

# ***Solutions for Blockchain Security Threats in International E-Commerce***

**Jiarui Yan<sup>1,a,\*</sup>**

<sup>1</sup>*Beijing International Studies University, Dingfu Zhuang South Li No.1, Beijing, China  
a. 374054630@qq.com*

*\*corresponding author*

**Abstract:** With the rapid development of global trade and the popularization of the Internet, cross-border e-commerce has become an important part of international trade and is often seen in the public eye together with blockchain technology, which provides innovative operational solutions for cross-border e-commerce with its decentralized, tamper-proof, transparent and open features. However, in practical application, blockchain technology also faces challenges such as security and differences in international laws and regulatory policies. As there are differences in legal perceptions and regulatory policies of blockchain technology in different countries and regions, as well as legal loopholes, this also brings challenges to the operation of cross-border e-commerce. In order to solve these challenges, this paper will comprehensively analyze the problems and propose solutions in combination with specific cases, and these measures will help cross-border e-commerce enterprises better adapt to the legal environments of different countries and ensure the compliance and stability of their business.

**Keywords:** Block-chain technology, cross-border e-commerce, risk of attack.

## **1. Introduction**

### **1.1. Background of the study**

Under the wave of global economic integration, cross-border e-commerce has become an important pillar of international trade. However, with the rapid growth of global business, cross-border e-commerce is also facing increasingly complex challenges.[1] In order to improve efficiency and achieve integration, blockchain technology has been successfully integrated into cross-border e-commerce trade. Blockchain technology is a technology that does not rely on a centralized authority or a third-party trust institution. It is a chained structure consisting of multiple blocks of data (blocks) connected in chronological order, where all participants are able to participate and verify transactions equally in a distributed network. Each block is constructed based on the principles of cryptography, containing the hash value of the previous block as a link. This structure ensures the security and integrity of information through a variety of mechanisms such as timestamps, hash functions, and random numbers, and is essentially a distributed database that does not require a centralized trust institution, but is maintained by all participating nodes. This decentralized and de-trusted characteristic makes the data on the blockchain highly traceable and tamper-proof, thus ensuring the

authenticity and trustworthiness of the data. For cross-border payment and clearing, blockchain technology can simplify the process and improve efficiency.

However, in recent years, with the globalization of technology, the security issues of blockchain technology have been particularly prominent, with the frequency of hacker attacks rising and the security and integrity of transaction data being seriously threatened. In addition, there are differences in legal perceptions and regulatory policies of blockchain technology across countries, leading to legal uncertainties and compliance risks for cross-border e-commerce in cross-border transactions. [2] Meanwhile, the protection of personal privacy and sensitive information cannot be ignored, and the risk of data leakage and misuse persists. In addition to this, due to the lack of uniform international standards and norms, cross-border e-commerce companies face many operational difficulties and misunderstandings in the application of block chain technology, which further increases transaction costs. Therefore, it is of great significance to deeply explore and address the risks and security threats of block chain technology in cross-border e-commerce to promote the healthy development of global trade.

## **1.2. Status of research**

### **1.2.1. Current status of domestic research**

Domestic scholars have made significant progress in the deep integration of blockchain technology and cross-border e-commerce. The problems faced by cross-border e-commerce, such as lack of trust and data security risks, are specifically analyzed, and specific solutions based on blockchain features are proposed. In addition, the logistics traceability system based on blockchain also provides more transparent and trustworthy logistics information for cross-border e-commerce; in terms of the construction of trust mechanism, domestic scholars also put forward a basic trust construction program to improve the security and reliability of transactions. For the main dilemmas faced by cross-border e-commerce in the process of development, such as the lack of trust, regulatory difficulties and data security risks, domestic studies have put forward corresponding coping strategies and suggestions.

### **1.2.2. Current status of foreign research**

The relevant foreign literature explores the application opportunities and challenges of blockchain technology in cross-border e-commerce, mainly including the analysis of technology implementation, data security, transaction efficiency, cost reduction, etc., as well as the analysis of the methods and effects of blockchain technology in cross-border e-commerce supply chain to achieve transparency and traceability, including product traceability, logistics tracking, optimization of supply chain management and other aspects of the research, including identity authentication, transaction verification, credit system construction and other aspects are discussed to improve the security and reliability of transactions.

## **1.3. Conclusion**

In summary, the application of blockchain in the field of currency and finance is in the process of continuous innovation and development, both from the theoretical and empirical levels, and this study need to reduce the risks in a timely manner, both in the practical and theoretical significance, which also need to solve them in a timely manner. After comprehensively considering the current economic situation and globalization background, the first problem that should be solved is the most direct and urgent problem that affects business operations and consumer trust when facing the challenges of

blockchain technology in cross-border e-commerce, and this paper will focus on the "security of blockchain technology" and "differences in international legal and regulatory policies". This paper will discuss and analyze the issues of "security of blockchain technology" and "international legal and regulatory policy differences".

