Criminal Records and Reporting System

Prof. S. Sonkamble[1], Arnav Kadu[2], Prithviraj Ghorpade[3], Om Ingule[4], Vineet Dhage[5]

[1,2,3,4,5]Department of Computer Engineering, JSPM Narhe Technical Campus, Maharashtra, India

ABSTRACT

Long with other technologies, Block chain has been used in order to produce felonious data record operation in another system. The conception of the exploration is grounded on the confidentiality of felonious data and conservation from the original Police Officers' perspective. The study aims to contribute to the security protocol of felonious record data through Block chain. The work focuses on the security protocols and the system armature from both the stoner and device' sides. Felonious records are largely sensitive public records. By incorporating felonious records in a block chain, the authenticity and severity of records can be maintained; which also helps to keep the data safe from adversaries. Adding crime rates directly obstruct the growth of any nation thus it's and has always been a primary concern of every nation around the globe to control or maybe have an upper hand on ongoing as well as unborn felonious conditioning. A peer- to- peer pall network enables the decentralization of data. It helps help unlawful changes in the data. This paper introduces a felonious record storehouse system by enforcing block chain technology to store the data, which helps to attain integrity and security. Low- position culprits, who do the legwork in a felonious association are the most likely to be arrested, whereas the high- position bones Tend to avoid attention.

Keywords: Criminal records · Block chain · Authenticity Cloud network · Decentralization · Law enforcement

INTRODUCTION

An important function of government is to maintain trusted information about individualities, associations, means, and conditioning. Original, indigenous, and public agencies are charged with maintaining records that include, for case, birth and death dates or information about connubial status, business licensing, property transfers, or felonious exertion. The ideal of crime data analysis is to identify the structure and patterns which live among the culprits and anti-social rudiments. Similar analysis will help to break numerous unsolved cases and can also give pivotal information to the investigative agency about the association among culprits. Police departments generally maintain their own database in which crime details, apprehensions, geolocation of crime, and important other applicable information related to the crimes are stored. Indeed though these systems are slightly different from agency to agency, the introductory purposes and functions are the same with the growingsize of records, a good record- keeping and information- sharing system has come necessary in moment's globalterrain. The study aims to contribute to the security protocol of felonious record data through Block chain. One of the points of our system is to insure that substantiation information isn't tampered with during court proceedings by storing the data in the pall and keeping the sale log and provenance data in the block chain. In our system, similar problems won't arise since we use block chain to store the data sale logs alongside cracking the data so it cannot be altered. This is a problem in a situation where a police officer refuses to file a complaint against influential people, druggies won't have evidence of registering a complaint. In the being system homemade styles are used for maintaining felonious records which aren't effective data. There's a chance of losing data. This operation will break these problems and give a database for storing data. The being system that's being used by police departments pertaining to the information of the captures, stores the name of the captures, information of the crime, date of FIR, the background of the felonious, and duration of the captivity.

For the felonious justice system to cover public safety and make defensible judgments about people's felonious history, felonious records must be pivotal that felonious records are accurate and current. Yet, inefficiencies, crimes, and a lack of translucency in traditional record- keeping procedures have presented serious difficulties for those involved in the felonious justice system. By enabling safe and decentralized record- keeping, the development of block chain technology has the implicit to offer a result to these problems. Our design is concentrated on creating a block chain-grounded felonious record- keeping and reporting system that attempts to address the failings of conventional record-keeping practices while offering a solid and secure volition for felonious justice stakeholders. The system we propose will give a tamper- evidence library for felonious records, guaranteeing that they're accurate, accessible, and transparent. We can make a decentralized database vulnerable to the same excrescencies anguishing conventional record- keeping ways by employing block chain technology. This will allow felonious justice stakeholders to safely and efficiently access and update records, removing the need for multitudinous sources of information. Our system will have a record- keeping element as well as a reporting medium that will let courts, law enforcement, and other applicable party's access and updatefelonious records incontinently. As a result, agencies will be suitable to work more effectively together and the felonious record check procedure will not be delayed or inaccurate, allowing for judgments to be made grounded on the most recent information.

