Original Research Article

Blockchain technology and antitrust compliance: Data traceability and trusted governance ecosystem

Haishui Yan[1], *Yajun Wang*[2]

1 Chairman of the Board, Zhonghe Digital Union (Beijing)Technology Co., Ltd., Beijing, 102218
2 Senior Partner, Deputy Director, Capital Equity Legal Group (Shanghai), Shanghai, 201199

Abstract: In the context of the rapid development of the national digital economy and platform economy, the risk of platform companies abusing data and algorithms to monopolize markets has become increasingly prominent. Traditional antitrust compliance models face challenges such as information asymmetry, difficulty in evidence collection, and delayed post-event supervision, which make it difficult to address the covert and dynamic nature of platform monopolistic behaviors. Blockchain technology, with its features of decentralization, immutability, traceability, and smart contracts, provides new pathways for building a trusted data traceability system and a multi-party trusted governance ecosystem. This paper, starting from the national antitrust policy and regulatory needs, explores the practical paths for blockchain-enabled antitrust compliance, such as data on-chain, smart contract regulation, privacy protection, and industry standard-setting. Through case studies and application scenarios, the paper demonstrates the technological feasibility and regulatory value. Additionally, the paper proposes countermeasures to address implementation challenges related to technical costs, legal validity, privacy protection, and industry coordination. The research suggests that blockchain technology is expected to play a foundational supporting role in future antitrust compliance, contributing to the establishment of an efficient, transparent, and sustainable fair competition order.

Keywords: Blockchain Technology; Antitrust Compliance; Data Traceability; Trusted Governance; Platform Economy

1. Introduction

In the context of the accelerated development of the national digital economy, the platform economy has driven innovation and enhanced consumer welfare, but it has also introduced potential market monopolies and unfair competition risks. In recent years, regulatory authorities have strengthened antitrust enforcement and data governance requirements for platform companies. These regulations not only aim to combat overt monopolistic behaviors but also focus on identifying and preventing competition distortions hidden within data and algorithms. However, traditional antitrust compliance methods primarily rely on post-event investigations, manual reviews, and offline evidence collection, which are ill-suited to handle the challenges posed by the massive data, rapid data flow, and covert nature of behaviors in the platform economy.

Faced with this predicament, the rise of blockchain technology offers new possibilities for antitrust compliance. The core characteristics of blockchain—decentralization, data immutability, traceability—make it uniquely advantageous in recording market transaction trajectories, storing key data on-chain, and building a trusted governance ecosystem. When antitrust regulation and platform compliance practices face issues like data asymmetry, difficulty in evidence collection, and opacity, blockchain technology has the potential to provide a solution by creating a distributed ledger and trusted data verification system that facilitates real-time supervision, transparent review, and automated compliance management.

Current regulatory trends have highlighted the demand for data credibility and traceability in supervision. The revision of the "Antitrust Law" and implementation guidelines increasingly focus on the legal use of platform data, the fairness of algorithmic behaviors, and the dynamic monitoring of market shares. At the same time, the industry has become aware of how blockchain technology can support compliance reviews and evidence preservation in areas such as supply chain finance, distribution management, and pricing mechanisms. Enterprises, industry associations, and technology service providers are attempting to move business data and compliance rules onto the blockchain using consortium blockchains and smart contracts to reduce data falsification, evidence loss, and regulatory delays from the very start.

This study aims to explore the integration of blockchain technology with antitrust compliance in the national context. Beginning with an analysis of national antitrust policies and the pain points of compliance, the paper will explain the core features of blockchain technology and its potential in building a trusted data governance ecosystem. The study will then examine practical paths for antitrust compliance using blockchain, such as data on-chain, smart contracts, and tiered permission management, and demonstrate the actual effects and challenges of blockchain enablement through case studies and industry comparisons. Finally, the paper will provide countermeasures to address challenges in implementation, including technical costs, legal effectiveness, privacy protection, and industry coordination.

