"Cyber Management of Risk: An Artificial Intelligence in Finance Research Issue"

Dr. Vipul Nimbalkar
Assistant Professor, Maharashtra Institute of Management, Kalamb, Pune, MH, India.
nimbalkarvipul@gmail.com

Keywords: Regulatory era, supervisory generation, block-chain, massive records analytics, artificial intelligence, peer-to-peer lending (p2p lending), robo advisory, cryptographers

Abstract:
Artificial intelligence (AI) solutions are becoming more popular among asset managers since they automate decision-making and provide efficiency. Increased use of AI and sophisticated data analytics, on the other hand, may modify how risks are appraised for compliance reasons, posing additional hazards to funds. Due to the fact that they speed up decision-making by automating processes and provide efficiency, artificial intelligence (AI) solutions are becoming more and more popular among asset managers. A rise in the use of AI and advanced data analytics, on the other hand, could change how risks are evaluated for compliance's sake and could also put funds in more danger.

Introduction:

The Financial Stability Board (2017b) defines Financial Technology as "technologically enabled economic innovations that ought to result in new commercial enterprise models, programs, tactics, or products with a related material effect on financial markets and institutions and the provision of monetary offerings."

While innovation in finance is not a brand new concept, the point of interest in technological improvements and its pace have increased extensively. Fintech solutions that make use of huge data analytics, artificial intelligence, and blockchain technology are currently being added at an unheard of rate. These new technologies are changing the character of the monetary industry, developing many opportunities that provide an all-inclusive right of entry to financial offerings. The blessings notwithstanding, FinTech answers leave the door open to many risks that can bog down consumer safety and economic stability. Relevant examples of such risks are underestimation of creditworthiness, marketplace danger, uncompliance, fraud detection, and cyber-assaults. Indeed, fintech chance management constitutes a primary factor of interest for regulatory authorities and requires studies and improvement of novel measurements.

Across the sector, there may be a robust need to enhance the competitiveness of the fintech region by introducing a risk management framework that may supervise fintech innovations without stifling their monetary capacity. On one hand, fintech firms want recommendations on how to discover opportunities for innovation procurements, for example in superior regulatory technology (RegTech) solutions; on the other hand, the supervisory bodies' capacity to screen progressive monetary products proposed by using fintechs is limited, and superior supervisory technology (SupTech) answers are required. An important step in remodelling compliance and supervision is to expand uniform and era-pushed risk control tools, which could reduce the limitations among fintechs and supervisors.

We believe that a focused global research activity, coordinated at the level of a particularly reputed open access medical journal with more than one key focus, such as Frontiers in Artificial Intelligence, can assist in closing the gap between technical and regulatory understanding, specifically offering risk management techniques not unusual to both facets. It should lead to the improvement of a regulatory framework that encourages innovations in massive information analytics, synthetic intelligence, and blockchain technology

that, at the same time, satisfies supervisory concerns to follow guidelines in a powerful and efficient manner and protects consumers and investors.

Regulations and related supervisory requirements are setting splendid cognizance on threat management practices, which in turn drives the want for deep, transparent, and auditable record analyses across companies. Technologies such as big data analytics, artificial intelligence, and blockchain ledgers may also help to better manage risk control requirements and associated costs.These technologies can, in particular, (i) reduce credit score scoring bias and improve fraud detection in peer-to-peer lending; (ii) measure and reveal systemic risk in peer-to-peer lending; (iii) measure and monitor market risk and volatility in economic markets; (iv) enhance client risk profile matching in robo-advisory; (v) identify illegal activities in crypto markets, such as fraudulent preliminary coin services and money laundering; and (vi) identify and p

In line with those developments, the strong point segment "Artificial Intelligence in Finance" of Frontiers in Artificial Intelligence objectives to create a global research forum that offers and publishes key research on shared chance management answers that automatize compliance of fintech organisations (RegTech) and, at the same time, will increase the performance of supervisory activities (SupTech). The Artificial Intelligence in Finance section also builds synergies with the broader tech-focused specialisations with its very own magazine and within Frontiers in Big Data and Frontiers in Blockchain.

Currently, supervisors and fintechs do not have a common framework to understand the opportunities and risks of stability, leading to distinct perceptions. The Artificial Intelligence in Finance conference aims to provide a discussion forum for solutions that effectively automate fintech compliance (RegTech) and supervisory tracking (SupTech).

The vision of synthetic intelligence in finance is to build a collaborative, modern environment from which both supervisory bodies and regulated institutions can gain. We intend to connect the two sides of the coin by organising a discussion board for research discussion with the goal of sharing risk-size solutions that meet the needs of each regulated establishment and regulators.

The discussion will draw on the contributions from three types of project participants:

Fintech and financial companies that know a lot about how business models are built around financial technologies;

Regulators and supervisors who know everything there is to know about the rules and risks of financial technologies.

research centers, which have a detailed understanding of the risk management models that can be applied to financial

Conceptually, the research content of the journal will be classified around three types of FinTech risk manage ment models, which will constitute the conceptual map of the journal The classification is based on the three main technologies that drive FinTech innovations:

Bigdata analytics, with its application to peer-to-peer lending, with the main risks arising from credit risk and systemic risk;

Artificial intelligence, with its application to financial robo-advice, with the main risks arising from market risk and compliance risk;

Blockchain technology, with its main application to crypto-assets, faces the main risks arising from fraud detection, money laundering risk, IT operational risk, and cyber risks. Artificial Intelligence in Finance will take into account research from all three of the aforementioned areas. Research in Big Data and Blockchain, but also in AI more generally, neatly connects to other Frontiers journals, such as Frontiers in Big Data and Frontiers in Blockchain. This infrastructure is meant to help researchers from different fields work together and share their knowledge, which is at the heart of FinTech innovation.

