Research on the Application of Blockchain Technology in the Traceability of Intellectual Property Infringement Liability in Cross-Border E-Commerce

Jingjie Li

School of Public Administration and Law, Liaoning Technical University, Fuxin, China

1750374422@qq.com

Keywords: Cross-Border E-Commerce; Intellectual Property Infringement; Blockchain Technology

Abstract: Against the backdrop of economic globalization and the rapid development of digital trade, cross-border e-commerce has become an important form of international trade. However, frequent intellectual property infringement issues have posed numerous challenges to traditional tracing methods. Research on the tracing of intellectual property infringement liability in cross-border e-commerce is of great significance. It can not only maintain market order, but also protect the legitimate rights and interests of right holders, and promote the healthy development of the industry. This paper sorts out the main forms of intellectual property infringement in cross-border e-commerce. These forms include trademark counterfeiting and imitation, patent infringement, and copyright piracy. At the same time, it summarizes the core difficulties of traditional tracing methods. These difficulties include information silos, evidence tampering, unclear liability subjects, and cross-border collaboration obstacles. In addition, this paper focuses on analyzing the immutability and traceability of blockchain technology and explores its application advantages in the tracing of infringement liability. On this basis, this paper further discusses the specific application paths of blockchain technology in intellectual property right confirmation, evidence preservation, and supply chains information transparency. Meanwhile, it points out the practical obstacles of blockchain in terms of technical implementation, legal protection, economic costs, and promotion and application. Overall, blockchain technology provides a new solution path for the tracing of intellectual property infringement liability in cross-border e-commerce. However, to achieve comprehensive promotion, it is still necessary to overcome various difficulties.

1. Introduction

1.1. Research Background

In recent years, digital technologies have promoted the rapid development of cross-border e-commerce, which has become an important force in global trade growth. However, the cross-border transaction characteristics of cross-border e-commerce have increased the risk of Intellectual Property infringement, and problems such as trademark counterfeiting, Patent Infringement and copyright piracy are not uncommon, which have seriously damaged the interests of right owners and consumers. According to statistics, about 10% of cross-border e-commerce commodities globally have Intellectual Property Dispute. Concealment and transnationality make the qualification of infringement Liability complicated. Traditional accountability methods face many problems, including fragmented supply chain Information, easy Change of electronic exhibits, unclear definition of liability subjects, and cross-border legal conflicts. These problems lead to difficulties in the rights protection process. Infringing acts often involve production, warehousing and sales links across multiple countries, intellectual property (IP) protection Standards of various countries are not unified, and efficiency of transnational law enforcement cooperation is relatively low, forming a situation of "easy to infringe, difficult to protect rights". In this context, blockchain technology provides a new path for solving traceability problems. Its distributed ledger can integrate the whole-process Information of cross-border supply chains, smart contracts can realize infringement monitoring and exhibits fixing, and time stamping technology provides strong support for judicature. At present, blockchain has achieved initial results in the field of domestic e-commerce logistics traceability.

  DOI: 10.25236/gemmsd.2025.111

However, in cross-border businesses, adaptability of technical application, legal Compliance Guarantees and multi-party collaboration mechanisms still need to be further improved.

1.2. Research Significance

The application of blockchain technology in tracing intellectual property infringement liability in cross-border e-commerce has significant theoretical and practical value. From a theoretical perspective, exploring the application of blockchain characteristics in the field of intellectual property protection can enrich the theoretical system of intellectual property protection. It can also bring new perspectives and insights to related academic research. Through an in-depth analysis of blockchain technology, it can provide useful references for the formulation of future relevant laws and regulations. From a practical perspective, with the rapid development of cross-border e-commerce, the demand of enterprises and consumers for intellectual property protection is becoming increasingly urgent. The application of blockchain technology can significantly improve the efficiency of infringement liability traceability. It can also strengthen the protection of intellectual property rights and promote the formation of a fair market competition environment. This study provides feasible solutions for cross-border e-commerce platforms, regulatory agencies, and legal service institutions. It is conducive to the healthy development of the cross-border e-commerce ecosystem. The exploration of blockchain technology in the traceability of intellectual property infringement liability has profound practical significance.

