2020 IOSCO Stakeholder Meeting, 28 February 2020

Disrupting Markets, Disrupting Money, Disrupting Finance

Remarks by Mark Yallop, FMSB Chair

Thank you for the invitation to speak here today.

I must start with a note of caution about my qualifications to speak on technology, since it is exactly 20 years since I was appointed CIO for the Deutsche Bank Group and even longer than that since I was involved in the earliest development of DB's electronic trading platform, Autobahn. But since that platform catapulted DB to the top of the FX and government bond trading league tables, and as far as I know is still used today, we must have got something right.

I will in any event talk about trends that I believe will shape the future, rather than about ancient history; and from the perspective of the FMSB rather than any single firm or regulator.

We are here to talk about disruption, and specifically the technology that is disrupting markets, disrupting money and even, potentially, the entire financial system: three highly topical issues that profoundly affect both the public and private sectors.

For those of you who don't know FMSB, the FICC Markets Standards Board was established in 2016 to address behavioural problems in wholesale markets. We are a private sector, global, body whose goal is to raise standards of behaviour and conduct in markets, making them fairer and more effective for users across the world.

The UK authorities who called for FMSB to be created, and have been strong advocates for our work since then, recognized that wholesale markets pose some special challenges for regulators: the global scope; the information asymmetry between private sector and regulators; and the pace of innovation and product development, among other factors, make it very difficult for regulation to stay ahead of competitive private sector firms.

Instead it is much more powerful to engage the private sector in the process and encourage it take responsibility for identifying and fixing problems in market behaviour and structure that damage the functioning and reputation of markets and their businesses. Indeed, they saw that rebuilding trust in wholesale markets required the private sector to be seen to take a lead in reinforcing orderly, fair and effective markets.

With 50 firms as members today, 14 recommendations on market behaviour published over the past three years and five more in preparation, this is what FMSB has been doing.

Disruptive technology: artificial intelligence in markets

FICC markets are undergoing transformational change, driven partly by the new regulation that emerged at the prompting of the G20 after the financial crisis; but also - and equally important - as a result of new technology and data science that has evolved in the past decade.

In the financial markets arena, electronic trading has been at the heart of this transformation. So called algorithmic trading has been a feature of equity markets for well over two decades and is now widespread also in liquid government bond markets, repo and FX.

The traditional form of algorithmic trading which dominates activity today uses static or deterministic logic to enable a computer to decide when and how to trade. A computer's trading rules are devised by human programmers and are fixed, or change only in ways specified by those programmers: every time a trade is executed by the computer it is made using the same logic, at least until a human programmer decides to change part of the logic.

Algorithmic trading of this sort has already been immensely disruptive of the trading landscape: changing the nature of jobs in the industry (as humans become less relevant in sales and trading roles), market structure (as firms with successful technology have found it possible to capture and maintain much higher market shares), and the nature of liquidity (as new participants with less capital have taken over the role of traditional market makers).

It has brought very significant benefits for market participants - in terms of lower costs, greater certainty of execution, more transparent prices and clearer auditability of market activity. And it has created some new challenges: latency arbitrage, flash events and on market manipulation to name just three.

FMSB has been working actively in this domain for a couple of years and has already published a draft Standard for the governance of algorithmic trading and has a further piece of work on how electronic trading venues should operate about to be published.

The already published Standard sets out our views on how governance structures should operate and the need for clear management responsibilities to be allocated; the kind of minimum operating standards that should be established; the demand for algo inventories and good pre- and post-trade controls; for written policies and effective controls over software development and change control; and the requirement for ongoing oversight of algorithms and appropriate record keeping and staff training. It, and all other FMSB Standards and publications are available on our website, fmsb.com, for those of you who are interested.

This form of algorithmic trading is an example of a primitive form of artificial intelligence: trading

is ‘automatic’ but essentially the computer just performs exactly the tasks previously carried out by humans, precisely as it has been instructed.

From the 1960s a much more powerful form of artificial intelligence has been emerging: machine learning. Artificial intelligence and machine learning are, confusingly and wrongly, sometimes used interchangeably. They are very different; and machine learning has far more disruptive potential for financial markets than anything we have seen so far with deterministic, rules-based algorithmic trading.