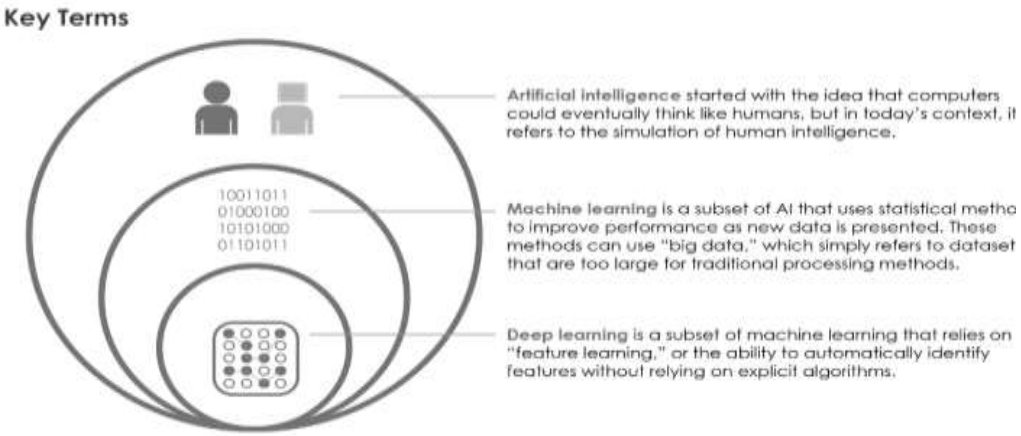
Internet utilisation is globally increasing at a rapid pace. The International Telecommunications Union (ITU) says that between 2010 and 2016, 1.5 billion extra people were given online. 1 Although net access fosters virtual, social, and monetary inclusion, the ever-expanding digitalization of existence increasingly affords opportunities for adversaries. Criminals can use those openings to thieve money or records, and extra-skilled hackers can use them to release attacks that are annoying or even negative.

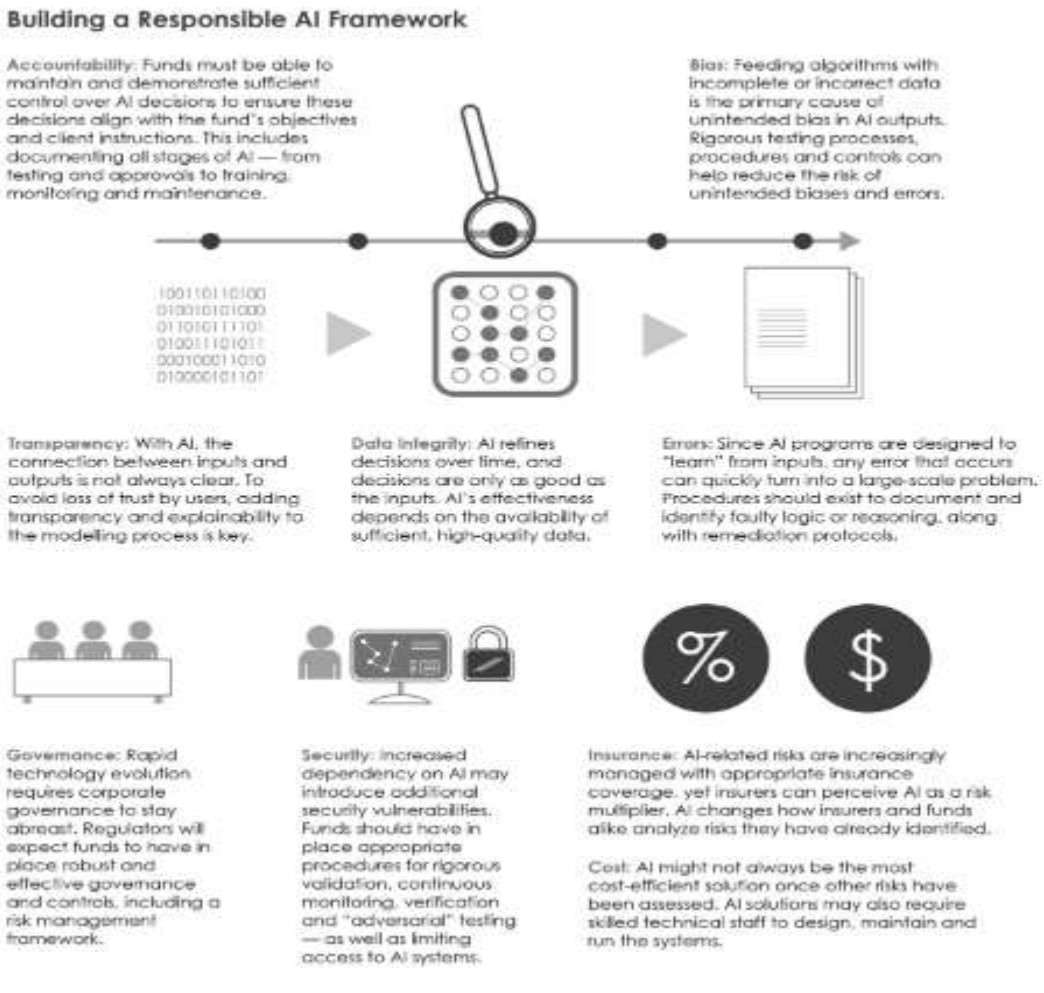
Assessing and coping with systemic cyber risk remains hard. So far, larger cyber attacks have not harmed the financial system.Some people, though, say the device hasn't been tested for a truly systemic event.2 As the hyperlink between cyberspace and the real economic system grows stronger and as extra interdependence, connectivity, and complexity are anticipated, the danger that an external shock will affect the monetary machine and turn into a systemic event rises. Three Furthermore, the inherent lack of transparency, particularly when it comes to operations and interdependencies, complicates the ex-ante assessment and quantification of systemic cyber threat.Data is scarce, and the most effective hardly ever is cyber chance measured in terms of monetary costs. Finally, modelling strategies for each idiosyncratic and systemic cyber danger are much less superior than they're for different insurable dangers, and it seems that extra work needs to be executed to position them on stable footing.

