Research and Application Analysis of Logistics Encryption Technology Based on Blockchain

Ren Li

International college, Guangxi University, Guangxi, 530004, China
renli@seu.edu.mk

Abstract. The rapid development of logistics industry provides a broad prospect for the application of blockchain technology, such as logistics information tracking, supply chain transparency, and de-trusted transactions, which have been widely used because of its advantages such as data sharing, labor cost reduction, and efficiency improvement. However, blockchain technology currently has security problems, such as leakage of information, so further research and application of security technologies are needed. There are many problems in the current application of blockchain technology in the logistics industry, such as the existence of security vulnerabilities, high cost of technology, and the use of encryption algorithms. These problems have seriously affected the normal application and development of blockchain technology. In order to solve the security problems of blockchain technology, this paper proposes a security scheme to guarantee logistics information by using Shang Yong Mi Ma(SM2) algorithm, which improves the reliability and integrity of logistics information by means of multiple signatures and distributed storage. Firstly, distributed storage is used for logistics information storage, and logistics information is stored on multiple nodes in a decentralized manner, thus avoiding single point failure of nodes. Then, SM2 algorithm is used to encrypt and digitally sign the logistics information to protect the privacy and integrity of the information, and prevent the information from being tampered. Finally, multiple signature technology is used in combination with smart contract function to make the transaction orderly and fault-tolerant, and improve the trustworthiness and security of the transaction. This paper studies the scheme of using SM2 algorithm to guarantee the security of blockchain logistics information, which provides a feasible solution for the information security of enterprises in the logistics field. In addition, the successful application of the scheme in the logistics industry can improve the security and reliability of logistics information and help to promote the digital and intelligent transformation of the logistics industry, which has wide application value and practical significance.

Keywords: Blockchain, SM2 Public key cryptographic, Multisig, Distributed storage, Logistics

P. Kar et al. (eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)*, Advances in Computer Science Research 108,
https://doi.org/10.2991/978-94-6463-300-9_80

1 Introduction

Blockchain technology has emerged as a crucial area of research in the realm of digital economy and information security. Its decentralized, peer-to-peer data interaction system effectively addresses trust-related issues. The role of digital signatures is of pivotal importance in ensuring this trust. Several cryptographic algorithms and encryption techniques are employed in blockchain technology to secure the information within the blockchain [1]. The SM2 Elliptic Curve Public Key Cryptographic Algorithm, introduced by the National Commercial Cryptography Administration Office in December 2010, presents a potent solution. As an elliptic curve public key cryptographic algorithm, SM2 holds a significant advantage in blockchain applications due to its high cryptographic complexity, rapid processing speed, and comparatively minimal machine performance consumption, especially when contrasted with the Rivest Shamir Adleman(RSA) algorithm. The SM2 algorithm, with its robust security, can be employed to protect data security in domains such as e-commerce, mobile payments, and cloud computing. Utilizing the SM2 algorithm in blockchain technology can boost the security and reliability of the blockchain, thus enhancing its utility in commerce, finance, and other sectors [2].

The incorporation of blockchain technology in the logistics industry can dramatically improve efficiency and security, enabling transparent and reliable management of supply chain data. This offers innovative technical support for the progression and improvement of the logistics industry. In the current trend of informatization and intelligence, operational, managerial, and data flow issues in the logistics industry are becoming increasingly prominent. Thus, improving the quality and efficiency of management and services associated with the logistics industry is both an important and urgent endeavor. The application of blockchain technology can provide the strong support needed to achieve this goal, and the digital signature technology in the SM2 algorithm can offer practical and effective anti-counterfeiting measures for the logistics industry [3].

2 Basic Theory

2.1 Blockchain

Blockchain is a groundbreaking digital ledger technology that operates in a distributed, decentralized, and tamper-proof manner. It offers unparalleled security, transparency, and immutability [4]. Originally conceptualized in 2008 as the foundational technology for the cryptocurrency Bitcoin, blockchain has rapidly gained widespread adoption across numerous industries, including finance, healthcare, supply chain management, and various others. At its core, blockchain is a distributed database system that relies on a peer-to-peer network comprising multiple independent nodes. Each node in the network maintains a copy of the blockchain, ensuring redundancy and eliminating the need for a central authority. This decentralized nature of blockchain enhances its resilience, making it highly resistant

to hacking and data manipulation. One of the key features of blockchain is its immutability. Once a transaction or record is added to the blockchain, it becomes virtually impossible to alter or delete. This attribute is achieved through the use of cryptographic algorithms and consensus mechanisms that ensure agreement among the network participants [4]. As a result, blockchain provides a reliable and transparent audit trail, making it an ideal solution for applications where trust and accountability are paramount.

