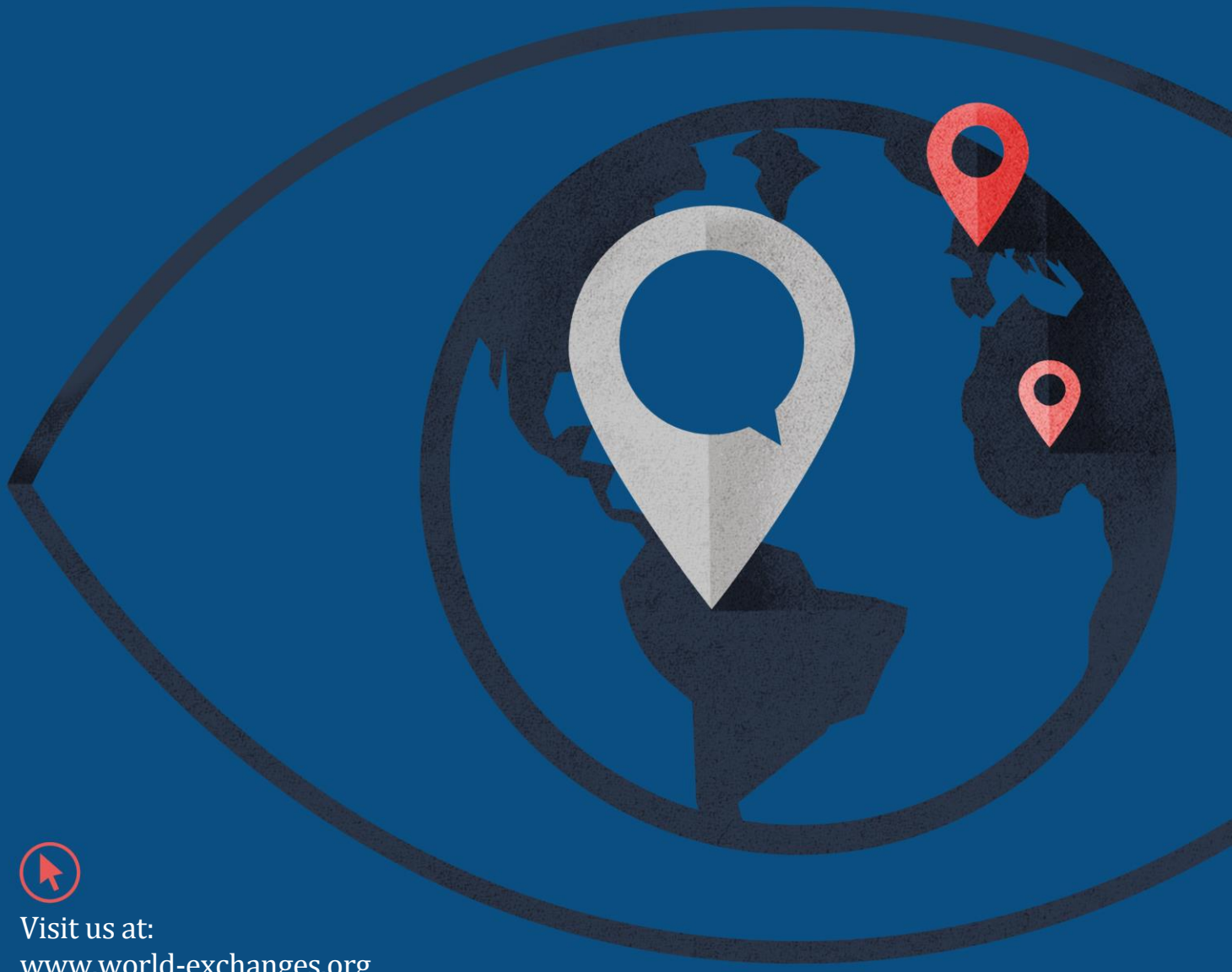
WORLD FEDERATION OF EXCHANGES

June 2017

European Commission Public Consultation: FinTech: A More Competitive and Innovative European Financial Sector



Visit us at:
www.world-exchanges.org

Background

The World Federation of Exchanges (WFE) is the global industry association for exchanges and clearing houses. We represent more than 200 market infrastructure providers, of which more than 100 are Central Counterparties (CCPs) and Securities Depositories (CSDs). Our members include exchange groups and standalone CCPs.[1]

