Algorithmic Collusion in Financial Markets: Regulatory Dilemmas and Legal Responses in Digital-age Securities Markets

Shuhui Wang*
School of Law, Anhui University of Finance and Economics, Bengbu 233000, China
*Corresponding email: 1446267600@qq.com

Abstract

The proliferation of algorithmic trading, artificial intelligence (AI)-enabled credit assessment and automated investment consultancy has facilitated the digital transformation of securities markets. Such technological progress has spawned a new regulatory concern: algorithmic collusion. Unlike traditional cartels formed via human negotiation and explicit coordination, algorithmic collusion relies on automated price signaling, shared data channels and reinforcement learning technologies, allowing market participants to realize tacit behavioral coordination without human interaction. Focusing on digital securities trading scenarios, this paper divides algorithmic collusion into four primary categories, namely indirect messenger collusion, hub-and-spoke collusion, predictive agent collusion and autonomous learning collusion, and analyzes the unique regulatory dilemmas corresponding to each category. Based on over ten domestic and foreign legal research achievements, alongside the regulatory practical experience of the European Union and the United States, this study verifies notable defects in the existing antitrust system, which fails to clarify relevant legal liabilities, identify coordinated behaviors or implement targeted regulatory enforcement. This research develops a full-spectrum governance solution that incorporates pre-supervision transparency enhancement, substantive liability standard refinement, regulatory institutional capacity building and market trust restoration. The findings indicate that regulators should update traditional supervisory logic, phase out scattered, penalty-oriented supervision modes, and build a flexible regulatory system that adapts to technological updates. The optimized governance framework can effectively balance market technological innovation, protect investor legitimate rights and interests, and sustain long-term financial stability.

Keywords

Algorithmic collusion, Securities regulation, Digital finance, Antitrust, Generative artificial intelligence, High-frequency trading, Smart regulation

Introduction

Digital transformation of securities markets is one of the biggest changes in modern finance. Algorithmic trading accounts for a significant portion of daily turnover at major global exchanges. AI driven decision making encompasses order execution, liquidity provision, investor suitability assessment, margin lending credit scoring and automated investment advice [1]. Digital finance has grown rapidly in China. It comprises online brokerages, robo-advisory services and big data credit platforms. The rapid development has led to multiple regulatory actions. Legal risks from algorithmic systems attract scholars' increasing interest. Algorithmic collusion brings particularly hard to address risks. It undermines core foundations of market competition. Based on opaque code and machine learning, renders enforcement under conventional antitrust rules difficult.

Algorithmic collusion takes place when two or more market participants use algorithms to align their business behavior. Such behavior includes pricing, order routing and credit-term setting, and requires no explicit human agreement or direct human communication. Firms may pursue this coordination on purpose. For instance, they build algorithms to track and follow competitors' pricing moves. Coordination may also emerge spontaneously. Reinforcement-learning algorithms may independently identify that cooperative strategies yield higher profits than competitive strategies [2]. Either scenario produces market results similar to those of conventional cartels.

Prices rise, output falls, innovation weakens, and consumers suffer losses. Nevertheless, legal assessment faces unprecedented challenges. The alleged agreement may exist solely within program code. Algorithmic convergence may supplant traditional consensual agreement. Relevant contractual intent may be wholly absent or dispersed across multiple developers and operators.

Securities markets are especially prone to algorithmic collusion due to multiple structural factors. Firstly, these markets are highly concentrated with only a few major exchanges and brokerages which facilitate tacit coordination. Secondly, many trading algorithms share the same data feed, risk model or optimization objective leading to cognitive and information convergence. Thirdly, the quickness of algorithmic adjustments allows for fast detection and punishment of deviation thus resulting in remarkably stable collusive equilibria. Fourthly, the proprietary and technical characteristics of algorithms shield them from regulatory scrutiny providing a “black box” concealing collusive design. Together with the increasing role played by generative AI and large language models in financial services, algorithmic collusion has become an issue of great concern for regulators around the world.

Regulatory context adds additional complexities in China. The revised 2022 Anti-monopoly Law explicitly prohibits monopolistic conduct enabled by algorithms, data and technology. However, real world enforcement mostly focuses on classic abusive practices such as exclusive dealing and merger review [3]. The draft Financial Law is still under the legislative process. It proposes full coverage supervision and the substance over form principle. These rules may provide legal basis for algorithm related supervision although supporting implementing rules are not yet mature. Securities authorities tend to use campaign style enforcement. They launch concentrated short-term crackdowns against peer to peer (P2P) lending, virtual currencies and platform based financial services. They work well to address urgent risks. But it fits poorly for algorithmic collusion. Algorithmic collusion continuously evolving over time generates scarce traceable evidentiary trails.

Against the foregoing backdrop, this paper addresses three core research questions:

(1) In what ways can algorithmic collusion manifest itself in securities markets, and how do its operations unfold?

