

Implement a Block-Chain-Based High-Level Secure Network to Maintain Crime Detail Information

Reddi Swapna, Ch.Usha, Jajula Nalini

Assistant Professor, Department of Computer Science and Engineering,
Dadi Institute of Engineering and Technology, Anakapalle.

swapnareddi1995@gmail.com, chusha@dict.edu.in, nalinijajula@gmail.com

Abstract

Block chain is a time-stamped collection of unchangeable recordings of data that is run by a number of independent computers. These data blocks are all connected to one another and safeguarded using cryptographic concepts. In this study, an administrator and customers were added to a network. The IPFS administrator will keep track of criminal statistics. The reference case is provided by the administrator depending on the customer request. Here, the hash transaction is generated using SHA 256 to establish a connection between the administrator and the client. so that confidence between the smart contract systems can be established.

Keywords: Block chain, IPFS, SHA 256, Smart-contract.

Introduction

Block chain is a technology that was developed to speed up exchange transactions, do away with the requirement for a reliable third party to notarize and verify them, and safeguard data confidentiality and privacy. In order to suit the need for this technology, such as in law enforcement, a new structure of the block chain has been developed. Every criminal case that is registered with law enforcement is kept on file. The project's primary purpose is to speed up any case's inquiry.

Block chain is a de-centralized network solution that offers excellent data security. Every transaction is recorded in a growing collection of records known as blocks that are connected via encryption. Each block contains information on the transactions, a timestamp, and a cryptographic hash of the block before it. Utilizing the solidity programming language, block chain technology is implemented on the ethereal platform. Block chain technology was also implanted by the serpent, which was influenced by python, and by LLL, which was influenced by lisp. However, the most widely used language for implementing Block chain technology is solidity. One sort of online data storage is IPFS, where the data base is kept.

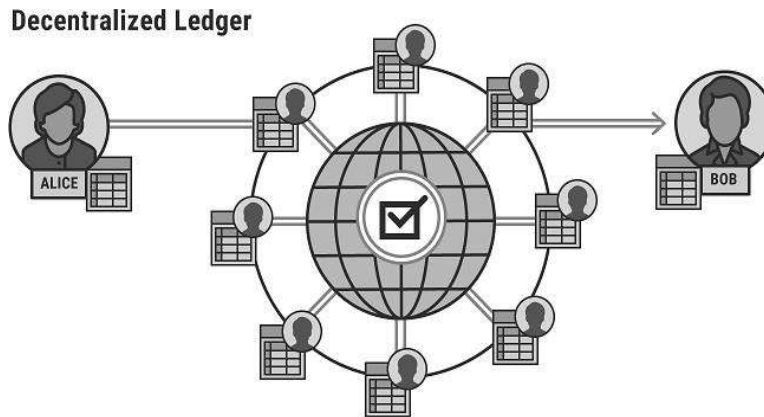


Fig.1. Decentralized Network

Block Chain model is cropped in two ways:

Permission less Block chain:

Permission-less Although block chain is nothing, we can participate in its network or use it without asking for permission. The public who is present in that network or block chain verifies the data or transaction information kept in this permission-less block chain.

Permission Block chain:

Private Block chain is another name for Permission Block chain. We need demand permissions in this Block chain because not everyone will be a part of a network.

Several of a permission and permission-less system's essential features include:

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

We are utilizing permission Block chain because the administrator grants the client permission to view IPFS data. The network of today is expensive, inefficient, and centralized, which restricts opportunities. These are the drawbacks of the current internet. All the network drawbacks are overcome by one item. i.e., IPFS. All that the IPFS is a distributed web. It is mostly used to maintain enormous amounts of database and share huge files online. In IPFS we can

Emerging Trends in Computer Engineering

store all type of data like text and photos and video also IPFS provides hash value for every individual files or records. Based on the hash value, files and records can be exchanged. The first two letters of the hash value must be "Q" and "m," and it must be 46 bits long. Otherwise the hash values is not valid.