SYSTEM REQUIREMENTS

Database Requirements

Block chain: Block chain is a decentralized system where there is no central database. So, there is no central point of failure. The database is stored and distributed in various nodes over a peer-to-peer network in blocks.A node can be any electronic device that has a copy of BC on it. The blocks are connected in a chain. Any transactions with the product is stored on all copies of the distributed nodes in the network; these actions thatoccur are immutable, irreversible and time-stamped, and visible to all entities in the chain. The blocks containthe data like- product data, transaction records, the hash of the previous block, the hash of itself, timestamp, etc. which is securely encrypted through hashing algorithms. Even a slight change in any part of information changes the hash code completely causing a mismatch of hash codes in the chain. Thus, it is an efficient way to keep track of every action taking place and avoid hacking of data. Only limited access can be provided to the nodes depending on the sharing contract between them. Thus, customers will have access to the informationabout the product they bought and nothing else. Any wholesaler will have access to information in the previousblock only. If an item travels from one entity to another its data will be stored in BC (Block chain) and thus it will be easy to track it. The Smart contracts between each node can be predefined and replace the involvementof third-party members and enable automatic reinforcement.

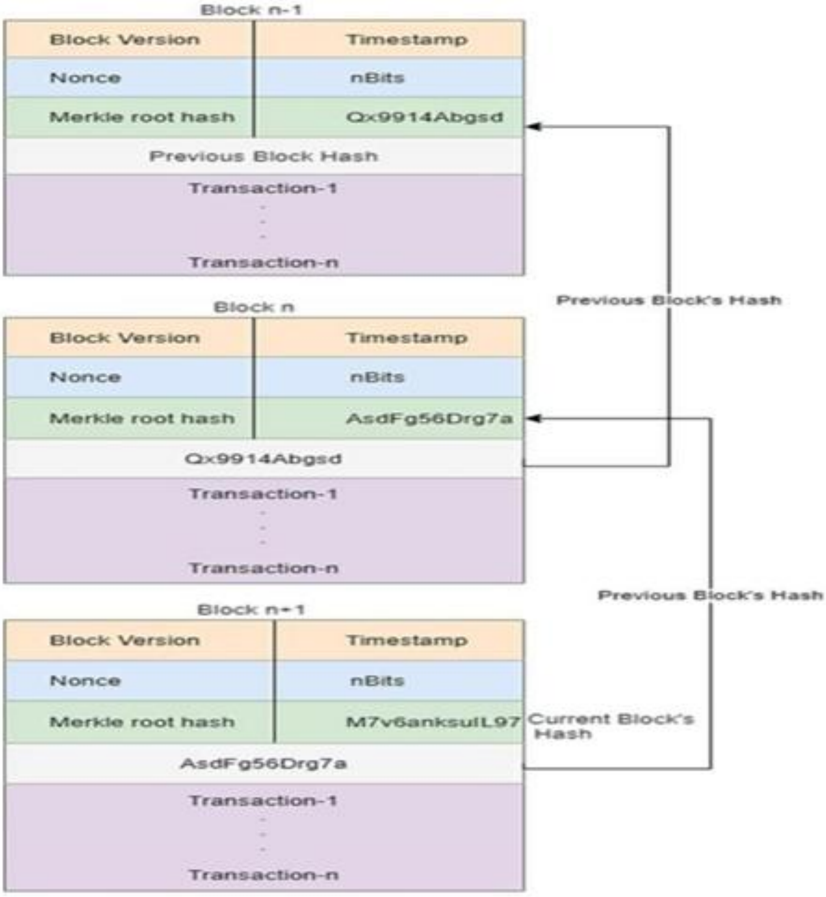
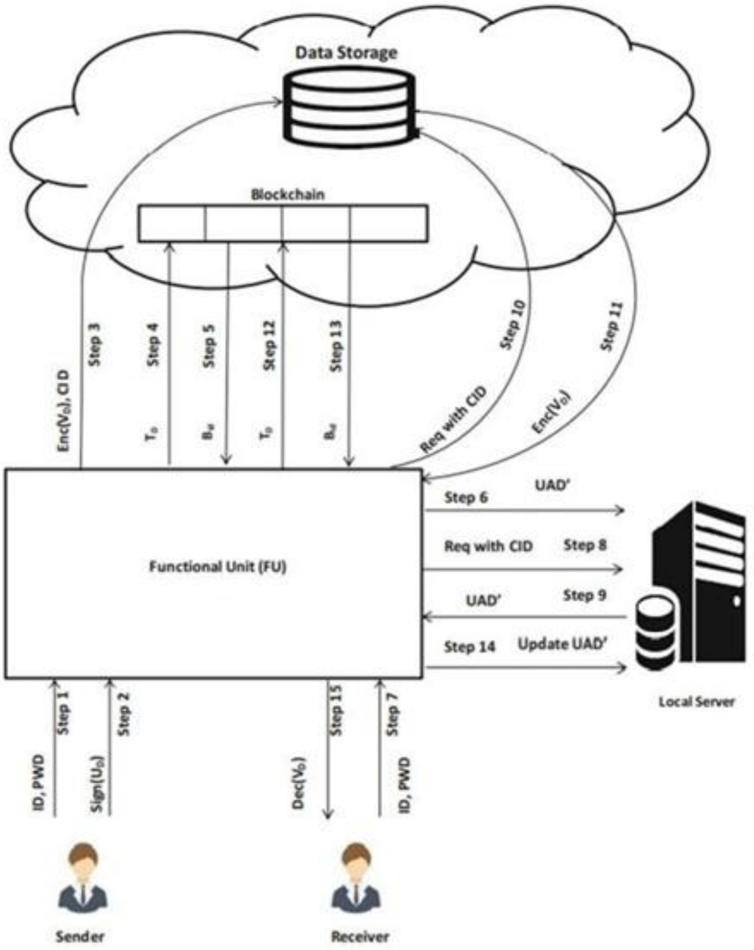
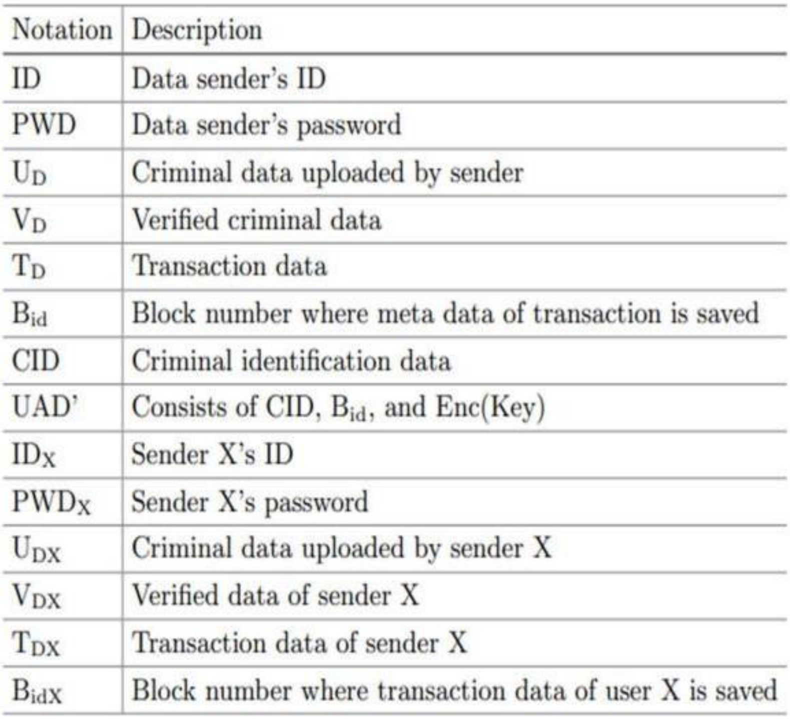


Fig.1 Chain of Blocks

The working of block chain can be explained with the help of an example, suppose if a person has to send moneyto his friend, that simple transaction can be put on the block. The same block also contains other transactions,and it has a fixed size. It is distributed on the network with each and every node. As soon as the transaction takes place, all the participating nodes in the network confirm the transaction using the consensus algorithm decided between the participant nodes in the block chain network. This algorithm in Bit coin is called Pow (Proofof Work) and in Ethereum, it is referred to as Pos (Proof of Stake). The calculation of Pos in Ethereum takesa few minutes. Each block contains the hash of the previous block and the data of the transactions which thencreates a chain of blocks, and the algorithm like Pow, Pos, or some other is calculated for each modification inthe blocks thus maintaining the integrity of the system and making it impossible to be changed by the third party.