(2) Why does the current legal and regulatory framework fail to adequately detect, prove and sanction algorithmic collusion?

(3) What comprehensive procedural, substantive and institutional reforms are required to regulate algorithmic collusion? Reform efforts must ensure protection of market competition and investor interests without introducing unnecessary barriers to innovation.

This paper references more than a dozen recent legal studies drawn from both domestic and international sources together with comparative experience from Europe and the United States. Our analysis is rooted in the particularities of securities markets, namely high-frequency trading, automated credit scoring for margin loans and robo-advisory services, however our findings will be relevant beyond the scope of securities markets to digital finance in general.

This paper follows the structural arrangement below. First, it builds a systematic conceptual framework. It defines what algorithmic collusion means and differentiates its four typical forms. It also explores trust-related and interpretability flaws within digital securities markets, which make the market vulnerable to algorithm-driven coordinated conduct. Second, it discusses three core regulatory dilemmas. Regulators meet real-world barriers when assigning legal liability, proving collusive conduct and delivering effective enforcement. Against China’s institutional background, it further explains the built-in drawbacks of campaign-style regulation. Third, it develops a multi-dimensional governance framework. This framework includes procedural improvements, refined substantive legal standards and strengthened institutional capacity. Finally, the conclusion restates key research outcomes and puts forward targeted policy suggestions for legislators, regulators and market participants.

Algorithmic collusion in securities markets: Forms, mechanisms, and vulnerabilities

Defining algorithmic collusion and its four typologies

The phenomenon of algorithmic collusion refers to that two or more market participants coordinate their actions through algorithms for manipulating market competition. Typical examples are price fixing, output restriction and customer allocation. This kind of coordination does not

require explicit human agreement but rather depends on the operations performed by algorithms. There are two mainstream types: One type involves human-led coordination using algorithms as tools to carry out and monitor collusive arrangements; another type is emergent coordination involving machine learning systems autonomously identifying and maintaining stable collusive market states. Collusions occur in various scenarios in securities markets. They affect the pricing of transaction services and the setting of order routing priorities. They interfere with margin lending credit terms and the timing and content of influential market information releases [4].

Drawing on extant literature, this paper identifies four ideal-type categories of algorithmic collusion, each featuring distinct operational mechanisms and regulatory ramifications.

In indirect messenger collusion, platforms or trading firms employ algorithms for communicating their pricing intentions and monitoring each other's adherence to an implicit or explicit understanding [5]. A high-frequency trading firm could have programmed its algorithm to increase its bid-ask spread every time its competitor increased it and then revert only once the competitor reverted. Such an algorithm functions as a "messenger" which conveys and enforces this collusive signal. Although such an agreement might be initiated by humans, it is automated through the algorithm and significantly mitigated against any deviation. Indirect messenger collusion has been seen in securities markets where there is coordination around make-or-take fees on alternative trading systems, or coordination among various proprietary trading desks regarding latency-arbitrage strategies. Evidencing such conduct requires distinguishing between legitimate competitive benchmarking and unlawful signaling. However, traditional documentary evidence may remain if communications are present.

Hub-and-spoke collusion involves a common algorithmic framework or data feed that connects multiple downstream competitors [6]. In securities markets, this often takes the form of a shared risk-scoring model or a common order-execution engine provided by a third-party vendor. Several broker-dealers may adopt the same AI-powered credit-scoring application programming interface (API) for margin lending. The algorithm could adjust credit scores in a consistent manner. It narrows the interest-rate gaps among these brokers. Such outcomes may produce collusive effects, even if brokers never communicate with one another. Third-party service providers function as the hub and subscribing broker firms act as spokes. The hub itself may hold no collusive intention. Its algorithm design may generate coordinated market outcomes by accident. This category creates notable regulatory difficulties. The hub can be a fully legitimate service vendor. The subscribing spokes might not even realize coordinated effects are taking place. Under these conditions, regulators struggle to prove the existence of any collusive agreement.

Predictive agent collusion happens when firms use programs to continuously monitor the actions of their competitors and adjust their own plans according to the forecasting models of the rival's responses [7]. These programs are not specifically designed for collusion but are set to maximize personal profits by properly adjusting to the market changes. However, if several such programs cooperate, they may reach a state of collusion because the forecasting models indicate that intense competition would lead to counterattacks and reduce the long-term profits, whereas cooperation would bring more total returns. In the securities market, predictive agent collusion may be observed in the algorithmic market-making where the programs of different liquidity providers agree to raise the spreads at the same time during low volatility periods and earn higher profits from the investors. The difficulty in regulation lies in the fact that each company can argue rationally that its program is only operating independently, which complicates the proof of a "concerted practice".