The negotiation or fulfilment of a contract may be digitally facilitated, verified, or enforced using a smart contract, which is a computer protocol. Smart contracts permit the completion of legitimate transactions without the involvement of third parties. These transactions are untraceable by unit and final. Many different understanding provisions, according to proponents of sensible contracts, may even be made to be partially or entirely self-executing, self-enforcing, or both. The purpose of intelligent contracts is to reduce all associated catching costs and to offer security that is superior to that of old law. Different crypto currencies have wise contract regulations in place.

In Block chain 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.

Related Work

We have seen studies that discuss the use of block chain technology in criminal investigations. Some of the articles explain how to construct a private Block chain, provide security and security types for a network utilizing Block chain technology, and transform data between peer-to-peer networks. The remaining papers go over how to begin an investigation for a case, how to locate proofs, how to solve a case both with and without a reference case, and how to access a reference case that is stored in a centralized criminal database.

In this study, "Wu Lifeng, Wang Yinao" proposed the "Grey System Model of Criminal Investigation and Solving Cases". The grey natures of conducting criminal investigations and solving cases are examined using the principles of informational differences, non-uniqueness, limited information, recognition base, and acceptance of the grey system theory. The fundamental procedures for developing a model of the grey system and creating pertinent computer programmes for aiding in criminal investigations and case resolution are presented [1].The author of this work, "Qihong Zheng," proposed an IPFS-based block chain data storage model to address this issue in "An innovative IPFS-Based Storage Model for Block chain". In this study, the miners upload the transaction data to the IPFS network and

Emerging Trends in Computer Engineering

include the transaction's returned IPFS hash in the block. The block chain data is significantly condensed by utilizing IPFS hash and network characteristics. The Bit coin block chain is used to implement the scheme. The experimental findings show that the compression ratio might go as high as 0.0817. The investigation shows that it also performs well in terms of security and new node synchronisation speed [2].The author suggested "Raj Patel," "Block chain - Future of Decentralized Systems,".

In this study, the miners upload the transaction data to the IPFS network and include the transaction's returned IPFS hash in the block. The block chain data is significantly condensed by utilizing IPFS hash and network characteristics. The Bit coin block chain is used to implement the scheme. The experimental findings show that the compression ratio might go as high as 0.0817. The investigation shows that it also performs well in terms of security and new node synchronization speed [2].This paper examines the study of Block chain technology and articulates the need and concept, which establishes it as a suitable alternative to conventional methods, its various types, the actors involved, the operation of Block chain, and the execution of a transaction on the Block chain. The author, Raj Patel, proposed, "Block chain - Future of Decentralized Systems."

The primary approaches to reaching agreement are described. Its advantages and disadvantages have been discussed in a brief comparison to centralized systems. Additionally, a thorough discussion of its applications in many fields is included. A summary of the applications that are now in use in these fields, such as bit coin for crypto money, is provided, and the role of block chain in these applications is examined [3]."Smart Contract Development: Challenges and Opportunities," by Weiqin Zou and David Lo, was proposed.

primarily on the examination of just this subset of smart contracts. These smart contracts have gained ground steadily and have a wide range of significant real-world applications. They conducted an exploratory study in this paper with a focus on Ethereum to better understand the existing situation and potential difficulties that developers may encounter while creating smart contracts on Block chains[4].

System Design

Existing system:

There are many criminal cases and other cases that are currently under investigation. Some instances are simple to resolve because they don't require a reference case. However, certain cases require a reference case and are waiting till one is found. The central police department keeps a criminal data bank with three degrees of access to every reference case. Local police launch an investigation, gather evidence, and question the accused. If a case is satisfactorily resolved, a database is where it is kept. The criminal data base is maintained by center police department in three levels of accessing any reference case. Local police launch an investigation, gather evidence, and question the accused. If case is successfully completed then it is stored in a database. In the absence of a reference case from the central police department, the state police department must take the measures below. A state government is asked by the state police agency. This request will be forwarded by the state government to the federal government. Finally, the central government issues an order to the central police department, which then searches its database for the reference case. If a reference case is found, give it to the state police agency; if not, make recommendations for how to solve the matter.