2.2 SM2 Signature Algorithm

SM2, developed by the National Cryptologic Authority and released in 2010, is an advanced public-key cryptographic algorithm rooted in the complexity of the elliptic curve discrete logarithm problem. The suite comprises three fundamental components: a digital signature algorithm, a key exchange protocol, and a public key encryption algorithm.

The digital signature algorithm enables data authentication and integrity verification. It allows a party to sign digital content with their private key, with any receiver able to verify the signature using the corresponding public key. This ensures the authenticity of the data and the identity of the sender, bolstering the security of digital communications. The key exchange protocol of the SM2 algorithm facilitates the secure sharing of cryptographic keys over an unsecured communication channel. It establishes a shared secret key between two parties without disclosing it to potential eavesdroppers, supporting secure communication. The generated shared keys can then be used to encrypt and decrypt data, ensuring secure and confidential information exchange. The public key encryption algorithm enables the secure transmission of sensitive data. The sender can use the recipient's public key to encrypt the data, ensuring that only the individual with the corresponding private key can decrypt and access the information. This feature significantly strengthens the privacy and security aspects of data communication.

The SM2 algorithm, given its robust security features, has widespread applications across various sectors, including but not limited to secure communications, digital signatures, and secure key exchanges in networking, e-commerce, and blockchain technology. Its deployment has become increasingly prominent in ensuring the secure and reliable transmission, storage, and handling of digital information.

2.3 Multisig

Multisig is a cryptographic technology that verifies or authorizes the execution of a transaction, contract, or other operation through the digital signatures of multiple participants [5]. It is a means to enhance security and protect against risk, and is commonly used for cryptocurrency transactions, contract execution, and scenarios that require multiple parties to participate.

2.4 Distributed storage

Distributed storage, also known as distributed file systems or distributed data storage, is a computing technology that enables the storage and retrieval of data across multiple physical or virtual resources. Unlike traditional storage systems that rely on a single centralized storage device, distributed storage breaks down data into smaller pieces and stores them across a network of interconnected nodes.

In a distributed storage system, data is typically divided into chunks or blocks, and each block is replicated and distributed across multiple storage nodes. This distribution offers several advantages, including improved performance, high availability, fault tolerance, and scalability.

Examples of popular distributed storage systems include Hadoop Distributed File System (HDFS), Gluster File System, Ceph, and Apache Cassandra. These systems have been widely adopted in various industries, including cloud computing, big data analytics, and content delivery networks [5].

3 Application analysis of blockchain in the logistics industry

3.1 Specific form

Logistics companies inherently need to trace the origin of goods to assure quality and safety. Blockchain technology's decentralized nature and data immutability can enhance the reliability and efficiency of such traceability systems, mitigating issues such as damage or loss of goods. By utilizing blockchain technology, each link in the transit process of goods, from origin to destination, generates a blockchain record. This record tracks and updates real-time information and status of goods, including location, transportation time, method, freight cost, and more, ensuring real-time traceability.

The application of blockchain technology allows for the creation and management of smart contracts - codified agreements that autonomously process and validate contractual terms without third-party interference. This capability aids logistics companies in achieving paperless, automated, and transparent management. Smart contracts facilitate automatic payments and settlements, while simplifying logistics operations. Logistics companies can automate and bring transparency to the preparation, signing, management, and execution of contracts, reducing the risk of disputes.

Noteworthy examples of deploying smart contracts include Ethereum, which has implemented a near-Turing-complete language on its blockchain, making it a prominent smart contract framework. RootStock (RSK) represents another example - a smart contract platform connected to the Bitcoin blockchain via sidechain technology, compatible with smart contracts created for Ethereum [6].

Blockchain technology enables the custody and flow of assets, assisting logistics enterprises in realizing digital asset management, thus boosting the efficiency and security of asset utilization. Traditional trade finance transactions usually involve

intermediaries like banks, escalating transaction costs and time. With blockchain technology, direct communication between parties reduces intermediary involvement, resulting in less time-consuming and less costly transactions. Furthermore, blockchain technology permits the decentralized flow of assets. Through blockchain technology, logistics participants' credit assessment and risk control can be actualized, enabling information sharing and authenticity verification, reducing the possibility of fraud and risk. Logistics companies share and verify participant data on the blockchain, enhancing participant credibility and authenticity. Additionally, blockchain technology supports data sharing and privacy protection, safeguarding the trade secrets and privacy of logistics participants.

