they need reference case. To access the reference case more permission is required from the administrator. This could take long time, so Blockchain technology could be the solution for this problem. By using this technology, the investigation process reduces the maximum amount of time

In proposed system, avoid the present three levels in centralized crime database. In this approach simply we develop a peer to peer system. This approach is used to reduce the investigation time, Local police start investigation process to find the evidences, depends on the evidences request is placed into Blockchain network for reference case without involving the state and central government. The authentication process complete then verify reference case is available or not. If the central crime database has reference case then it provides to local police, otherwise he suggest how to solve the case in an offline mode.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

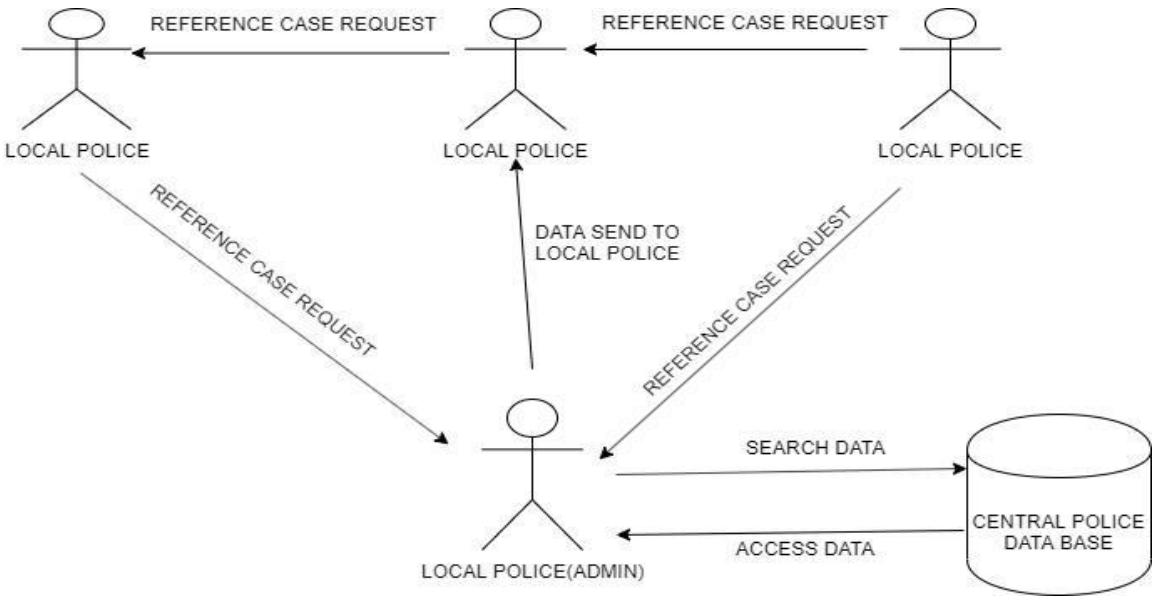

Fig 3: Proposed system architecture

ALGORITHM:

Input: Casename , input , hashvalue

Output: Casename , input value , hashvalue

1. **Begin**

2. Algorithm crime (Casename ,input ,hashvalue ,owner ,client ,authclient)

3. {

4. String memory A<-"case not found";

5. String memory B<-"case found"

6. Casename<-Casename;

7. require(authclient<-_client, ' invalid client');

8.input <-input;

9. if(input<-0)

10. Return A;

11.Else

12. Return B;

13. Hashvalue<-hashvalue;

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

14. bytes memory strBytes<-bytes(_hashvalue);

15. require(strBytes.length<-46,'not valid hashvalue');

16. require(strBytes[0]<-'Q' && strBytes[1]<-'m','enter valid hashvalue');

17. return hashvalue;

IV. IMPLEMENTATION

Step1: Initially the client will send a request to a network. The request is nothing but reference case for present investigation case.

Step2: The administrator first verifies the client details for authentication. After completion of authentication client will search the reference case in IPFS. If the reference case is found then send a message to a network i.e. “the case is found”, otherwise send “the case is not found”. The IPFS hash code must contain 46 bit length and starting two letters are ’Q’ and ’m’. Otherwise the IPFS hash code is not valid.

Step3: The reference case is found then copy hash code of particular case and put in network. Then client copies the hash code and search in IPFS. Finally he got reference case at dashboard.

V. EXPREMENTAL RESULTS

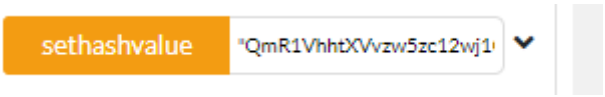

Fig 4: set hash value

Fig 4: Admin copy the hash value of reference case in IPFS and put in set hash value block.

=>In case the hashvalue not valid then display the below error.