2. Current Situation of Intellectual Property Infringement in Cross-Border E-commerce and Difficulties in Traceability

2.1. Main Forms of Intellectual Property Infringement in Cross-Border E-commerce

2.1.1. Trademark Counterfeiting and Imitation

In cross-border e-commerce, trademark counterfeiting and imitation are the most common and direct forms of infringement. Counterfeiting means the unauthorised use of a registered trademark that is identical to the genuine one on the same type of goods [1]. Its main feature is “passing off the fake as genuine.” Infringers copy the original product’s appearance to deceive consumers. Imitation is more hidden. It usually refers to the unauthorised use of a similar trademark on related goods or the use of another person’s product name, packaging, or decoration. This causes market confusion and makes the public believe that the product has a connection with the right holder.

In cross-border e-commerce, infringers take advantage of distance, information gaps, and the complexity of logistics. They build independent websites, attract customers through social media, or open shops on third-party platforms. Fake and imitation goods are then sold to the global market. Such actions harm brand reputation and market share. They also damage consumer rights, disturb fair competition, and affect the image of the country.

2.1.2. Patent Infringement

Patent infringement in cross-border e-commerce mainly involves invention patents, utility model patents, and design patents. These types of patents have high technical content and strong concealment. This makes it difficult to identify infringements. For invention and utility model patents, infringement often appears as unauthorised manufacturing, use, sale, or import of patented products or methods. Such cases are common in technical goods such as electronic devices and mechanical parts. Infringers use design changes, small adjustments, or reverse engineering to avoid patent protection. This increases the difficulty of monitoring and collecting evidence.

Design patent infringement focuses on product shape or pattern. It often appears in clothing, household goods, and toys. Infringing goods usually look very similar to the original ones and rely on low prices to gain market share. This reduces the motivation for innovation. In cross-border trade, patents are valid only within certain regions. Infringement often occurs in countries where the patent is not registered [2]. Through complex supply chain networks, infringing goods reach the target market. This makes tracing and jurisdiction much harder.

2.1.3. Copyright Piracy

In cross-border e-commerce, copyright infringement occurs when protected works are reproduced and distributed without authorization [3]. Such infringing content includes software, films, music, and e-books. Digital products like games, design templates, and educational courses are also frequent targets of infringement. The growth of digital trade has transformed infringement methods. Infringement has evolved from selling physical discs to transmitting digital files online. Infringers distribute pirated content through illegal download sites or cloud storage links. Some individuals also sell pirated activation codes and video resource packages at low prices on e-commerce platforms. Additionally, unauthorized designs and texts are printed on merchandise for commercial sale. These activities undermine rights holders' revenues and diminish their incentive to create.Pirated software may contain viruses, creating significant security vulnerabilities. Counterfeit goods suffer from inconsistent quality, directly impairing consumer experience. These problems undermine the healthy development of the digital content industry.

2.2. Main Difficulties in Traceability of Infringement Liability

2.2.1. Information Silos: Fragmented Data in the Supply Chain

Cross-border e-commerce supply chain has the characteristics of multi-subject participation, lengthy chain and cross-region. Supply chain involves multiple roles such as raw material suppliers, manufacturers, exporters, logistics service providers, warehousing enterprises, importers and platform retailers [4]. Under traditional operation mechanism, subjects of each link adopt independent information management systems. Due to inconsistent data standards, interfaces cannot be docked, forming a typical "information island". The flow of commodity information is fragmented from production to consumption. The lack of data association and verification in each link makes it difficult to trace the source of infringing products. After intellectual property infringement occurs, rights holders cannot obtain complete supply chain data records. The circulation track and final destination of infringement products are difficult to identify. Data fragmentation significantly increases the time and economic cost of traceability investigation. The tracing process may also be interrupted due to certain information opaque links. This situation cannot construct a complete exhibits chain, which causes serious obstacles to the accurate tracing of infringement liability.

