ISSN 2616-5783 Vol.7, Issue 10: 36-40, DOI: 10.25236/AJHSS.2024.071007

Feasibility Analysis of Blockchain Technology in Assisting Police Intelligence Work

Yigan Zhang

School of Smart Policing, China People's Police University, Langfang, Hebei, 065000, China

Abstract: *As an innovative distributed ledger technology, blockchain brings scientific solutions to police intelligence work through its decentralization, transparency, and immutability features. This paper provides an overview of the core principles of blockchain technology and analyzes the current issues in police intelligence work. Based on this, the paper proposes specific measures to optimize police intelligence work using blockchain technology, including the establishment of standardized databases, providing new models for intelligence collection, and optimizing intelligence transmission and sharing. By applying blockchain technology, police intelligence work efficiency and security can be improved, ensuring the authenticity of intelligence and enhancing collaboration between departments, thus providing more efficient and secure intelligence support for public security agencies.*

Keywords: *blockchain technology; assistance; police intelligence work; feasibility*

1. Introduction

With the rapid development of information technology, police intelligence work faces unprecedented challenges and opportunities. Traditional methods of intelligence collection, processing, and sharing are proving inadequate in the face of increasingly complex criminal activities. Police intelligence work requires more efficient, secure, and transparent technological means to improve its efficiency and accuracy. Blockchain technology, with its decentralized and tamper-proof characteristics, provides powerful technical support for police intelligence work. Applying blockchain technology in this context not only enhances data security but also optimizes the mechanisms for intelligence sharing and collaboration, enabling real-time updating and sharing of intelligence information, reducing information silos, and improving the accuracy of intelligence analysis. Therefore, this paper will first give an overview of blockchain technology, introducing its basic principles and main features. It will then analyze its application in police intelligence work and explore the challenges and solutions of using blockchain technology in this field, aiming to provide valuable suggestions for public security departments.

2. Overview of Blockchain Technology

Blockchain technology is an innovative solution based on distributed ledger technology, with the core idea of decentralization to achieve transparent, secure, and immutable data. By using distributed ledgers, blockchain stores data on multiple nodes, with each node holding a complete copy of the ledger, increasing data redundancy and avoiding the risk of single points of failure. Unlike traditional centralized systems that rely on a single server for data storage, blockchain eliminates this dependence by allowing all nodes to have equal rights and responsibilities in maintaining the system.

Blockchain technology employs various encryption algorithms, such as hash functions and asymmetric encryption. Hash functions convert data of any length into a fixed-length hash value, ensuring data integrity and immutability. Asymmetric encryption uses a pair of keys (public and private) to encrypt and decrypt data, protecting privacy (as shown in Figure 1). Blockchain ensures consistency across nodes through consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), allowing all nodes to reach consensus in a decentralized environment and preventing data discrepancies and conflicts [1].

