



College of Humanities
Master of Financial
Technology-
Fin Tech

Artificial Intelligence for Financial Technology

FNT 626

Lecture 07

Prepared By:

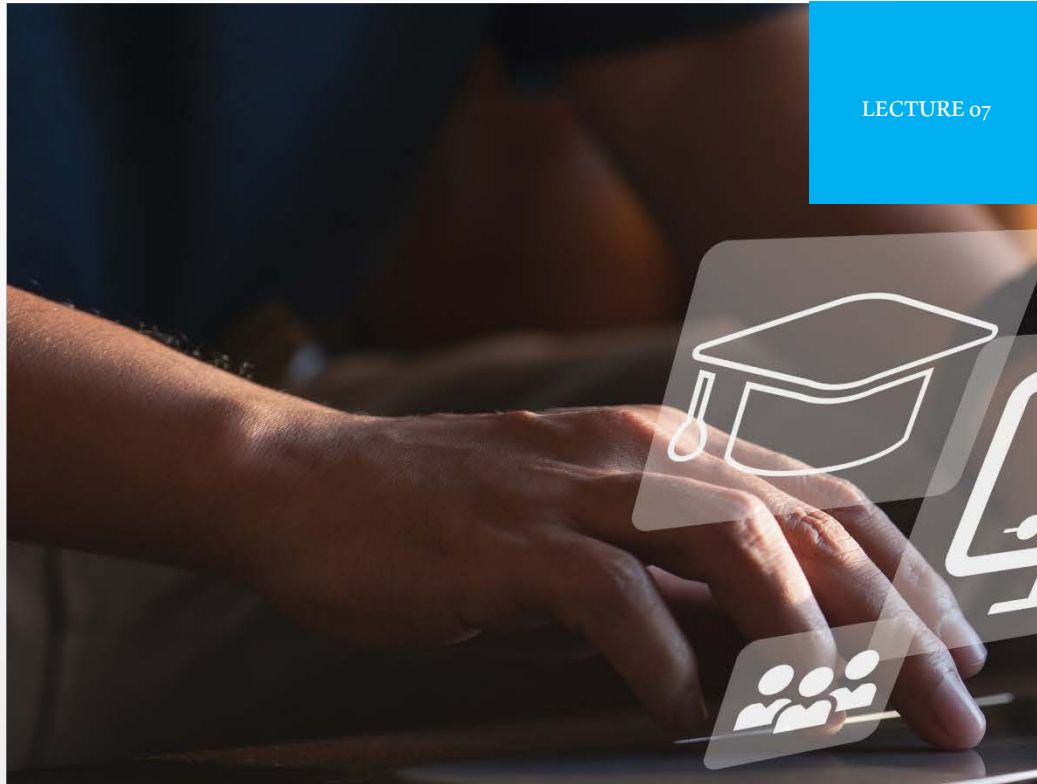
Dr. Abeir Moussa



Artificial Intelligence for Financial Technology

FNT 626- AI for Fin Tech

Lecture 07



**Regulating AI Trading from an AI
Lifecycle Perspective**

LECTURE 07

Ch. 9- Regulating AI trading from an AI lifecycle perspective

Learning Objectives

1. Understanding AI Trading in Financial Markets
2. Explore the AI lifecycle in trading
3. Examine the regulatory challenges associated with AI trading
4. Understand the regulatory responses to AI trading from an AI lifecycle perspective
5. Address the ethical considerations in AI trading
6. Explore the data governance practices and compliance requirements specific to AI trading
7. Understand the significance of algorithmic transparency and explainability in AI trading
8. Explore the risk management practices and model validation requirements in AI trading
9. Address the role of market surveillance and oversight in regulating AI trading

LECTURE 07

Ch. 9- Regulating AI trading from an AI lifecycle perspective

Chapter outline

1. INTRODUCTION
2. ML AND ALGORITHMIC TRADING: A PRIMER
3. AI TRADING 'MISBEHAVIOUR': MAPPING THE RISKS
4. THE *STATUS QUO*: UNCERTAINTIES AND FAILURES
5. DISENTANGLING COMPLEXITY IN AI TRADING
6. CONCLUSION

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective

1. INTRODUCTION

Understanding the main factors of complexity due to AI, particularly its subfield of **machine learning (ML)**, can help better identify the risks associated with the technological aspects of AI trading. It offers an initial attempt to explain how the sophistication of AI tools for financial trading may adversely influence market functioning, thus calling for regulatory responses to risks associated with it. In particular, the speed and pace of advancements in AI in financial trading leave markets vulnerable to novel causes of market disruption and failure, including unprecedented risks of market manipulation and even 'tacit' collusion by autonomous AI trading systems regardless of human intent. And, indeed, the incremental risks associated with AI trading and their possible negative consequence to market stability and integrity urge us to consider and analyze whether these have outpaced existing risk-mitigating measures, such as established risk management practices and other control tools. As our analysis will reveal, existing regulatory requirements and other legal safeguards may have already become obsolete, thus perilously inadequate to deal with the additional layer of complexity introduced by the technical specificities of AI.