2.2.2. Evidence Easily Altered: Problems in Preserving Electronic and Physical Proof

In cross-border e-commerce infringing traceability, evidence preservation and Acknowledgement are very important. Evidence is divided into electronic and physical categories, both of which have respective difficulties in collection. Electronic evidence includes web page cache, Transactions Information and communication records [5]. Such evidence is volatile, easily tampered with, and easily lost. infringing parties can easily erase infringing facts by deleting data or clearing logs. Even if evidence is fixed through notarization, the technical process is often questioned. The state of physical evidence is prone to change during cross-border transportation. The packaging and markings of goods may be replaced or erased, weakening their relevance to infringing acts. Cross-border seizure, saisie and handover procedures are complex. The qualification Standards for evidence effectiveness also vary among different jurisdictions. Right holders find it difficult to construct a complete exhibit chain with judicial credibility. This situation significantly reduces the probability of successful rights protection.

2.2.3. Unclear Responsibility: Multiple Parties Make Attribution Difficult

The complex ecosystem of cross-border e-commerce leads to diversified and fragmented infringement liabilities, making it harder to determine responsibilities. An infringing product may involve multiple links and participants. The identity of overseas manufacturers as the source of infringement is often difficult to verify. Distributors and agents disperse liability through multi-level resales. As an information intermediary, the scope of application of the "safe harbor principle" of e-commerce platforms is unclear, and there are relatively large disputes over liability division. Logistics service providers may participate in the Infringement chain without knowledge. The multi-party

participation structure leads to the decomposition of Liability, and each subject shifts Liability to each other, making it difficult to clarify the Vesting of legal Liability [6]. Right holders face high cost and complex procedures when pursuing accountability one by one. If the core liable party cannot be identified, legal deterrence is difficult to form, and Infringement phenomena are repeatedly prohibited but not stopped.

2.2.4. Barriers to Cross-Border Cooperation: Differences in Laws and Enforcement

The territorial Limitations of Intellectual Property conflict with the globalized nature of cross-border e-commerce, leading to prominent cooperation obstacles [7]. Countries have legal divergences in terms of protection scope, infringing determination, Compensation amount and burden of proof. Some acts are infringing in one Country but legal in another. Judicial and law enforcement systems operate independently, lacking coordination mechanisms. Cross-border investigation and evidence collection, judicial assistance and Judgments enforcement face problems such as complicated procedures and long time-consuming. Differences in language, culture and business practices increase the communication cost. Institutional barriers enable infringing parties to exploit legal loopholes and commit infringing in countries with loose supervisory. Right holders are caught in "transnational rights protection dilemma" and find it difficult to form an effective global collaboration mechanism.

3. Theoretical Basis of Blockchain Technology Empowering Responsibility Traceability

3.1. Core Technical Features of Blockchain

3.1.1. Immutability and Traceability

The immutability of blockchain comes from its chain-based data structure and the use of hash algorithms. Each block contains the hash value of the previous block. The Merkle tree root hash integrates all transaction data in the current block [8]. These blocks form a tightly linked encrypted chain. Any small change in historical data will cause the hash values of all subsequent blocks to change. The system can detect and reject such actions immediately. This guarantees the integrity and stability of the data on the chain.

Both the time and the path of every transaction on the blockchain are recorded and indelible. All data could be tracked back to their historical path through the hash pointer. This is the solid technical support for the traceability of intellectual property rights. From rights to confirmation, information about rights confirmation to the circulation of the product cannot be tampered or deleted by any individual. It creates a credible and true evidence chain that can be traced.

3.1.2. Decentralisation and Distributed Ledger

The core of blockchain lies in its decentralized schema, which breaks the traditional centralized server patterns and adopts a peer-to-peer Networking structure. All participating nodes jointly maintain a synchronously copied distributed ledger, and data updates take effect only after being verified by the majority of nodes through consensus mechanisms (such as PoW, PoS), thereby avoiding the risks of centralized controls and single-node crashes [9]. In the process of constructing traceability in cross-border e-commerce, manufacturers, logistics enterprises, customs, platforms and consumers can all become data recording and verifying subjects of the supply chain and form a shared and credible data space. This method overcomes the trust crisis caused by Information asymmetry and power differential, and promotes the collaborative governance of all interested parties.