Although businesses have become increasingly aware of the need to prevent cyber breaches, the idea of systemic cyber danger remains largely abstract. Some view cyber threat as a simple operational risk, a cost of doing business in an interconnected world, and do not factor systemic cyber risk into their risk assessment.Others go with the flow Armageddon-fashion eventualities of a large cyber attack that might carry our modern monetary and social systems to their knees, though rarely in a manner that is useful for danger control. In order to help people better understand how cyber hazard would possibly show up, we present a systematisation of feasible cyber threat activities, which range from small, particular conditions to huge, systemic ones.

This paper aims to help give a boost to the knowledge and increase the awareness of systemic cyber risk among stakeholders within the economic system. First, we discuss the properties of cyber danger, including hazard aggregation and the exceptional dimensions of cyber threat. To make cyber threats much less abstract, we outline various scenarios, starting from company-precise operational risks to upstream infrastructure disruptions and outside shocks. Reading about potential outcomes can help policymakers gain a more comprehensive understanding of how cyber risk can occur. Second, we outline a framework for assessing systemic cyber hazard on a country-wide level, primarily based on cyber risk exposures, cybersecurity preparedness, and resilience to shocks.

ISSN: 2278-4632
Vol-11 Issue-01 March 2021





The power of AI and superior record analytics lies in its capability to enhance human decision-making. Although computers are more and more able to carry out obligations which have been traditionally related to human intelligence, there is no "independent" era and firms using AI techniques ought to put in force guidelines and strategies to appropriately take a look at them before and after deployment, and hold tracking to help ensure compliance. Here, the term "AI" is used at a high level and interchangeably with "gadget

studying" and "deep learning" in regard to technology that makes use of data, no matter its shape and quantity, to enhance performance. There are a few key issues for building a responsible AI framework.

Accountability is number one.

The more complex the program, the more difficult it is probably to hint at a right-away line from the programme to the result. However, for compliance purposes, funds ought to be able to keep and reveal enough control over AI decisions. This is vital under U.S. securities laws and guidelines to reveal that the fund is nicely executing patron commands. Additionally, under the General Data Protection Regulation (GDPR) within the EU, budget ought to be able to provide an explanation to clients about what records are being collected and exactly how their statistics are used, and this calls for explaining how any computerised solutions work. Finally, funds have to be able to hint at AI selections to make sure these choices align with the fund's very own targets. This means keeping a record of all levels of AI answers, including testing and approvals, training, tracking, and maintenance.

Bias

We are all familiar with the concept of "rubbish in, garbage out." Feeding algorithms with incomplete or incorrect data is the primary cause of faulty AI outputs. Risk managers across all industries are becoming increasingly concerned about the unintended bias of AI, which includes when statistical assets are incomplete or contain biassed statistics by chance. Using strict testing methods and controls in statistics, versions, and how people use AI can help to make sure that the data is accurate and reduce the risk of biases and mistakes that weren't meant to happen.

Transparency is number three.

AI is occasionally called a "black box" because the connection between inputs and outputs is not always clear and the internal workings are hard to understand. This poses the risk of a discrepancy between the program's code and the ensuing transactions. The "black field" hassle may additionally create the perception of a loss of transparency for asset managers and clients alike—e.g., if they don't recognise how AI comes up with its choices, they'll no longer trust them. And managers may not be capable of giving an explanation to regulators about how decisions are being made in complicated AI transactions that comprise hidden selection-making layers. A key part of any accountable AI framework is making the modelling system clear and easy to understand.

Data Integrity is number four.

As cited, AI solutions are programmed to treat statistics differently by refining the manner in which selections are made over time. The result of this method is that AI decisions are best when they are based on the most accurate information possible. The first outcomes are probably less first-class than subsequent ones. Second, if statistics continue to be constrained or inaccessible after the first decisions are made, the effects may not be enhanced on the expected charge. Simply put, AI's effectiveness relies upon the availability of sufficient, extremely good data.