2. ML AND ALGORITHMIC TRADING: A PRIMER

2.1 AI-induced Complexity in Global Capital Markets

2.2 An 'ABC' of ML in Algorithmic Trading

2.3 From 'Deep Learning' to Autonomous Trading Agents



LECTURE 07

**Ch. 9- Regulating AI trading from an AI
lifecycle perspective**

Ch.9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

2. ML AND ALGORITHMIC TRADING: A PRIMER

When analyzing global capital markets under the lens of complexity theory, we can observe how they have been gradually evolving as an increasingly complex (eco-)system. But it can also refer to the fast-changing and adaptive socio-technical system of capital markets, its functioning and behavior, given the dynamic and evolving nature of economic relationships among market actors, also due to technological innovation. Undoubtedly, the first emergence of electronic trading contributed to increasing levels of overall system complexity. Indeed, the ultra-fast and interconnected character of algorithmic trading has created new risks to financial stability and market integrity. In response, most advanced jurisdictions have promulgated ad hoc regulations to mitigate technology-driven risks, aiming at counteracting the effects of flawed or malicious design, development and use of algorithmic trading systems and strategies. Yet, due to advancements in AI and particularly ML research, the sophistication of algorithmic trading practices, businesses, and related industries is adding an extra layer of complexity on top of a dynamic system – i.e., global capital markets – that inherently tends to be quite complex anyway. On the one hand, complexity matters to those market players, such as financial institutions, which need to make productive use of it to inform their business decisions under conditions of uncertainty while also complying with the law.

Ch.9- Regulating AI trading from an AI lifecycle perspective

2. ML AND ALGORITHMIC TRADING: A PRIMER

On the other hand, financial regulators and supervisors must take utmost account of the complexity spurred by AI to navigate all related technical and regulatory aspects with confidence while pursuing their institutional mandates. With these aspects in mind, the following provides a high-level overview of how a new generation of algorithmic trading techniques and strategies, based on ML, have further shaped the relationship between complexity and financial markets. As will be argued, all these developments urge global regulators to assess the need to improve their regulatory theory and practice in order to understand the sources of system complexity and their properties (e.g., stability, fragility, etc.

LECTURE 7

Ch.9- Regulating AI trading from an AI lifecycle perspective

2.1 AI-induced Complexity in Global Capital Markets

The rapidly growing and widespread use of AI techniques and tools in finance is among the most captivating developments in financial technology (FinTech) in recent decades. Today, the case of financial institutions using ML to automate trading and investment activities represents just one of many ways in which AI is fueling an escalating trend towards greater system complexity in our global capital markets. On the one hand, the rise of AI-driven trading responds to the particular business needs of market participants, in part with a view to best serving their clients. Investment firms can now integrate ML applications into their trading systems and strategies to carry out various innovative activities. These include, for instance, sentiment analysis based on social media content, automated text analysis of financial reports and other documents, visual analysis of charts, optimization of tasks within the trading cycle (e.g., pre-trade analysis, trading signal generation, trade execution, etc. **First**, both computational power and data storage have become relatively cheap and accessible, with technology market players offering outsourcing services (e.g., cloud computing, software as a service and even AI as a service). **Second**, thanks to both market and regulatory developments, there is an exploding availability of data that, through the use of algorithms, market participants can leverage to inform their trading and investment decisions. Besides traditional market data and other financial data, investment firms can extract valuable insights on markets from so-called 'alternative data'.

Ch.9- Regulating AI trading from an AI lifecycle perspective

2.2 An 'ABC' of ML in Algorithmic Trading

Depending on the actual level of human involvement in the learning process (e.g., data curation, model choice, hyperparameters optimization, human-in-the-loop-and-control, etc. First, in '**supervised learning**' (SL), computer trading algorithms are trained with empirical data, pre-labelled by human experts in order to learn a function that maps from input to output. For instance, a human trader can feed an SL algorithm with historical market data (e.g., asset prices, returns, volatility) to train an ML model in order to predict the future price movement of a particular financial instrument or to rank/ classify different assets according to specific distinguishing criteria (e.g., in terms of risk). Second, in '**unsupervised learning**' (UL), algorithms infer patterns (e.g., regularities) from input data by identifying similar but distinctive features with limited or even no human feedback. For instance, a human trader can use UL methods to perform a pre-trade cluster analysis among a given portfolio of financial instruments based, for example, on their likelihood of having a positive daily return in light of past observations in order to inform subsequent trading decision-making Third, '**reinforcement learning**' (RL) allows for the creation of software agents, the knowledge and behavior of which are developed through series of reinforcements (i.e., rewards and punishments) in order to reach pre-specified goals defined as objective functions.

Ch.9- Regulating AI trading from an AI lifecycle perspective

2.2 An 'ABC' of ML in Algorithmic Trading

RL agents are, thus, oriented towards discovering best policy action, via trial and error, within a partially unknown and unpredictable dynamic action environment, such as the globalized financial system. Relatively, RL-based trading agents may resemble how human traders generally acquire market knowledge through trading experience (e.g., through successes and failures). Unlike both SL and UL methods, RL enables the creation of trading agents that can explore their environment to learn the best trading strategies for profit maximization under some sort of risks control, while also accounting for real markets' constraints (e.g., liquidity and transaction costs, market impact, etc.). In the field of **high-frequency trading (HFT)**, for instance, RL methods are shown to enhance trading performance by predicting directional price movements from order book signals or optimizing trade execution or smart order routing tasks.

Ch.9- Regulating AI trading from an AI lifecycle perspective

2.3 From 'Deep Learning' to Autonomous Trading Agents

As a more recent subfield of ML, '**deep learning**' (DL) methods have substantially contributed to a fresh impetus in ML research, with tremendous promise behind a variety of applications, including classification of audio, image and video data, but also financial trading. DL methods are computational approaches based on a model of the human cortical structure in order to best analyze input data through learning on multiple levels of abstraction (i.e., through so-called 'hidden layers'). Apart from increasing computational cost, DL methods can offer a number of advantages over traditional linear statistical approaches to finance in that they can learn non-linear functions to discriminate latent patterns in the data. As DL is also used in combination with other ML methods, a recent wave of published works in computational finance research is exploring the potential offered by different ML-based approaches in financial trading. As will be seen, DL makes it possible to build increasingly capable and autonomous algorithmic trading systems, up to and including artificial trading agents. DL methods – like other ML paradigms – are well known for being strongly dependent on the quantity and quality of training data. In addition, as another more general issue in ML research, DL methods are not free from human-induced biases (e.g., inductive biases from statistically irrelevant training data). Thus, the often opaque nature of specific DL-based trading systems contributes to the growing complexity of global capital markets, which, if not adequately regulated, can impose severe risks to financial stability and market integrity.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