Autonomous learning collusion is the most advanced type. By using reinforcement learning and other machine learning techniques, the algorithms can independently discover and implement collusive strategies. Human programming or collusive intention does not affect this procedure. The developers only define profit maximization as a reward function. Then the algorithms try out different possible actions. Through repeated market interactions, they find that cooperation brings higher returns than competition. They may converge toward a collusive market equilibrium. This process does not need human communication, shared codes or any explicit coordination means [8]. Autonomous learning

collusion has been simulated in experimental settings for pricing algorithms in securities markets, and it is known that similar phenomena may occur in the actual algorithmic trading systems. Therefore, the regulatory implications are that the concept of "agreement" which means a consensus among people, is invalid, because no human participant intended or even imagined the collusive result.

Trust reconfiguration and algorithmic vulnerabilities

Securities trading relies heavily on trust. Market participants need fair pricing, reliable order execution, trustworthy counterparties and accurate credit evaluation. Traditional markets build such trust via institutional reputation, regulatory supervision, personal connections and long-run business norms. On digital securities platforms, algorithms take over much of this trust-building work. Algorithms judge credit status and investor suitability. They also decide order priority and execution performance. This shift creates new weaknesses that make algorithmic collusion easier to occur.

Recent studies describe this as computable trust. Such trust originates from algorithmic models instead of social or institutional mechanisms. Computable trust works through three interrelated channels. First is the investor-platform channel. Investors place trust in platforms according to public rules, historical performance and service response quality. Second is the platform-algorithm channel. Platforms delegate core tasks to algorithmic systems. These tasks cover risk detection, credit evaluation and trading judgment. Third is the algorithm-investor channel. Algorithms produce outputs including credit scores, investment suggestions and execution summaries. These outputs directly influence investor benefits and further reshape their trust and market actions [9].

Algorithmic risks such as discrimination, opacity and monopolistic power can damage any of these channels. Once this happens, the whole trust network becomes fragile. The resulting uncertainty and distrust may unexpectedly create favorable conditions for collusion. For example, opaque algorithm-driven pricing may make investors lose faith in a platform. Investors may become less sensitive to price differentials, which weakens competitive pressure and facilitates coordinated increases in service fees among platforms. Platforms may lack sufficient understanding and control over their own algorithms due to black-box opacity It may hand over more decision-making work to outside service providers. This raises risks of hub-and-spoke collusion. Besides, algorithms from different platforms may adopt similar credit-scoring models when they draw on identical data sources. Such uniform outputs lock in collusive effects. Investors cannot easily seek better service terms across competing platforms.

Algorithmic discrimination, black-box opacity and algorithmic monopoly represent three distinct risk types. They consistently weaken the above-mentioned trust channels. Credit-scoring algorithms may impose unfair penalties on investors from specific regions or occupational groups. This form of discrimination breaks trust between investors and platforms. It lowers user activity, discourages truthful data submission, and pushes users to switch platforms. Risks can spread across the whole market in this process. Opacity creates another set of problems. A platform may fail to offer valid explanations for rejected trades or elevated margin requirements. This damages trust between platforms and their embedded algorithms. Platforms lose capacity to control internal risks. They may turn to conservative industry-wide parameters that align with competitors. Unintentional market coordination can emerge under such conditions. If one algorithm or data supplier gains market dominance and forms an informal industry standard, algorithmic monopoly takes shape. Trust-related feedback mechanisms stop working well. Investors have few alternatives to switch service vendors. They cannot fix wrong algorithmic assessments. Collusive market results become deeply rooted across the whole sector.

The interpretability deficit and its governance implications

Algorithmic cooperation is difficult to detect because of the uncertainty in understanding the models. The complex machine learning systems are generally obscure. It is hard for people to know the reason for certain decisions and cannot easily distinguish whether the coordination is intentional or accidental [10]. In the securities markets, algorithmic trading strategies have a large number of parameters, nonlinear transformations and high dimensional feature spaces. Even their creators cannot completely understand the model outputs. This

uncertainty is not only a technical problem, but also a fundamental trade-off for improved prediction results. Models delivering the highest prediction accuracy such as deep neural networks and gradient-boosted trees tend to have the poorest interpretability.

New research points out four key sources of interpretability risk. Algorithmic complexity makes manual checking difficult. Large numbers of parameters and model layers stop humans from tracking the link between input data and final results. Training data contains unseen biased content. Mistakes in sample selection, defects in measurement and long-term discriminatory patterns may produce unfair results and outcomes that favor collusion. Such risks cannot be identified merely through observation of model architectures. Model design goals might go against standard regulatory goals. Trading algorithms focus only on raising profit levels in most cases. They pay no attention to fair market rules and overall system stability. This situation can bring about unplanned collusive acts. Continuous model revisions change the explainable features of models. Regulatory interpretations that work for a specific model version lose validity after model retraining. This problem greatly lowers the effectiveness of regulatory supervision.