SYSTEM ARCHITECTURE





Notation	Description
ID	Data sender's ID
PWD	Data sender's password
U_D	Criminal data uploaded by sender
V_D	Verified criminal data
T_D	Transaction data
B_{id}	Block number where meta data of transaction is saved
CID	Criminal identification data
UAD'	Consists of CID, B_{id}, and Enc(Key)
ID_X	Sender X's ID
PWD_X	Sender X's password
U_{DX}	Criminal data uploaded by sender X
V_{DX}	Verified data of sender X
T_{DX}	Transaction data of sender X
B_{idX}	Block number where transaction data of user X is saved

Fig.2 System Architecture

The system architecture for a criminal record-keeping and reporting system based on block chain would typically involve several key components, including:

The user interface is the system's front end that allows criminal justice stakeholders, such as law enforcement officers, prosecutors, judges, and correctional facility personnel, to interact with the system. This component would typically include a web-based or mobile app that provides access to the system's features and functionalities. The block chain network is the core of the system and provides the infrastructure for storing and managing criminal records. Depending on the system's specific requirements, the network would typically be based on a public or private block chain. Smart contracts are self-executing programs that automate the execution of predefined rules and conditions. In the context of a criminal record-keeping and reporting system, smart contracts can be used to manage the creation, verification, and sharing of criminal records between criminal justice agencies. The criminal record keeping and reporting system would require a robust and secure data storage mechanism for storing criminal records. The block chain network provides immutable and tamper-proof storage, which can help to enhance the accuracy and reliability of criminal records. Data analytics can beused to analyze the vast amounts of data generated by the criminal record-keeping and reporting system. This component can help to identify patterns and trends in criminal activity, support decision-making by criminal justice stakeholders, and improve the effectiveness of crime prevention and law enforcement efforts. Identity management: Identity management is a critical component of the criminal record-keeping and reporting system, as it ensures that only authorized users have access to the system. This component would typically include a robust authentication and authorization mechanism, such as multi-factor authentication, biometric authentication, and access control.

The reporting and notification component of the system provides stakeholders with real-time updates and notifications on criminal records. This component can help to enhance the timeliness and accuracy of criminaljustice processes, such as investigations and prosecutions. In conclusion, the system architecture for a criminal record-keeping and reporting system based on block chain technology would typically involve several key components that work together to provide a secure, transparent, and efficient data management system for the criminal justice system.

METHODOLOGY

The following is a proposed methodology for developing a criminal record-keeping and reporting system based on block chain technology:

Requirements gathering: The first step is to identify the needs and requirements of criminal justice stakeholders, including law enforcement agencies, courts, and other relevant parties. This involves conducting a thorough analysis of the current record-keeping process, identifying challenges and opportunities for improvement, and defining the specific features and functionalities required for the new system.

Design and architecture: Based on the requirements gathered, the system's design and architecture will be developed. This involves determining the block chain technology and platform to be used, as well as defining the system's data model, smart contracts, and user interface.

Development and implementation: With the design and architecture in place, the development and implementation phase can begin. This involves coding the smart contracts and other components of the system, configuring the block chain network, and integrating the system with existing criminal justice databases and systems.

Testing and validation: Before the system can be deployed, rigorous testing and validation will be conducted to ensure that it meets the specified requirements, performs reliably, and is secure and resilient. This includes testing the system's functionality, security, and performance under various scenarios.