2.3 From 'Deep Learning' to Autonomous Trading Agents

According to a growing number of published works in the field of computational finance, however, there is at least initial evidence of the benefits of DRL applications in algorithmic trading. DRL-based systems can be used to establish autonomous trading agents that can discover how to manipulate markets as optimal and rational behavior when certain conducive market conditions and factors are present. In effect, modern algorithmic trading systems should be better conceived as complex 'ecosystems' of algorithms, potentially also requiring the involvement of the human factor (i.e., in order to achieve accurate, reproducible, reliable, predictable and explainable outcomes). Various ML methods and techniques can be combined in complex AI architectures, integrated or hybrid systems, or ensemble strategies. Several algorithmic agents may act in concert in multi-agent systems under different learning and collaborative/competitive approaches with the final goal, in any case, to generate alpha (i.e., extra-returns). However, a key issue is to which degree such complex systems satisfy not only explainability requirements, but also, for example, those of human accountability and liability. With the prospect of greater automation of ML-powered trading up to the point of autonomous trading agents, it will become necessary to ensure that the use of AI systems is reliable for the private interest of profit but also for the public interest of preserving the stability and integrity of financial markets.

3. AI TRADING 'MISBEHAVIOUR': MAPPING THE RISKS

3.1 AI Trading 'Misbehaviour': The Four Basic Scenarios

3.2 ML and Market Manipulation

3.3 Algorithmic Trading Agents and 'Tacit' Collusion



LECTURE 07

**Ch.9- Regulating AI trading from an AI
lifecycle perspective**

Ch. 9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

3. AI TRADING 'MISBEHAVIOUR': MAPPING THE RISKS

Algorithmic trading and, notably, HFT have effectively contributed to making financial trading faster, more interconnected, cheaper and, perhaps, markets overall more efficient. With a focus on the latter, this section explores the many ways in which increasing reliance on AI agency can exacerbate old regulatory struggles and even result in new risks to the safety and integrity of capital markets through novel forms of algorithmic market manipulation and 'tacit' collusion. Because of the greater autonomy and growing complexity of algorithmic trading systems, it will be increasingly challenging for enforcement bodies to assess the real motives for a given AI-driven market misconduct or crime, as these could be due to a variety of different causes. On the other, financial supervisors face the burdensome task of safeguarding financial stability and market integrity by detecting, investigating, and prosecuting algorithmic misconduct. Yet, whenever AI-driven market manipulation occurs and passes undetected, malicious AI users expose markets to fragility, creating a host of negative externalities and harm to society. Thus, if we fail to adequately govern and regulate AI trading, global capital markets will likely be prone to market failures and systemic instability.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.1 AI Trading 'Misbehavior': The Four Basic Scenarios

The unconscious, negligent, and malicious use of AI in financial trading can cause a range of market inefficiencies and even be the cause of systemic risk, thus leading to more fragile global capital markets. In short, there are four basic scenarios in which AI trading can create market distortions, including disruptive market events (e.g., flash crashes), market misconduct or crime. First, an AI system may be involved in a market accident or crime as a victim itself. In principle, an attacker can influence the behavior of an algorithm trading system by introducing manipulated information into the input data stream. Second, algorithmic trading can result in a number of unintended consequences (e.g., market accidents) due to some operational failures emerging from poor human design, use, or control (e.g., due to a system bug). In fact, most common events of exceptional market disturbance are often the result of some flawed design leading to software errors. Other times, market accidents may be due to technical glitches in trading algorithms that lead to abnormal trading conditions, putting some market participants at an unfair disadvantage. Even with more deterministic systems, the unintended consequences of algorithmic trading can often defy human comprehension to the point of complicating effective regulatory compliance and law enforcement.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.1 AI Trading 'Misbehavior': The Four Basic Scenarios

Third, more underhandedly, malicious actors can consciously develop and train manipulative AI systems to perpetuate unfair market practices, seeking to gain illicit profits that would not otherwise be available to them. Thus, the use of increasingly powerful but sophisticated AI applications for financial trading can cause additional information asymmetry between financial firms and market conduct supervisors, thereby exposing markets to risks of market failures. Finally, we have the trickiest scenario in which autonomous AI trading agents are so advanced that they can self-learn how to game market rules as an optimal and rational strategy regardless of any specific human intent. As will be discussed, this is the most problematic scenario for public authorities faced with regulating algorithmic trading and enforcing market conduct rules against increasingly autonomous and often black-box AI trading systems.

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.2 ML and Market Manipulation

With progress in computational finance, algorithmic trading practices and strategies continue to evolve, we envisage the emergence of new forms of market manipulation. Under the current algorithmic revolution, AI offers innovative tools for malicious market participants to optimize traditional forms of manipulation and even discover new manipulative strategies. With these risks in mind, it is therefore time to reflect on how to deal with the additional complexity introduced by AI in financial trading and the associated risks to the safety and integrity of global capital markets. There is also increasing evidence of human traders at financial institutions consciously developing and using trading algorithms to accomplish profitable but unlawful trading practices. Indeed, the growing number of prosecuted cases against algorithmic traders manipulating markets clearly indicates financial authorities' increased focus on risks to market integrity associated with technologically advanced forms of trading. Though, it also seems reasonable to assume that the potential of a given AI trading system to manipulate markets successfully is likely to largely depend on a number of both micro- and macro-economic factors. Among those, for instance, one could think of a given AI user's degree of market access and market power as two main practical aspects to assess the ability to effectively manipulate markets while at the same time being exposed to financial risks. Previously, we conceptualized some of the aforementioned risks, focusing on market manipulation by AI and using the proprietary trading industry as a case study. Indeed, the potential offered by increasingly 'intelligent' trading algorithms, based on ML, can be expected to develop in less speedy and less transparent markets as well.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.2 ML and Market Manipulation