## 2. Overview of blockchain technology

### 2.1. Application of blockchain technology

#### 2.1.1. Financing and finance

Blockchain technology dates back as far as 2008. On November 1, 2008, a person who called himself Satoshi Nakamoto (Satoshi Nakamoto) published the paper "Bitcoin: A Peer-to-Peer Electronic Cash System", which detailed the concept of the architecture of the electronic cash system constructed on the basis of P2P network technology, cryptography, timestamping technology, blockchain technology, etc. Two months later, that is, on January 3, 2009, the the first serial number 0 of the genesis block was born, a few days later on January 9, 2009, the block with serial number 1 appeared, and connected with the serial number 0 of the genesis block to form a chain, which marked the official birth of the blockchain, nowadays, the blockchain technology is developing at a high speed, and the use of blockchain technology in the financial field is becoming more and more extensive: digital currencies, such as bitcoin, are precisely the most well-known and successful blockchain technology Case in point. The emergence of digital currencies is reshaping our monetary habits, and their security, convenience, and low transaction costs are particularly suitable for business activities in the Internet age.

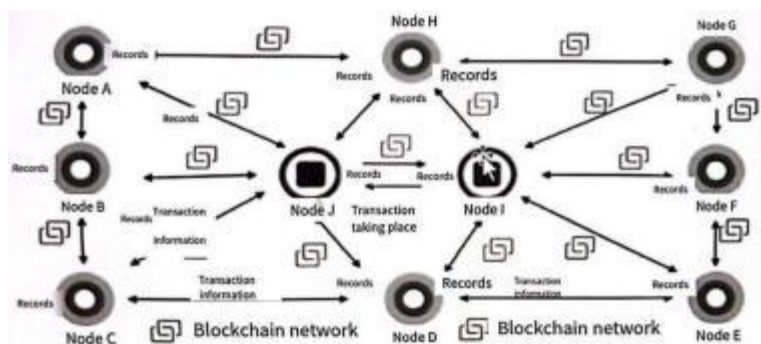


Figure 1: Blockchain operation process

In the field of supply chain financing, blockchain technology enhances the transparency and credibility of financing by tracking logistics and inventory data in real time[2]. Whether it is stocks, bonds, real estate or artworks, blockchain technology can realize the digitization and decentralized management of assets, thus improving the efficiency and transparency of asset transactions. In addition, a smart contract is another important application of blockchain technology. It is automatically executed based on certain conditions without human intervention, greatly reducing the cost and risk of contract execution. Blockchain technology can also enhance regulatory compliance in the financial industry. With traceable transaction records and smart contracts on the blockchain, regulators are able to monitor and manage risks in the financial market more effectively. Blockchain technology can also play a huge role in the insurance business. It helps to digitize and automate the management of insurance contracts and improve the efficiency and accuracy of claims processing.

### **2.1.2. Significance of blockchain technology**

Blockchain technology does not rely on a central governing body or a third-party trust institution, and all participants are able to participate and validate transactions on an equal footing in a distributed network, as blockchain is a chained structure consisting of multiple blocks of data (blocks) connected in chronological order, each constructed based on cryptographic principles and containing the hash value of the previous block as a link. This structure ensures the security and integrity of information through various mechanisms such as timestamps, hash functions, and random numbers. Blockchain is essentially a distributed database that does not require a centralized trust authority, but is maintained by all participating nodes. This decentralized and de-trusted nature makes the data on the blockchain highly traceable and tamper-proof, thus ensuring the authenticity and trustworthiness of the data. For cross-border payment and clearing, blockchain technology can simplify the process and improve efficiency. Traditional cross-border payment involves many intermediaries, which is not only a cumbersome process, but also a high cost, while blockchain technology can build a decentralized, peer-to-peer payment network, reduce intermediate links, lower transaction costs, and accelerate the speed of transactions.

## **2.2. Integration with e-commerce platform trade**

### **2.2.1. Highly integrated with blockchain technology**

Blockchain technology provides many conveniences for cross-border e-commerce through its unique mechanisms such as distributed ledgers and smart contracts. For example, according to data released by the General Administration of Customs, China's cross-border e-commerce imports and exports totaled 1.98 trillion yuan in 2021, a year-on-year increase of 15 percent. [3] Against this backdrop, Alibaba Tmall International announced the application of blockchain technology in its cross-border logistics business to achieve real-time tracking of all imported goods, including details such as origin, mode of transportation, port of route, customs reports, and third-party validation, which greatly improves the transparency and traceability of transactions.