3.2 Advantages

1)Enhanced transparency and traceability: Blockchain technology can provide a decentralized and shareable data storage and exchange platform, enabling all participants in the logistics chain to share data in real time and achieve full traceability and transparency. This can help solve the information asymmetry problem in the logistics process and reduce the risk of data tampering and fraud [7].

2) Improve efficiency and reduce costs: Blockchain technology can simplify many tedious operations and document processing in the logistics chain. Through smart contracts, processes such as contracts, payments, and cargo tracking can be automated and optimized, reducing manual intervention and intermediate steps, increasing efficiency and reducing operational costs.

3)Enhanced security and tamper resistance: Blockchain ensures data security and integrity with its distributed and encrypted nature. Every data transaction is encrypted and verified, and data is stored on multiple nodes and cannot be tampered with once it is stored on the blockchain. This helps prevent data from being stolen, tampered with or lost, providing greater security.

4)Facilitate collaboration and trust building: Blockchain provides a platform for participants to trust and share, enabling closer collaboration between different organizations and participants in the supply chain. By sharing sensitive data and real-time tracking information, it can strengthen trust between participants, improve collaboration efficiency, and drive overall synergy in the supply chain [8].

5)Enhanced user experience and satisfaction: Blockchain technology provides faster, transparent and reliable logistics services. With real-time tracking and shared data, users can better understand the logistics process, cargo location and delivery status. This improves the user experience and increases customer satisfaction with logistics companies.

3.3 Limitations

Security Issues: Smart contracts, as previously discussed, carry certain security risks. Vulnerabilities within smart contracts can be exploited by hackers to either steal or manipulate data. A smart contract, defined as a "computer transaction protocol enforcing the terms of a contract," is visible to all users on a blockchain.

Consequently, all vulnerabilities, including security loopholes, are on display and may not be rectifiable promptly. Resolving such attacks can be particularly challenging, as demonstrated by the Decentralized Autonomous Organization(DAO) Ether vulnerability in June 2016, which led to a loss of $50 million while developers sought a consensus solution. DAO's program had a delay that allowed hackers to remove funds. A hard fork of the Ether software managed to recover the attacker's funds before the time limit expired.

Technological Costs: The implementation of blockchain technology demands significant computing and storage resources, alongside efficient network connections for data exchange and consensus building. For logistics enterprises, the adoption of blockchain technology also necessitates substantial system architecture reconstruction and application development. This entails considerable investment in terms of both capital and human resources. Moreover, security and reliability requirements exceed those of traditional logistics systems, necessitating additional testing and auditing, which can further escalate costs.

Encryption Algorithm Utilization: While encryption algorithms can ensure the data security and integrity of the blockchain system to a degree, the risk of hacking or password cracking persists, posing a significant threat to the logistics industry. If encryption algorithms demand greater computational power and resources, this could lead to a degradation in performance for logistics industry applications [8].

4 Blockchain Signature Scheme Based on SM2

Within blockchain systems, digital signatures validate the authenticity and legitimacy of transactions. Utilizing the SM2 algorithm allows for the creation and verification of these digital signatures, ensuring transactional integrity and authentication. The SM2 algorithm is rooted in the security foundation of the elliptic curve discrete logarithm problem, thus providing a robust digital signature function. Outlined below are the key steps of the process:

SM2 Key Pair Creation: Participants within a blockchain network are capable of generating their own public-private key pairs using the SM2 algorithm. The private key is employed to sign transactions and data, while the public key is used to verify these signatures and encrypt the data [9].

Data Signing and Verification: Within the blockchain, users can sign transactions or data using their private keys. Other participants can then use the corresponding public key to verify the signature's validity. This process ensures the integrity and authenticity of the transaction or data.

Key Exchange: The SM2 algorithm can facilitate secure key exchange protocols, like the Diffie-Hellman key exchange. Using the SM2 algorithm, participants can generate temporary shared keys to encrypt and decrypt data communications.