Five Governance

The rapid tempo at which an era evolves requires corporate governance to stay informed and abreast of the era. To improve accountability, transparency, and satisfaction, it is important to make AI operating models and procedures that work well. Regulators will expect financial institutions to have strong and effective governance and controls in areas such as a risk control framework (RMF) to identify, determine, manipulate, and monitor risks associated with each piece of AI software. In this way, AI can also speed up the RMF lifecycle and make it more likely that food statements will be made.

6-Mistakes

With the rate at which AI evolves comes the potential for the magnification of errors. Since AI is designed to

"research" from inputs, any mistakes that happen early in the program's execution may quickly grow to be a large-scale hassle. Updates have to be accomplished as smoothly as possible whilst minimising any danger to upcoming, pending or finished transactions. Still, system faults or "insects" may occur when AI is upgraded, and there may be issues with the accessibility or use of legacy statistics. Funds need to have ways to record and find mistakes in logic or reasoning, as well as ways to fix them.

Security

Increased dependency on AI might also introduce extra safety vulnerabilities. Funds should have in this area suitable approaches for rigorous validation, non-stop monitoring, verification, and "adverse" check out. Limiting access to AI structures to the right people may also help keep records from being manipulated or used for bad purposes.

COST is number eight.

Although AI solutions have been adopted with the aid of funds that allow you to pressure price efficiencies, they might not always be the most value-efficient answer as soon as different risks have been assessed. This depends on the degree of personalization required by using the fund and the fee at which it's offered. AI solutions additionally require a professional technical group of workers to design, preserve, and run the structures. Additionally, what works in a single quarter might be one of a kind in another region. For instance, a recent survey conducted by the European Financial Management Association in partnership with Deloitte suggests that the banking and coverage sectors investigate the impact of AI in another way. For banks, AI is a good way to help their customers, but insurance companies are much less likely to use it. This could be because certain transactions require a different level of interaction. On the other hand, AI might be a better way to get back to work or operations in the insurance industry than in the banking industry.

Insurance is number nine.

Funds and different groups increasingly control the dangers posed by their AI solutions with suitable coverage insurance. Although new products are being created to fulfil increasing demand, insurers every so often understand AI as a hazard multiplier. In addition to increasing risks of its very own, AI changes how insurers and funds alike analyse risks they've already recognized.

AI ought to be used responsibly. Although there are an increasing number of funds thinking about AI solutions, they need to look cautiously at how AI affects current dangers and creates new criminal and compliance dangers for their organization. We assume regulators will closely screen AI programmes and stay competitive in bringing enforcement moves against companies for the misuse of AI. Building a responsible AI framework will help the price range keep up with prison and regulatory requirements while continuing to provide high levels of customer service in a way that is good for the environment.

Innovative Technologies

The European Commission (2018) argues that the term "big data" refers to "large amounts of different types of data produced with high velocity from a large number of various types of sources." Big data analytics is a group of technologies, models, and procedures for analysing large amounts of data to find insights, patterns of cause and effect, and ways to predict the future. It is similar to data science and its predecessor, data mining (see, for example, Giudici, 2003).

Over the years, academics and experts in computer science and statistics have developed advanced techniques to obtain insights from large datasets combining a variety of data types obtained from a variety of sources (see Brito, 2014). These models are able to utilise the ability of computers to perform complicated tasks by learning from experience. Following a definition offered by the Financial Stability Board (2017a), artificial intelligence is a broad term capturing "the application of computational tools to address tasks traditionally requiring human sophistication." It is important to mention that often the terms "AI" and "machine learning"

are used interchangeably. However, Artificial Intelligence is a broader term, of which machine learning represents a subcategory, the difference being that machine learning is a data-driven way to achieve AI, but not the only one. Similarly, big data analytics is broader than machine learning, as it includes statistical learning. For a further discussion on the difference between AI and machine learning, see also Kersting (2018).

Among the emerging technologies with significant potential to change the financial systems and industry from their core, blockchain has received a significant amount of attention over the last few years. A blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties (De Filippi and Hassan, 2016). Each transaction in the distributed database of records is verified by the participants through a majority consensus and, once confirmed, the transaction can never be altered or deleted (see, e.g., Tasca and Hayes, 2016). So, the blockchain has a record of every single transaction that has ever been made between people in a network (see, for example, Pontiveros et al., 2018).

Financial Applications, Many fintech applications rely on big data analytics and, in particular, those based on peer-to-peer (P2P) financial transactions, such as peer-to-peer lending, crowdfunding, and invoice trading. The concept of peer-to-peer captures the interaction between units, which eliminates the need for a central intermediary. In pa rticular, peer-to-peer lending enacts disintermediation by allowing borrowers and lenders to Borrowers and lenders communicate directly, using the platform as an information provider, which, among other things, assesses the credit risk of borrowers. From a regulatory perspective, a key point of interest is whether such credit risk measurements reflect the actual capacity of borrowers to repay their debt. Regulation must be technologically neutral and, therefore, credit risk compliance should be imposed on fintechs as it is on banks. At the same time, making it hard for alternative financial service providers to grow shouldn't be so hard (see Talonen et al., 2016).

Automated consultants, known as "robot advisors," are considered the main application of AI in financial services. The European Supervisory Authorities' joint report defines the phenomenon of automation in financial advice as "a procedure in which advice is provided to consumers without, or with very little human intervention and with providers relying on computer-based algorithms and/or decision trees." In practice, robot advisors build personalised portfolios for investors on the basis of algorithms that take into account investors' information such as age, risk tolerance and aversion, net income, and family status. It is against the law not to get this information, so robot advisors use online questionnaires to get it.

