Regulatory Aspects of FinTech: Beyond the Blockchain

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

Tuesday 23 January 2018

Joanna Perkins, Chief Executive, FMLC

Slide 1—Beyond the blockchain

My fellow panellists have provided a fascinating account of DLT applications. Since the vast majority of DLT applications are also blockchain applications (that is, systems in which unrelated transactions are bundled into blocks, which are linked together using hashes and circulated to all participating nodes), I have chosen "Beyond the blockchain" as the title for my remarks today.

As we have heard DLT has the potential to be an exciting and disruptive influence on the market for financial services but it is far from comprising the whole domain of what is elliptically called "FinTech", it may not even be the most powerful disruptor. What I am going to do today is give a very brief introduction to some other technologies with the potential to change the conduct of financial business and influence what happens in the wholesale financial markets.

I am going to offer remarks on:

1. Algorithms and co-location, neither of which is a very "new" technology any more but which, in combination, are presenting regulatory challenges which we have scarcely begun to address.

2. AI and machine learning, technologies which posit machines as independent self-determining entities and which often appear to the Luddites among us to have been lifted straight from the pages of a science fiction novel.

3. The Cloud—a strange place which is so far away that no one has ever seen it but so close at hand that we can always get there instantly. It is to this strange place that, increasingly, all our personal data is consigned, with or without our consent.

Slide 2—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. stock market. 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,[1] 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" (*per* author 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. If there are any unscrupulous individuals at high-frequency trading firms, they have the ability deliberately to manipulate markets by front running orders or, in some cases, by triggering price volatility to their own advantage.

Slide 3—Market manipulation at speed and volume

The E.U. has in recent years attempted to get a grip on the ability of new technologies to facilitate market manipulation in part by revising the 2003 Market Abuse Directive. ("**MAD**"). The new market abuse regime came into force in the E.U. on 3 July 2016 and is chiefly constituted by a new regulation on market abuse (known as **"MAR"**).

Market manipulation is prohibited in Article 15 of MAR defined in Article 12. A list of indicators of manipulative behaviour appended in an annex to the Regulation reflect the new regulatory focus on high frequency trading. One of the indicators of market manipulation is "the extent to which orders to trade given or transactions undertaken are concentrated within a short time frame".

---

[1] Co-location is the purchase of commercial property as physically close as possible to the servers run by an Exchange in order to bring orders and trades a few milliseconds "up the wire" and gain a corresponding advantage.

The definition is given further specificity by a Commission Delegated Regulation which lists specific instances of abusive practices. Those are shown here on the slide. Many of these transactions are more effective (i.e. more manipulative) if undertaken algorithmically at speed and volume.

For example, spoofing is the activity of placing fake orders at prices outside the current price range to create the impression of a volatile market and provoke trading in the preferred direction by other participants in the market. This technique, which was adopted by Navinder Sarao as part of his 2015 market sting, is more effective the more orders one can muster and most effective when undertaken algorithmically and at high-frequency, so that the spoofer gains a time advantage in which he can cancel the trades without any real financial exposure.

Other regulatory measures in European law which reflect a response to incidents like the Flash Crash of 2010 include the provisions of MiFID II on high-frequency trading, which require the testing of algorithms by participants, as well as increasingly sophisticated risk management regulation by national supervisors.

Slide 5—AI—introduction

At the heart of AI lies "machine learning"—the capacity for machines to learn and take independent decisions. Methodologically, we should understand this as the development of technology to make decisions about decision-making or, if you prefer, it is the introduction of "meta-decision-making". Machines can decide for themselves which data points are relevant, how to weigh input data and which lessons to extrapolate.

Thus, not only will a machine now make a decision when the traffic light should be red and when it should be green but it can make a decision about how that decision should be made. Rather than simply processing contemporary environmental data to generate an efficient solution in terms of accident prevention and traffic flow, the machine could "learn" to identify new features in the environment which it has not yet been told are relevant. In theory, it could come to recognise, for example, that young pedestrians—which are identifiable from their demeanour, appearance or accessories—cross the road faster than older ones. The machine may make this cognitive leap independently.

This can lead to some very unpredictable outcomes. For example, 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.

This evolution in technical ability impliedly raises questions about intention and causation.