These interpretability flaws affect antitrust enforcement directly. Model interpretability is limited. Regulators cannot tell the cause of observed price parallelism in markets. The pattern may result from separate firm optimization. It may arise from fixed technical boundaries. It may also come from deliberate joint business conduct. Regulators cannot locate exact algorithm elements that produce collusive market results. Regulators cannot confirm if platforms have put in place proper safeguards against market coordination. Low interpretability protects platforms from legal accountability. Platform operators may invoke lack of awareness as a defense during regulatory investigations. They can attribute collusive market conduct to automatic algorithm operation. This status makes legal liability attribution extremely difficult.

Recent studies suggest interpretability should become a formal regulatory requirement instead of an optional technical preference [11]. Regulators may impose mandatory rules for algorithms undertaking core market tasks. These tasks cover order execution, margin-loan credit scoring and investor suitability evaluation. Relevant algorithms need to supply explainable outputs, alongside records for feature importance, decision boundaries and potential influences on different investor groups. Interpretability assessment cannot only take place upon deployment. It needs continuous checks across the full algorithm lifecycle, and revalidation shall follow every major model update. Besides, regulators should demand interpretability reports readable for non-specialists. Investors and social organizations can then watch for possible collusion or discriminatory practices.

Regulatory dilemmas: Legal responsibility, proof, and enforcement

The attribution of legal responsibility

The first regulatory dilemma concerns the identification of the proper subject of legal responsibility for algorithmic collusion. Traditional antitrust law assigns liability to natural people, legal people, or other organizations that enter into anticompetitive agreements. This framework presupposes that there is an identifiable "actor" who intends to collude and takes steps to implement that intention. In algorithmic collusion, especially in autonomous learning cases, this presupposition breaks down entirely.

Consider a real-world case. Two brokerage firms run separate reinforcement learning algorithms for market-making work. No built-in collusive functions exist within these algorithms. The systems only receive one core goal. That goal is to raise trading profit levels. The algorithms keep interacting with one another over many market cycles. They find out they can earn more money by widening spreads at the same time. They gain less profit when they try to undercut one another. The systems finally settle into a collusive equilibrium state. Developers never intended this type of market outcome. Firm managers who launched these algorithms had no advanced knowledge of this risk. The algorithms cannot hold any form of moral judgment. Nevertheless, tangible market harms still materialize: Investors confront widened bid-ask spreads and degraded trade-execution quality. These market effects mirror results created by illegal cartel groups.

Who should bear legal liability under these circumstances? Developers write program codes, yet they give no instruction for collusive conduct. Operators deploy the system but cannot predict emergent

algorithmic behavior. Data providers shape the training setting, though they cannot steer the algorithm's learning path. The algorithm itself does not qualify as a legal entity. Failure to assign liability deprives aggrieved parties of effective remedies and erodes the deterrent effect of antitrust law. Excessively broad liability, by contrast, may restrain innovation and place unfair burdens on parties that act in good faith.

A typology-based method has been put forward to resolve this dilemma. For indirect messenger and hub-and-spoke collusion, where algorithms are purposely built or adjusted to achieve coordination, primary liability falls on the platform operator deploying the algorithm. Developers who knowingly create collusive functions bear secondary contributory liability. For predictive agent collusion, collusive effects arise from optimized responses toward market conditions. Operators should take liability when they skip proper anti-collusion safeguards such as randomization, privacy-preserving noise or independent audit tools. For autonomous learning collusion with genuinely unforeseeable outcomes, strict liability applies. Operators are accountable for market harm caused by their algorithms. They may avoid punishment only if they prove full adoption of industry-standard precautions and confirm that collusion could not be predicted upon deployment [12].

One extra theoretical viewpoint supports a social-digital institutional framework. This framework does not treat algorithmic systems as plain technical tools. It sees them as institutional participants. These participants reshape market behaviours via their design and running logic. It adjusts existing rules for liability assignments. Responsibility gets divided according to each participant's role and influence inside the algorithmic ecosystem. Traditional legal standards built on subjective intent and direct causation no longer serve as the main reference. It sets collective liability for systemic harm caused by collusion. Cross-platform algorithm interactions may produce collusive results. Relevant market actors take liabilities matching their contributions to the collusive institutional environment. This idea carries noticeable innovative features. It offers practical responses to the decentralized and multi-causal features of algorithmic collusion [13].

Proving concerted action and causal linkage

The second regulatory dilemma targets proof of concerted action. Such proof acts as a necessary condition to identify an illegal agreement under most competition laws. Algorithmic collusion seldom comes with open communication. It lacks written records or witness statements. Such materials constitute key evidence in traditional cartel investigations by competition authorities. Coordination takes place within code. It does not come from verbal talks. It draws support from data. It does not rely on paper documents. It arises out of automatic system responses. It does not rest on explicit promises. An evidentiary gap forms under these conditions. It creates major obstacles for regulatory enforcement.