Financial institutions can nowadays research artificial trading agents that, once tasked with a trading goal, can successfully discover the best strategy with increasing autonomy by learning from experience. As losing control over trading algorithms can lead to various and severe market failures, the risks introduced by increasingly autonomous trading agents should be thoroughly assessed by financial regulators, given the high potential to hamper financial stability and market integrity. Particularly, the human component may still be critical to induce AI trading agents to learn a manipulative strategy. Nevertheless, consciously implementing AI for manipulative or other disruptive market conduct can be challenging, given the many practical and technical limitations AI-based agents can generally face in real markets. Yet constant progress in ML research may soon overcome some of these limitations. In effect, according to a growing number of in-lab studies, there is at least initial evidence regarding the ability of trading agents to discover market manipulation as an optimal strategy, regardless of any human intent. Nevertheless, it still remains unclear which learning frameworks (e.g., via back-testing, simulated market environments, or real-time) are best for ML-powered trading agents to autonomously discover and engage in market manipulation.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.2 ML and Market Manipulation

Overall, the potential for AI-driven trading to hinder market integrity has become a 'moving' target for global financial regulators. Ascertaining whether AI trading misconduct is the result of specific human intent and strategic business planning or, instead, just a matter of negligent development and/or oversight has become increasingly challenging for financial law enforcement authorities. At the same time, global financial regulators, while remaining cautious and vigilant regarding developments in AI within the ramifications of algorithmic trading, have not yet taken any specific regulatory measures. Nevertheless, the prospect of extremely cynical trading agents capable of self-learning how to manipulate markets while pursuing a predefined goal today seems more than mere imagination. Although perhaps still highly unlikely to materialize, this scenario leaves unanswered a number of troubling questions regarding the suitability of the current legal systems and regulatory framework in dealing with all such risks.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.3 Algorithmic Trading Agents and ‘Tacit’ Collusion

Delegating cognitive agency and financial decision-making to ML-based trading agents may also expose markets to novel forms of algorithmic collusion. With the prospect of the widespread adoption of increasingly capable AI trading tools by market players, it is safe to assume that unprecedented and harmful forms of algorithmic market coordination may soon materialize on global capital markets. If so, we urge global financial regulators to monitor and examine these technological developments carefully and scrupulously to ensure the fair and proper functioning of capital markets. Previously, it was discussed the relevance of a number of market factors can facilitate ‘tacit’ collusion among competing trading algorithms (i.e., market transparency, trading frequency, traded assets homogeneity, market power, entry barriers, and technological sophistication). To the extent that these facilitating factors are present in specific segments of capital markets, competing trading algorithms will be more likely to show a tendency to achieve cartel-like outcomes. However, it is also reasonable to assume that the capability of a given software agent to engage in collective forms of market manipulation closely depends on its ability to take risks and execute trading in an economically efficient way. Second, the very level of sophistication of AI trading systems certainly plays a central role in allowing collusion to emerge without any direct human involvement.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.3 Algorithmic Trading Agents and ‘Tacit’ Collusion

Consider, for instance, the case of RL-based agents. As a primary technical limitation, the ability of competing RL-based trading agents to self-learn how to coordinate their behavior autonomously can be largely constrained by the complexity and high-dimensionality of their action environment (i.e., the specific application domain of RL on capital markets). In other words, given a potentially infinite number of variables to monitor simultaneously, RL-based agents might find it hard or even impossible to achieve dynamic strategic coordination with rivals’ algorithms while also pursuing a predefined business objective. At least in principle, however, it seems plausible that algorithmic trading agents could be trained by humans to discover ways to coordinate with rivals (e.g., by reverse engineering their algorithms). Moreover, it could also be expected that as advances in ML augment the capabilities of software agents, autonomous AI trading will seek to implement ‘tacit’ forms of collusion as a rational and optimal strategy. While it is hard to assess the exact need for communication required by RL algorithms to coordinate their trading strategies, the enhanced analytical capabilities offered by their combination with DL methods could offer a fruitful avenue for future research in this field.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

3.3 Algorithmic Trading Agents and ‘Tacit’ Collusion

Notwithstanding all these technical difficulties, some recent computational research studies provide at least the first evidence, from in-lab experiments, about the ability of independent RL-based agents to coordinate behaviors in dynamic competitive games. The spectacular conclusion of these studies is that ‘tacit’ collusion will almost inevitably arise as an optimal strategy in all those markets increasingly dominated by algorithms. Because these results are derived from simulated and controlled environments, the reader should treat them with caution. Although, without a shadow of a doubt, RL-based agents have shown a rather natural aptitude to collude under significantly simplified constraints and stylized market settings; however, this conclusion can hardly be generalized in the context of more complex domains, such as trading in capital markets. When exposed to real market configurations, RL agents may indeed find it extremely hard to scale well and master the higher dimensional complexity of their action space before strategically coordinating behaviors with rivals to achieve the best rewards. Arguably, with the increased analytical capability offered by DL methods that could help relax many of these mathematical constraints, some forms of algorithmic coordination among competing AI trading agents may soon become easier to accomplish. Nevertheless, it is certainly fascinating to observe that the scientific community is employing and researching the same ML paradigms as discussed above (i.e., DRL methods) to assess the likelihood and potential impact of new and emerging risks of algorithmic collusion. Therefore, one can even postulate that global capital markets will soon face new and unprecedented risks of algorithmic collusion, the likelihood and related social harm of which have yet to be concretely determined.