3.1.3. Automatic Execution of Smart Contracts

A smart contract is a program deployed on the blockchain. The contract terms or business rules are set in code. When preset conditions are met, the contract executes automatically. It does not require human participation or third-party coordination. The execution process is transparent, the result is certain, and the operation cannot be reversed.

In intellectual property protection, smart contracts have wide application potential. They can automatically pay licensing fees, monitor infringement, and store evidence. They can also send alerts

to regulators when certain standards are reached. This automation improves efficiency and accuracy in operations. It reduces trust costs and enforcement barriers. It turns the process from post-event legal action to proactive technical control. This reflects the idea that "code is law."

3.1.4. Authoritative Time Stamp Proof

Each transaction or data entry on the blockchain carries a timestamp created through the network's consensus mechanism. The timestamp is not issued by one central server. It is verified by many nodes and recorded in the block header. It has high credibility and cannot be tampered with. The timestamp marks the exact moment a piece of data is created or an event occurs.

These timestamps form a continuous and irreversible sequence. In confirming intellectual property and collecting evidence, such authoritative time proof is very important. It can prove the time of creation, transfer, or infringement. It provides strong and legally acceptable technical evidence. This solves the problem of fake or weak time evidence in traditional systems. It builds a solid time basis for determining ownership and tracing infringements.

3.2. Compatibility between Blockchain Technology and Traceability Needs

3.2.1. Breaking Information Silos and Building Reliable Data Flow

Data in the supply chain is often scattered. The main reason is the lack of a trusted data-sharing platform. Blockchain's distributed ledger provides a solution. Through a consortium chain, producers, brand owners, logistics providers, customs, and e-commerce platforms can jointly maintain a single and constantly updated product information record.

The data created at each stage (from raw materials' B2B records to production batches, quality reports, logistics and customs documents) is stored on the blockchain. The data is then publicly visible to authorised parties and cannot be altered, breaking the typical information silo. Scattered data points turn into a seamless, transparent and trustworthy chain of information. It enables total tracking from origin to end user and supplies a solid basis for accurate traceability.

3.2.2. Securing Infringement Evidence and Improving Legal Credibility

Electronic evidence is easy to alter, and physical evidence is easy to lose. Blockchain's immutability and timestamp functions offer an effective solution. When an infringing product link, transaction record, or physical item is found, key data such as the hash value, webpage screenshot, or product ID can be stored on the blockchain [10]. The timestamp records the exact moment of storage. The chain structure ensures that the evidence remains unchanged after being uploaded.

This "technical notarisation" improves the originality and integrity of electronic evidence. Courts are more likely to accept such data. Key details of physical evidence, such as serial or batch numbers, can also be linked to blockchain records. This builds a strong connection between online and offline evidence and forms a closed and reliable proof chain.

3.2.3. Clarifying Responsibility Chains and Achieving Accurate Accountability

Within a complicated supply chain, many parties are involved. Blockchain can record each participant's identity and action at every stage. This creates a clear responsibility chain. As items travel down the supply chain, each handling step, from warehousing to shipping, requires a signature in the form of a timestamp on the blockchain. The timestamp also records the exact time, operator, and action.

This allows anyone from production to sales to be tracked and documented. So, when counterfeiters are caught red-handed with an infringing product, investigators can follow the money trail back through the chain to identify the exact point and party at that point in time that committed the infringement. This precludes blame-shifting and vague liability. It transforms the fuzzy "networked responsibility" into a clear "linear responsibility" that is a sound basis for accountability and penalties.

3.2.4. Optimising Supervision and Improving Cross-Border Cooperation Efficiency

Barriers to cross-border cooperation come mainly from a lack of trust and coordination between

national authorities [11]. Blockchain can provide a shared and reliable data platform for customs and market regulators in different countries. Each participant can use the verified information on the chain to conduct supervision. This reduces repeated inspections and information verification costs.