Our members are both local and global, operating the full continuum of financial market infrastructure in both developed and emerging markets. Of our members, 41 percent are in the Asia-Pacific region, 40 percent in EMEA and 19 percent in the Americas. WFE exchanges are home to nearly 45,000 listed companies, and the market capitalisation of these entities is over $67.9 trillion; furthermore, around $84.18 trillion in trading annually passes through the infrastructures our members safeguard.[2]

The WFE works with global standard setters, policy makers, regulators and government organizations to support and promote the development of fair, transparent, stable and efficient markets. We share their goals of ensuring the safety and soundness of the global financial system. There are significant benefits to the wider population of integrated financial markets, and we think it important to have strong common principles, approaches and supervisory coordination to promote financial integration and market integrity, whilst safeguarding supervisory coordination. This is fundamental to well-functioning and safe markets in which investors can have confidence.

Executive Summary

The WFE appreciates the opportunity to respond to the EU Commission (the Commission) Public Consultation on FinTech[3]. We applaud the proactive and considered approach to the examination of the various issues surrounding the impact of FinTech on the EU financial sector. Whilst FinTech applications can bring significant benefits to the industry, risks must be managed carefully. Technological advances, regulatory pressures and capital constraints are pushing the financial services industry to rethink the entire value chain. In particular:

- Markets are increasingly international, and FinTech innovation may have global applications and uses. As such, the Commission and other EU authorities should work alongside international regulatory organisations and groupings[4] to develop a common approach and ensure an appropriate level playing field.

- The scope of existing EU regulations should be sufficient to extend to most potential FinTech use cases (as they typically relate to new *technologies* as opposed to new *activities*). A multi-layered approach to regulation should be avoided, only adapting legislation or supervisory practice if the activity doesn't already fit into it. Generally, we believe services based on new technology need to abide to the same rules as incumbents to ensure investor protection as well as preserve the integrity and stability of the financial system.

- Whilst much focus to date has been on Distributed Ledger Technologies (DLT), we believe other technological areas will develop that are at least as important – if not more so – to the exchange and post-trade space. This would include Cloud Computing, Artificial Intelligence, Big Data and Robotics.

- Innovation should be market driven (as opposed to driven by regulation) and needs to take place in a safe and controlled environment in which participants can have confidence. Any regulatory approach should encourage innovation whilst ensuring appropriate investor protection and security in the system.

- EU Authorities should continue to proactively engage with the market to identify the nature of the application, understand the technology behind it, and ensure an appropriate regulatory framework if existing frameworks are not deemed appropriate.

[1] The WFE membership list can be found here
[2] As at end 2016
[3] European Commission. FinTech: A More Competitive and Innovative European Financial Sector
[4] Such as IOSCO and the G-20

- We note a potential risk where non-financial, un-regulated players lead the development of FinTech solutions related to traditional core market functions. The risk is that a lack of awareness of the regulatory environment may result in negative consequences for investor protection, and secure and orderly markets.

Specific Comments

SECTION 1: FOSTERING ACCESS TO FINANCIAL SERVICES FOR CONSUMERS AND BUSINESSES

GENERAL

1.1. What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

The WFE is an industry association that itself is not currently seeking to develop or use FinTech.

The WFE's membership consists of exchanges and clearing houses (CCPs) that are significant in size in their home jurisdiction, and whose own direct participants are generally wholesale market participants as opposed to retail consumers. As such, the bulk of our response is contained within sections 2, 3 and 4 of this public consultation.

Nevertheless, more generally and within that context, WFE's member base has been actively exploring how FinTech can be applied to the exchange and CCP space to improve processes and efficiency. This has been both individually, through the setting up of venture capital funds which invest in promising FinTech initiatives, and also through industry consortia (for example the Linux Foundation Hyperledger Project and the Post-Trade Distributed Ledger Group).

Whilst much focus to date has been on Distributed Ledger Technologies (DLT), other technological areas will also likely develop and offer solutions relevant to the WFE constituency, which may include areas such as Artificial Intelligence, Big Data, Cloud Computing and Robotics. As such, WFE members are actively examining these and other FinTech solutions, which we further discuss in sections 2, 3 and 4.

ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYTICS FOR AUTOMATED FINANCIAL ADVICE AND EXECUTION:

1.2. Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.) and at what pace? Are these services better adapted to user needs? Please explain.

This is not a priority area for WFE members.

1.3. Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place? What could be effective alternatives to such a system?