4. THE *STATUS QUO*: UNCERTAINTIES AND FAILURES

4.1 Challenges of the 'Deep Computational Finance' Research

4.2 Black-box Trading and Ethical–Legal Dilemmas

4.3 Deficient Regulatory Regimes and Uncertain Law Enforcement

4.3.1 Liability rules

4.3.2 Regulatory frameworks

4.3.3 Market conduct supervision



LECTURE 07

Ch.9- Regulating AI trading from an AI lifecycle perspective

Ch. 9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

4. *THE STATUS QUO*: UNCERTAINTIES AND FAILURES

In the previous part, the potential offered by AI tools for financial trading, both for good and evil will be discussed. Therefore, in light of these emerging threats to the safety and integrity of markets, this section addresses how existing financial law and regulation can fall short of dealing with the increased complexity invoked by AI trading. In addition, since black-box AI trading can result in misconduct and harm, there is a need to explore the ability of the current legal systems and enforcement regimes to deal with such technology-specific risks and related issues of liability.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

4.1 Challenges of the 'Deep Computational Finance' Research

Like any other ML research field, **'deep computational finance'** integrates interdisciplinary scientific knowledge and methodologies. More than merely advancing financial practice, the development, training and testing of algorithmic trading systems are nowadays related to an engineering approach for the purpose of mastering complexity, in the context of the 'AI lifecycle'. In as much as it relies on a complex mix of emerging and fast-evolving technologies, the development and implementation of trustworthy AI systems and infrastructures can indeed present significant challenges for market players. To disentangle the complexity brought about by AI, the following addresses some of the technical specificities and related practical challenges to achieving effective and reliable use of AI tools in algorithmic trading.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

4.1 Challenges of the 'Deep Computational Finance' Research

The starting point is acknowledging that modern AI trading systems look less like traditional trading desks and more like experimental laboratories or industrial production lines. Actually, the ML training process can be thought of as an experiment in itself, whereby the ability to assess its performance and ensure its explainability is critical to proving successful results. Generally, the specific use case and application domain heavily influence the performance of any real-life ML solution. In fact, achieving effective and reliable applications of ML for solving problems of a financial trading nature can present a number of technical challenges that may ultimately inhibit their safe use and adoption, given the need to comply with legal and regulatory requirements. One such technical issue concerns the critical role of data in ML research. As data-driven approaches to empirical discovery, ML methods offer innovative tools for dealing with financial uncertainty. However, ML methods are also well known for their strong dependence on data quality and quantity. Training an ML algorithm heavily relies on copious amount of available data, which can be gathered and even augmented from multiple sources. In addition, training data must be of the utmost quality, for instance, by ensuring statistical representativeness, including bias independence. Moreover, data scientists must take all reasonable steps to handle data inconsistency, such as irregular or invalid input data, which can negatively affect any learning method. When data are not sufficient in terms of volume, they can also be augmented through synthesized data. More generally, ML methods applied to financial trading must address the mathematical problem of dealing with the non-deterministic behavioral properties of capital markets, which are notoriously complex to model.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

4.1 Challenges of the 'Deep Computational Finance' Research

The noisy, non-stationary and sometimes simply unpredictable nature of financial markets complicates, even for most sophisticated ML approaches, the task of modelling market dynamics given all the complexity embedded in capital markets. In order to achieve its goal through an optimal sequence of actions, a trading agent not only has to explore the entire action space, which is partly defined by the stream and evolution of empirical data, but also has to take into account the market effects of its trading strategy as well as other market constraints. But resorting to DL methods can also render trading agents more prone to issues of over-fitting and model selection, two common risks that underpin the crucial role of model validation tasks (e.g., back-testing) to make sure that a given model can actually achieve its intended purpose. Finally, most sophisticated ML approaches to financial trading (e.g., based on DL) can often invoke black-box problems, thus leading to various ethical and legal issues. Indeed, as history has shown, the use of data analysis technology without sound scientific methodology and in the absence of ethical considerations can lead to unintended consequences and even harm markets and society as a whole.

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective

4.2 Black-box Trading and Ethical–Legal Dilemmas

Whenever an algorithmic trading system or strategy entails black-box algorithms or processes, several ethical–legal questions arise. Notably, financial institutions using AI trading tools must ensure their compliance with market conduct rules and other regulatory requirements, such as engaging in fair and permissible activities and taking due care of their algorithmic systems to avoid disrupting markets. In a financial trading context, the black-box problem arises when human experts cannot fully understand or explain why and how their trading algorithms have reached a particular solution/decision in the face of specific input data, thus leading to an accountability gap and associated liability issues. Financial institutions that utilize AI for unfair practices or illicit purposes, thereby polluting the informativeness of markets, actually externalize the costs of their risky activities to other market participants. First, the phenomenon may simply manifest itself as a deliberate design choice made by the same users in order to keep the details of their AI-based trading secret from others, with the goal of securing a competitive edge. Alternatively, opacity may occur as an unintended consequence of using sophisticated trading systems due to a lack of specialized human expertise in the design, development, deployment, and use of AI. Whereas the inner working of more traditional, hence non-ML, approaches to algorithmic trading are determined by human knowledge encapsulated in algorithms and data structures, ML methods render possible self-learning from empirical domain data up to dynamically adjusting to changing situations due to new observations. Therefore, understanding and mitigating causes of opacity in ML become imperative to ensure the acceptance of innovative AI-based trading solutions and strategies from a legal and regulatory perspective.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

4.3 Deficient Regulatory Regimes and Uncertain Law Enforcement

As discussed previously, the technical specificities of ML-powered trading systems leave several unanswered questions regarding the integration of ML with financial theory and practice. As such, human experts using ML methods should always be able to understand and provide effective reasoning regarding the market activity of their trading system to be compliant with the law. Nevertheless, whenever a given AI system exhibits the black-box problem, it can make any attribution of liability for market misconduct and harm de facto impracticable. This limitation is particularly troublesome and worrisome whenever AI trading can be involved in serious cases of market abuse, such as market manipulation, as enforcement bodies need to prove some relevant mental state with compelling evidence to succeed in enforcement. Specifically, increasing levels of autonomy and complexity in AI trading systems are likely to further exacerbate existing legal problems inherent to delegating financial decision-making to algorithms.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