Smart contracts can be used for automated compliance checks. When goods arrive at customs, the contract can automatically compare blockchain records of intellectual property authorisation. It can then allow quick clearance or accurate interception. Consensus-based coordination reduces communication costs and trust barriers. This lays a foundation for efficient and transparent cross-border joint enforcement and regulation of intellectual property.

4. Application Paths and Real Challenges of Blockchain Technology in Traceability

4.1. Analysis of Application Paths of Blockchain in Traceability

4.1.1. Intellectual Property Confirmation and Evidence Storage

Blockchain technology plays an important role in the confirmation and depositing of intellectual property rights, providing authoritative, efficient, and economical "identity proof" for original creations and patent technologies. Creators can instantly upload core information such as the digital fingerprint, design blueprint, or patent explanation of their works to the blockchain for depositing upon completion of creation or submission of the requisition. The timestamp feature provides exact time evidence for the deposited data, and the tamper-proof attribute ensures the originality and integrity of the materials. Blockchain transforms the traditional time-consuming and high-cost enlistment method into a technology-based right confirmation pattern that takes effect instantly and is globally endorsed. This application provides preliminary vouchers for disputes over entitlement ownership and offers a reliable foundation for licensing, reassigning, and rights protection, consolidating the legal status of right holders.

4.1.2. Supply Chain Transparency across the Full Process

Rebuilding information sharing in cross-border e-commerce supply chains is a key direction. Distributed ledger technology can assign each product a unique digital identity (hash ID). It records important data from raw material purchase, production, testing, storage, logistics, customs, to final sale. Each stage uploads its data according to permission rules. All nodes keep a shared digital record that no one can alter. Authorised brands, regulators, and consumers can check the circulation and condition of goods at any time. Full transparency stops fake and low-quality goods from entering the market. When infringement happens, the source can be traced quickly. The accuracy and timeliness of tracing improve greatly.

4.1.3. Smart Detection and Evidence Collection for Infringement

Blockchain can work together with artificial intelligence and big data analysis to build a smart monitoring system. Web crawler tools can watch e-commerce platforms all the time. When a suspicious link appears, the system records the hash of the webpage and transaction data on the blockchain [12]. Evidence is fixed at the moment of discovery. Smart contracts can also check if a product's record matches official authorised channels. If the product code is repeated or inconsistent, the contract gives an automatic warning and saves related evidence. This makes the process proactive instead of passive. Infringement can be recognised, recorded, and reported immediately. The right holder gains valuable time to protect their rights and can use strong electronic proof.

4.1.4. Multi-Party Collaborative Governance Mechanism

Blockchain's decentralisation and consensus mechanism enable parties from different sectors to collaborate on a consortium chain comprising brands, e-commerce sites, logistics firms, payment institutions, industry associations and even government agencies can join a consortium chain may set rules for sharing data and governance smart contracts perform compliance checks and rules for handling disputes if parties cannot reach an agreement if a breach of contract is confirmed, the smart contract sends an instruction to the platform to kick out or block the seller. It also informs logistics

and payment institutions to take related actions. This system connects information and actions among all participants. It replaces isolated operations with a joint enforcement network that is efficient, transparent, and fair. It also upgrades the system from single-party protection to cooperative governance.

4.2. Real Challenges in the Application Process

4.2.1. Technical Challenges: Performance, Data Privacy, and Cross-Chain Issues

Blockchain has strong potential, but technical barriers remain. The speed of transaction processing is still low. Public chains cannot meet the high transaction volume of cross-border e-commerce. Consortium chains are faster but lose some decentralisation. Data privacy also causes concern. The need for supply chain transparency conflicts with the need to protect trade secrets. How to make data usable but invisible to unauthorised parties is a key issue. Privacy tools like zero knowledge proofs are still far from being widely used. Moreover, companies and organisations often use different blockchain platforms, and the lack of cross-chain communication creates new “on-chain silos”. Without secure and efficient cross-chain protocols, data flow and value transfer are hindered.