Crypto assets are the main application of blockchain technology and are considered one of the largest markets in the world which remains unregulated. Within the last decade, digital currencies, operating independently of central banks, have massively grown in popularity, price, and volatility. Bitcoin is the oldest, most popular, and widely used digital currency, and it offers a low-cost, decentralised transfer of value anywhere in the world, with the only constraint representing the availability of an internet connection. However, many other crypto assets are available, and new ones are continuously emerging through Initial Coin Offerings, in which a company sells digital tokens that can eventually be exchanged for goods, services, or other currencies. It is a new way to raise money that takes parts from both crowdfunding and traditional initial public offerings.

Risk Concerns and Management

Although there are many existing laws that are intended to serve in the interest of consumer and investor protection, lending to fintechs gives rise to "disintermediation," which requires the need for further protection of consumers and investors. In the case of peer-to-peer lending, there are two main causes of concern. First, P2P platforms have less information on their borrowers than classical banks do and are less able to deal with asymmetric information. Second, in most P2P lending platforms, the credit risk is not held by the platform but,

rather, by the investors. Both these causes lead to a high likelihood that the scoring system of P2P lenders may not adequately reflect the "correct" probability of default of a loan. A further issue associated with the nature of P2P platforms is that they give rise, by construction, to globally interconnected networks of transactions. This suggests that they cannot avoid the measurement of systemic risks arising from contagion mechanisms between borrowers.

In the context of P2P lending, a key risk to measure is the risk associated with the default of borrowers: credit risk. Statistical

Theory offers a great variety of supervised models for credit scoring and credit risk management and, in particular, logistic regression and generalised linear models (Bernè et al., 2006). When it comes to peer-to-peer lending, the same models can be used to solve similar classification problems, such as finding consumer fraud and money laundering.

A key issue that arises in employing generalised linear models for P2P classification problems is that the event to be predicted is multivariate. To solve this issue, Lauritzen (1996) introduced graphical models to model dependencies between random variables by means of a unifying and powerful concept of a mapping between probabilistic conditional independences, missing edges in a graphical representation, and suitable statistical model parametrisations. In parallel, Mantegna (1999) introduced hierarchical structures in financial markets based on correlation matrices, developing a powerful distance-based statistical model able to uncover similarity relationships among financial assets. Reviews by Giudici (2003) and Guegan and Hassani (2017) are provided.

In line with these developments, Giudici and Hadji-Misheva (2018) suggest modelling the credit risk of peer-to-peer lending, taking advantage of their natural interconnectedness, by means of correlation network models, a subset of graphical models that have been introduced in finance to measure systemic risk (see e.g., Arakelian and Dellaportas, 2012; Battiston et al., 2012; Billio et al., 2012; Diebold and Yilmaz, 2014; Vrost et al., 2015). This allows us to improve the accuracy of credit risk models and, furthermore, to measure a risk type that is particularly evident in P2P lending: systemic risk, recently applied to banks and sovereign default. Giudici and Hadji-Misheva (2018) show how to build a correlation network for P2P lending: by associating each borrower with a statistical unit, at each time point many variables can be observed for that unit; in the case of SME lending, balance sheet variables; in the case of consumer credit, transaction account variables. A correlation network (Mantegna, 1999) between borrowers can then be built on the basis of the observed values of one variable over time. Associating each borrower with a node in the network, each pair of nodes can be thought to be connected by an edge, whose weight is equal to the correlation coefficient between the two-time series of the chosen variable, each corresponding to a specific borrower. If we consider all pairs of borrowers, we will get a matrix of correlation weights, also known as an "adjacency matrix." Once the adjacency matrix is derived, summary network centrality measures suggest which are the most important units in the network or, in financial risk terms, which are the most contagious borrowers (Giudici and Spelta, 2016; Tomaev et al., 2016). Also, Giudici and Hadji-Misheva (2018) use real P2P lending data to show that network centrality measures can improve the accuracy of credit scoring algorithms when they are built into a generalised linear model specification.

Moving to asset management fintechs, note that the advantages associated with automatized advice may be offset by the greater risks that are brought on board, among which the risks of making unsuitable decisions (due to lack of information

or fewer chances), as well as mistakes and tool functional limitations.As is the case with big data analytics, there are several regulatory requirements that already exist and apply to automated advice. However, some risks are yet to be fully considered and measured. Among them, we believe the following are the most relevant:

(i) compliance risk is when expected and actual investment risk classes don't match up. (ii) market risk is the chance that bad movements and volatility in traditional or new (crypto) financial markets will cause investors to lose money they didn't expect to lose.

As for peer-to-peer lending, the increased risks connected with the use of robot advisory platforms can be mitigated by an appropriate analysis of the data they generate. In this way, robot advisors generate a lot of data automatically. This data can be used to improve the service and make it more personalized, but it can also be used to reduce compliance risk, especially the risk of a wrong profile match between "expected" and "actual" risk classes (see, for example, Valkanov, 2016).