LECTURE 7

4.3.1 Liability rules

Attributing liability for AI-related accidents, market misconduct, and associated harm can be highly problematic. Existing legal systems are often criticized for their overly vague definitions of market manipulation, which, while perhaps able to cope with traditional human misbehavior, seem far from safely regulating AI trading and the risks associated with it. The increased complexity introduced by AI can lead to liability issues for market misconduct and harm whenever something can go wrong or control is lost in AI trading. Established liability concepts underpinning existing market conduct rules can hardly find a safe application for cases of market manipulation by AI. Given the automated, fast, interconnected, and increasingly sophisticated nature of algorithmic trading systems due to AI, traditional liability rules and tests – e.g., intent, causation, foreseeability, negligence – will find an increasingly challenging scope of application. Moreover, the speed at which these systems operate and interact may preclude human experts from accurately foreseeing a priori the conduct and failures of algorithmic trading. In global algorithmic capital markets, the autonomous and black-box nature of specific AI-based trading strategies is therefore inherently prone to undermining the safe application of established prohibitions of market manipulation as these rely on traditional liability concepts and rules. Even assuming the ability to detect market misconduct by AI trading, enforcement authorities would still need to find ways to ascertain the exact contribution of all possible individuals involved in designing, developing, using, and maintaining a given AI system to impute liability.

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective**4.3.2 Regulatory frameworks**

Most advanced jurisdictions have sector-specific regulations for the governance of algorithmic trading. Whilst these regulatory regimes generally aim at mitigating risks to the orderly functioning of markets and their integrity, they are inherently entangled with somewhat outdated assumptions that can hardly fit all the complexity of modern and future algorithmic trading. As a first matter of concern, legal systems use their own definition of algorithmic trading. As a common denominator, however, legal regimes usually subject HFT practices to more stringent requirements due to their higher potential to distort markets and cause systemic risk. Apart from that, in all jurisdictions, algorithmic trading is not differentiated according to the specific uses of various AI technologies and applications, notwithstanding that the criticality of AI-related risks largely depends on the actual degree of complexity and capability of a given AI system. Second, the tasks of mitigating risks inherent to algorithmic trading are mostly left to their developers and users. Financial institutions using algorithmic trading are subject to specific legal requirements. Regulatory focus is mostly placed on algorithmic trading market behavior and measurable outcomes (i.e., trading patterns). To this end, the activity of algorithmic traders needs to be flagged, and firms must keep records of their trading history to support supervisory action. In addition, financial institutions must comply with a set of organizational requirements aimed at ensuring adequate investment in precautionary measures. High de jure requirements are imposed on the testing, validation, and deployment phases of algorithmic trading to ensure reliable applications. However, as recently highlighted by some regulatory reports, the conformity assessment of a given AI trading system remains largely an internal task for investment firms.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

4.3.2 Regulatory frameworks

They need to find a compromise between the rigorous screening of algorithms, including market surveillance, and the objectives of a profit-seeking private business under fierce competitive pressure from alternative venues. Also, an algorithmic trading firm can simultaneously be the operator of a trading platform (e.g., a dark pool), thus leading to a possible conflict of interest. As another cause of ineffective oversight, algorithmic traders that use direct market access – an arrangement that allows firms to interact directly with a trading venue's order book by using the IT facilities of other financial institutions – can find ways to bypass some market access rules. Finally, being exclusively in charge of the oversight of their own platforms, trading venues are not in a position to provide cross-market and cross-border market surveillance, which indeed is one of the main limitations of the current supervisory architecture, given the ubiquity of specific AI trading strategies. As AI technology risks evolving within somewhat 'shadowy' algorithmic trading markets, financial regulators must find innovative ways to promote a responsible culture in the design and use of AI. In light of the above, it seems rather doubtful whether and effectively how self-regulation by industry participants and delegation of key supervisory tasks to market operators can together promote a 'good market conduct' culture within the AI trading industry.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

4.3.3 Market conduct supervision

To be effective, financial regulation needs to be backed by robust enforcement. Financial law enforcement, for its part, is intimately intertwined with the ability of financial supervisors to detect, investigate, and prosecute cases of market misconduct in the best cost-efficient way, within a reasonable timeframe, and in full respect of private interests in taking legal action. Furthermore, while suffering from technological inferiority compared to private organizations, both are confronted with the daunting task of mitigating risks of market misconduct and crime by increasingly sophisticated and optimized AI-based trading strategies. Notwithstanding continuous efforts to achieve near real-time, cross-market and cross-border surveillance of trading activity through enhanced cooperation among national financial supervisors, market conduct supervision is still mainly single-market-oriented, with significant responsibilities delegated to market players themselves. However, this other set of precautions mostly requires substantial investments in IT systems, testing facilities and other risk management tools and expertise by the same market players, all of which need to be tailored to their specific use of trading technology. In the prospect of a future dominated by artificial agents operating autonomously on markets, the direct auditing of AI-based trading systems could perhaps become more realistic with advances in the research and practice of regulatory/supervisory technology (e.g., via machine-readable regulation, XAI, etc.). Finally, we can also fairly expect some progress towards AI-driven market conduct supervision to materialize soon, especially considering the current trends and efforts by global financial supervisors to narrow their technology gap vis-à-vis market players.