ISSN 2616-5783 Vol.7, Issue 10: 36-40, DOI: 10.25236/AJHSS.2024.071007

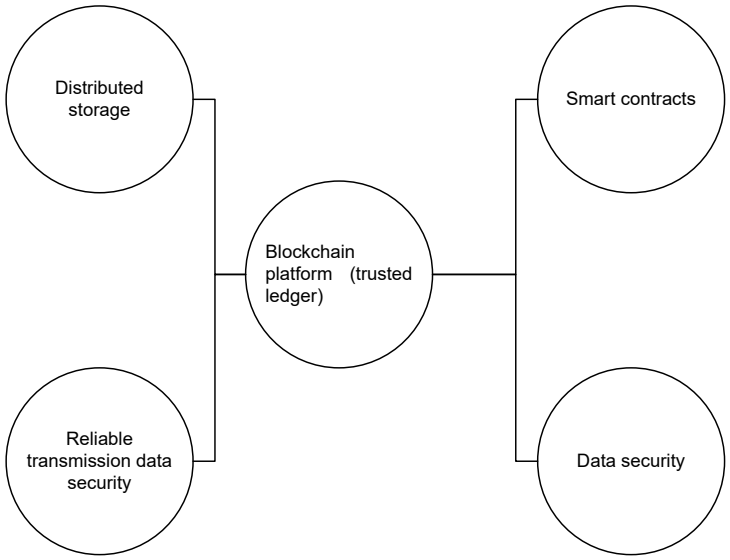

Figure 1: Blockchain technology

3. The importance of Blockchain Technology in Public Security Intelligence Work

3.1 Data Security And Privacy Protection

In the public security intelligence work, data security and privacy protection are very important, traditional data storage and transmission methods often rely on centralized servers, easy to become the target of hackers, resulting in sensitive information leakage. The decentralized nature of blockchain technology makes data no longer stored centrally on a single server, but distributed across multiple nodes, greatly improving the security of the data, each node keeps a complete copy of the data, and any tampering with the data will be detected by other nodes, thus ensuring the integrity and authenticity of the data. In addition, blockchain technology uses encryption algorithms to encrypt data, and only users with corresponding keys can access and modify data, effectively protecting the privacy of data. In public security intelligence work, a large amount of sensitive information is involved, such as personal identity information, case clues, etc. The encryption characteristics of blockchain technology can ensure that these information will not be illegally obtained during transmission and storage, thus protecting citizens 'right to privacy.

3.2 Data Transparency and Traceability

Public security intelligence work requires a high degree of transparency and traceability to ensure the authenticity of intelligence. The transparency and immutability of blockchain technology provide strong support for this demand. Every data operation on blockchain will be recorded in block and linked into chain through encryption algorithm to form an immutable ledger, which means that any modification of data will leave traces, which can be traced back to the source, thus ensuring the credibility of data. In public security intelligence work, data transparency and traceability are particularly important. For example, in the process of case detection, it is necessary to comprehensively record the source, processing process and result of clues to ensure the fairness and transparency of the case. Blockchain technology provides a transparent and trusted platform for these records, so that the operation of each link can be traced back, thus improving the efficiency of intelligence work.

3.3 Information Sharing and Collaboration

Public security intelligence work involves cooperation among many departments and agencies, and information sharing is the key to achieve efficient cooperation. However, there are many problems in traditional information sharing methods, such as information island, data redundancy, low sharing efficiency, etc. The decentralized and distributed characteristics of blockchain technology provide new ideas for information sharing and collaboration. Through blockchain technology, different departments and institutions can exchange data and collaborate on a shared blockchain platform to realize real-time sharing and synchronous updating of information. Each participant can access and verify shared data to

ISSN 2616-5783 Vol.7, Issue 10: 36-40, DOI: 10.25236/AJHSS.2024.071007

ensure accuracy of information.

4. Issues in Police Intelligence Work

4.1 High Difficulty in Collecting Police Intelligence

In the information age, police intelligence work has increasingly diversified sources, including social media, surveillance systems, and online platforms. However, this diversity also results in a significant amount of irrelevant information, increasing the time and effort required for intelligence officers to filter out valuable data. For instance, meaningful intelligence in social media is often buried under massive daily communications, increasing the difficulty of analysis and reducing efficiency.

Moreover, under the daily performance assessment framework, frontline police officers' efficiency in intelligence collection is further constrained, with many officers lacking the motivation to deeply explore and proactively gather intelligence. This passive approach negatively impacts intelligence collection quality and limits the overall effectiveness of police intelligence work. Additionally, some criminal groups use hacking techniques to breach databases. Once compromised, highly confidential intelligence may be leaked, severely damaging the credibility of police agencies and hindering effective crime prevention efforts. For example, certain criminal groups might access police action plans through hacking, allowing them to destroy evidence in advance and significantly reducing law enforcement's effectiveness.

4.2 Lack of a Comprehensive Police Intelligence System

In the current system, different police divisions collect intelligence based on their specific business needs, establishing respective intelligence databases. While this model meets each division's specific requirements to some extent, it results in fragmented intelligence resources. When one division needs information from another, a lengthy approval process is often required, delaying intelligence transmission and impacting its timeliness.

Although public security agencies promote the "intelligence-led policing" model, its implementation and application remain limited. The intelligence work in many cases still focuses on basic information collection and statistical processing, lacking in-depth analysis and comprehensive assessments. This limitation restricts the value of intelligence and slows down police responses to complex cases [2].