Encryption and Decryption: The SM2 algorithm is effective for encrypting and decrypting sensitive data within the blockchain. Participants can encrypt data using the receiver's public key, and only the corresponding private key can decrypt the data, thus ensuring data confidentiality and privacy.

Anonymous Authentication: By leveraging the SM2 algorithm, it's possible to implement anonymous authentication and ensure the anonymity of participants within the blockchain network. Data privacy protection during authentication can be achieved through techniques such as zero-knowledge proofs.

Secure Communication: The SM2 algorithm can be employed for encrypted communication, safeguarding the confidentiality and integrity of messages. The algorithm helps protect communications within a secured blockchain network from tampering and information theft.

Contract and Smart Contract Security: The SM2 algorithm can verify and enforce contracts and smart contracts within the blockchain. By signing and verifying contracts using the SM2 algorithm, the security and trustworthiness of these contracts can be guaranteed.

5 Application implementation

5.1 Committed step

Participants in logistics such as suppliers, carriers, and consignees must generate their own public-private key pairs. The SM2 algorithm, a domestically developed elliptic curve encryption standard in China, is utilized to generate these pairs where the private key serves for data signature and the public key for signature verification and authentication. The generation process involves several steps, including the selection of elliptic curve parameters, random private key selection, public key computation, public key compression, and finally, key storage and use. Public key registration and authentication involve a multi-signature process. Participants begin by generating their key pairs, which includes a public key and a private key, using the SM2 encryption algorithm. These public keys are then shared with relevant participants or system platforms either directly, stored within the blockchain network, or transmitted via secure channels. Each participant associates its public key with a specific system or platform during the registration process, which involves authentication information provision and public key validity verification. The system or platform then registers the participant's public key in its database, blockchain, or another storage medium.

During the multi-signature process, the system or platform checks whether the public key used is valid and legitimate. This may include ensuring that the public key aligns with the pre-defined format and algorithm requirements, verifying the participant's identity and authority to whom the public key belongs, and checking the public key's status [10]. Identity verification involves five main steps: providing identity information, sending authentication requests, generating signatures, verifying authentication, and returning authentication results. In the logistics process, each node records relevant information, such as goods' origin and destination, timestamps, logistics nodes, and transporter details. This information is encrypted and digitally signed using the SM2 algorithm, ensuring the data's integrity and tamper-evidence. Each node uploads the signed logistics information to form a block, and consensus on the new block is achieved through consensus algorithms such as proof of workload or proof of stake. Only blocks that reach consensus are added to the blockchain's

distributed ledger. The blockchain's distributed storage method allows logistics information to be stored in a decentralized manner across multiple network nodes. If one node fails, others remain available, ensuring system continuity. The data is protected by encryption and authentication mechanisms, ensuring it cannot be tampered with or falsified.

Participants can query logistics data and records via the blockchain, enabling goods traceability and tracking. By verifying digital signatures and data on the blockchain, the integrity and trustworthiness of logistics information are ensured. In smart contracts, logistics participants can agree on payment conditions and rules. When these conditions are met, the smart contract automatically executes the payment operation. The SM2 algorithm is used for digital signature verification, ensuring transaction security and trustworthiness. Using public-private key pairs generated by SM2, participants can authenticate themselves in blockchain smart contracts, ensuring only authorized individuals can perform specific operations or access certain data. This prevents unauthorized access and malicious attacks. In conclusion, the application of the SM2 algorithm in smart contracts and payment systems can enhance user identity protection and payment information security, thereby improving the overall trustworthiness and security of the blockchain system..

5.2 Application

Leveraging China's domestically developed elliptic curve encryption algorithm, SM2, blockchain implementations can deliver enhanced data security and privacy protection. By employing robust data encryption during both transmission and storage phases, it safeguards logistics information against malicious attacks, data tampering, and information leakage, thereby boosting the reliability of logistics data. Furthermore, the utilization of blockchain technology for storing logistics data results in seamless traceability and verification across the entire supply chain. With the SM2 algorithm ensuring data integrity and authenticity, it creates tamper-proof records, improving traceability and verification capabilities at every stage of logistics. This is particularly beneficial for dispute resolution, quality tracing, and legal compliance. Lastly, blockchain applications in the logistics industry enable real-time sharing and transparency of information. Relying on the SM2 algorithm for secure data transmission, the process automates transaction verification, eliminating the need for traditional intermediaries and resulting in lowered transaction costs and time. Moreover, transparent transaction information provides stakeholders with a comprehensive view of the entire logistics process, thereby enhancing collaboration efficiency.The logistics industry traditionally experiences information asymmetry, leading to high trust costs and risks among participants. By incorporating the SM2 algorithm within blockchain applications, it becomes possible to establish a decentralized trust mechanism. Logistics data is verified and stored by multiple nodes, allowing all participants to share and access the data. As a result, this reduces trust costs and mitigates risks.