5. DISENTANGLING COMPLEXITY IN AI TRADING

5.1 Current Regulatory Policy Trends

5.2 The Rationale to Regulate AI Trading

**5.3 Grounding the Case for a Rules-based and Risk-oriented
Regulatory Approach**

5.4 Delving Into the 'AI Lifecycle'



LECTURE 07

**Ch.9- Regulating AI trading from an AI
lifecycle perspective**

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5. DISENTANGLING COMPLEXITY IN AI TRADING

As mentioned before due to constant progress in ML research, humans today can craft trading systems that enjoy greater autonomy and are capable of self-learning from empirical data. We have also discussed how ML increasingly presents universal challenges to financial regulators, who need to understand the implications of the interplay between AI trading, financial stability and market integrity. Even though existing regulatory frameworks and supervisory practices approaches may have done a relatively good job with respect to first-generation AI algorithmic trading, it has to be prevented that they will fail to account for the increasing complexity introduced by more-advanced AI methods and techniques (i.e., based on ML and particularly DL) to be embedded in a globalized financial market characterized by unprecedented complexity in terms of structure, processes, and technology. By remaining almost entirely neutral regarding the precise levels of technological sophistication and complexity of AI trading systems, the current regulatory approach does not allow regulators to develop a solid understanding of AI trading technology and how different ML methods can impact the operations of investment firms as well as market functioning. Particularly, industry players may not have adequate incentives to develop and use trading machines for fair practices that fully comply with financial law and regulation.¹⁶¹ Malicious market participants may even face greater incentives to use black-box ML for improper purposes. As a necessary starting point to alleviate this growing tension, global financial regulators are being called upon to gain deeper knowledge of AI trading – i.e., ML methods and their criticality – rather than just focusing on the tip of the iceberg when it comes to regulating the risks associated with it.

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.1 Current Regulatory Policy Trends

There is little doubt that technological innovation within the ramifications of algorithmic trading gives rise to an increasing complexity characterising the structure and functioning of global capital markets. First, consider the model complexity of specific ML approaches. While ML methods are generally intended to assist humans in handling market uncertainty, their often black-box nature can constitute a source of uncertainty multiplication in itself. This is particularly the case with DL-based systems, as these can alter agency problems inherent to algorithmic trading in substantial ways. Moreover, the widespread adoption of, and ever-greater reliance on ML trading tools can have several implications for capital markets, such as shaping the economic relationships and the degree of interconnectedness among market players. In this evolving landscape, financial regulators at least appear increasingly vigilant about the risks and related legal issues introduced by the novel relationships between AI and algorithmic trading. But no major regulatory policy reforms have yet been taken across jurisdictions to tackle the additional uncertainty and incremental system complexity induced by advances in algorithmic trading due to AI/ML. In many jurisdictions, however, policymakers have adopted soft-law instruments targeting AI applications in finance. Although focusing so far on retail financial services, financial regulators aim to steer AI innovation towards socially beneficial and responsible outcomes while avoiding the risks posed by specific AI applications in risky domains for people's fundamental rights and safety. Differently, algorithmic trading, particularly the proprietary trading industry, remains a somewhat less explored AI application domain by global regulators. In reality, current regulatory approaches are largely unsuccessful in providing a sound normative framework for AI-related technology to develop and flourish within the financial trading industry in the interest of society.

LECTURE 7

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.2 The Rationale to Regulate AI Trading

While policymakers worldwide are considering somewhat different approaches to the regulatory governance of AI, no significant reform has addressed the financial trading industry to date. The only notable exception pertains to AI-related regulatory guidance for consumer-facing financial services. However, in light of the risks discussed above, the fundamental issue facing global financial regulators is not so much whether or not to regulate AI in financial trading, but rather how best to approach this challenging task in order to foster innovation and competition without sacrificing market integrity and safety. Following the mantra of technological neutrality, the current regulatory paradigm is largely focused on an ex-ante control of AI trading at market access rather than ensuring effective due diligence and final quality assurance of specific AI-powered trading tools. As discussed before, however, both regulators and supervisors face an even more daunting task when confronted with the speed and pace of AI research and practice, which in fact are often left without public scrutiny. In our view, solutions to this problem can either be addressed with enhanced supervisory effectiveness or by novel regulatory approaches that are better able to disentangle the complexity inherent to the growing sophistication of algorithmic trading technology. Nevertheless, we here discuss the merits of improving the regulation of algorithmic trading to account for the technical specificities of AI and the resulting additional risks – under the assumption that both policymakers and regulators lack proper awareness and a clear understanding of AI trading technology. In principle, any AI-targeted regulation should build upon existing legal and regulatory regimes for algorithmic trading and work incrementally based on the additional risks posed by specific AI applications.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.3 Grounding the Case for a Rules-based and Risk-oriented Regulatory Approach

By acknowledging the process of developing AI-based trading systems as an industry line of production, we are prompted to reflect on the necessity of making the best use of an engineering approach to regulating the 'AI lifecycle'. As an ideal, instead, regulators should maintain the role of co-producers of markets, along with economic actors, in order to install a culture of a responsible and fairly regulated industry, which is ultimately able to guarantee financial stability and market integrity. To achieve this goal, not only must they properly understand technology-specific aspects of AI tools for financial trading that can be the cause of additional uncertainty and risks to capital markets, but they must also consider how these aspects are shaping agency problems within firms as well as business relationships among market players themselves. Since not all AI trading applications present the same criticality, financial regulators should therefore adopt a rule-based and risk-oriented regulatory approach. As an advantage, this approach would allow them to rely on a framework to classify different AI trading tools and applications according to their perceived risks. Risk-based regulation can also allow public authorities to dispose of objective means for the use of enforcement resources and to focus their attention on relevant issues based on a well-defined risk framework. The ability to categorize AI-based trading systems and components according to certain risk-based metrics can concretely contribute to updating existing regulatory frameworks on the governance of algorithm trading.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.3 Grounding the Case for a Rules-based and Risk-oriented Regulatory Approach