Machine learning algorithms are programmes that teach themselves, by training on large data sets using huge computing power and ‘deep learning’ techniques, to make their own decisions. There are no fixed, deterministic rules; rather the computer teaches itself to improve its performance all the time by experimenting with new data that it scans and each decision may be different, because based on updated data and using revised logic, from the preceding ones.

Such a machine is much closer to the inquisitive, generalised learning that characterises humans and is perhaps more deserving of the term ‘artificial intelligence’.

I should say at this point that I am a big optimist for machine learning in markets and finance more generally. We are surrounded by machine learning technology in our daily lives.

Whether we are buying books on Amazon or videos on Netflix; talking to Alexa or translating foreign languages using Google; spell checking on our phone or computer; buying airline tickets or booking vacations online; purchasing food in supermarkets whose layout was devised by learning algorithms; applying for or using credit cards that can predict our creditworthiness and the incidence of suspicious transactions that aren’t ours; walking down a street made safer by algorithms that decide where to allocate police resources; watching our football team win using tactics developed by machine learning; or having illness diagnosed by a doctor assisted by machines interpreting our symptoms - at almost every step our lives are made simpler, safer and more productive by machine learning algorithms.

So there is absolutely no reason in due course why it cannot be successfully deployed in financial markets as well; and I believe it inevitably will. At present its main applications are in second lines of defence, including compliance and risk management tasks, for which techniques such as natural language processing are well suited. But even bigger benefits will likely flow from deploying machine learning directly in the ‘front end’ of trading.

Such benefits could include, for example: increasing the speed and accuracy of processing orders, by using natural language processing to decipher requests from clients; improvements to pricing from combining very large amounts of market data and better evaluation of venue, timing and

order size choices; better estimation of the probability of order-filling given prevailing market conditions; better order-routing choices and evaluation of venue, broker and execution algorithms.

These disruptive benefits will be accompanied by risks. Among the risks that machine learners and regulators - and bodies like FMSB that are concerned about market functioning - need to be discussing are:

Model drift: the risk that models do something unexpected. This is particularly challenging with machine learning because of the continuous cycle of training that machine learning involves. The algorithm will likely make different decisions after it has seen more data, and it will be very hard or impossible to trace how these decisions were 'made'. It will therefore become very difficult to predict in advance, or to correct afterwards, undesirable model outputs. And it will be particularly hard to know how a machine trained on historical data will react when it is live and encounters events that weren't present in the data used to train it - for example the arrival of a pandemic virus.

Bias: machine learning is all about discriminating between data signals. The way in which this is done is susceptible to bias by the machine, potentially for unknown 'reasons', which could in turn result in harmful and unforeseeable outcomes: for example, changes in pricing or rationing of liquidity for specific types of market user. Further, we must expect that a machine optimising on its own might 'discover' that unethical, manipulative trading is more profitable than ethical trading. How to devise an 'ethical governor' to sit alongside and influence the algorithm may be extremely tricky.

Market concentration: the insatiable demand for data that machine learning creates may create monopolistic or oligopolistic network effects among data suppliers. If this happens, such networks might raise new barriers to entry in markets; and it is hard to predict whether such barriers would consolidate the power of current incumbents, or change market structure significantly at the expense of today's big firms. Either way, concentrated market structures need careful thought, as regulators are well aware. Data hungry machine learners may also, by their trading activity, create new correlations between the economic and other variables that their algorithms use, and in so doing make markets more fragile and vulnerable. And bad actors might try to anticipate and manipulate these vulnerabilities.

Resources: machine learning skills are in short supply in both the private and the public sectors; and are concentrated in two countries which have commanding technology sectors and a strong will to succeed - the US and China. What the implications are of these countries (potentially) dominating FICC markets in future perhaps also needs some thought.

FMSB will be starting work on some of these machine learning challenges this year. To begin, we will shortly be publishing a 'Spotlight Review' on developments in algorithmic trading which will look at model risk, the use of algorithmic trading in less liquid asset classes, the deployment of machine learning in markets and the consequences of the increasing use of execution algorithms in FICC markets.

Disruptive technology: new forms of money

Technology is driving equally profound disruption in the basic unit of account for finance: money.

Of course, the concept of what money is has evolved significantly over the years. On the island of Yap in Micronesia, money was until relatively recently a Rai stone: massive carved stone rings, up to four metres in diameter, and resembling upended millstones, that were deposited on the Micronesian equivalent of the village green. They never moved physically, but a simple accounting system transferred partial ownership of the stones from buyer to seller when goods or services were paid for.