This is not a priority area for WFE members.

1.4. What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

This is not a priority area for WFE members.

1.5. What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

This is not a priority area for WFE members.

SOCIAL MEDIA AND AUTOMATED MATCHING PLATFORMS: FUNDING FROM THE CROWD:

1.6. Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? In what way? What are the critical components of those regimes?

Whilst this is not a core component of activity for exchanges and CCPs, it does provide additional avenues for capital formation for enterprises and we hence see potential in tapping new sources for financing growth companies. However, we are also cautious as regards the inherent risks such platforms pose for investors, especially when they fall short of well-established transparency and investor protection standards. The regulatory requirements applicable to peer-to-peer and marketplace lending should therefore be aligned with the framework applied to financial institutions in the event they are providing the same service. At the present time, the size of actionable activity for this purpose remains relatively modest. Legislators should keep track of evolution in this space to ensure the necessary investor protection measures remain adequate to the business conducted.

1.7. How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

Whilst this has not been identified as a priority area for WFE members generally, as inferred in Q 1.6, these are nevertheless areas that may be of potential interest - particularly to those in Emerging Markets. As such we would suggest – if the Commission were to consider further work in this area - it be cognisant of the wider effects, and should work alongside international regulatory organisations and groupings, such as IOSCO and the G-20, to develop a common approach and understanding in order to ensure international regulatory coherence.

1.8. What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

This is not a priority area for WFE members.

SENSOR DATA ANALYTICS AND ITS IMPACT ON THE INSURANCE SECTOR:

1.9. Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

This is not a priority area for WFE members.

1.10. Are there already examples of price discrimination of users through the use of big data? Can you please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

This is not a priority area for WFE members.

OTHER TECHNOLOGIES THAT MAY IMPROVE ACCESS TO FINANCIAL SERVICES:

1.11. Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

This is not a priority area for WFE members.

SECTION 2: BRINGING DOWN OPERATIONAL COSTS AND INCREASING EFFICIENCY FOR THE INDUSTRY

GENERAL:

2.1 What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

The WFE is an industry association that itself is not currently seeking to develop or use FinTech applications.

The WFE's membership consists exchanges and clearing houses (CCPs) that are significant in size in their home jurisdiction, and who's own direct participants are generally wholesale market participants.

WFE's member base has been actively exploring how FinTech can be applied to the exchange and CCP space to improve processes and efficiency. This has been both individually, through the setting up of venture capital funds which invest in promising FinTech initiatives, and also through industry consortia (for example the Linux Foundation Hyperledger Project and the Post-Trade Distributed Ledger Group).

Whilst much focus to date has been on Distributed Ledger Technologies (DLT), other technological areas will also likely develop and offer solutions relevant to the WFE constituency, which may include areas such as Artificial Intelligence, Big Data/Data analytics, Cloud Computing and Robotics. As such, WFE members are actively examining these and other FinTech solutions.

There are a number of technologies and use cases that the WFE's global membership is considering and/or developing (in no particular order):

Distributed Ledger Technology:

WFE members are investigating various use cases for DLT, primarily for cost savings, to enhance efficiency, and to reduce risk. These benefits are integral to the technology, as it is envisaged they will allow for a) further automation and streamlining of processes, b) the reduction in the need for authentications and manual reconciliations, c) the reduction in the time needed to finalise transactions, and d) the facilitation of greater data integrity and system resilience.

Further, WFE members consider that (in relation to clearing and settlement and collateral management) DLT could result in greater capital efficiency for market participants through an overall reduction in operating costs, an increase in clearing and settlement efficiency and a potential reduction in capital requirements (due to a reduction in risk).

The WFE's members are assessing DLT applicability on a case-by-case basis to see what, if any, efficiencies can be generated in streamlining individual processes and what role the technology can play in reducing costs.

Big Data / Data Analytics:

Data analytics capability and automation may provide opportunities for assessing regulatory compliance. Data analytics tools are already used in trading markets for surveillance purposes (e.g. to assess irregular trading patterns) and there are many automation tools (such as accounting packages) that reduce the manual burden of preparing information in compliance with listings requirements. Further, exchanges or relevant intermediaries may be able to customise data analytics tools to assess the extent to which regulatory documents comply with the relevant requirements.