[vm] from: 0xca3...a733c **to:** crimedatabase. Sethashvalue (string) 0x692...77b3a **value:** 0 wei **data:** 0xa48...00000 **logs:**0 **hash:**0xd09...47b12

Transact to crimedatabase.sethashvalue errored: VM error: revert. revert The transaction has been reverted to the initial state. Reason provided by the contract: "not valid hashvalue". Debug the transaction to get more information.

=>In case the hashvalue is valid then show transaction like given below:

[vm] from:0xca3...a733c **to:**crimedatabase.sethashvalue(string) 0x692...77b3a **value:**0 wei **data:**0xa48...00000 **logs:**0 **hash:**0x5d0...16edb

Status:	0x1 Transaction mined and execution succeed
Transaction hash:	0x5d0440c6de28518b36c806836a49b917d29e044c954e94176760236041e16edb
From:	0xca35b7d915458ef540ade6068dfe2f44e8fa733c

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

To:	crimedatabase.sethashvalue(string) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
Gas:	3000000 gas
Transaction cost:	86589 gas
Execution:	61733 gas
Hash:	0x5d0440c6de28518b36c806836a49b917d29e044c954e94176760236041e16edb
Input:	0xa48...00000
Decode input:	{ "string _hashvalue": "QmRW3V9znzFW9M5FYbitSEvd5dQrPWGvPvgQD6LM22Tv8D" }
Decode output:	{}
Loge:	[]
Value	()wei

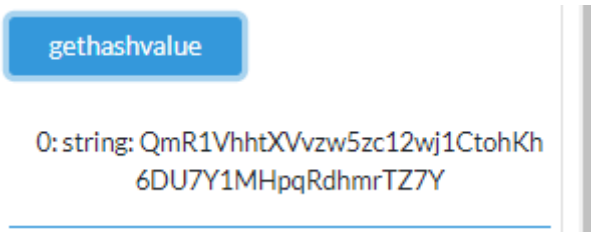

Fig 5: gethashvalue

Fig 5: The authenticate client access the hashvalue after completion of verified hashvalue process.

=>After completion authenticates client access hashvalue process transaction details are displayed in network.

[call]from:0x583031D1113aD414F02576BD6afaBfb302140225**to:crimedatabase.gethashvalue**()**data:**0x287...5de98

Transaction hash:	0xee52e71b3c5f77ae89e4e71b7682fd71f0ad315573575e986edb2c6d9db255a5
From:	0x583031D1113aD414F02576BD6afaBfb302140225
To:	crimedatabase.gethashvalue() 0x692a70D2e424a56D2C6C27aA97D1a86395877b3A
Transaction cost:	23461 gas (Cost only applies when called by a contract)
Execution:	2189 gas (Cost only applies when called by a contract)
Hash:	0xee52e71b3c5f77ae89e4e71b7682fd71f0ad315573575e986edb2c6d9db255a5
Input:	0x287...5de98
Decode input:	{}
Decode output:	{ "0": "string: QmRW3V9znzFW9M5FYbitSEvd5dQrPWGvPvgQD6LM22Tv8D" }
Loge:	[]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

VI. CONCLUSION

In this paper we implement highly secured network for a central crime database. By using this network we can easily access reference case, reduce the investigation process time and avoid three levels network of present centralized crime database.

REFERENCES

[1] Raj Patel and Akhil Sethia and Shyam Patil "Blockchain–Future of Decentralized Systems" 978-1-5386-4491-1/18/$31.00 2018 IEEE.
[2] Wu Lifeng, Wang Yinao "Grey System Model of Criminal Investigation and Solving Cases" 978-1-4244-3531-9/08/ 2008 IEEE.
[3] Qiuhong Zheng and YiLi and Ping Chem "An innovative IPFS –Based Storage Model for Blockchain" 978-1-5386-7325-6/18 2018 IEEE
[4] Oksana Lukmanova, Elena Volkova, Anton Zabolotnyi and Aleksandr Gorelik "Blockchain Technology for Public Utilities" 978-1-7281-0339-6/19 2019 IEEE
[5] Weiqin Zou, David Lo, Pavneet Singh Kochhar, Xuan-Bach Dinh Le, Xin Xia, Yang Feng, Zhenyu Chen, Baowen Xu" Smart Contract Development: Challenges and Opportunities" 0098-5589 (c) 2019 IEEE
[6] Solidity programming essentials , "A Beginner's guide to build smart contracts for ethereum and blockchain", by ritesh modi
[7] V. Singla, I. K. Malav, J. Kaur and S. Kalra, "Develop Leave Application using Blockchain Smart Contract," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2019, pp. 547-549.
[8] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to Know about the Blockchain", IEEE Consumer Electronics Magazine, Volume 7, Issue 4, July 2018, pp. 06–14.
[9] IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3) by Juan Benet, juan@benet.ai
[10] P. Bailis, A. Narayanan, A. Miller, and S. Han, "Research for practice : cryptocurrencies, blockchains, and smart contracts; hardware for deep learning", Communications of the ACM, Vol. 60, No. 5, 2017, pp. 48-51.