In recent years, a large number of SMEs have been actively integrated into the competition with China's favorable policy environment, the surge in market demand and the innovation of the international supply chain business model. China's cross-border e-commerce platform leaders, such as Alibaba International, continue to strengthen the whole industry chain and the whole supply chain of integrated services, helping China's cross-border e-commerce industry chain and supply chain ecosystem construction. China's small and medium-sized enterprises in cross-border trade is characterized by the small amount of transactions, high-frequency transactions, which are accompanied by high trade costs and relatively difficult to regulate. In particular, there are bottlenecks and challenges that need to be addressed in key aspects such as cross-border payment and logistics. The improvement of the management efficiency of each node enterprise inside and outside the supply chain is the basis for maximizing the efficiency of the cross-border e-commerce supply chain. Build an information sharing mechanism with the help of Internet information platforms such as supply chain platform, e-commerce platform and cross-border payment platform, optimize the integration and allocation of supply chain resources, improve cross-border logistics platform, and improve the efficiency of logistics storage and distribution system [4].

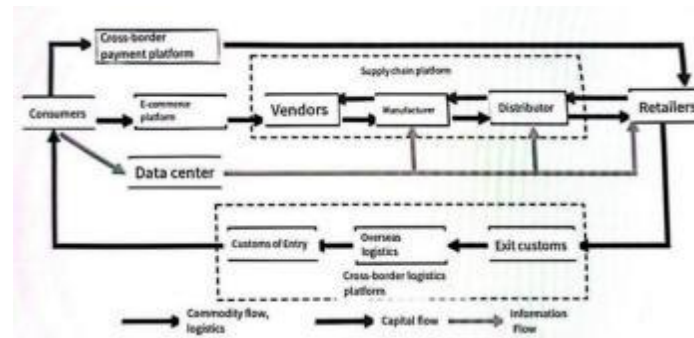


Figure 2: Supply chain logistics distribution system

In order to maximize the efficiency of cross-border e-commerce supply chain, it is fundamental to improve the management efficiency of each node enterprise inside and outside the supply chain. This requires the construction of an efficient information sharing mechanism through the supply chain platform, e-commerce platform and cross-border payment platform and other Internet information platforms, optimization of the integration and allocation of supply chain resources, improvement of the cross-border logistics platform, and enhancement of the efficiency of the logistics storage and distribution system.

### 2.2.2. The importance of such integration and its advantages

First of all, in terms of commodity traceability and anti-counterfeiting, blockchain technology can help enterprises realize the traceability of commodities and ensure that the data is not tampered with. Consumers can more intuitively understand the whole process of production and transportation of commodities, thus enhancing the sense of trust. Blockchain effectively solves the problem of counterfeit goods in cross-border e-commerce by identifying the authenticity of goods through smart contract technology and preventing data from being tampered with. The advantages of decentralization, convenience, high security, and low cost possessed by blockchain can be applied to the cross-border e-commerce industry to create new cross-border payment methods, such as peer-to-peer payment, bypassing the intermediate links of third-party financial institutions [5]

After a panoramic understanding of theoretical research on blockchain enabled supply chain through bibliometric analysis and inductive deductive analysis, the thesis summarizes the topic clustering and core viewpoints of research schools. This research mainly discusses the research debate on blockchain enabled supply chain and puts forward the blind area of blockchain enabled supply chain research [6].

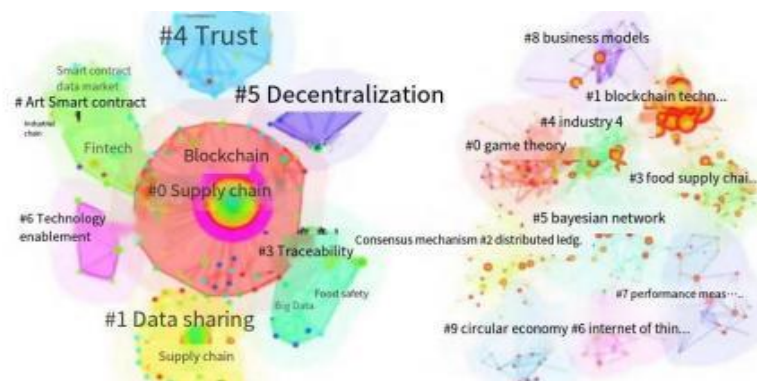


Figure 3: Related literature topic clustering graph

### 3. Security threats to convergence

#### 3.1. Two major challenges

In cross-border e-commerce, blockchain technology faces two main challenges, security and legal regulatory differences, and these two challenges are closely linked and interact with each other.