Cloud Computing:

A combination of commoditised hardware and the widespread adoption of software capabilities has led to a greater use of cloud-based services in recent years – particularly given the global access to these services provided for by the internet. Exchanges and CCPs are starting to develop IT strategies in which they consider moving non-core aspects of their infrastructure from the traditional corporate "data-centre" model into cloud-based arrangements – largely as a result of the scale, resiliency, privacy, security and cost/time to market benefits they offer.

Artificial Intelligence / Machine Learning:

As with the more general use of big-data and data analytics, artificial intelligence is another area in which exchanges are seeking to lever the data they have access to in order to more effectively monitor their markets. Machine learning and artificial intelligence can be used to eliminate human bias in the market surveillance function, analysing and discovering new patterns in the data. For example data from electronic communications can be linked with order, cancellation and amendment data, providing an holistic view of a trader's (or group of traders') activity – critical to assist the exchange in the monitoring, detection and deterrence of abusive trading activity on its market.

2.2 What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

Innovation should be market-driven as opposed to driven by regulation. Nevertheless innovation needs to occur in a safe and controlled environment in which market participants can have confidence.

The WFE considers that EU authorities should be proactive in engaging with the industry in order to identify the nature of the application, to understand the technology which underpins it, and to work with industry to ensure the existence of an appropriate regulatory framework (if existing frameworks are not deemed appropriate). Regulatory sandboxes have proven to be a useful tool for the FinTech industry and so we suggest these should be extended where relevant in order to ensure that appropriate collaboration and exchange of information occurs between industry (whether regulated, or not) and regulator. This will also enable regulatory applications to be tested and examined before they go to market.

Whilst the WFE supports a coordinated European approach to FinTech innovation, we also emphasise the need for global consistency based on international guidelines and principles. Markets are increasingly international, and FinTech innovation may have global applications and uses. As such, we suggest the Commission – and other EU authorities - should work alongside international regulatory organisations and groupings, such as IOSCO and the G-20, to develop a common approach and understanding in order to ensure international regulatory coherence amongst the wide range of current and potential FinTech providers and participants.

2.3 What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

The effects on employment of technology solutions and automation are widely discussed and not restricted to the financial sector.

It is possible FinTech solutions have an effect on employment inasmuch as automation potentially leads to fewer people needed to complete certain functions. Further, digitisation may reduce the need for broad networks of branch offices for serving clients.

However, experience has shown that technology typically leads to a net increase in numbers of human roles, redefining them in ways that reduce costs and boost demand.

Nevertheless, the changes we are seeing in all sectors require a redefining of the skillsets of employees, making IT literacy more critical for most businesses – in particular including in legal and compliance functions within financial services.

REGTECH – BRINGING DOWN COMPLIANCE COSTS:

2.4 What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

There are currently many use cases for technologies that can assist firms to meet their regulatory obligations (RegTech). These may include:

- Legislation / regulation gap analysis tools;
- Compliance universe tools;
- Management Information tools;
- Transaction reporting tools;
- Regulatory reporting tools;
- Activity monitoring tools;
- Training tools;
- Risk data warehouses;
- Case management tools;
- National Know Your Client (KYC)/Anti-Money Laundering (AML) registries;
- Trade finance facilities;
- Asset registration facility (such as real estate);
- Database on agricultural receivables;
- Digital assets and associated products.

As with our comments to Q2.2 (relating to wider FinTech innovation), we consider that EU authorities should be proactive in engaging with the industry in order to identify the nature of the application, to understand the technology which underpins it, and to work with industry to ensure the existence of an appropriate regulatory framework (if existing frameworks are not deemed appropriate). Consistency of rules being applied to similar services should be taken as a general principle.

Markets are increasingly international. FinTech and RegTech innovation may have global applications and uses. Particularly with applications such as trade and transaction reporting, it will be important that authorities coordinate their requirements so that RegTech can scale and be as cost efficient as possible, and reduce the compliance burden.

As such, we suggest the Commission – and other EU authorities - should work alongside international regulatory organisations and groupings, such as IOSCO and the G-20, to develop a common approach and understanding in order to ensure international regulatory coherence amongst the wide range of current and potential FinTech and RegTech providers and participants.

RECORDING, STORING AND SECURING DATA: IS CLOUD COMPUTING A COST EFFECTIVE AND SECURE SOLUTION?

2.5 What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services? Does this warrant measures at EU level?

Due to the systemic importance of exchanges and CCPs, and the volume and nature of data held by them, regulatory and public policy considerations must be addressed when considering whether to move functions from a traditional corporate data-centre model to one based on cloud technology. Whilst our view (see Q 2.6 below) is that properly managed facilities can indeed provide safe and secure (and potentially exceed locally managed) facilities, risks may exist around the public perception and understanding of these types of facilities.