Three elements make this problem harder. Algorithmic decisions carry high technical complexity and follow non-linear paths. People struggle to tell the real driver behind price parallelism. The pattern may come from collusion. It may also come from independent optimization amid comparable market surroundings. The actual behavioral logic behind algorithmic collusion remains concealed. Platforms achieve coordination with zero direct contact between parties. A "meeting of minds" cannot be confirmed. This holds true even when market results align with collusive patterns. Many interfering factors weaken links between algorithm design and final market results. Market price shifts can come from algorithmic collusion. They can result from common supply shocks. Shared data sources may drive such changes. Similar technical system architecture plays a part. Random market fluctuations can also move market prices.

Scholars put forward multiple doctrinal adjustments to handle these practical barriers. The substantial factor test draws inspiration from United States (U.S.) tort law. Courts can confirm causation when algorithmic coordination works as a substantial factor behind anticompetitive outcome. The factor does not need to be the only or primary cause. These standards changes what parties need to show for evidence. It asks for proof of material contribution instead of exclusive causation. It fits the technical limits present in algorithm-driven markets. Burden-of-proof reversal represents another adjustment. Platform operators take on proof-giving duties for suspected algorithmic collusion cases [14].

They need to show their algorithms do not generate anticompetitive coordination. Platforms possess more

internal information about their algorithmic systems. They are in a stronger position to interpret visible market changes. Rules forcing platforms to offer defensive explanations fix existing information imbalance. This imbalance previously gave advantages to firms engaged in collusion. Regulators can turn to indirect evidence to reduce concerted action. Direct proof may not exist in some cases. Acceptable evidence covers algorithm structures supporting market monitoring and punitive responses. It includes parallel market moves without reasonable business grounds. It also includes existing contact channels connecting algorithm developers.

Extra barriers appear within China's institutional setting. The Anti-monopoly Law and its supporting rules have no established interpretations for algorithmic collusion scenarios. Courts lack practical experience judging technical evidence. The campaign-style enforcement model depends on obvious violations and quick sanctions. It cannot meet demands for delicate, evidence-heavy analysis for algorithmic collusion cases. Authorities need to improve judicial and administrative competence for algorithm-related evidence assessment. This work deserves high priority.

Enforcement effectiveness and institutional capacity

The third dilemma concerns the effectiveness of enforcement, even when collusion is detected and proven. Traditional remedies, injunctions, and divestiture may prove inadequate for algorithmic collusion [15]. Fines calculated according to affected commerce can appear insignificant compared with collusive profits. This situation is especially prominent in high-frequency trading. Profits accumulate within microseconds, and total gains can reach huge amounts. Injunctions targeting specific practices are easy to bypass via algorithmic adjustment. Banned strategies may reappear under revised parameters or new labels. Divestiture measures may become technically unworkable if collusion roots in shared data infrastructure or common third-party APIs.

Moreover, tackling algorithmic collusion calls for regulatory capacity that most agencies do not possess. Complex algorithmic systems require expertise in computer science, data science and machine learning, and such skilled personnel remain scarce within traditional competition authorities. Algorithmic adjustments happen far faster than administrative enforcement procedures. Regulators struggle to keep up with evolving market conditions. In addition, securities markets operate on a global scale. Collusive algorithms can run across multiple jurisdictions. This hinders coordination among national regulators and opens room for regulatory arbitrage.

China's regulatory model features campaign-style enforcement. Regulators launch intensive short-term crackdowns targeting specific practices including P2P lending, virtual currencies and platform-based financial services. Such campaigns can swiftly eliminate acute risks, yet they poorly fit persistent adaptive threats such as algorithmic collusion. Campaign-style regulation carries multiple shortcomings. It generates regulatory uncertainty, harms market expectations and discourages lawful innovation. It depends on heavy-handed ad-hoc intervention measures instead of stable institutional capacity, leaving enforcement gaps between campaign cycles. It also encourages regulatory arbitrage, as sophisticated market participants learn to operate within regulatory cycles' grey areas. Furthermore, it lacks procedural safeguards and proportional assessment required by rule-of-law governance, which raises risks of excessive deterrence and improper enforcement.

For algorithmic collusion, the intermittent nature of campaigns creates special difficulties. Collusive patterns may re-emerge upon the conclusion of enforcement campaigns, and adaptive algorithms may produce outputs that circumvent inspection triggered by such campaigns. A fundamental policy shift is therefore required. Regulators shall move from periodic crackdowns toward sustained intelligence-driven monitoring, and shift focus from punitive sanctions to preventive governance. Preventive governance covers regular algorithm audits, mandatory transparency rules and incentive mechanisms for industry self-regulation.

Data security and its relationship to collusive governance

All forms of algorithmic governance build upon data security. Data may come incomplete, damaged or carry built-in bias. These conditions lower model reliability. Reliable detection of collusive patterns becomes impossible under such circumstances. Unauthorised data access opens doors to front-running and market manipulation. It creates information gaps that help market players carry out coordinated conduct. Poor-quality data protection wears away investor trust.