First, security is the primary challenge for the application of blockchain technology in cross-border e-commerce. Although blockchain technology has the characteristics of decentralization, transparency and openness, and non-tampering, these characteristics also make it face a series of security threats. The security problems of blockchain technology can be divided into the following categories, in order of data layer, network layer, consensus layer, incentive layer, application layer and contract layer, because of its specificity, there is mainly a "consensus layer problem" in cross-border e-commerce, for example, 51% attack, phishing attack and routing attack, etc., are the security problems that blockchain technology needs to face. For example, 51% attacks, phishing attacks and routing attacks are all security issues that blockchain technology needs to face[7]. These attacks may lead to data leakage, transaction tampering, or loss of funds, which seriously undermines the security of cross-border e-commerce transactions and consumer trust. At the same time, legal regulatory differences also bring challenges to the application of blockchain technology in cross-border e-commerce. There are differences in legal perceptions and regulatory policies of blockchain technology in different countries and regions[8], which makes cross-border e-commerce companies need to comply with laws and regulations of different countries in the course of their operations, increasing the complexity and risk of operations.

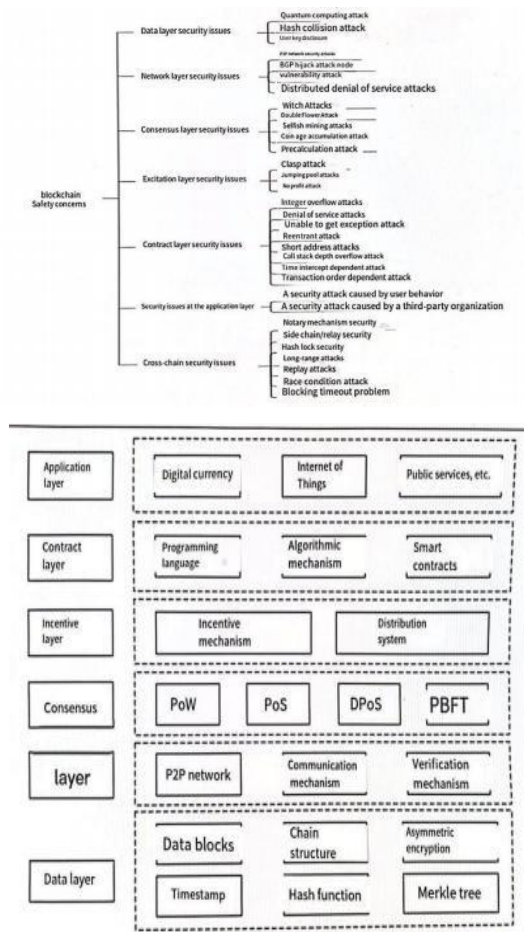


Figure 4: Classification of blockchain security issues

### 3.1.1. Major security threats to blockchain technology

As the research of blockchain technology continues to deepen and the application fields continue to expand, the defects of blockchain technology and the complexity and diversity of the application scenarios and other security problems are gradually revealed[8]. The number of security incidents in blockchain is increasing yearly, and the representative security incidents in the history of blockchain development are shown in the table. The security problem has become an important factor restricting the development of blockchain [8]. Therefore, research on blockchain security has become the focus of the industry.

| Time          | Security incidents                                                                | Incident impact                                                                                                                                                |
|---------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| December 2013 | At least five users' accounts on the OKcoin exchange were stolen at the same time | In total, nearly 640,000 yuan worth of Bitcoin and Litecoin was lost                                                                                           |
| February 2014 | Mt.Gox, the world's largest bitcoin exchange, is hacked                           | 850,000 bitcoins were stolen and the damage was worth nearly half a billion dollars                                                                            |
| January 2015  | Bitstamp, the world's third largest bitcoin exchange, is hacked                   | 19,000 bitcoins lost                                                                                                                                           |
| June 2016     | The DAO, the Ethereum star project, is hacked                                     | About 3.6 million ether tokens were stolen                                                                                                                     |
| July 2017     | Multi-signature wallet service Parity is hacked                                   | 153,000 ether tokens were stolen                                                                                                                               |
| January 2018  | Japanese Bitcoin exchange Coincheck is hacked                                     | 523 million NEM coins were stolen and the damage was worth \$530 million                                                                                       |
| November 2019 | South Korean cryptocurrency exchange Upbit was hacked                             | 34,000 ether coins were stolen                                                                                                                                 |
| December 2020 | Old public chain Aeternity was hacked 51%                                         | Lost more than 39 million AE tokens                                                                                                                            |
| August 2021   | Polynetwork, a cross-chain interoperability protocol, is hacked                   | \$110 million worth of crypto assets were stolen                                                                                                               |
| March 2022    | Ruin, a blockchain project platform, is hacked                                    | 173,000 ETH and 25.5 million USDC were stolen, with a loss value of approximately \$625 million. It was by far the largest security incident in DeFi's history |