Deployment and adoption: Once the system has been thoroughly tested and validated, it can be deployed in a controlled environment, such as a pilot project or limited rollout. This will enable us to assess the system's performance, user experience, and impact on the criminal justice system. The system can then be further refined and scaled up as needed.

Maintenance and support: After the system has been deployed, ongoing maintenance and support will be required to ensure its continued reliability, security, and functionality. This involves monitoring the system, providing user support, addressing any issues that arise, and updating the system as needed to keep it current and relevant.

In conclusion, the development of a criminal record-keeping and reporting system based on block chain technology requires a rigorous and well-structured methodology that includes requirements gathering, designand architecture, development and implementation, testing and validation, deployment and adoption, and ongoing maintenance and support. This methodology ensures that the system meets the needs of criminal justice stakeholders, is secure and reliable, and has a positive impact on the criminal justice system.

FUTURE SCOPE

The use of block chain technology in criminal record keeping and reporting has enormous potential for improving the criminal justice system's efficiency, accuracy, and transparency. Here are some possible future directions for this technology.

Expansion of the System: The criminal record-keeping and reporting system can be expanded to cover a broaderrange of criminal justice processes, including investigations, prosecutions, and sentencing. This can provide a more comprehensive and integrated view of the criminal justice system, allowing stakeholders to better track and manage cases.

Integration with Other Systems: The block chain-based criminal record-keeping and reporting system can be integrated with other systems, such as law enforcement databases, court records, and correctional facility records. This can help improve the accuracy and completeness of criminal records, reduce duplication of effort, and enhance information sharing between criminal justice agencies.

Use of artificial intelligence: Artificial intelligence (AI) can be used to analyze the vast amounts of data generated by the block chain-based criminal record-keeping and reporting system. This can help to identify patterns and trends in criminal activity, support decision-making by criminal justice stakeholders, and improve the effectiveness of crime prevention and law enforcement efforts.

Incorporation of biometric data: Biometric data, such as fingerprints and facial recognition, can be integrated into the block chain-based criminal record-keeping and reporting system. This can help to improve the accuracy and reliability of criminal records, reduce the risk of identity theft and fraud, and facilitate the identification of suspects and perpetrators.

Global adoption: The block chain-based criminal record-keeping and reporting system can be adopted on a global scale, enabling criminal justice stakeholders from different countries to access and share criminal records. This can help to enhance international cooperation in the fight against crime and terrorism, facilitate extradition and deportation procedures, and improve border security.

In conclusion, the future scope of the criminal record-keeping and reporting system based on block chaintechnology is vast and promising. Its potential to transform the criminal justice system is enormous, and ongoing research and development will continue to drive its evolution and adoption.

CONCLUSION

Public records frequently are tampered with, and their goods are adverse. Our system lets us remove all similar problems by means of a decentralized data storehouse. Digital signatures confirm the authenticity of uploaded data. Each data sender bears complete responsibility for the data contents. Encryption furthers the security ideal of this system. The aimlessly generated encryption keys ensure that no two lines have the same key, which exponentially reduces the threat of attacks. The pall factors, which are data storehouse and block chain, aren't directly accessible by any stoner.

REFERENCES

[1]. M. S. R. Maisha Afrida Tasnim1 and M. Z. A. Bhuiyan3, “CRAB: Block chain Based Criminal Record Management System,” Springer, 2018.

[2]. Moubarak, E. Filiol and M. Chamoun, “On Block chain Security and Relevant Attacks,” IEEE, 2018.

[3]. . “From Bit coin to Cyber security: a Comparative Study ofBlock chain Application and Security Issues,” IEEE, 2018

[4]. R. N. M. Auqib Hamid Lone, “Forensic-chain: Ethereum block chain based digital forensics chain of custody,” Scientific and practical cyber security journal — ISSN 2587-4667.imiblockchain.com

[5]. K.-H. Y. Shi-Cho Cha, “An ISO/IEC 15408-2 Compliant Security Auditing System with Block chain Technology,” IEEE, 2018.

[6]. Luciano Garcia-Banuelos Fredrik Milani, Block chain Application - Case ˜ Study on Hyper ledger Fabric, Tartu,2018