5. Optimizing Police Intelligence Work with Blockchain Technology

5.1 Establishing Standardized Databases

First, reduce technical differences between systems. Traditional police intelligence systems are often composed of multiple independent subsystems, each with different technical standards and data formats, making cross-system data transmission difficult. Blockchain, through its decentralized nature, provides a unified data interface and standardized format, allowing systems to access and share data in a consistent manner. This reduces technical disparities between systems, facilitating smoother data flow.

Second, enhance internal coordination within police agencies. Traditionally, different departments transmit data through cumbersome procedures, which not only consumes time but also leads to inconsistencies in data. Blockchain allows all departments to store data in a unified ledger, enabling real-time access and updates across departments, improving efficiency and strengthening collaboration.

Finally, resolve inter-system conflicts. Blockchain's immutability ensures that data from different systems are encrypted and hashed to generate unique block identifiers, ensuring data consistency across systems. Additionally, smart contracts can automatically execute data integration and validation rules, further reducing human intervention and improving efficiency [3].

5.2 Providing New Models for Intelligence Collection

The immutability of blockchain is its core feature. Traditional intelligence collection relies on centralized databases, which are vulnerable to attacks and tampering. Blockchain records each online activity on the chain, creating immutable "timestamps," ensuring that any online behavior — whether communication, transactions, or social media activity — leaves an indelible trace. This feature offers

ISSN 2616-5783 Vol.7, Issue 10: 36-40, DOI: 10.25236/AJHSS.2024.071007

solid data assurance for police intelligence work, allowing officers to trace the source of online activities and ensure the authenticity and reliability of intelligence (as shown in Figure 2). At the same time, the transparency of blockchain also makes the sharing and collaboration of intelligence more efficient. Different departments and agencies can analyze based on the same data source to avoid the problem of data isolation[4].

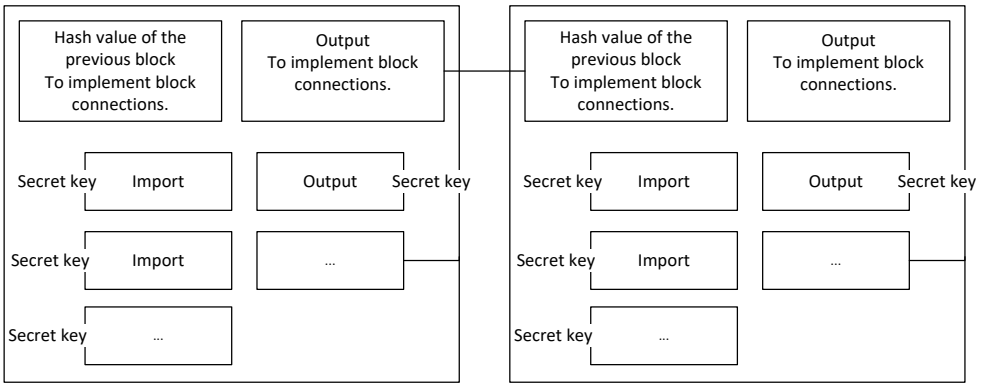

Figure 2: Blockchain foundation module

Blockchain combined with smart contracts also sets up early warning mechanisms and crisis triggers for the intelligence system. Smart contracts, which are self-executing codes, automatically trigger actions when preset conditions are met. In police intelligence work, smart contracts can set warning thresholds. When a certain indicator (e.g., abnormal network traffic or suspicious transactions) exceeds the threshold, the smart contract automatically triggers a warning, notifying relevant personnel for further investigation. This mechanism increases the system's responsiveness while reducing human error, ensuring timely and accurate alerts.

In addition, blockchain technology, combined with biometric technology, provides new solutions for monitoring key individuals. By using unique biometric identifiers such as fingerprints, iris scans, or DNA, a tamper-proof digital identity system is created. This system records key individuals' whereabouts on the blockchain, forming an immutable "tracking chain" and improving data accuracy [5].