| Comparison items            | Blockchain                            | League members                                                  | A single person or organization                         |
|-----------------------------|---------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------|
| Participating subjects      | Any person or organization            | League members                                                  | A single person or organization                         |
| Access rights               | Freedom to join and exit              | Authorize joining and exiting                                   | Attribution to a person or internal organization custom |
| Billing node                | All participants                      | League negotiated decision                                      |                                                         |
| Consensus mechanism         | PoW, PoS[9], DPoS[10], etc            | PBFT[11], Raft[12], DPoS, etc                                   | PBFT, Paxos[13], Raft, et al                            |
| Identity information        | Anonymity                             | Known                                                           | Known                                                   |
| Degree of centralization    | Decentralization                      | Multi-centralization                                            | Centralization                                          |
| Transaction efficiency      | Low                                   | Higher                                                          | High                                                    |
| Security                    | Low                                   | Higher                                                          | High                                                    |
| Application characteristics | Nodes do not need to trust each other | A small number of nodes on the chain have a high level of trust | There needs to be a high degree of trust between nodes  |
| Typical representative      | Bitcoin, Ethereum                     | Hyperledger, Enterprise Ethereum Alliance                       | Centralized exchange                                    |

Figure 5: Security incidents in history

At the beginning of the period, the attacks that blockchain is most likely to receive belong to quantum attacks, against quantum computing attacks, although at this stage, quantum computing is not enough to pose a serious threat to cryptographic algorithms in blockchain, but it is necessary to speed up the research of post-quantum cryptography (Post-Quantum Cryptography) algorithms that are resistant to quantum computing attacks. At present, the CRYSTALS-Kyber algorithm (for key encapsulation) and CRYSTALS-Dilithium algorithm (for digital signature) developed by IBM, the Falcon algorithm (for digital signature) developed by France's Thales, the SPHINCS+ algorithm (for digital signature) developed by Germany's Infineon has been selected by the U.S. National Institute of Standards and Technology (NIST). National Institute of Standards and Technology (NIST) PQC (Post-Quantum Cryptography) standardized algorithm [1].

In addition to this, the main threats are as follows:

a. Double Spending Attack (Double Spending Attack), mainly for the PoW consensus mechanism of an attack, the attacker with the transaction validation time there is a delay and other factors, and constantly initiated and withdrawn transactions, in order to achieve the repeated use of the same digital assets so as to achieve the purpose of illegal profits. At present, there are mainly five forms of double-flower attack, namely, 51% attack (51% Attack), Vector76 Attack (Vector76 Attack), Race

Attack (Race Attack), Finney Attack (Finney Attack) and Alternative History Attack (Alternative History). Attack.) Taking 51% attack as an example, the attacker uses the same digital asset to trade with two node objects. The attacker first initiates transaction A to node 1, and puts a certain number of tokens to the exchange, and when transaction A is confirmed, the tokens are exchanged, and transaction A is recorded into the blockchain; meanwhile, the attacker initiates transaction B to node 2, and due to the strong arithmetic power of the attacker, it can be achieved by forking the blockchain if its arithmetic power is more than 51%.[6] When the attacker has a strong computing power, when his computing power exceeds 51%, he is able to create a new chain for mining by forking , and according to the principle of the longest chain of the blockchain [9] when the length of the new chain exceeds that of the original main chain, the original chain will be invalidated, the new chain will become the main chain, the transaction B will be confirmed, and the transaction A will become invalid. The tokens placed by the original chain will revert back to the attacker's account, but the attacker has obtained the exchange gold of the previous transaction, thus successfully realizing the double spend.

b.Witch (Sybil) Attack: in blockchain network, the cost of creating a new identity or a new node by the user is extremely low, the attacker can join the blockchain network with a large number of forged identities, and after controlling a number of nodes and node identities, he/she performs malicious behaviors, such as misleading the routing table of the normal nodes, and decreasing the lookup efficiency of nodes of the blockchain network, etc. [10].

c.Endpoint Vulnerabilities: Although the blockchain technology itself is considered virtually "unbreakable", most of the endpoint computing devices where blockchain transactions take place are not secure. Hackers can observe user behavior and target vulnerabilities in endpoint systems to steal keys [11].

Security Threats of Asymmetric Cryptographic Algorithms: asymmetric cryptographic algorithms used in blockchain are central to ensuring blockchain security, but attacks against the algorithms are well established. Brute-force key breaking and interception of key exchange messages are the most common attacks.

### 3.1.2. Specific cases

DAO is a decentralized autonomous organization based on the ethereum blockchain that automatically performs management through smart contracts. In cross-border e-commerce, it helps automate supply chains and payment settlements. However, on June 18, 2016, a vulnerability in the DAO contract led to hackers stealing over 3.6 million Ether, triggering a crisis in the Ether community.

In the blockchain space, technological instability and security breaches have led to company closures and project shutdowns. For example, on April 22, 2018, Romania's BTCxChange exchange shut down as most operations had been suspended. [11]In May of the same year, a court in Florence, Italy banned the BitGrail exchange from resuming trading due to security concerns, after BitGrail announced that it had been hacked to steal approximately \$170 million in NANO coins.

Clearly, addressing blockchain security and its urgency.