The significance of this study is that it offers a new compliance approach and technical toolbox for regulatory agencies, platform companies, and industry participants in the ever-evolving digital economy landscape. By deeply integrating blockchain with antitrust compliance, this research aims to shift from passive, delayed post-event regulation to real-time, transparent, and intelligent preemptive warnings and preventive measures. This study also offers insights for future policy refinement and the creation of industry standards, laying the foundation for increasing the country's influence in international data governance and antitrust sectors.

2. Antitrust compliance pain points and data credibility issues

2.1. Current national antitrust regulation and policy direction

In recent years, the national government has gradually strengthened antitrust regulation in the platform economy sector. Since the formal implementation of the "Antitrust Law" in 2008, regulatory authorities have accumulated considerable enforcement experience in traditional sectors such as bulk commodities, pharmaceuticals, and financial services. However, with the rise of the platform economy, new monopolistic issues have emerged. For example, some large e-commerce platforms restrict merchants from operating across multiple platforms through "exclusive contracts" or manipulate search rankings and price signals using algorithms, which damages the competitive position of small and medium-sized merchants and new entrants.

Against this backdrop, the revision of the "Antitrust Law" and related supporting policies increasingly emphasize data governance and compliance requirements in the platform economy. Regulators require platform enterprises to assess the compliance of their data collection, storage, and usage, and take greater responsibility for the fairness and transparency of algorithmic strategies. These policy initiatives reflect the regulatory authorities' efforts to deal with emerging market players and competitive behaviors, as well as their urgent need to enhance data credibility and improve enforcement efficiency.

2.2. Traditional compliance models and evidence collection challenges

Traditional antitrust compliance practices rely more on post-event investigations and document reviews. The enforcement process often involves substantial manual evidence collection and verification. However, market behaviors in the digital era are highly dynamic, with diverse and decentralized data sources. Platforms continuously alter market environments through real-time pricing strategies, recommendation algorithms, and traffic allocation mechanisms. This reality has led traditional models into the following difficulties:

1. **Information asymmetry and delay**: Regulatory bodies often struggle to access accurate, complete data evidence in a timely manner. They typically acquire information only after a significant time has passed, missing the opportunity to intervene promptly.
2. **Difficulty in evidence preservation**: Internal company data may be altered, deleted, or difficult to trace after an event, making it challenging for regulators to gather solid evidence chains.
3. **Lack of cross-platform and cross-region coordination**: Platform monopolistic behaviors often involve multiple entities and cross-regional operations. Traditional evidence collection requires collaboration across various stakeholders, making it difficult to quickly establish a unified data view.

2.3. The need for data credibility and traceability

In platform economy compliance, data is not only the basis for assessing corporate behavior but also an essential reference for regulatory decision-making. Without data credibility and traceability, regulatory authorities may find it difficult to determine whether a company has abused its market dominance or engaged in anti-competitive agreements. Credible data should possess the following characteristics:

1. **Immutability**: Once data is recorded, it should not be modified arbitrarily to maintain the integrity and authority of the evidence.
2. **Traceability**: Regulators need to quickly trace the full history of data generation and changes, including its origin, timestamps, and responsible entities.
3. **Multi-party participation and verification**: A trusted data system should support multiple stakeholders in the data recording and validation process to reduce information silos and data monopolies.

In this context, finding a technology that enables cross-entity trusted data sharing while ensuring data immutability and high traceability is essential for antitrust compliance. Blockchain technology offers a new solution to achieve these goals. Through distributed ledgers, consensus mechanisms, and smart contracts, blockchain lays the foundation for building a trusted data ecosystem. The following sections will explore the core features of blockchain technology and how it can empower antitrust compliance through data governance and regulatory practices.

3. Core features of blockchain technology and its compliance application potential

Having established the urgent need for trusted data and traceability in antitrust compliance, it is essential to examine the core features of blockchain technology. Based on distributed ledgers, immutability, and smart contracts, blockchain provides the infrastructure and toolkit for creating a multi-party governance ecosystem. When enterprises, regulators, industry associations, and third-party certification bodies can all participate as nodes in the blockchain network, blockchain can break down information silos and achieve trusted data sharing and regulatory collaboration.

