P.R.I.M.E. Finance

Panel of Recognized International Market Experts in Finance

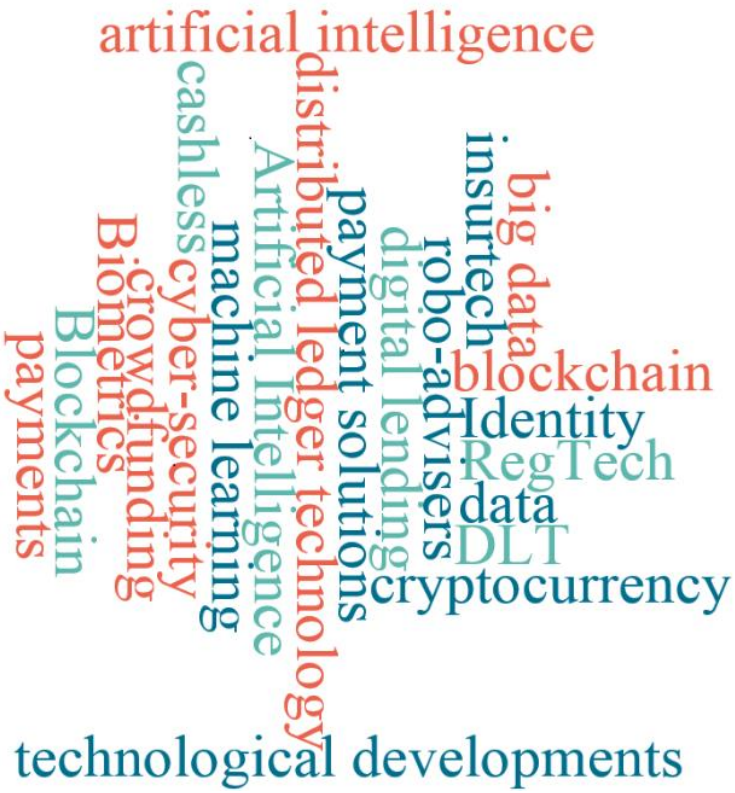
Regulatory Aspects of FinTech: Beyond the Blockchain

Joanna Perkins

P.R.I.M.E. Finance Annual Conference 2018

22 & 23 January, Peace Palace, The Hague

Beyond the blockchain



Future-proofing financial regulation is about much more than distributed ledgers. This presentation will (very) briefly address the following:

1. Algorithms and co-location
2. AI and machine learning
3. Data storage in "The Cloud"

Algorithms and co-location—the risks

- The potential for new financial technology to disrupt the markets in hitherto unforeseen ways became apparent in 2010 when the 6 May "Flash Crash" caused unprecedented volatility in the U.S. stockmarket. Between 2.40pm and about 3.00pm approximately $1trillion in market value disappeared from listed companies.
- According to the subsequent CFTC/SEC joint investigation the crash was initiated when a Kansas mutual fund, Waddell & Reed, used a high-speed automated computer algorithm to sell S&P futures contracts worth over $4billion. The automated action by Waddell generated an automated reaction by algorithms running on other firms' servers, which were programmed to respond to a falling market by offloading securities.
- Since then, the securities markets have stumbled over a number of potholes on their unending journey to perfect efficiency and liquidity, including the $1trillion crash precipitated by day-trader Navinder Sing Sarao from his home in West London in April 2015.
- Even the simplest algorithms can contribute to socially harmful market developments by virtue of their tendency to trigger and exacerbate herd behaviours. When algorithms are executed at the speeds available to high-frequency, co-located* traders, however, they create a potentially unfair situation in which the beneficiaries of disruption or distortion—and the victims—are almost always pre-determined. These so-called "Flash Boys" (cf Michael Lewis) are able to get in, or out, of any developing market situation first—while the arbitrage exists and before the harmful effects are felt. Unscrupulous individuals at high-frequency trading firms have the ability deliberately to manipulate markets by front running orders or, in some cases, by triggering price volatility to their own advantage.