## 4. Strategies and recommendations

### 4.1. Solutions to security threats

#### 4.1.1. Introduction of more advanced encryption algorithms and consensus mechanisms

You can choose the current internationally recognized encryption algorithms, such as, for example, AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), etc. These algorithms have been widely tested and applied, and have been proven to be safe and reliable.

Or assess the security strength of an algorithm, as the security of an encryption algorithm is usually related to its key length and the complexity of the algorithm. Longer key lengths usually imply higher security, and cross-border e-commerce companies and related administrators can increase security by strengthening key lengths because of the increased difficulty in cracking the keys. In addition, complex algorithms are more difficult for attackers to analyze and crack. We can also build a systematic security protection architecture[12].

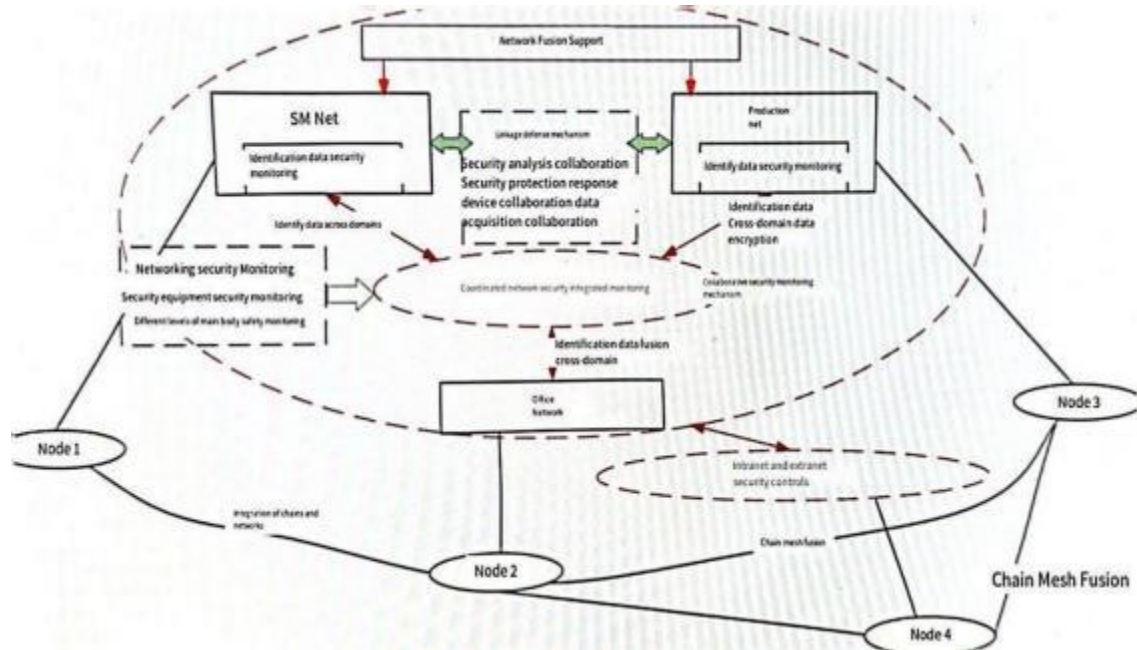
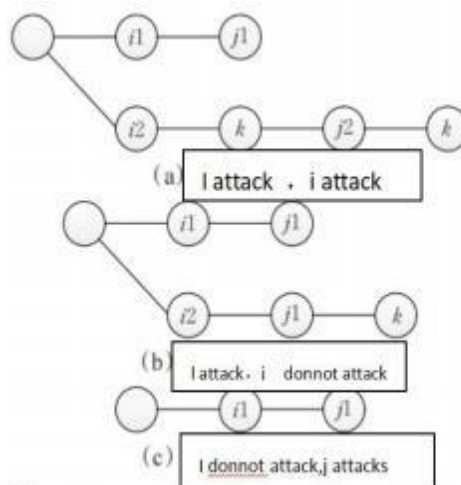


Figure 6: A systematic security architecture

#### 4.1.2. For problems such as double-flowering attacks

Researchers can make the arithmetic power as decentralized as possible by expanding the node size. As follows, we can construct relevant experimental models to try out the attack willingness[13]:



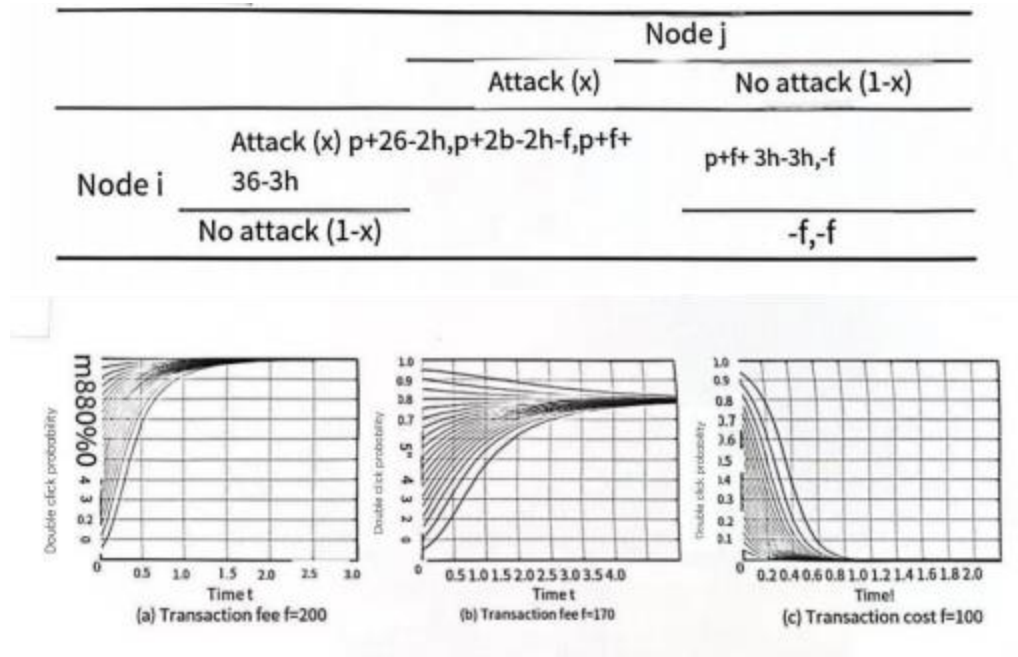


Figure 7: 51% double-flowered attack node revenue matrix

For this, researchers can use the following strategies.

#### 4.1.2.1. Combination of platform regulation and market regulation

The platform needs to set strict transaction fee standards. For transactions with different transaction prices, the corresponding maximum value of transaction fees should be set, and the initiator of the transaction needs to pay the transaction fees within the specified range, which will make the nodes tend to choose the no-attack strategy based on the consideration of maximizing revenue. In addition, considering the incentives for miners, the minimum fee for each transaction can be decided by miners. This method of combining platform regulation with market regulation is conducive to ensuring the efficiency of resource allocation on the basis of improving blockchain security.

#### 4.1.2.2. The corresponding risk monitoring level is divided according to the price interval

Although regulating the transaction cost can effectively inhibit the emergence of 51% double-flowering attack, it cannot be completely eliminated, so it is necessary to formulate the monitoring mechanism of the platform to constrain and punish the malicious behavior of the nodes. According to the conclusion obtained in the previous section, the evolution of node attack willingness in different transaction price intervals is different, and the effect of suppression is also different. Therefore, the transactions in the platform can be divided into four risk levels based on different prices, from low to high: slightly dangerous, generally dangerous, highly dangerous, and extremely dangerous. Transactions with higher risk levels have a greater likelihood of attack and produce greater harm, and require focused supervision. In the course of supervision, various risk-related information is collected and analyzed, possible risks are predicted, and early warnings are given in a timely manner. For attacks that have already occurred, the transaction and mining activities of nodes are immediately restricted and penalized. This method can more effectively and timely reduce the harm generated by the 51% double-flower attack. Experiments have proved that people can predict the nodes' willingness to attack by controlling their location, the

## 4.2. Solutions to international legal and regulatory policy differences

### 4.2.1. Errors caused by different legal provisions

In countries where blockchain technology and cryptocurrencies are prohibited or strictly regulated, cross-border e-commerce companies may face strict market access restrictions, and we are unable to utilize blockchain technology to optimize the transaction process and reduce costs due to the risks associated with blockchain technology, which leads to an increase in the risk of the success rate of buying and selling. In addition to this, differences in regulatory policies lead to significant differences in the operating environments faced by cross-border e-commerce in various countries. In countries with strict regulations, cross-border e-commerce companies need to invest more resources to ensure compliance, which increases operational costs.

Differences in regulatory policies lead to significant differences in cross-border payment costs. In countries that support blockchain technology, cross-border e-commerce companies can utilize blockchain technology to reduce the cost of cross-border payments, such as reducing intermediaries and handling fees. In countries with strict regulation, however, cross-border e-commerce companies may need to make cross-border payments through multiple intermediaries, leading to an increase in payment costs.

### 4.2.2. Solution

Solutions to international legal and regulatory policy differences in the application of blockchain technology can be summarized as follows:

First, companies or organizations conducting cross-border e-commerce should conduct in-depth research on the laws and regulations of different countries and regions involved in the application of blockchain technology. As there are significant differences in the regulatory policies for blockchain, digital currencies and smart contracts and other technologies in different countries, it is important to fully understand and comply with local legal requirements. Detailed legal advice and risk assessment can also be provided to the enterprise by engaging professional legal and financial advisors.