2.6 Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Should commercially available cloud solutions include any specific contractual obligations to this end?

Standard contracts provided by cloud services providers may not always be suited to the needs of financial infrastructure providers, which in those situations instead require bespoke arrangements and negotiations. Areas of contention may include resilience, the handling of data, and security.

Further, many national and international institutions have issued guidelines or expectations with regard to cloud services, specifically targeting these areas – and including outsourcing. In the US these include the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), the US Federal Reserve, the Federal Risk and Authorisation Management Programme (FedRAMP), as well as SEC and CFTC guidelines on systems safeguards. In the UK the FCA has issued guidance for firms outsourcing to the cloud and other third party IT services, in Singapore the MAS has issued guidelines around “outsourcing” to the cloud, and in Hong Kong the Office of the Government Chief Information Officer (OGCIO) published a practice guide for procuring cloud services. Furthermore, many governmental and regulatory agencies globally have moved – or are planning to move - certain functions of their own to the cloud.

As noted in responses to other questions – specifically relating to outsourcing (Q2.10, 2.11) - in principle, the use of FinTech including cloud solutions provided by a third party to a regulated entity should be no different to the outsourcing of any other function, with the fundamental concept being that responsibility for the outsourced function/activity should remain with the regulated entity. This would include ensuring the fitness and properness of the outsourced provider, and responsibility for aspects of governance, policy definition, management of services (i.e. contracts, service levels, monitoring), SLA reviews and control audits.

DISINTERMEDIATING FINANCIAL SERVICES: IS DISTRIBUTED LEDGER TECHNOLOGY (DLT) THE WAY FORWARD?

2.7 Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

Exchanges and CCPs are exploring a variety of potential use cases for DLT which may have an impact on the ability for SMEs to access finance. These include securities issuance (particularly for private issuances) and crowd-funding.

2.8 What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

- **Privacy Issues**: Financial services organisations have a need and obligation to keep certain information private and confidential. The identity of a party to a transaction is usually not public unless legal provisions require the disclosure of this information. As such, it is important that DLT-based networks are designed in a way that protects privacy when necessary without hampering the benefits of the technology. The extent of the issues relating to privacy will depend on the type of information that is being stored on the ledger/blockchain and on the governance of the system;

- **Cyber Risk & Resilience**: Systems based on DLT are inherently more resilient to single point of entry failures due to their distributed nature. The distributed and shared nature of such systems could facilitate recovery of both data and processes in the event of a cyber attack. However, DLT has the potential to present risk due to the shared nature of the ledger, the risk of contagion, the complexity of DLT protocols and lack of clear oversight and responsibility. Since there is not necessarily clear governance of Blockchain-based systems, this could potentially result in problems updating security. Notwithstanding, we consider this more a question of appropriate governance of such systems rather than a shortfall of the technology itself;

- **Scalability:** The scalability of DLT-based systems is a key determinant for effectively putting it to use in financial services. Systems need to be able to process large volumes of data on a daily basis and to handle potential peak trading volumes in times of market stress or volatility;

- **Determining Applicable Law:** It is yet clear how one determines the applicable jurisdiction or relevant laws in a decentralised system. It is, for example, difficult to pinpoint the jurisdiction in which data in a blockchain is being processed, and therefore what data protection laws may be relevant;

- **Recourse Mechanisms**: A key challenge will be determining an industry-wide solution to correct errors given no application is likely to be able to guarantee a zero-failure regime; and

- **Governance Framework**: Clarity and consistency around systems accountability and responsibility will be particularly important – for example being clear who is responsible for claims resolution and system misbehaviour.

There are also risks associated with the **migration** to a DLT environment, including the need to run parallel systems, extensive testing of internal systems as well as connections to all firms sharing the DLT, and increased monitoring in the period after launch. Interoperability between each other, and with legacy systems, will be a key requirement for most use-cases to allow the efficiency gains of the technology to materialise.

Additionally, because DLT is designed to be a live record, with no downtime contemplated in the currently defined solutions, the risks posed in respect of the on-going support of the system must be considered.

Further, updates will require the agreement and technological support of every firm connected to the DLT, which could make the actioning of maintenance or updates in urgent circumstances more difficult and cumbersome when compared to the current framework.