4.2.2. Legal Challenges: Validity of On-Chain Evidence and Data Compliance

Legal adaptation is another barrier. Currently, it is unclear when blockchain evidence will be legally recognized. The technology can guarantee authenticity, but laws and regulations vary among legal systems, and many countries lack clear-cut laws and judiciable standards. Data sovereignty and compliance create extra burdens. E-commerce data is usually transboundary data, but laws like the EU's GDPR and China's Data Security Law have very stringent requirements on data storage and transfer. If personal or trade data is recorded on the blockchain, it may conflict with localisation requirements. This increases compliance risks and legal uncertainty for enterprises.

4.2.3. Economic and Promotion Challenges: Cost and Lack of Incentive Mechanisms

The widespread use of blockchain is limited by costs. The on-chain cost covers development cost, maintenance cost, hardware upgrading cost, training cost and transaction cost. The above costs constitute the cost barrier for the application of blockchain in large, small, medium and micro enterprises. Moreover, the absence of collaborative incentive mechanism leads to the lack of participation of all parties. Stronger parties are unwilling to share because of the uneven cost and benefit. Weak parties are also unwilling to participate because of the cost. Establishing an incentive mechanism to balance cost and benefit is very important for the commercial application of blockchain.

5. Conclusion

Blockchain technology provides an innovative approach to trace the liability of intellectual property infringement in cross-border e-commerce. Through its non-tamperable, traceable, and distributed attributes, blockchain can address problems such as data silos, evidence tampering, unclear liability, and cross-border cooperation barriers. It promotes rights confirmation, supply chain transparency, and smart detection of infringement behaviors, boosts regulatory efficiency and judicial endorsement, and lays the foundation for building a high-impact protection mechanism.

But there are also challenges for blockchain applications at the levels of technology, law and economy. At the level of technology, they should solve the problems of performance limitations, protection of privacy and cross chain. At the level of law, they should prove the evidential validity on the chain and solve the problem of data sovereignty. At the level of economy, they should reduce cost and design the incentive mechanism. In the future, with the optimization of technology, law and participation of all parties, and will apply blockchain in the protection of intellectual property, punish counterfeiting and promote the standardization of cross border e-commerce.

References

[1] Zhu Chaoyu. Judicial Identification of the Objective Aspect of the Crime of Counterfeiting

Registered Trademarks [D]. East China University of Political Science and Law, 2019.

[2] Wei Jiali. Reflection and Revision on the Principles for Determining Design Patent Infringement [D]. Southwestern University of Finance and Economics, 2020.

[3] Wang Qian. The Legitimacy of Technological Measures Protected by Copyright Law [J]. Chinese Journal of Law, 2011(4):18. DOI: CNKI:SUN:LAWS.0.2011-04-007.

[4] Li Xianghong, Lu Minfeng. Research on the Application of Blockchain Technology in Supply Chain Finance under the Cross-Border E-Commerce Scenario [J]. Financial Theory and Practice, 2023(6):51–59.

[5] Yang Lu. Conflicts and Solutions in Cross-Border Criminal Electronic Evidence Collection [D]. East China University of Political Science and Law, 2022.

[6] Du Xin. Research on the Countermeasures against Intellectual Property Infringement Risks in China's Export Cross-Border E-Commerce [D]. Dalian Maritime University, 2023.

[7] Zheng Luying. Governance of Intellectual Property Rights in Cross-Border E-Commerce: Dilemmas, Causes and Solutions [J]. Journal of International Trade Issues, 2021(10):110–118.

[8] Zhang Liang, Liu Baixiang, Zhang Ruyi, et al. A Survey of Blockchain Technology [J]. Computer Engineering, 2019.

[9] Wang Xiaoguang. A Review of Consensus Algorithms in Blockchain Technology [J]. Information & Computer, 2017(9):3. DOI: CNKI:SUN:XXDL.0.2017-09-028.

[10] Luo Yong. Specific Identification and Easy Comparison: Legal Definition of Personal Information in the Context of Blockchain [J]. Study and Exploration, 2020(3).

[11] Cheng Xuejun. International Experience in Regulating Blockchain Technology and China's Strategies [J]. China Circulation Economy, 2021, 35(3):13.

[12] Zhang Zijie. Research on Digital Copyright Protection from the Perspective of Blockchain Technology [D]. Hunan University of Commerce, 2020.