Recent studies have shown that an accurate analysis of risk propensity questionnaires can allow robo-advisors to estimate the "expected" risk class of each investor. Data analysis algorithms can be implemented on the supply side by considering the returns of the available financial products to classify them into homogeneous "actual" risk classes. By connecting an investor's "expected" risk classification with its "actual" risk classification, it is possible to see if a robot advisor respects its risk profile (Kabainskas et al., 2017). This is one of the most important requirements of the MIFID regulation, and it becomes a verifiable requirement in the context of robot advisory, both from a formal and an operational point of view.

The literature on the measurement of expected risks in robot advisory is very limited. Scherer (2016) investigates, within a machine learning approach based on tree models, the key investor characteristics that can predict financial market participation; Alexy et al. (2016) is a related work. Similarly, the literature on the measurement of the actual risk of a given set of financial products is also very limited. (2005) and Tola et al. (2008), who employ clustering models to construct homogeneous asset classes, and Baitinger and Papenbrock (2017), who consider interconnectedness risk, are noticeable exceptions.

Giudici and Polinesi (2018) extend Scherer’s approach by deriving expected risk classes from the responses to the MIFID questionnaire and building correspondence analysis models on the observed contingency table that results from the cross-classification of the responses to the questionnaire. They also show how to employ feed-forward neural network models to estimate the risk class of a given investor’s portfolio on the basis of the observed returns. By comparing the expected risk class with the actual risk class for a sample of investors, it is possible to automatically figure out if the robot advisor fits the investor's risk profile.

We remark that specific concerns arise, from a market risk viewpoint, when crypto assets are combined with classical ones in investment activities. In particular, bitcoins and crytpoassets

have been linked to unusually high volatility and price sensitivity (Jabecki et al., 2015; Traian et al., 2017; IKOVIC SAA, 2017; Chen et al., 2018). Indeed, fluctuations are very common throughout the existence of crypto assets, which in turn raises the question of whether this behaviour is attributed to general market conditions or to idiosyncratic factors (as discussed by Makrichoriti and Moratis, 2016). To address these concerns, network models take the central stage, as could be expected. Nakamoto (2009) described Bitcoin as a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. Hence, in its essence, bitcoin represents a solution to the double-spending problem using a peer-to-peer network. This means that a correct way to measure the risks of this technology must take into account how network transactions connect to each other.

In this context, correlation network models can be employed to detect the main determinants of volatility (as in Papenbrock and Schwendner, 2015; Barucci and Marazzina, 2016). More recently, (Giudici and Abu-Hashish, 2018) used correlation VAR models to check if price contagion between different bitcoin exchange markets exists. They found that it does, especially for smaller exchanges.

Many innovative fintechs have payment deals with the application of blockchain technology. The main concerns about blockchain applications in finance relate to operational risks. Many international regulatory

authorities have raised significant concerns suggesting that, in most cases, small investors do not adequately understand the risks involved with initial coin offerings. Although many legitimate start-ups use ICOs for the purpose of raising money, many projects also exist that do not intend to deliver any value to the investors. The market has seen many such cases of fraudulent ICOs, which raises deep concerns for investor protection and overall financial stability. To identify the main determinants of fraudulent ICOs, text mining analytics methods that use network models to reduce their curse of dimensionality can be applied. According to the most recent statistics, 99% of all ICOs use Telegram as a channel for interacting with their communities. Typically, the Telegram groups are characterised by many members and detailed discussions about the value of the individual projects, as well as by the expectations of the community concerning the success of the ICO and the company. By collecting data from the Telegram ICOs (including the corresponding white papers) and discussions on Telegram chats relating to the value and prospects of the projects in question, we can build, train, and test supervised models to discriminate and classify ICOs by their probability of fraud, using, for example, the methods shown in Hochreiter (2015).

Another cause of concern is that crypto assets allow for a multi-billion dollar global market of anonymous transactions, which does not undergo any control. Hence, its emergence and growth can create considerable challenges for market integrity, particularly from money laundering activities. Money laundering is any action that hides the illegal source of money, makes it look like it came from a legal source, or makes it easier to move.

the subsequent reinvestment in the lawful economy. A recent study conducted by Foley et al. (2018) aims at quantifying and characterising the illegal trade facilitated by Bitcoin to provide a better understanding of the nature and scale of the problem facing this technology. The results from the study suggest that approximately one-quarter of Bitcoin users and half of Bitcoin transactions are associated with illegal activity. The authors found that around $72 billion of illegal activity per year involves Bitcoin, which is close to the scale of the US and European markets for illegal drugs. In the context of money laundering detection, network-based community detection models can be employed. They exploit the transactional network topology for the purpose of identifying communities of users and, in particular, identifying communities of money launderers using the transactions between them. More formally, the method that can be applied is a network cluster analysis algorithm that takes as inputs the set of users ("nodes" in network terminology) and the trades between users ("edges" or "links" in network terminology) (Foley et al., 2018). Foley et al. (2018) say that the algorithm gives users access to communities in a way that maximises the "modularity" of the communities, which is the number of links within a community and the number of links between communities.

An additional cause of concern is that cryptoassets are fully digital and, therefore, may lead to higher IT operational risks, such as errors in the functioning of the algorithms and hacking and manipulation of the algorithms (cyber attacks), to name only a few. While the literature on the quantitative measurement of operational risk constitutes a reasonably large body (see, for example, Cruz, 2002), that on cyber risk measurement is very limited. Cyber risks are unique, rare, and rarely happen again. Because of this, an ordinal-based scorecard approach, similar to that used in self-assessment-based operational risk management (see, for example, Giudici, 2015), reputation measurement (see, for example, Cerchiello and Giudici, 2015), or portfolio analysis using stochastic dominance (Post and Pot, 2016), is a good way to measure them.