Market-oriented disciplinary mechanisms lose much of their power. Collusive practices can sustain for longer periods. Investors with low trust show little willingness to switch service providers.

Recent academic work calls for balance between data security and data practical value. Over-tight rules for data sharing can block cross-platform data collection work. Such data collection supports the discovery of collusive patterns. Loose regulatory settings leave room for improper data usage. A tiered classification framework can strike this needed balance. Transaction data, orderbook data and investor profile data receive separate protection standards. Privacy-oriented tools include federated learning. These tools support model training across separate datasets. Raw source data stays in its original location without transfer. They offer a practical middle-ground choice for collusive pattern detection.

China's draft Financial Law lays down tiered standards for data protection. The Data Security Law supplies a broad regulatory framework. Detailed implementing provisions for securities-related data remain insufficient. This paper puts forward suggestions for securities regulators. They ought to release clear guidelines for algorithm-related data governance. These guidelines cover data quality standards, access permission controls, data retention rules and data breach reporting duties. Data infrastructure can offer support for algorithmic collusion detection and prevention. It should not weaken these regulatory goals.

A comprehensive governance framework and policy implications

Procedural reforms: Transparency, impact assessment, and audit

Sound governance over algorithmic collusion needs procedural adjustments. These adjustments raise transparency and accountability for algorithm-driven decision-making. Three concrete mechanisms carry essential value.

Algorithm registration and disclosure. Securities platforms and trading firms must register every algorithm handling core market function with regulatory bodies. These core tasks cover order execution, pricing, margin loan credit scoring and investor suitability evaluation. Registration materials require full records on algorithm architecture, training data sources, key parameters, validation results and embedded risk controls. High-risk algorithms with systemic influence or effects on retail investors demand public disclosure. Market participants, researchers and civil groups can keep watch over potential anticompetitive design features [16]. A tiered regulatory approach works well here. Algorithms dealing with sensitive investor data go through mandatory registration and complete document submission to regulators. Algorithms built upon public market data can use simplified formalities. This setup keeps regulatory oversight in place. It takes administrative efficiency into account. It also shields lawful trade secrets.

Algorithmic impact assessment. Algorithms receive independent fairness and competition impact checks before deployment. They also get such checks on a regular basis after launch. These checks look at how algorithms act on different investor groups. They spot possible collusive or discriminatory risks. They judge whether mitigation controls work well. They put forward corrective steps when circumstances call for them. Assessment reports need third-party examination and public release. Proprietary business information stays protected under confidentiality rules. The assessment system adopts measurable indicators. Price dispersion, order execution quality and equal credit access fall within these indicators. These indicators support objective evaluation work.

Algorithmic audit and accountability. Qualified third-party auditors shall carry out continuous audits for algorithmic systems. Audit work covers code review, data validation, outcome testing and back-testing based on market data. Audit outcomes shall be submitted to regulators and released to the public under suitable circumstances. Once algorithmic collusion is identified, clear accountability rules need to be applied. Platform operators shall take liability for insufficient internal oversight. To facilitate enforcement, audit reports need detailed explanations for algorithmic decisions and reasons for major model adjustments. Regulators can therefore reconstruct decision-making logic even for complicated cases.

Substantive legal standards: Expanded agreement, reverse burden, and strict liability

Substantive legal reform is equally necessary to bring antitrust doctrine into alignment with algorithmic realities.

(1) Expanded definition of agreement

Competition law needs clear acknowledgement of algorithmic coordination. This kind of coordination may count as an "agreement". This ruling does not require direct human communication to take effect. Algorithms may keep generating parallel market results. Independent optimization cannot give reasonable explanations for such results. Platforms may also skip proper safeguards meant to stop coordinated market conduct. Regulators are allowed to draw an inference of agreement under these circumstances. Platforms have space to push back against such an inference. They need solid and persuasive evidence for their defence. They have to prove parallel market behaviour comes from lawful driving forces. Shared market conditions or separate technical limitations fall among these lawful driving forces.

(2) Reversal of the burden of proof

Platforms should take up the burden of proof for algorithmic collusion cases. They need to show their algorithm produces no anticompetitive coordination. This shift makes practical sense. Platforms hold far more internal information about their algorithm systems. They are better placed to interpret visible market outcomes. Platforms must hand over evidence to clear themselves from suspicion. Such materials cover algorithm design records, training data descriptions and internal test outputs. These materials work to rule out collusive purpose or real-world collusive effects. Regulators may draw an inference of collusion. This happens when platforms cannot supply the required supporting materials.

(3) Strict liability for autonomous learning

For autonomous learning algorithms producing collusive outcomes without human intent, strict-liability rules apply to operators. Operators may claim exemption only when they prove three conditions. First, they have adopted all industry-standard precautions against collusion. Second, they keep continuous monitoring for emergent collusive behaviors of algorithms. Third, the collusive result is truly unforeseeable and gets reported immediately upon discovery. This framework balances deterrence and fairness. It assigns obligations to parties most capable of risk control and meanwhile sets reasonable exceptions for genuinely unforeseeable market consequences.