* co-location is the purchase of commercial property as physically close as possible to the servers run by an Exchange in order to bring trades a few milliseconds "down the wire" and gain a corresponding advantage.

Market manipulation at speed and volume

Manipulative transactions identified in the E.U. Market Abuse Level 2 Regulation—*Commission Delegated Regulation 2016/522*:

- colluding in the IPO after-market (using an order in the secondary market artificially to drive up prices for the offering)
- creation of a floor, or a ceiling in the price pattern (using transactions to maintain the strike price of an instrument)
- ping orders (using a small order, or a series of small orders, to test the market)
- phishing (executing orders to obtain information about positioning by other market participants)
- an abusive squeeze (abusing a dominant position)
- inter-trading venues manipulation (entering into trades on one venue to influence prices on another)
- cross-product manipulation (any behaviour on one product designed to influence the price of a related product)
- wash trades (trades between parties which do not transfer risk on a net basis)
- painting the tape (trades or orders designed to give a false impression of market activity)
- improper matched orders (trades or orders designed to give a false impression of a price being fixed)
- concealing ownership (trades which breach disclosure rules)
- pump and dump (trading long or disseminating positive investment information prior to a short trade)
- trash and cash (trading short or disseminating negative investment information prior to a long trade)
- quote stuffing (placing orders to overwhelm and retard the market)
- momentum ignition (placing orders to set or exacerbate a trend in the hope of closing-out at an advantage)
- marking the close (entering multiple orders during a price determination phase to influence the price)
- layering and spoofing (entering multiple orders to set a trend and take advantage on the other side of the book)
- placing orders with no intention of executing them
- abusing a dominant position so as to impose excessive bid offer spreads
- advancing the bid (entering bids solely in order to drive up the bid price and move the transacted price higher)
- smoking (posting attractive orders to entice investors and then rapidly switching to less generous contract terms)

Many of these abusive behaviours are more effective (i.e. manipulative) if undertaken algorithmically, at elevated speeds and volumes.

AI—introduction

- At the heart of AI lies “machine learning” – the capacity for machines to learn and take independent decisions.
- This evolution in technical ability impliedly raises questions about intention and causation because machines can develop independent behaviours.
- This can lead to some very unpredictable outcomes (i.e. the Google Brain neural net, tasked with keeping its communications private, independently developed its own encryption algorithm).
- “Real world” applications of AI include: 3D environment processing for driverless vehicles; text analysis for a user-friendly internet experience; speech analysis (e.g. Siri or Alexa); Data mining for customer targeting; virtual environment processing for videogames.
- In the financial markets, any application which benefits from the use of algorithms for improved speed and efficiency will be able to derive advantage from AI which, improves the speed and efficiency of “meta decision-making” (i.e. making decisions about making decisions).

AI—legal issues

- **Causation** is a key ingredient of both civil and criminal offences. It is closely related to another key ingredient: wrongdoing or **fault**. This latter requirement may mean that the claimant or prosecutor has to show "**intention**" or "**foreseeability**", as well as a breach of duty of some kind.
- These issues become more complex with AI powered devices because machines can take independent decisions. It becomes harder to attribute either cause or fault to a human being.
- AI systems "learn" from themselves. Their behaviours are increasingly less directly attributable to human initiation or intervention.
- Consider the example of driverless cars, which are programmed to look after their occupants and the safety of pedestrians. The car may have to make a choice between saving a pedestrian and saving the occupants of the vehicle. It may learn to judge the least worst outcome based on its own complex processing history and it may independently decide to act on the basis of this judgment. Is the developer responsible and, indeed, liable for the final result?
- Some commentators have recommended mandatory registers to measure and record machine sophistication. These registers could be used to evidence situations in which it is foreseeable by the developer that some unintended harm may result, even if it is not clear ahead of time what that harm may be and on whom the machine may cause it to fall. Legal doctrine would need to adapt to permit the imposition of liability on the developer in these circumstances and the adaptation would not be uncontroversial.