2.9 What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

Generally, the current European legislative framework for financial services would not prevent the introduction of DLT-based services. Services based upon new technologies – whether in the area of DLT or other technologies – need to be subject to, and satisfy, the same rules as applicable to incumbents in the interests of investor protection and maintaining the integrity and stability of the system.

There are certain challenges affecting the governance framework employed with respect to DLT within securities markets. In this regard, it is highly likely that distributed ledgers as applied to processes and procedures within securities markets would be permission-based, whereby only certain actors in the network have permission to maintain and validate the data recorded in the relevant distributed ledgers.

Additionally, there are several other legal and regulatory issues that might need to be addressed or clarified to enable the implementation of the specific use cases exchanges and CCPs are currently working on. These range from the general – namely data privacy laws, data governance considerations, conflict of laws issues, intellectual property laws, and investor protection laws - to more specific examples. These are set out below:

- Use cases being examined include integrated processes across trading, clearing, and settlement. However, the legal and regulatory frameworks often see these elements of the cycle in a discrete fashion;

- In collateral management use cases, it is important to have certainty regarding the legal status of digitised assets as a means of transferring and granting security over interests in such assets as well as treatment in insolvency, and applicability of insolvency protection;

- Certain types of DLT implementations do not fall neatly into current regulatory frameworks dealing with settlement finality. For example, in fully decentralised DLT schemes, it is not clear who would define the relevant finality concepts under EU law (i.e. what constitutes a 'transfer order', moment of entry, moment of settlement, law governing the 'system', etc.). An extension of the legal protections provided under the Settlement Finality Directive (which are a precondition for legal certainty of settlement) to DLT schemes would require changes to the existing legal regimes;

- Smart contracts, which are widely deemed part of the innovation of DLT, still require the need to clarify how errors are identified and resolved, and in what circumstances 'undoing' a smart contract would be permitted; and

- As identified in question 2.8, identifying the applicable jurisdiction or relevant laws in a decentralised system will be an inherent challenge for DLT.

We note a potential risk in a situation where non-financial players lead the development of DLT solutions, resulting in fewer regulated entities performing core market functions, many of which are subject to established regulatory frameworks. The risk is that a lack of awareness of the regulatory environment, or lack of formal oversight whilst DLT solutions are being developed, may result in negative consequences for investor protection and orderly markets.

Thus, as DLT use cases gain validation and transition into the securities and derivatives markets, there may be a need for regulators to provide clarification as to how existing regulatory regimes (e.g. EMIR, MiFID2) may apply to certain future financial service offerings which involve DLT solutions

OUTSOURCING POTENTIAL TO BOOST EFFICIENCY:

2.10 Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

Due to the systemic importance of exchanges and CCPs, regulatory and supervisory considerations naturally must be addressed when considering outsourcing of key functions to a third party. In principle, the use of FinTech provided by a third party to a regulated entity should be no different to the outsourcing of any other function. There are well established regulatory/supervisory processes to address those already in existence, with the fundamental concept being that responsibility for the outsourced function/activity should remain with the regulated entity. This would include ensuring the fitness and properness of the outsourced provider, and responsibility for aspects of governance, policy definition, management of services (i.e. contracts, service levels, monitoring), SLA reviews and control audits.

2.11 Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and how are they supervised? Please specify, in which areas further action is needed and what such action should be.

It seems to us that the current financial services legislation governing outsourcing – in which activity but not responsibility can be outsourced to a third party – remains appropriate. In principle, there is no reason why the legislation surrounding the outsourcing of FinTech solutions by a regulated entity should be different to any other service – specifically mandating primary responsibility for ensuring the appropriateness of the outsourced provider should lie with the regulated entity that commissions its services.

Existing legislation already envisages the outsourcing of activity to other – sometimes unregulated – entities. To facilitate this, there are well established regulatory/supervisory processes already in existence, with the fundamental concept being that responsibility for the outsourced function/activity should remain with the regulated entity. This would include ensuring the fit and properness of the outsourced provider, aspects of governance, policy definition, management of services (i.e. contracts, service levels, monitoring), SLA reviews and control audits.

Whilst the technology itself may present new risks (operational, cyber, etc.), the underlying principles of outsourcing remain sound and appropriate.