Slide 6—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 are 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.

Although there is more emphasis on liability for negative outcomes—rather than on fault—under regulatory law, concepts which presuppose human agency can be identified here, too. For example, where a firm has engaged in a manipulative transaction under MAD, the individuals involved will only be penalised for market manipulation if they have "*participated in the decision*" to enter into the transaction. There is a very real question as to whether it can be said that a human being has participated in the decisions taken by machines running smart algorithms.

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.

Slide 7—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 that 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.

If it helps, you can think of it this way: shopping on the web via a data centre used to mean that when the data centre became overwhelmed the system (and your shopping cart) would reset and you would 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.

Slide 8—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, certain wariness remains. Some of the most pressing legal and regulatory issues associated with greater reliance on the Cloud are set out on the slide and include data protection; risk management in an outsourcing context; resolution and insolvency; access by the client's supervisors and conflict of laws issues.

At the heart of all these issue is the same problem: how to adapt regulation and supervisory practices which are delimited by geographical location to a service for which the chief characteristics are that it is distributed across a network and can only be accessed through virtual platforms.

Slide 9—And finally, a word about the blockchain

Whatever the answers may be, the questions are very similar to those being asked with respect to blockchain applications. The technical aspects of these applications and their potential to change the way the financial markets do business has been addressed by my fellow panellists but I have been asked to say a very (brief) word about some of the regulatory implications.

The broad point to make, I think, is that the regulatory and legal issues facing DLT applications are not necessarily the same as the issues facing virtual assets that are often transacted on the blockchain, including anonymised currencies like Bitcoin, or the increasingly popular sale of such rights by means of an "Initial Coin Offering" ("ICO") also and, more accurately, known as an "Initial Token Offering" ("ITO").

The issues for DLT systems are likely to be the same as those as are currently being addressed for the Cloud: from the highly theoretical (what law governs the proprietary effects of transactions?) to the eminently practical (can a regulator access the system and obtain data without informing the system participants?).

The issues for virtual currencies, on the other hand, are largely about their place in existing regulation of secondary financial markets: including money laundering regulation, commodities markets regulation and securities regulation. It appears to be the case for now, that a single virtual currency can for different regulatory purposes be classified as money and commodities and securities, all at the same time. For example, the CFTC has concluded that Bitcoin is, for the purposes of its regulatory jurisdiction, a

commodity.[2] A US court has ruled that Bitcoin-denominated units or shares are securities.[3] And , while a Florida court declined to categorise Bitcoin as money for the purposes of anti-money laundering legislation in 2016, a NY court subsequently reached a decision that it would qualify as money.[4]

With ICOs, in contrast, the regulator's attention moves away from questions about infrastructure and assets to questions about the scheme by which tokens are promoted and sold. Should that scheme be left with minimal oversight in the space reserved for unregulated collective investment schemes or should it be regulated in the manner of an initial public offering? In some countries, as we have seen, the answer is not to regulate but to suspend issuers' activities entirely.

Slide 11—Conclusion—what next?

Is there a role in the fast-evolving world of Fintech for P.R.I.M.E Finance?

Suddenly the term "future proofing" is in vogue in the context of law and regulation for the financial markets as market participants and regulators alike begin to absorb the enormity of the changes coming our way with this the Fourth Industrial Revolution.

P.R.I.M.E Finance can make a contribution to this thinking about future proofing our world.

But the points I've highlighted today also show us areas where it can play a more practical role in resolving the disputes which will necessarily emerge as questions like the locus of proprietary entitlements to assets on a distributed platform or a distributed network become contentious and as those who have suffered financial loss look for *real* persons to blame when the proximate cause is the act or omission of a *mechanical* one.

---

2 See Order of the CFTC (Docket No. 15-29) in the Matter of Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan. See also complaint in the Southern District of New York, filed 21 September 2017, against Gelfman Blueprint, Inc for operating a fraudulent commodities scheme in respect of Bitcoin spot transactions.

3 *SEC v Shavers (No-4-13-CV-416) Eastern District of Texas, September 18, 2014.*

4 *Florida v Espinoza* (Case No. F14-2923), concerning unlicensed money transmission; and *US v Murgio* (Case No. 15-cr-00769).