3.1. Blockchain technology basics and features

1. **Decentralization and distributed ledger**:

Blockchain maintains ledger data collectively through multiple nodes, eliminating the need for a single centralized institution. This structure weakens individual entities' control over data, reducing the likelihood of data being tampered with. In the antitrust compliance scenario, various stakeholders (platform enterprises, regulators, industry associations, third-party service providers) can simultaneously maintain and access the data, improving information transparency.

2. **Immutability and traceability**:

Blockchain uses cryptographic algorithms and consensus mechanisms (such as PoW, PoS, PBFT, etc.) to ensure that once data is confirmed, it is difficult to alter. When market transaction data, pricing strategies, traffic allocation information, or related proof materials are stored on the blockchain, no single node can alter historical records. In addition, each data record contains a timestamp and hash value, which makes it easy to trace its origin and change process, providing technical assurance for compliance audits and evidence preservation.

3. **Smart contracts and automated execution**:

Smart contracts are programmable logic that runs on the blockchain and automatically executes preset instructions when specific conditions are met. By encoding antitrust compliance rules into smart contracts, real-time monitoring and automatic alerts can be achieved. For example, once transaction data reaches a certain market concentration threshold, the smart contract can automatically notify regulatory nodes or restrict the continuation of certain behaviors.

3.2. Blockchain's logic in supporting antitrust compliance

1. **Trusted data preservation**:

By recording key market transaction data, price changes, platform policy adjustments, and other critical information on the blockchain, blockchain provides a foundation for evidence preservation. Regulators can directly obtain trusted data from the blockchain without relying on self-reported data from enterprises or post-event verification.

2. **Multi-party validation and real-time oversight**:

In consortium or permissioned blockchain scenarios, regulatory bodies, industry associations, and enterprises together form nodes in the blockchain network. Regulators can access blockchain data in real time and intervene in abnormal behaviors promptly. Industry associations can act as neutral nodes, endorsing and supervising the quality of data, thus introducing more diverse scrutiny into the competitive order.

3. **Rule embedding and automated compliance**:

By embedding legal standards, administrative guidelines, and industry standards into smart contracts, blockchain links rules and data deeply. Once compliance conditions are triggered, the contract can automatically block potentially monopolistic trading strategies or prompt enterprises to self-check and correct, reducing post-event penalties and delays.

3.3. Coordinating technology with legal compliance

Although blockchain offers technical support for antitrust compliance, its application still requires alignment with legal systems and regulatory frameworks.

1. **Legal effectiveness of data on the blockchain**:

It is necessary to clarify whether data stored on the blockchain has legal validity as evidence. Regulatory bodies and judicial authorities should formulate standards and related interpretations for blockchain-based electronic data preservation to ensure that blockchain data can be smoothly used in administrative enforcement and judicial review.

2. **International experience and standardization efforts**:

With the rise of cross-border e-commerce, international payments, and multinational platform enterprises, global standardization of blockchain compliance is particularly important. Drawing from the experiences of economies like the EU and the US in digital regulation and data governance can help countries improve their own blockchain compliance standards, laying the foundation for future international cooperation.

Blockchain technology, with its "trusted data, rule embedding, and co-building" model, offers feasible solutions for building a trusted data system and automated supervision in antitrust compliance. The following sections will further explore the specific implementation paths of blockchain in antitrust compliance scenarios, including data on-chain, smart contract applications, privacy protection, and industry standard-setting, and provide empirical research through case studies and practical exploration.

4. Practical Path Design for Blockchain Empowering Antitrust Compliance

Having clarified the technological features of blockchain and its compliance application potential, it is now necessary to explore the specific practical paths for implementing blockchain technology in antitrust compliance. This practical exploration aims to build a trusted data ecosystem through comprehensive measures such as data on-chain, multi-party collaboration, smart contract deployment, privacy protection, and standardization. These strategies provide feasible guidance for transforming antitrust compliance from concept into reality.

4.1. Data on-chain and multi-party co-construction and sharing platforms

1. **Unified data standards and interfaces**

The first task in enabling data on-chain is to establish unified data standards and structured interfaces. Through the efforts of industry associations or standardization organizations, key data such as platform transaction data, price information, traffic allocation records, and compliance evidence can be standardized to ensure that different enterprises and regulatory bodies can efficiently access and exchange information on the blockchain.