(4) Enhanced penalties

Penalties for algorithmic collusion need enough severity to deter highly profitable collusive coordination. This may call for revisions to fine-calculation methods. Regulators should take into account the duration and scope of collusive conduct, detection difficulty, algorithm opacity and the operator's degree of fault. The existing penalty framework under the Anti-monopoly Law allows fines up to 10 percent of the previous-year revenue and offers a solid deterrence foundation. Nevertheless, enforcement practice must ensure penalties are imposed at substantive levels. Individual executives ought to bear personal liability where circumstances warrant.

Institutional capacity: Specialized review, regulatory technology, and international coordination

Institutional capacity is the foundation of effective enforcement. Without adequate expertise, resources, and coordination, even the best legal standards will remain unenforced.

(1) Specialized algorithmic review bodies

Securities regulators ought to set up dedicated teams equipped with expertise in algorithmic systems, data science and competition economics. These units shall hold authority to launch technical investigations, demand algorithm-related documents, issue binding corrective orders and impose relevant sanctions. In China, current financial regulatory bodies include the People's Bank of China, the National Financial Regulatory Administration and the China Securities Regulatory Commission. Their capacity can be strengthened by adding specialized algorithm review functions, either via joint task forces or the establishment of a new independent agency.

(2) Regulatory technology (RegTech)

RegTech investment carries great importance for real-time detection of algorithmic collusion. One three-pronged strategy gets put forward. Comprehensive risk detection platforms rely on big data analytics and artificial intelligence. These platforms pick up suspicious market patterns. Parallel price shifts coordinated order flows and similar credit-score outputs fall among these patterns. Dynamic monitoring and early-warning systems get built. These systems trigger alerts. Alerts appear when algorithmic actions deviate from past benchmarks or peer-group norms. Automated compliance checking tools get developed. These tools keep validating algorithm registration files on a

continuous basis. These technical tools raise enforcement speed and accuracy by a large margin. Regulators can take intervention actions. They act before collusion creates serious market damage.

(3) International coordination

Securities markets and algorithmic systems operate across national borders. International cooperation becomes hard to replace under such conditions. Regulators share information linked to algorithm-related market practices. They align their enforcement actions. They work toward consistent standards for algorithm transparency and accountability. They set up mutual legal assistance frameworks for algorithm-related legal cases. The European Union (EU) open banking frameworks include Payment Services Directive 2 (PSD2), Third Payment Services Directive (PSD3) and Financial Data Access Regulation (FiDAR). U.S. policy drafts on algorithmic accountability serve as additional reference materials. These sources supply useful experience for interoperability rules and cross-jurisdictional data sharing. China can take an active leading role in shaping global industry norms. It takes part in major international forums. These bodies cover International Organization of Securities Commissions (IOSCO), Bank for International Settlements (BIS) and the Financial Stability Board. It also promotes bilateral agreements with its major trade partners.

Trust reconstruction and the role of data portability

Trust reconstruction sits at the core of all these reform measures for algorithm-driven securities markets. Trust is more than an abstract notion. It acts as a tangible factor. It shapes investor participation levels. It influences the intensity of competition among platforms. It also affects how long collusive coordination can keep going. Investors tend to switch service providers when they perceive unfair market conditions under high-trust circumstances. Platforms face heavier competitive pressure as a result. Low trust leaves investors passive and unreacting. Collusive conduct gains more room to persist.

Data portability works as an effective instrument to rebuild trust and hold collusion in check. Investors hold the right to move their trading records, risk profiles and other relevant data over to competing platforms. Switching costs drop with this right. Investors gain more power to seek out more favourable service terms. Smooth data transfer mechanisms incentivize platforms to compete on price, service quality and fair conduct. Platforms lose motivation to join collusive arrangements. Breaking away from such arrangements brings greater benefits for them. Within securities business scenarios, portability covers order-execution records and margin-credit histories. Data portability needs proper balance with data security and personal privacy. Sensitive data can only get transferred with clear user approval. Transfer processes must adopt safe encrypted channels. Aggregate anonymized data can circulate freely for portability purposes.

Interoperability functions alongside data portability. Platforms may use incompatible APIs or exclusive data formats. User switching costs get raised artificially by such technical setups. Regulators can enforce standardised interfaces. Common order-routing APIs and consistent credit-scoring formats fall within these interfaces. Market entry barriers get lowered. Market competition gets stimulated. The EU's open banking experience shows interoperability can come true without security losses. Solid identity verification and data protection measures need to be put in place. China can roll out similar standards for securities market infrastructure. Its well-developed fintech ecosystem offers support. An open, competitive and trustworthy market environment can take shape from these efforts.