5.3 Optimizing Intelligence Transmission and Sharing

First, data anonymization. Blockchain only transmits the summary information of the block header, while the actual data content is stored in the blockchain's distributed ledger. Even if the block header is intercepted, attackers cannot access the detailed content without specific permissions, further enhancing data security[6].

Second, locking data ownership. In police intelligence, securing the core information is crucial. Blockchain uses asymmetric encryption and timestamp technology to lock data ownership. Core information is encrypted and stored in the blockchain, and only users with specific keys can decrypt and use it. Non-core information can be publicly accessible, allowing the separation of data ownership and usage rights. Asymmetric encryption employs a pair of keys (public and private) to protect data, ensuring only the data owner has access to core information, preventing unauthorized use [7].

5.4 Establish an incentive mechanism

With the rapid development of information technology, public security intelligence work is facing unprecedented challenges and opportunities. Traditional intelligence collection, analysis and sharing methods have gradually shown their limitations in efficiency and security. In order to meet these challenges, blockchain technology, as a distributed ledger technology, provides new ideas and solutions for the optimization of public security intelligence work with its decentralized, tamper-proof and transparent characteristics. By recording every transaction or message in tamper-proof blocks and using encryption technology to ensure data integrity, blockchain technology provides a reliable data storage and transmission platform for public security intelligence work. In police intelligence work, incentive mechanism is particularly important. Traditional incentive mechanism relies on manual recording and evaluation, and has some problems such as subjectivity and opacity. Blockchain technology provides a dedicated channel for public security intelligence personnel to record their online behavior and ensure the immutability of information. In this way, every piece of intelligence information can be labeled as an

ISSN 2616-5783 Vol.7, Issue 10: 36-40, DOI: 10.25236/AJHSS.2024.071007

intelligence officer, which becomes a powerful basis for organizational incentives and intelligence officer ratings. This not only helps to improve the motivation and efficiency of intelligence personnel, but also ensures the fairness and transparency of incentive mechanisms. It can be seen that the application of blockchain technology in public security intelligence work can not only optimize data management and transmission, but also provide solid technical support for the establishment of incentive mechanism. This paper will discuss in depth how blockchain technology can help optimize public security intelligence work, and elaborate on its specific application in incentive mechanism construction.

6. Conclusion

In conclusion, the application of blockchain technology in police intelligence work has significant practical importance. By establishing standardized databases, offering new intelligence collection models, and optimizing intelligence transmission and sharing, blockchain technology can effectively address many of the current issues in police intelligence work and enhance its efficiency. However, challenges such as technical standards, data privacy, and system scalability still need to be addressed. As blockchain technology continues to evolve, its application in police intelligence work will become more widespread, providing more efficient intelligence support for public security agencies and driving intelligence work toward a more intelligent future.

References

[1] Dai Zhuoming. Feasibility Study of Blockchain Technology in Assisting Police Intelligence Work [J]. Insight, 2022(6):44-46.
[2] Guo Jinpeng, Yang Lianzheng. Optimization of Police Intelligence Sharing Based on Blockchain [J]. Network Security Technology & Application, 2022(4):126-128.
[3] Cui Mengtian, Dong Guoqing, Jiang Yue, et al. Data Sharing and Incentive Methods for Police Intelligence Based on Consortium Blockchain [J]. Journal of Intelligence, 2022, 41(9):108-111.
[4] Chu Delin. Research on Intelligence Sharing Model for Environmental Crime, Food and Drug Crime Based on Blockchain [J]. Network Security Technology & Application, 2023(2):48-50.
[5] Chen Chao, Shen Zhanghui. Research on Electronic Data Sharing Model Combining Cloud Storage and Blockchain [J]. Modern Computer, 2024, 30(12):57-61.
[6] Li Mohan. Analysis of Countermeasures Against Money Laundering Crimes Using Virtual Currencies [J]. Network Security Technology & Application, 2023(10):147-149.
[7] Gao Hongmei, Li Baodong. Identity Prediction of Terrorist Personnel Based on Evidence Weight and Logistic Regression [J]. Software Guide, 2023, 22(8):17-23.