In this way, a cyber risk measure can be used to rank cyber risks and prioritise interventions, preventing failures and reducing ex ante the impact of risks. This is on the basis of ordinal random variables that represent the levels of frequency and severity of different cyber risk events in different business areas. A similar approach can be consistently undertaken to measure operational risks deriving from the use of robo-advisors, caused by their malfunctioning rather than by cyber-attacks. Note also that an ordinal-based

measurement of operational risks and cyber risks. They are easy to change for scenario testing, which is one of the best ways for the financial industry to protect itself from them, especially when they are done across the industry.

CONCLUSIONS

In this paper, we have focused on the emerging subject matter of the economic era. We have first diagnosed the main technological drivers of exchange: big data analytics, synthetic intelligence, and blockchain generation; and their predominant monetary programs: in banking (peer-to-peer lending); in asset control (robotic advisory); and in price systems (crypto belongings).

Our vision is to encourage the improvement and growth of financial technologies, making them sustainable and minimising their possible terrible influences on consumers and traders. This goal can be reached by coming up with better ways to control threats, whose compliance requirements can be made easier by the technology itself.

To achieve this intention, the paper has offered the main hazard worries that arise with the development of the most critical economic technologies and has cautioned study directions in threat size models, suitable to manage and mitigate the worried dangers.

Strict collaboration and open discussion among lecturers, fintech specialists, and regulators can assist us on this path, growing fintech control fashions that, while limiting the negative effects of disrupting technologies, encourage their improvement. The journal Frontiers in Artificial Intelligence, with its study area of expertise in Artificial Intelligence in Finance, may be key in fostering collaborations and stimulating research debates on dangerous management practices. The goal is to share the beneficial practises for reducing fintech risks with the network. practises that might be employed to offer "computerized" danger management tools for both RegTech and SupTech purposes, as a result, making fintech improvements aggressive and sustainable.

REFERENCES

Alexy, M., Georgantzis, N., Kacer, M., and Péliová, J. (2016). Risk attitude elicitation methods: do they tell similar stories? Ekonomick-Casopis 64, 847–877.

Arakelian, V., and Dellaportas, P. (2012) Contagion determination via copula and volatility threshold models. doi: 10.1080/14697680903410023

Baitinger, E., and Papenbrock, J. (2017). Interconnectedness risk and active portfolio management. J. Invest. S trate. 6, 63–90. doi: 10.2139/ssrn. 290983

Barucci, E., and Marazzina, D. (2016) Asset management, high water mark and flow of funds. Operat. Res. Lett. 44, 607–611. doi: 10.1016/j.orl.2016.07.002 Battiston, S., Delli Gatti, D., Gallegati, M., Greenwald, B., and Stiglitz, J. E. (2012) .

Liaisons dangereuses: Increasing connectivity, risk sharing, and systemic risk. Econ.Dyn. Control 36, 1121–1141. doi: 10.1016/j.jedc.2012.04.001

Bernè, F., Ciprian, M., Fanni, N., Marassi, D., and Pediroda, V. (2006). Multi criteria credit rating (MCCR): a credit rating assignment process for Italian enterprises according to BASEL II. J. Finan. Dec. Making 2, 1–26.

Billio, M., Getmansky, M., Lo, A. and Pellizzon, L. (2012) Econometric measures of systemic risk in the finance and insurance sector. J. Finan. Econ. 104, 535–559. doi: 10.1016/j.jfineco.2011. 12.010

Brito, P. (2014) Symbolic data analysis: another look at the interaction of data mining and statistics. WIREs D ata Mining Knowl. Disc. 4, 281–295. doi: 10.1002/widm.1133