In an effort to provide further clarity and effectiveness to the proposed EU regulatory framework for AI, a recent interesting proposal suggests categorizing AI systems according to a three-dimensional classification scheme based on: (i) the specific algorithmic methods employed in the system (i.e., ‘Methods’); (ii) the capabilities to be achieved by that system (i.e., ‘Capability’); and (iii) the level of criticality that can be attributed to it (i.e., ‘Criticality’). First, in terms of ‘Methods’, we have provided a high-level overview of how different ML paradigms can be used and combined within a given algorithmic trading system. Second, with regard to ‘Capability’, we have argued that any given AI application to financial trading poses its own risks according to the specific use case. Thus, depending on their capabilities within the whole trading cycle and the socio-economic context in which they operate, AI trading tools can present very different levels of risk. Finally, in matters of ‘Criticality’, we have pointed out that the potential of a given AI trading system or agent to result in harm to others ultimately depends on a number of techno-economic factors (e.g., the specific use case, ML model selection, mastering of complexity with regard to action/state space and hyperparameters, trading efficiency, market power, cybersecurity, etc.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.3 Grounding the Case for a Rules-based and Risk-oriented Regulatory Approach

As an ex-ante solution, however, mandating testing for AI trading systems – in order to check for their reliable and legally compliant development before their actual implementation on real markets – seems an inevitable regulatory policy innovation to be explored. Ex-ante and ex-post regulatory solutions can contribute to disentangling the sources of increased system complexity introduced by AI. But since the most innovative algorithmic trading systems can involve very different ML methods, techniques and strategies, financial regulation should provide, in a well-balanced way, for varying degrees of regulatory requirements and duties for both their developers and users. In the following, we provide some preliminary thoughts on how regulators could co-produce greater standardization of ML methods, components, and processes to render the potentially shadow business of AI-based algorithmic trading a truly regulated industry in the interest of society.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.4 Delving Into the 'AI Lifecycle'

Delving into the 'AI lifecycle' would allow financial regulators to both strengthen their knowledge and develop a greater understanding of the risks associated with AI-induced system complexity. Based on a rule-based and risk-oriented regulatory approach, ML applications to financial trading could be subject to different regulatory requirements, such as testing and certification regimes. According to a recently published study by the Bank of England, software validation for ML-powered systems today presents completely new challenges compared with more deterministic AI approaches to algorithmic trading. Generally, software-related risks in ML systems can be grouped into three main categories: (i) 'model risk', i.e., the risks that a given ML algorithm may not work as intended (e.g., because of false model assumption); (ii) 'technology risk', i.e., operational failures (e.g., due to incompatibility among system components or a system error); and (iii) 'data risk', i.e., all possible circumstances under which input data lack quality or availability. However, as another recent study points out, while perhaps addressing the peculiarities of more deterministic systems, established software validation frameworks in the financial sector perilously neglect key governance aspects of the AI lifecycle, including feasibility assessment, documentation, model monitoring and evaluation, and model risk assessment. With an engineering approach to regulating the 'AI lifecycle', regulators could therefore start targeting risks arising from ML-powered algorithmic trading at the level of software validation.

Ch. 9- Regulating AI trading from an AI lifecycle perspective

5.4 Delving Into the 'AI Lifecycle'

More generally, based on a risk assessment, AI systems or components could be subject to more or less stricter pre-approval requirements (i.e., testing and certification) and other regulatory obligations (e.g., on human control, re-validation, etc.). To illustrate, extremely 'high-risk' AI applications (or components) could even be prohibited when society cannot afford the related risks. For 'no-risk' or 'low-risk' AI trading tools, instead, an exemption regime could be provided. As a general rule, however, regulators will apply stricter regulatory requirements as the risk criticality of AI trading tools increases. Being able to rely on a framework as outlined above to categorize AI trading systems according to their specific technical risks and exact use case is a more reliable tool for global financial regulators and supervisors to deal with the increasing system complexity due to ML. Although the proposed framework represents only one of the possible technical-legal solutions to address the additional risks introduced by ML applications in such a critical domain for society as capital markets, the real challenge faced by legislators/regulators is to develop a solid and sufficient theoretical and technical knowledge for being aware of and deal with increasing levels of complexity introduced by AI and the resulting risks for the stability and integrity of global capital markets.

Conclusion

This chapter has discussed the increasing levels of system complexity of global capital markets and the related additional risks due to constant progress in AI, particularly ML methods applied to financial trading, from an interdisciplinary perspective. In this chapter, we have argued that in order to overcome the deficiencies and limitations of the current regulatory regimes applicable to advanced AI/ML in financial trading, the risk-based approach of the EU AI Act has to be put in perspective with regard to the novel concept of the 'AI lifecycle' (as derived from classical software engineering), which in turn is related to institutional issues of AI governance. As a consequence, we advocate careful consideration of and in-depth discussion in the political, legal, institutional, industrial and academic arena on how to bring to bear an effective synergy among the three, currently rather disconnected, regulatory layers of legislation/regulation, AI governance, and the 'AI lifecycle' for the sake of a future-proof financial trading sector.

Artificial Intelligence for Financial Technology

References:

Required Reference:

Remolina, N. and Gurrea-Martinez, A. eds., 2023. Artificial intelligence in finance: Challenges, opportunities and regulatory developments. Edward Elgar.

Recommended Readings

Chishti, S., 2020. The AI book: the artificial intelligence handbook for investors, entrepreneurs and fintech visionaries. John Wiley & Sons.

The background of the slide is a grayscale photograph of a person's hands typing on a laptop keyboard. Overlaid on this image are several semi-transparent icons representing education and technology: a graduation cap, a target with an arrow, an open book, a magnifying glass, a presentation screen with a bar chart, a group of people, and a computer monitor. The title 'The End of Lecture' is written in a white, italicized serif font across the center of these icons.

The End of Lecture

Thank You