2. From a technical perspective, standardized APIs and data cleaning tools should be developed for data exchange between blockchain nodes, converting fragmented and inconsistent business data into a unified format that can be used on the blockchain. This will help mitigate the issue of data silos and lay a solid foundation for automated compliance reviews.

3. **Consortium blockchain and permissioned blockchain architectures**

Given the high requirements for participant identity verification, security, and performance in regulatory and compliance scenarios, adopting consortium blockchains or permissioned blockchain architectures is more appropriate. In this model, regulatory bodies, platform companies, industry associations, and third-party compliance service providers join the blockchain network as trusted nodes.

Co-maintaining the ledger in this way reduces the risk of any single entity manipulating the data and improves the transparency and trustworthiness of the data. At the same time, regulatory nodes can be granted access and auditing privileges, enabling them to monitor market behavior in real time and providing technical support for proactive warnings and rapid interventions.

4.2. Smart contracts and automated compliance review processes

1. Embedding compliance rules on the blockchain

By embedding national laws, regulatory guidelines, industry standards, and internal compliance codes into smart contracts on the blockchain, antitrust compliance rules can be automatically enforced when market behavior data enters the blockchain. For example, when a platform's price fluctuation frequency or magnitude exceeds a reasonable range, the smart contract can trigger an alert event, notifying regulatory nodes or sending compliance rectification suggestions.

This shift from manual, post-event audits to automatic, real-time detection greatly shortens the response time for regulation and reduces the pressure on businesses to react passively.

2. Dynamic adjustment and exception handling

Smart contracts should not be static. Regulatory bodies can update and iterate the smart contracts based on market changes, policy adjustments, or emerging business models. This means that the compliance rules themselves should be flexible and scalable.

Additionally, exception handling mechanisms should be designed for compliance smart contracts. When exceptional circumstances arise (such as sudden market fluctuations or price adjustments triggered by public safety events), regulatory bodies and business nodes can negotiate and adjust the contract logic to avoid overly mechanical execution that might harm normal market activity and innovation.

4.3. Privacy protection and data access control

1. **Application of privacy computing and zero-knowledge proofs**

The fully transparent nature of blockchain might raise concerns about data privacy and the protection of commercial secrets. To address this, privacy computing technologies such as homomorphic encryption, federated learning, and zero-knowledge proofs can be used to store sensitive data on the blockchain in encrypted form. Only nodes with the appropriate permissions can view or decrypt the data. This ensures the credibility of compliance reviews while also protecting the legitimate business interests and privacy rights of enterprises.

2. **Multi-level access rights design**

Access control levels should be established in the blockchain network based on compliance needs and the intensity of regulation. Regulatory bodies, as the highest level nodes, should have access to core evidence data; enterprise nodes should only have access to compliance information relevant to themselves; industry associations, acting as intermediaries, should have access to aggregate data and compliance statistical reports. This tiered access strategy ensures that each stakeholder's access to data is appropriately bounded, preventing excessive information disclosure or data misuse.

4.4. Industry alliances and standardization

1. **Role of compliance alliances and industry self-regulation organizations**

Building a blockchain-driven antitrust compliance ecosystem requires active participation from industry organizations. Industry associations, standardization bodies, and compliance alliances can guide companies in establishing unified technical standards and protocols, reducing the costs of technology implementation and minimizing the risk of trial and error.

These organizations can also issue blockchain compliance guidelines, offer training and consulting services, and help small and medium-sized platform companies integrate into the blockchain-based compliance system, thus improving the overall compliance level of the industry.

2. **Policy guidance and regulatory sandbox pilots**

Governments can encourage the establishment of blockchain-based compliance pilot projects in key industries (such as e-commerce, transportation, and payment). By offering a "regulatory sandbox," they can provide businesses with regulatory flexibility and encourage technological exploration and scenario experimentation. Based on pilot projects, successful experiences and challenges can be summarized, which will lay a good foundation for large-scale implementation in the future.

5. Case Studies and Application Scenarios

Blockchain-driven antitrust compliance is still in the exploratory and experimental stages globally. By analyzing existing application cases and proposed solutions in relevant fields, this section explores the potential applications of blockchain technology in antitrust compliance across different industries, focusing on supply chain traceability and platform data governance.