OTHER TECHNOLOGIES THAT MAY INCREASE EFFICIENCY FOR THE INDUSTRY:

2.12 Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

As per the response to question 2.1, the main types of financial innovation being explored by the exchange and CCP community to reduce operational costs and increase efficiency are:

- Distributed Ledger Technology;
- Big Data / Data Analytics;
- Cloud Computing; and
- Artificial Intelligence

SECTION 3: MAKING THE SINGLE MARKET MORE COMPETITIVE BY LOWERING BARRIERS TO ENTRY

GENERAL:

3.1. Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

As a general matter, the WFE believes the scope of existing EU regulations should be sufficient to extend to most potential FinTech use cases as they typically relate to new technologies as opposed to new activities. However, it is possible some of the new technologies do not work in the same way as existing and therefore do not *appear* to perform the same activity. We consider the EU should seek to avoid a multi-layered approach to regulation in this area, and in doing so should carefully consider the activity in question. It should only adapt existing legislation or supervisory practice if the activity in question does not already fit into existing legislation – or in order to ensure a level playing field amongst new and incumbent market participants.

3.2. What is the most efficient path for FinTech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants? If so, at what level?

Innovation should be market-driven as opposed to driven by regulation. Nevertheless innovation needs to occur in a safe and controlled environment in which market participants can have confidence.

The WFE encourages European regulators to remain focused on ensuring investor protection and the safety of markets whilst at the same time enabling financial technology which improves capital markets.

Notwithstanding the proactive nature of regulatory scrutiny from national as well as regional authorities, we advocate that it is highly desirable for a globally harmonised approach in a topic as internationally relevant as FinTech. FinTech is innately international with global applications and uses and therefore any regulatory principles and/or guidelines should be developed at that global level.

FINTECH HAS REDUCED BARRIERS TO ENTRY IN FINANCIAL SERVICES MARKETS…BUT REMAINING BARRIERS NEED TO BE ADDRESSED:

3.3. What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide details.

It could be viewed that the barriers, if any, are there for investor protection and any drives to reduce these protections should be carefully assessed to ensure that the resulting new technologies deliver the same outcomes as originally envisaged from an investor protection perspective. Simply put, we should not change legislation and hope it all works ok.

3.4. Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If yes, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

The WFE encourages European regulators to remain focused on ensuring investor protection and the safety of markets whilst at the same time enabling financial technology which improves capital markets to advance unimpeded.

As a general matter, the WFE believes that the scope of existing EU regulations should be sufficient to extend to most potential FinTech use cases as they are typically relating to new technologies as opposed to new activities. As such, we consider the EU should seek to avoid a multi-layered approach to regulation in this area and only adapt existing legislation or supervisory practice if the activity in question does not already fit into existing legislation.

That said, the nature of FinTech innovation is such that non-financial companies may enter this market, some of whom may not have any experience of regulated environments; as such, any regulatory framework needs to ensure appropriate consistency between such firms and traditional regulated entities such as exchanges and CCPs not only to safeguard a level playing field but also to ensure adequate and effective investor protection and system resilience.

3.5. Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? If so, please explain in which areas and how should the Commission intervene.

Innovation should be market-driven as opposed to driven by regulation. Nevertheless innovation needs to occur in a safe and controlled environment in which market participants can have confidence.

The WFE considers that EU authorities should be proactive in engaging with the industry in order to identify the nature of the application, to understand the technology which underpins it, and to work with industry to ensure the existence of an appropriate regulatory framework (if existing frameworks are not deemed appropriate). Regulatory sandboxes have proven to have been a useful tool for the FinTech industry and so we suggest these should be extended where relevant in order to ensure that appropriate collaboration and exchange of information occurs between industry (whether regulated, or not) and regulator. This will also enable regulatory applications to be tested and examined before they go to market.

The WFE encourages European regulators to remain focused on ensuring investor protection and the safety of markets whilst at the same time enabling financial technology which improves capital markets to advance unimpeded and based off of level playing field principles.

3.6. Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? To what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross border financial transactions?

The WFE membership did not raise any specific response to this question.

ROLE OF SUPERVISORS: ENABLING INNOVATION

3.7. Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

The WFE encourages the European authorities to remain focused on ensuring investor protection and the safety of markets whilst at the same time enabling financial technology which improves capital markets to advance unimpeded.

The above principles do not appear inconsistent with that general objective – although WFE would suggest any approach should ensure appropriate consistency between new entrants and incumbent regulated entities not only to safeguard a level playing field but also to ensure adequate and effective investor protection.

3.8. How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation? Would there be merits in pooling expertise in the ESAs?