Second, compliance requirements should be fully considered during the design, development and implementation of blockchain technology. For example, in the preparation of smart contracts, it should be ensured that the terms of the contract are in compliance with local laws and that contents that may lead to legal disputes are avoided. Enterprises should regularly review and assess the compliance of the blockchain system to ensure that the operation of the system meets the requirements of laws and regulations.

Due to the transnational nature of blockchain technology, regulatory cooperation among countries is particularly important. Through the establishment of an international cooperation mechanism, uniform regulatory standards can be jointly formulated to reduce legal conflicts and uncertainties. International organizations such as the International Monetary Fund (IMF) and the World Bank (WB) can play an important role in promoting cooperation and exchanges among countries in blockchain regulation.

The regulatory policies of blockchain technology are constantly evolving and changing, and enterprises should pay close attention to international regulatory developments and trends. Understand and master the latest regulatory policies and regulatory requirements in a timely manner so as to adjust their business strategies and business models in a timely manner. Measures such as in-depth study of laws and regulations of various countries, compliance design and review, establishment of international cooperation mechanism, balance between technological innovation and regulation, strengthening enterprise self-discipline and risk management, and paying attention to

international regulatory developments can effectively reduce legal risks and promote the healthy development of blockchain technology.

#### 4.2.3. Specific cases

Between 2018 and 2020, an online casino case in Guangzhou involved 420 million virtual coins valued at up to RMB 8 billion. In the face of the security dangers posed by blockchain technology, the Chinese government has acted swiftly and successfully cracked down on such crimes by clarifying the regulatory framework and strengthening laws and regulations. Despite the complexity of blockchain technology, Chinese law enforcement authorities have ensured the applicability and fairness of the law by relying on methods such as analogical and purposive interpretation. In this case, Xie Moumou, Liu Moumou and 10 others were sentenced and fined for the crime of opening a casino[13].

By strengthening regulation, improving laws and raising legal awareness, we can not only reduce legal risks, but also promote the healthy and safe development of blockchain technology.

## 5. Conclusion

Legal perceptions of blockchain technology and regulatory policy differences in different countries and regions have far-reaching implications for cross-border e-commerce operations. Cross-border e-commerce companies need to carefully assess the regulatory environment and policy differences in each country's market and formulate appropriate operational strategies to meet these challenges. Meanwhile, cross-border e-commerce companies can also utilize blockchain technology to gain competitive advantages in terms of improving operational efficiency, reducing operational costs, and enhancing consumer trust. Therefore, this paper is of great significance in helping academics to understand the development, knowledge architecture, and hot topics of blockchain combined with cross-border e-commerce, and then suggesting how to address security threats in the Chinese context.

## References

- [1] Wang Yan<sup>1</sup>, Pan Zhensheng<sup>2</sup>, Jia Linpeng<sup>3</sup>. *Research on Intelligence Analysis of Virtual Currency Money Laundering Crime in the Era of Blockchain 3.0*, 2024(1) 1-7
- [2] Li Xianghong, *Blockchain-driven Cross-border E-commerce Supply Chain Collaboration and Symbiosis Management Innovation*, 2024(02) 1-4
- [3] QiqiWenku, *Blockchain Technology in Cross-Border E-Commerce: Opportunities and Challenges*, 2012(2) 2-7
- [4] Wu Tong, *The application of blockchain in the field of monetary finance: theory and demonstration*, 2020, 4-16
- [5] Liu Kunyang, *Research on blockchain technology adoption behavior of cross-border logistics enterprises*, 2024(04)
- [6] Li Qiuxiang<sup>1</sup>, Ma Caoyuan<sup>2</sup>, Huang Yimin<sup>3</sup>, Qi Ershi<sup>4</sup>, *Dynamics of blockchain empowerment supply chain research: perspectives, context, arguments, and blind spots*, 2024, 44(06)
- [7] Wang Lei<sup>1</sup>, Ren Nan<sup>2</sup>, Li Baozhen<sup>3</sup>, *Study on evolutionary game and prevention strategy of 51% double flower attack of blockchain*, 2020, 56(03)
- [8] SHENCHUAN-nian, *Summary of research on blockchain security issues*, 2024, 46(01)
- [9] Ning Ma, *Countermeasures of the Chinese Government to Prevent the Risks of Virtual Currency*, 2023(02)
- [10] Wu Tong, *Blockchain Application in Monetary and Financial Field: Theory and Empirical Evidence*, 2022(02)
- [11] *Challenges and Opportunities of Blockchain for Cross-Border E-Commerce in Developing Countries*, 2023(01)
- [12] Zhujun, *Research on Data Security Framework Based on the integration of identity and Blockchain*, 2024, 51(s1)
- [13] Shen Chuannian, *Summary of research on blockchain security issues*, 2024, 46(01)