5.1. Pilot applications in supply chains and e-commerce platforms

1. **E-commerce platform data preservation and price tracking on the blockchain**

One large e-commerce platform, after communicating with regulators, began experimenting with periodically recording price changes for certain key products on the blockchain. The platform recorded historical prices, discount strategies, stock quantities, and sales volumes of key products in a standardized format on a consortium blockchain. Regulatory bodies, as nodes in the system, can verify whether there are any abnormal price increases or signs of monopolistic behavior.

By using smart contracts, if the price fluctuations exceed a reasonable range (e.g., multiple merchants simultaneously raise prices without justifiable reasons), the system will automatically trigger an alert and notify the regulatory nodes and the platform's compliance department for verification. Although this attempt is still in its early stages, it has already demonstrated that blockchain can help alleviate problems such as data falsification, delayed evidence collection, and information asymmetry.

2. **Cross-platform data integration and market concentration monitoring**

In the context of competition between multiple e-commerce or transportation platforms, blockchain can provide the foundation for data integration and analysis. Some regional compliance pilot projects have recorded market share data, traffic allocation information, and other relevant data from several companies on the blockchain. Industry associations or third-party technology service providers periodically generate compliance analysis reports based on this data. Regulatory bodies can refer to these reports to assess whether regional monopolistic conditions are forming, allowing for early intervention.

Compared to the traditional post-event penalty model, this blockchain-based data sharing mechanism provides a technical means for real-time and proactive supervision, helping to establish a more active and flexible compliance ecosystem.

5.2. Comparison in the transportation services and payment fields

1. **Dynamic price auditing of transportation platforms**

The pricing mechanisms of transportation services platforms are highly dynamic, as they are influenced by factors such as different time periods, regions, and supply-demand relationships. By placing order data, regional pricing strategies, and vehicle allocation information on the blockchain, regulators can quickly identify whether monopolistic collusion is taking place (e.g., if multiple platforms simultaneously raise prices or reduce services without valid reasons) during sensitive times such as peak hours or holidays. If the smart contract identifies abnormal data trends, it will issue an alert.

Transportation platform companies are constrained by this technology but are also protected. If price changes occur due to objective conditions (e.g., sudden traffic controls), the data on the blockchain and relevant proof materials can be traced by the regulators to verify and avoid misjudgment.

2. **Transparency of online payment and transaction fee rates**

In the online payment sector, blockchain can be used to record transaction fees, channel distribution, and discount strategies. After publicly disclosing key fee rate data on the blockchain, regulatory bodies and industry observers can conveniently monitor the fairness and stability of the fee rates. If a specified fee rate limit is reached, the smart contract will automatically report it to the regulatory nodes.

This approach helps prevent payment platforms from using their data and channel advantages to squeeze out competitors, ensuring that small and medium merchants and consumers enjoy fair treatment within the digital payment ecosystem.

5.3. Algorithm auditing ideas for content distribution and media platforms

In addition to price and transaction data, algorithmic decision-making is also an important aspect of antitrust compliance. For example, in content distribution platforms such as short video and news aggregation services, if a platform's recommendation algorithm is excessively biased, it could unfairly treat competitors. While putting algorithms on the blockchain is challenging, blockchain can be used to back up key algorithm parameters periodically, leaving a trace of the recommendation results. Compliance audit nodes can periodically perform spot checks and verifications.

By comparing various industries, we can see that quantitative data such as pricing and transaction fees are easier to record on the blockchain and audit, while more complex issues like algorithmic logic or content ranking require blockchain to be supplemented with other technologies such as explainable AI and privacy computing in order to achieve the desired compliance monitoring effect.

Case studies and application scenarios indicate that the practical value of blockchain in antitrust compliance is gradually becoming evident. Whether in e-commerce, transportation, payment, or content distribution, blockchain provides feasible paths for data preservation, behavior traceability, real-time supervision, and automated alerts. Of course, there are still many challenges and difficulties in practical implementation that need to be resolved. The following sections will address common difficulties in the implementation process and propose corresponding countermeasures.