Conclusion

Algorithmic collusion in securities markets is no purely theoretical risk; it constitutes a pressing real-world regulatory challenge. It puts core logic of antitrust and securities regulation to the test. This paper shows existing legal frameworks take shape from old understandings of concerted agreement and subjective intent. Such frameworks struggle to handle hidden nature, fast speed and complexity of algorithm-led coordination. Four collusion categories cover indirect messenger, hub and spoke, predictive agent and autonomous learning. Each category creates distinct difficulties for legal liability, evidence gathering and enforcement work. The Chinese context adds further complexity. It features campaign-led regulatory cycles and legal infrastructure still under development.

This practical challenge can still be addressed. A fully-range governance framework brings procedural transparency, substantive liability rules, institutional

capacity building and trust reconstruction together. It identifies, discourages and punishes algorithmic collusion. It preserves efficiency benefits and innovation gains from algorithmic trading at the same time. Proposed reform items contain algorithm registration, impact assessment, audit systems, broader definition of concerted conduct, burden of proof reversal, strict liability, special review bodies, RegTech spending and international coordination. These reform items support one another. They permit step-by-step roll-out. Pilot projects in high-risk market segments can serve as the starting point.

Digital finance governance requires a mindset change. The old mode reacts after problems occur, acts in cycles and focuses heavily on risk avoidance. Authorities need to adopt a forward-looking, flexible and capacity-focused working mode. Such change does not mean losing regulatory control. It points toward more targeted regulatory approaches. Regulators make use of technology to improve oversight. Transparency and data portability give more power to market participants. Authorities build institutional resilience to match the speed of technical innovation. These combined actions protect investor interests. They maintain fair and efficient market operation. They support stable growth for digital finance. Public interests can be safeguarded amid rapid technological transformations.

Funding

This work was not supported by any funds.

Acknowledgements

The author would like to show sincere thanks to those technicians who have contributed to this research.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] Olanrewaju, A. G. (2025) Artificial intelligence in financial markets: optimizing risk management, portfolio allocation, and algorithmic trading. *International Journal of Research Publication and Reviews*, 6(3), 8855-8870.

[2] Calvano, E., Calzolari, G., Denicoló, V., Pastorello, S. (2021) Algorithmic collusion with imperfect monitoring. *International Journal of Industrial Organization*, 79, 102712.

[3] Jin, S. (2022) Anti-monopoly regulation of digital platforms. *Social Sciences in China*, 43(1), 70-87.

[4] Mazumdar, A. (2022) Algorithmic collusion. *Columbia Law Review*, 122(2), 449-488.

[5] Fzrachi, A., Stucke, M. E. (2019) Sustainable and unchallenged algorithmic tacit collusion. *Northwestern Journal of Technology and Intellectual Property*, 17, 217.

[6] Weber, B. C. (2023) Hub-and-spoke conspiracies: Can big data and pricing algorithms form the rim? *SMU Science and Technology Law Review*, 26, 25.

[7] Hansen, K. T., Misra, K., Pai, M. M. (2021) Frontiers: algorithmic collusion: supra-competitive prices via independent algorithms. *Marketing Science*, 40(1), 1-12.

[8] Klein, T. (2021) Autonomous algorithmic collusion: Q-learning under sequential pricing. *The RAND Journal of Economics*, 52(3), 538-558.

[9] Li, M., Zhao, C., Wu, F. (2026) Credit risk contagion and governance of digital financial platforms under trust mechanism reconfigured by algorithms. *Science & Technology Progress and Policy*, 43(9), 1-11.

[10] Deng, A. (2020) Algorithmic collusion and algorithmic compliance: risks and opportunities. *The Global Antitrust Institute Report on the Digital Economy*, 27.

[11] Buttaboni, C., Floridi, L. (2026) A regulatory taxonomy of AI opacity in the EU: rethinking transparency, traceability, interpretability, and explainability. *AI and Ethics*, 6(1), 100.

[12] Wang, Y., Zhou, Y. (2025) Can government incentive and penalty mechanisms effectively mitigate tacit collusion in platform algorithmic operations? *Systems*, 13(4), 293.

[13] Lianos, I. (2022) Value extraction and institutions in digital capitalism: towards a law and political economy synthesis for competition law. *European Law Open*, 1(4), 852-890.

[14] Wang, X., Wu, Y. C., Ji, X., Fu, H. (2024) Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence*, 7, 1320277.

[15] Xu, D., Tang, S., Guttman, D. (2019) China's campaign-style Internet finance governance: causes, effects, and lessons learned for new information-

based approaches to governance. *Computer Law & Security Review*, 35(1), 3-14.

[16] Chen, K., Cheng, H., Qin, Q. (2024) Assessing the impact of environmental accounting message disclosure quality on financing costs in high-pollution industries. *Journal of Cases on Information Technology (JCIT)*, 26(1), 1-18.