Cerchiello, P., and Giudici, P. (2015). How to measure the quality of financial tweets. Qual. Quant. 50, 1–19. doi: 10.1007/s11135-015-0229-6
Chen, C. Y. H., Härdle, W. K., Ai, J. H. and Wang, W. (2018) Pricing cryptocurrency options: the case of CR IX and Bitcoin. SFB DP. doi: 10.2139/ssrn.3159130
Cruz, M. G. (2002). Modelling, Measuring and Hedging Operational Risk.
New York, NY: Wiley Finance.
De Filippi, P., and Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. Chicago, IL: First Monday. doi: 10.5210/fm.v21i 12.7113
Diebold, F., and Yilmaz, K. (2014). On the network topology of variance decompositions: measuring the connectedness of financial firms. J. Econ. 182, 119–134. doi: 10.1016/j.jeconom.2014.04.012
European Commission (2018). Fintech Action Plan: For a More Competitive and Innovative European Financial Sector. European Commission.
Financial Stability Board (2017a). Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications. Financial Stability Board.
Financial Stability Board (2017b). Financial Stability Implications for Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention. Financial Stability, Board.
Foley, S., Karlsen, J. R., and Putnins, T. J. (2018). Sex, Drugs and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies. London: Working Paper.
Giudici, P. (2003). Applied Data Mining. London: Wiley.
Giudici, P. (2015). Scorecard models for operational management. Int. J. Data Sci.
1, 96–101. doi: 10.1504/IJDS.2015.069055
Giudici, P., and Abu-Hashish (2018). What determines bitcoin exchange prices: a network VAR approach. Finance Res. Lett. doi: 10.1016/j.frl.2018.05.013. [Epub ahead of print].
Giudici, P., and Hadji-Misheva, B. (2018). Network Scoring Models for P2P Lending.
London: Submitted Paper.
Giudici, P., and Polinesi, G. (2018). Risk classification methods in Robot Advisory Platform. Pavia: Submitted Technical Paper.
Giudici, P., and Spelta, A. (2016). Graphical network models for international finan cial flows. J. Bus. Econ. Stat. 34, 126–138. doi: 10.1080/07350015.2015.1017643
Guegan, D., and Hassani, B. (2017) Regulatory learning: how to supervise machine learning models? An application to credit scoring. J. Finance Data Sci. 4, 157–171. doi: 10.1016/j.jfds.2018.04.001
Hochreiter, R. (2015). Computing trading strategies based on financial sentiment data using evolutionary optimization. Adv. Intell. Syst. Comp. 378, 181–191. doi: 10.1007/978-3-319-19824-8_15
Jab 흕 ecki, J., Kokoszczynski, R., Sakowski P., Slepaczuk, R., and Wójcik, P. (2015). Volatility as an Asset C lass, Obvious Benefits and Hidden Risks. Frankfurt: Peter Lang.
Kabašinskas, A., Šutiene, K., Kopa, M., and Valakevic 뇁 us, E. (2017) The risk–return profile of Lithuanian private pension funds. Econ. Res. Ekonomska Istra 탐 ivanja 30, 1611–1630. doi: 10.108 0/1331677X.2017.1383169
Kersting, K. (2018). Machine learning and artificial intelligence: two fellow travelers on the quest for intelligent behavior in machines. Front. Big Data 1:6. doi: 10.3389/fdata.2018.00006
Lauritzen (1996). Graphical Models. Oxford: Wiley.
Makrichoriti, P., and Moratis, G. (2016). BitCoin's Roller Coaster: Systemic Risk and Market Sentiment. Athe

ns: Working Paper.
Mantegna (1999). The European Physical Journal B: Condensed Matter and Complex Systems, Vol. 11. Berlin , 193–197.
Nakamoto, S. (2009). Bitcoin: A Peer-to
Peer Electronic Cash System. White Paper. Papenbrock, J., and Schwendner, P. (2015). Handling Risk On/Ris k Off dynamics with correlation regimes and correlation networks. Finan. Mark. Portf. Manage.
29, 125–147. doi: 10.1007/s11408-015-0248-2
Pontiveros, B. B. F., Norvill, R., and State, R. (2018). Monitoring the
Transaction Selection Policy of Bitcoin Mining Pools. To appear in NOMS 2018 - IEEE/IFIP Man2Block
Post, T., and Potì, V. (2016) Portfolio analysis using stochastic dominance, relative entropy, and empirical likel ihood. Manage. Sci. 63, 153–165. doi: 10.1287/mnsc.2015.2325
Scherer, M. U. (2016). Regulating artificial intelligence systems: risks, challenges, competencies, and strategi es. Harvard J. Law Technol. 29, 1–48. doi: 10.2139/ssrn.2609777
Talonen, A., Kulmala, J., and Ruuskanen, O. P. (2016). "Co-operative platforms: harnessing the full potential of crowdfunding," in European Conference on Innovation and Entrepre neurship (Jyväskylä: Academic Conferences International Limited), 810.
Tasca, P., and Hayes, P. (2016). "Blockchain and crypto currencies," in The Fintech Book (London: Wiley). Av ailable online at: http://thefintechbook.com/
Tola, V., Lillo, F., Gallegati, M., and Mantegna, R. N. (2008). Cluster analysis for portfolio optimization. J. Ec on. Dyn. Control 32, 235–258. doi: 10.1016/j.jedc.2007.01.034
Tomašev, N., Buza, K., and Mladenic, D. (2016) Correcting the hub occurrence prediction bias in many dimensions. Comp. Sci. Inform. Syst. 13, 1–21. doi: 10.2298/CSIS140929 039T
Traian, P.D., Emese, L., and Alfonso, D. (2017). Information entropy and measures of market risk. Entropy 19 , 226–245. doi: 10.3390/e19050226
Tumminello, M., Aste, T., Di Matteo, T., and Mantegna, R. N. (2005). A tool for filtering information in complex systems. Proc. Natl. Acad. Sci. U.S.A. 102, 10421–10426. doi: 10.1073/pnas.0500298102
Valkanov, N. (2016). Financial Science – Between Dogma and Reality. Varna: Science and Economics, 400–445.
Výrost, T., Lyócsa, Š., and Baumöhl, E. (2015). Granger causality stock market networks: temporal proximity and preferential attachment. Phys. A Stat. Mech. Appl. 427, 262–276. doi: 10.1016/j.physa.2015.02.017
탐 ikovic´ Saša (2017). "Measuring financial risk in energy markets," in Applied Quantitative Finance 3rd Edn, eds C. Chen, W. K. Härdle, and L. Overbeck (Berlin; Heidelberg: Springer), 295–308.