6. Implementation Challenges and Suggested Solutions

Although blockchain technology provides innovative ideas and practical paths for antitrust compliance, many challenges remain in its actual implementation. These challenges include technical costs and performance bottlenecks, legal validity and a lack of standards, privacy protection, enterprise participation, and multi-party collaboration mechanisms. To address these issues, it is necessary to propose targeted countermeasures from multiple dimensions to create more favorable conditions for building the blockchain-enabled antitrust compliance system.

6.1. Technical costs and performance bottlenecks

1. **Optimizing the underlying technological architecture**

The scalability and performance limitations of blockchain may hinder its ability to handle high-frequency data on-chain and conduct real-time audits. Therefore, it is essential to prioritize blockchain frameworks with high throughput and low latency, such as consortium blockchains. Additionally, technologies such as sidechains, sharding, and off-chain computation should be used to improve system performance. Cloud computing and edge computing resources can also be utilized to offload heavy data processing tasks, which will help alleviate the pressure on the blockchain.

2. **Modular and standardized solutions**

Developing modular and pluggable blockchain compliance toolkits will enable businesses to select the appropriate functional modules based on their business scale, data types, and compliance needs. By building on standardized solutions, businesses can reduce their dependence on customized development, lowering technical costs and implementation thresholds.

6.2. Legal effectiveness and lack of compliance standards

1. **Improving legal guidelines for blockchain evidence**

Governments should expedite the issuance of legal interpretations regarding the validity of on-chain data as evidence, providing clear guidelines for regulatory enforcement and judicial review. Blockchain data should be recognized as electronic evidence in existing frameworks for digital evidence. Standards for hash proofs, timestamp services, data signature strategies, and other aspects should be defined to ensure blockchain data can be smoothly applied in administrative enforcement and legal proceedings.

2. **Developing industry standards and technical specifications**

Industry associations, standardization organizations, and research institutions should collaborate to issue technical standards and industry guidelines for blockchain compliance applications. These standards should cover data formats, consensus mechanism selection, smart contract security requirements, and privacy protection protocols. The issuance of these standards will reduce technical friction and redundant development between companies and improve the overall coordination of the compliance ecosystem.

6.3. Data privacy and balancing compliance

1. **Enhancing privacy protection with privacy computing technologies**

Privacy computing technologies, such as homomorphic encryption, verifiable computation, and zero-knowledge proofs, can ensure that compliance reviews are conducted without compromising sensitive commercial information or personal privacy. Regulatory bodies can perform data analysis and verification on encrypted data, obtaining necessary information without directly accessing sensitive plaintext data.

2. **Multi-level access rights and compliance review node Design**

Access rights should be appropriately set within the blockchain network, based on compliance needs and the intensity of regulation. Regulatory bodies, as the highest-level nodes, should have access to core evidence data. Enterprise nodes should only be able to access compliance information related to their own operations. Industry associations, acting as intermediaries, should have access to aggregated data and compliance statistical reports. This tiered access design ensures that the boundaries of data usage are maintained, reducing the risk of improper exposure or misuse of sensitive data.

6.4. Enterprise participation and optimizing the industry ecosystem

1. **Incentive and reward mechanisms**

Regulatory bodies can offer certain incentives to enterprises that voluntarily move their data onto the blockchain and accept compliance reviews. These incentives could include preferential treatment in administrative approvals, public policy support, improved credit ratings, and easier access to financing. Additionally, an award system can be established to recognize companies that actively promote data transparency and follow the law, encouraging greater voluntary participation.

2. **Public service platforms and industry collaboration**

Industry associations, third-party technology service providers, and government departments can jointly build public compliance blockchain service platforms. This would reduce the technical and financial barriers for small and medium-sized enterprises. With the support of public platforms, small and medium-sized enterprises would not need to independently develop and maintain complex blockchain systems, thus enabling them to easily integrate into the compliance system and improve their overall compliance capabilities.

3. **Education and talent development**

The successful implementation of blockchain-based antitrust compliance requires professionals with expertise in both legal regulations and blockchain technology. Governments, industry organizations, and universities should collaborate on training programs to develop a talent pool capable of handling both legal and technical aspects of blockchain compliance. This will ensure that the market has sufficient talent to support the implementation of blockchain-enabled antitrust compliance.