And we are familiar with the role that bullion, coins, paper money and electronic money - digital records on computers - have successively played in our increasingly sophisticated financial system over time.

Sophisticated as it may be, today's money has some material drawbacks: quite large numbers of people don't have bank accounts, can only transact in cash, and so can't participate fully in the economy; making payments through the existing financial system infrastructure is quite expensive; and that infrastructure is complex and prone to risk and failure.

There would be real benefits if a way could be found to disrupt the existing world of money: making payments cheaply without needing bank accounts and the multiple layers of expensive and risky infrastructure that support them.

In 2009, the launch of the first cryptocurrency, Bitcoin, and its blockchain infrastructure, was the most recent attempt at just such a radical disruption. For a variety of reasons, Bitcoin and the hundreds of imitator cryptocurrencies were not in fact attractive or successful replacements for money. Their value was extremely volatile and unpredictable; they were not very secure; and the costs of making payments were too high.

But a second generation of successors to the early cryptocurrencies, so called 'stablecoins' and 'tokenised assets', may be more successful and a viable step change in the transformation of money and payments; even if not, they are definitely an interesting and disruptive innovation.

By backing their tokens or stablecoins with real financial assets, the designers of these instruments should make them much less volatile. Because they operate outside the banking system stablecoins can in principle offer significant financial inclusion benefits to the unbanked but electronically connected. And supported by their own infrastructure, stablecoins have the potential to shrink the multiple layers, and complexity and risk, of the traditional payments architecture.

These benefits are non-trivial, but as with machine learning, quite a few practical issues need to be thought about, not all of which have easy solutions. For example:

- Stablecoin holders don't necessarily enjoy a solid legal claim over the assets used to back the coins; and changes in supply and demand for stablecoins may increase the fragility of the assets used to back them, potentially including the commercial banking deposit base - which would be a legitimate prudential concern for regulators.

- There is some 'exchange rate' risk between the stablecoin and its backing assets, which users would have to accept and isn't a feature of conventional money. It is also unclear how stablecoins design might deal with negative interest rates.

- As 'synthetic' money, stablecoins still pose a series of compliance risks in relation to money laundering and client identity and their anonymity is likely to make them even more attractive than traditional money to those engaged in financial crime, including the funding of terrorism.

- The proposed stablecoin ecosystems, with re-sellers, validators, wallet-holders, exchanges and other infrastructure, typically involve quite a few entities that aren't today subject to any financial services regulation, raising 'perimeter' questions about how far regulation of a 'stablecoin system' should extend and how it should operate across jurisdictions to mitigate or control the spillover of risk.

These practical questions reflect a deeper, structural challenge. Fundamentally, stablecoins and their infrastructure differ from traditional money and payment systems because they create the tokens or coins, and the associated value, that is transferred; they don't just transfer money created by other entities - central and commercial banks - as traditional payments systems do. This feature, the creation of money, runs headlong into the established monetary and financial stability policy responsibilities of central banks; and the impact of stablecoins on the conduct of monetary policy and macro financial stability are not clear.

Which explains why, at a recent count, over 60 central banks and regulatory standards bodies across the world are currently working on how stablecoins can be allowed to disrupt the global payments architecture without destroying the tools that central banks use to steer their

economies.

It may be that ‘official’ stablecoins - so called central bank digital currencies, or synthetic money issued by governments or central banks themselves - are a viable solution, and several countries are actively investigating such an idea.

Stablecoins and tokenised assets feature on the latest FMSB risk map - because of their potentially dramatic future impact on financial market structures and participants; and I believe FMSB will end up working on this topic in future years. Before we can do this, central banks and regulators need to make some critical decisions about the regulatory landscape for disruptive money; but when that has happened the private sector can take stock of the key remaining issues and how industry standards might help to address them.

Disruptive technology: exposing the whole system

As financial markets and money become more automated, more interconnected and more dependent on technology, data and computing power so they also become more vulnerable to completely new forms of disruption: the (very) broad category of cyber threat.

Cyber is a very big deal for financial markets, whether it is perpetrated by cyber criminals directly or (as is increasingly the case) by agents who offer ‘cybercrime as a service’ to less well equipped actors, and whether it involves: the theft or manipulation of data used to identify counterparties in markets or to drive algorithmic trading engines; intrusion into systems to facilitate insider trading or other manipulation - or equally worryingly to cause financial market or wider economic crashes by manipulation of trading machines; or the sabotage of critical pieces of infrastructure or supply chains on which markets rely.