6 Conclusion

In conclusion, this paper aimed to address the security challenges of blockchain technology in the logistics industry and proposed a security scheme utilizing the SM2 algorithm to guarantee the integrity and confidentiality of logistics information. The use of distributed storage, encryption, digital signatures, and multiple signature technology enhances the reliability, transparency, and security of logistics transactions. The application of blockchain technology in the logistics industry offers immense potential for improving efficiency, transparency, and trust in various aspects, such as information tracking, supply chain management, and trusted transactions. However, security concerns, including data leakage, pose obstacles to its widespread adoption.

By leveraging the SM2 algorithm and its capabilities in encryption, digital signatures, and authentication, this proposed security scheme provides a feasible solution for securing logistics information in the blockchain. The utilization of decentralized storage ensures the resilience against single point failures. The combination of encryption and digital signatures safeguards the privacy and integrity of logistics information, while multiple signature technology and smart contracts enhance transaction reliability and fault tolerance. The successful implementation of the proposed scheme in the logistics industry can contribute to the overall digitization and intelligence transformation of this sector. Furthermore, it enables enterprises in the logistics field to enhance the security and reliability of their operations, improving trust among stakeholders. Ultimately, this research has practical significance and promising implications for the broader application of blockchain technology in logistics and supply chain management.

Further research and development efforts should focus on refining this security scheme, addressing any remaining vulnerabilities, and exploring additional applications of SM2 algorithm in the logistics industry. By continuously improving the security measures and promoting the adoption of secure blockchain technologies, the logistics industry can fully harness the benefits of blockchain in terms of data sharing, cost reduction, and efficiency improvement while ensuring the integrity and confidentiality of logistics information.

References

1. Li, Y., Zhang, Y., & Li, W. (2022). A Survey on the Security of Blockchain Technology: Cryptography, Privacy Protection, Consensus Mechanism and Smart Contracts. Journal of Blockchain Law and Policy, 3(4), 57-79.
2. Zhang, W., Wang, W., & Liang, X. (2022). Blockchain-Based Logistics Information Exchange: A Solution Using SM2 Public Key Cryptography and Multisig Approach. Journal of Intelligent Logistics Systems, 31(2), 106-117.
3. Wang, F., Li, Y., & Zhang, W. (2023). Blockchain-Enabled Distributed Storage for Large-Scale Data Storage and Access in IoT Applications. Journal of Intelligent Internet of Things and Services, 16(3), 293-305.

4. Al-Fuqaha, A., Guizani, M., & Aledhari, M. (2022). Secure and Efficient Data Storage and Access in Cloud Computing Using Blockchain Technology. IEEE Transactions on Cloud Computing, 10(4), 699-712.
5. Chen, T., Li, Y., & Li, Z. (2022). Blockchain-Based Smart Contracts for Secure and Efficient Electronic Voting Systems. Security and Communication Networks, 58(3), 4547-4558.
6. Zhang, W., Wang, W., & Liang, X. (2022). Blockchain-Enabled Healthcare Supply Chain Management: A Solution Using SM2 Public Key Cryptography and Multisig Approach. Journal of Intelligent Decision Making and Systems, 28(4), 309-323.
7. Velichko AV, Cui J (2020). Efficient methods for temperature-based and event-based security in the Internet of Things: Encryption, hashing, and watermarking Journal of Network and Computer Applications 166: 108131-1 to -11
8. Rathore, V., Bansal, R., & Gupta, M. (2021). Advanced encryption standard (AES) and its implementation over RSA with certificateless public key cryptography for IoT security Journal of Network and Computer Applications, 108495
9. Wang Z, Xu Y, Zhang H (2019). A survey on the security of blockchain technology: Cryptography Journal of Network and Computer Applications. 163: 1 to 13
10. Li Y, Zhang Y, Li W (2019). Fully homomorphic encryption for polynomial evaluation privacy-preserving cloud computation Journal of Cloud Computing: Advances