By taking targeted measures in areas such as technical optimization, legal framework improvement, privacy protection, and talent development, the implementation of blockchain in antitrust compliance can be made more feasible. Multi-level, multi-party collaboration efforts will lay a solid foundation for building a highly credible, transparent, and sustainable compliance governance ecosystem. The following sections will summarize the key points of this research and explore potential future paths for development.

7. Conclusion and outlook

This research investigates the application potential of blockchain technology in the areas of data traceability and trusted governance ecosystems for antitrust compliance, against the backdrop of the rapid rise of the national digital economy and platform economy. The decentralization, immutability, traceability, and programmability of blockchain provide feasible solutions for establishing a trustworthy compliance data environment. Blockchain is expected to play a fundamental role in antitrust compliance by enabling real-time monitoring, proactive regulation, automated rule enforcement, and multi-party collaboration for data sharing.

The introduction of blockchain technology into antitrust compliance addresses several core challenges that traditional compliance models face, such as difficulties in data collection, information asymmetry, and delayed post-event supervision. By putting critical data—such as market transaction information, price strategies, and transaction trajectories—onto the blockchain, regulatory authorities can achieve real-time supervision and issue timely alerts, which facilitates the identification and correction of potential monopolistic behaviors. The use of smart contracts further enhances the compliance process by automating the enforcement of compliance rules. Once certain conditions are met, smart contracts can trigger automatic alerts, restrict certain behaviors, or prompt enterprises to make necessary corrections, thus reducing the need for reactive enforcement and its associated costs.

Moreover, the multi-party collaboration facilitated by blockchain ensures that different stakeholders—regulators, platform enterprises, industry associations, and third-party compliance service providers—can jointly maintain and verify data. This collaborative mechanism fosters greater data transparency, reduces the risk of data manipulation by a single party, and ensures the trustworthiness of the data. The integration of privacy protection technologies and tiered access rights within the blockchain ecosystem guarantees the privacy and security of sensitive business and personal data, which is essential for maintaining a balance between compliance and data privacy.

Despite the promising potential of blockchain in antitrust compliance, there are still several challenges that need to be addressed. From a technical standpoint, the scalability, performance, and interoperability of blockchain need to be enhanced to handle large volumes of data and real-time audits. Legally, there is a need for clearer guidelines on the legal recognition of blockchain-based evidence and for the development of industry standards to ensure the effective implementation of blockchain in antitrust compliance. Additionally, issues related to privacy protection, cross-border data flow, enterprise participation, and talent development must be tackled to optimize the blockchain-based compliance system.

With continued policy guidance, technological innovation, and industry collaboration, blockchain technology can become an essential infrastructure for antitrust compliance. As blockchain technology matures and integrates with other technologies such as explainable AI and privacy computing, it will become an increasingly important tool for creating a transparent, fair, and efficient competitive environment. Furthermore, international cooperation in data governance and the sharing of best practices will be key to enhancing global antitrust enforcement and establishing a more equitable digital economy.

In conclusion, blockchain technology holds great promise for transforming antitrust compliance by providing real-time, transparent, and automated solutions to address complex market behaviors and competitive issues. The successful implementation of blockchain in antitrust compliance requires a multi-stakeholder effort, involving governments, enterprises, industry associations, and technology providers. By leveraging the strengths of blockchain, regulators can improve the effectiveness of antitrust enforcement and promote fair competition in the digital economy.

References

[1] Xiaoye W. The Theory and Practice of Antitrust Regulation in China's Digital Economy Sector [J]. Journal of the Chinese Academy of Social Sciences, 2022(5): 31-48.

[2] Bing C. Algorithmic Collusion Risks in the Digital Economy and Antitrust Regulation Approaches [J]. Law Review, 2024, 39(4): 80-90.

[3] Aifei C. Antitrust Regulation of Blockchain Collusion [J]. Modern Jurisprudence, 2022(4): 145.

[4] Zhili D, Xiaohui L, Dong H. The Application and Challenges of Blockchain Technology in Data Security and Governance [J]. East China Science and Technology, 2024(9).