And cybercrime devoted to the outright theft of money or financial assets, whether real or digital/crypto, is a massive problem for the stability of the money and payment systems.

Unfortunately we do not have to look far for examples of all these things happening. In wholesale markets, critical market infrastructure - SWIFT - was attacked in 2016 to enable the heist on Bank of Bangladesh. In retail markets, ATM ‘jackpotting’, ‘cryptojacking’, ransomware and DDOS attacks are a regular feature. Of course, there have been much more worrying types of cyber incident (e.g. in Ukraine in 2014 and South Korea in 2013) aimed at disrupting entire economic systems. And for sure we don’t know about every incident that occurs.

While they weren’t cyber attacks, some measure of the damage that could be done by bad actors attacking markets can be obtained by looking at the 2010 US equity market ‘flash crash’, the 2012 collapse of Knight Capital, the 2014 US Treasury flash event, or the 2016 sterling ‘flash crash’.

Cyber is a problem tailor-made for public-private sector collaboration. Both public and private sectors have knowledge and assets that the other lacks, and needs, to combat cyber risk. No organisation can be immune; the question is how best to collaborate or partner with others to achieve an acceptable level of resilience. In the UK the regulators have pioneered a joint effort between firms, financial services regulators and the security services to understand the vulnerability of organisations (and by extension, markets) to cyber threat, through structured reviews of risk and penetration testing of firms' defences. What these exercises show is that:

- Cybersecurity is a team sport. A wide range of internal departments have to be aligned in any organisation behind the goal and processes to deliver resilience. Organisations need to share information between themselves about threats and effective defences. All this needs trust.

- Cyber defence is about good hygiene. Patching, authentication, data security, active directory management, and training for people who are vulnerable to psychological manipulation are all critical to achieving resilience.

- Not all user access is created equal. Organisations need to use a principle of 'least privileged access' to defend themselves.

- Email entry-points into the organisation are major points of vulnerability. They need to be well defended, and email users need to be well trained in email security.

- Organisations need to be very sceptical about supply chains: cyber security is only as strong as the weakest link. Many attacks originate outside an organisation, on suppliers who are already set up to let hackers in that organisation's systems.

- Crisis management and recovery plans need to be practiced relentlessly. Most data breaches are perpetrated by internal actors, whether accidentally or deliberately.

Beyond these technical risks, structural factors also accentuate cyber vulnerability. As market structure has become more concentrated and more interconnected small groups of key infrastructure providers pose increased risk: obvious examples include the CLS, SWIFT and LCH platforms which together provide the core of critical global FICC infrastructure.

For all these reasons, cyber is on the latest FMSB risk radar (among many other topics). For us the question is not whether cyber demands our attention, but rather whether there are aspects of cyber defence for markets that FMSB can develop better than other bodies.

FMSB is most effective when the collective wisdom of multiple private sector firms, representing

all interests in the market, can illuminate how business should get done, in more detail or with greater clarity or at greater speed than is possible with conventional legal or regulatory tools. This can happen because (for example) of information or resource asymmetry between private and public sectors.

In the case of cyber, much critical knowledge sits in public sector bodies - with regulators and the security services. In such cases a better model is normally public-private sector partnerships. For this reason, we think at present that there are probably other bodies better equipped to do this than FMSB; and that our energies should be focussed where we can add greater value.

Regulatory reforms since the 2008 crisis have brought many benefits for users of FICC markets, and accelerated structural changes that might otherwise have taken many more years to arrive. So great has the effort been on developing and implementing these regulatory changes that the revolution in technology happening at the same time has perhaps been overshadowed. But when finance is more interconnected than ever, and more dependent on technology and data science, the opportunities and incentives for technological disruption are immense. We should welcome these disruptive forces; without past disruptions we would not enjoy the capital markets that we have today.

Very often in finance the understanding of risk, and the need for appropriate controls, only follows some time after innovation: when things have already gone wrong, losses been incurred and damage suffered. Today we stand on the verge of technology disruption in markets and in money, before major change has yet happened. This creates an unusual opportunity to anticipate and mitigate risk that might crystallise in future: it behoves us all to take the chance to do just that.

FMSB and its members will certainly play their part.

Ladies and gentlemen, thank you for your attention.