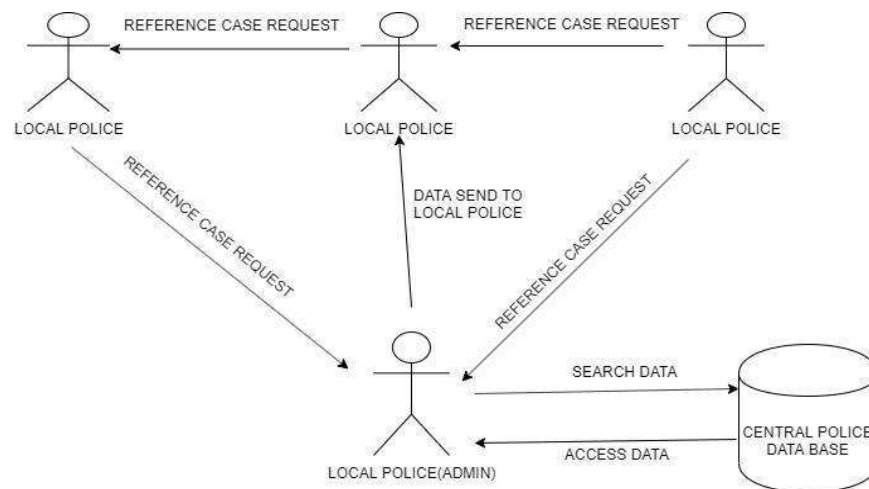


Fig 2: Existing system architecture

Avoid the current three layers in the centralized criminal database in the proposed system. In this method, we merely create a peer-to-peer system. This method is used to shorten the length of the investigation. Local police begin the process of investigating to gather evidence, and depending on the evidence, a request is submitted to the Block chain network for use in reference cases without

contacting the state or the federal government. Once the authentication procedure is complete, you can check to see if the reference case is available. Local police are given reference cases if they exist in the central crime database; otherwise, he suggests an offline solution.

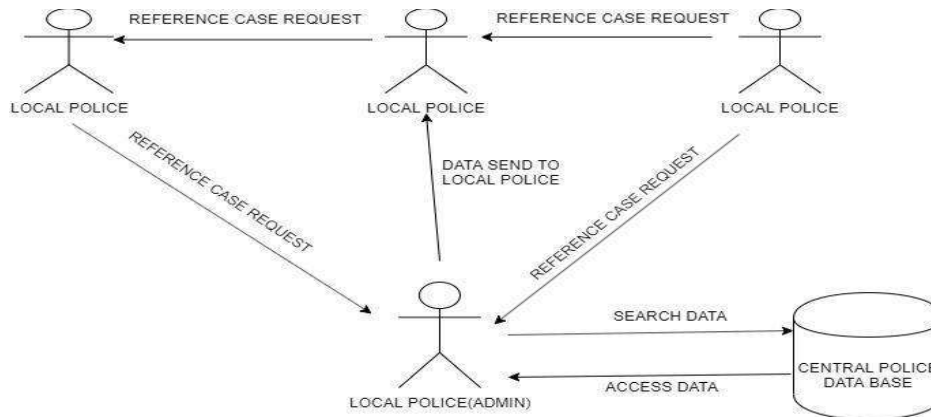


Fig 3: Proposed system architecture

Implementation

Step 1: The client will initially make a request to a network. The request is merely a case study for the current research.

Step 2: Before attempting to authenticate, the administrator first checks the client information. Following successful login, the client will search the IPFS reference case. Send "the case is found" or "the case is not found" to the network in the event that the reference case is located. The IPFS hash code must be 46 bits long, with Q and m as the first two letters. The IPFS hash code is invalid if not.

Step 3: After locating the reference case, the particular case's hash code is copied and entered into the network. Client then copies the hash code and performs an IPFS search. Finally, a reference case appeared on the dashboard.

Conclusion

For a central crime database, we construct a highly secure network. We can quickly access reference cases through this network, speed up the investigation process, and do away with the three-level network of the current 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

Emerging Trends in Computer Engineering

- Investigation and Solving Cases” 978-1-4244-3531-9/08/ 2008 IEEE.
- [3] Qihong 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.