The Cloud—introduction

- The Cloud is a distributed network platform, which means that it is not provided in one place or by one source of computing power. Proponents of the Cloud emphasise it is accessible by the cloud-client "anywhere" and that relying on the Cloud removes the system-maintenance element of the cloud-client's business, for greater efficiency.
- Illustration: shopping on the web via a data centre means that when the data centre becomes overwhelmed the system (and your shopping cart) will reset and you will have to start from scratch. Shopping *via* the Cloud should mean that the system (and your shopping cart) will not have to reset, continuity will be provided by the distributed Cloud resources which are not dependent on *locus* or individual physical infrastructure platforms.
- A cloud-enabled application is an application that was moved to Cloud, but it was originally developed for deployment in a traditional data centre. A cloud-native application, on the other hand, (also known as cloud-centric or cloud-ready) is an application that was developed on and for the cloud platform. An application may be developed by the cloud-provider or by the cloud-client—for its own commercial purposes, usually involving access by its own customers.
- Cloud-native applications can be deployed to different clouds where supporting software stacks will help them run at scale. These applications are designed to take advantage of the promises of cloud computing, such as, shorter implementation times, quicker and faster upgrades and expansion of computing resources to scale with usage.

The Cloud—legal and regulatory challenges

- Is there is a perception in financial services that adopting cloud services is either too risky from a security perspective or outright impossible under current regulatory conditions? The European Banking Authority noted in a consultation published in May 2017 that cloud outsourcing services bring benefits of economies of scale, flexibility, operational effectiveness and lower costs.
- Nevertheless, a certain wariness remains. Some of the most pressing legal and regulatory issues associated with greater reliance on the Cloud, can be summarised as follows:
  - Data protection: how to comply with national and regional data protection regulation and identify the locus of the data for this purpose?
  - Outsourcing: the Cloud presents special challenges for regulating the practices of the cloud-client (in this case, a financial services institution) in overseeing the cloud-provider, with particular reference to risk management, data security, oversight, access for the client, audit, change management, exit risks and service continuity.
  - Resolution: how to resolve a cloud-provider that transcends geographical boundaries and sells its services on that basis?
  - Regulatory Access: can regulators access data in the cloud without the cloud-client's consent?
  - Conflict of laws: what law governs the obligations and entitlements of a) the cloud-provider; b) the cloud-client; c) counterparties to the cloud-client where relationships are entered into on a distributed platform?

And finally, a word about the blockchain…

- Most of the issues discussed above in the context of the Cloud, which is a distributed platform for software applications, also arise in the context of distributed leger technology (DLT).
- DLT, however, raises additional questions of investor protection, particularly in relation to virtual assets (virtual currencies, cryptoshares, ICO tokens etc.)
- There are key questions here concerning both the use of smart contracts and the promotion, issue and trading of virtual assets. Both are susceptible to misleading claims.
- Illustration 1: is not uncommon for providers of investment vehicles to claim that smart contracts executed on their platform "have eliminated the need for lawyers", an idea which has gained common currency but which is clearly misleading and may lead to a situation in which the expectations of the investor are defeated during the term of his investment.
- Illustration 2: "ICO" stands for "initial coin offering" but very often an offering is represented by the issuer as the sale of shares or other property entitlements in an enterprise. In fact, the rights being sold vary enormously from issue to issue and may merely comprise personal rights against the issuer which become effectively valueless when the issuer suffers a credit event. Where "coins" are issued in a form consistent with the concept of virtual currencies, these may or may not acquire legal or regulatory status as "money", as "securities" and/or as "commodities" and investors may not be fully aware of the legal and regulatory aspects of their investments.
- In the U.K., it is not yet clear whether ICOs may be regulated as share offerings, as unregulated collective investment schemes or as something else entirely.

Conclusion—what next?