The WFE advocates an approach to prospective regulation that encourages prudent innovation and fosters the international collaboration and exchange of ideas between regulators at a global level. This approach would provide innovative businesses and technology providers with an opportunity to explore the potential applications of FinTech.

Regulatory sandboxes and innovation hubs have proven to be a useful tool for the FinTech industry and so we suggest these should be extended where relevant in order to ensure that appropriate collaboration and exchange of information occurs between industry (whether regulated, or not) and regulator. This will also enable regulatory applications to be tested and examined before they go to market.

However, in an area as internationally relevant as FinTech, it is highly desirable to adopt a globally harmonised approach. FinTech is innately international with global applications and uses and therefore any regulatory principles and/or guidelines should be developed at that global level. As such, we encourage the Commission to work alongside IOSCO and other global authorities including the G-20 to ensure a common approach, thereby ensuring international coherence and a level playing field amongst the wide range of current and potential FinTech participants.

3.9. Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? Please elaborate. If yes, please specify how these programs should be organised?

Regulatory sandboxes and Innovation Hubs have been a useful tool for the wider FinTech industry as well as regulatory authorities and so we advocate that these should be extended in order to ensure that appropriate collaboration and exchange of information occurs between industry (whether regulated, or not) and regulators.

As such, whilst not averse to the concept of a European “Innovation Academy”, it is important to recognise the existing initiatives and ensure minimal overlap or duplication.

3.10. Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Please elaborate. Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

Regulatory sandboxes have been a useful tool for the wider FinTech industry and so we advocate that these should be extended where relevant in order to ensure that appropriate collaboration and exchange of information occurs between industry (whether regulated, or not) and regulators.

It would be desirable for member state and EU regulators to coordinate not only between themselves, but also with international counterparts, especially with regards to a regulatory sandbox.

Whilst appreciating various local authorities need to ensure they continues to better understand the technological developments relevant to securities markets – which are fast moving and dynamic - due to the global, borderless nature of FinTech, we suggest engagement with international regulatory bodies, such as IOSCO and the G-20, to ensure any regional (i.e. European) initiatives and/or policy-formation in this area is complementary and does not encourage regulatory arbitrage.

3.11. What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above? If yes, please specify which measures and why.

The WFE membership did not raise any specific response to this question.

ROLE OF INDUSTRY: STANDARDS AND INTEROPERABILITY:

3.12. Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

Interoperability between each other and with legacy systems will be a key requirement for most FinTech use cases – not only relating to DLT – to enable the efficiency gains of the technology to materialise, particularly given we should expect a gradual deployment of such applications and different co-existing DLT-based networks.

Whilst the development of global technical interoperability standards would facilitate this by providing a base layer of connectivity, experience shows that such standards will be hard to establish in time to make a difference (for example, the complicated process to establish a Legal Entity Identifier).

The WFE would thus argue for markets-based solutions, including a commitment to the general necessity of interoperability.

3.13. In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?

The WFE and its members are focused on ensuring transparent and orderly public markets; as such, we applaud the willingness of regulators to scrutinise the risks as well as the benefits FinTech can bring in order to ensure this. The WFE encourages European regulators to remain focused on ensuring investor protection and the safety of markets whilst at the same time enabling financial technology, which improves capital markets, to advance unimpeded.

However, notwithstanding the proactive nature of regulatory scrutiny from national as well as regional authorities, we advocate that it is highly desirable for a globally coherent approach in a topic as internationally relevant as FinTech. FinTech is innately international with global applications and uses and therefore any regulatory principles and/or guidelines should be developed at that global level. As such, we encourage the Commission to work alongside IOSCO and other global authorities including the G-20 to ensure a common approach, thereby ensuring a level playing field amongst the wide range of current and potential DLT participants.

3.14. Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? What other specific measures should be taken at EU level?

The WFE membership did not raise any specific response to this question.

CHALLENGES:

3.15. How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

We believe that, while FinTech can bring significant benefits to the industry, risks must nevertheless be managed carefully in order to ensure the concept of a trusted, neutral, third party venue remains at the heart of well-functioning markets.

For example, in relation to clearing and settlement and collateral management, WFE members believe DLT could result in greater capital efficiency for market participants through an overall reduction in operating costs, an increase in clearing and settlement efficiency and a potential reduction in capital requirements (due to a reduction in risk). The use of cloud technologies could improve privacy of data and security, and the use of big data analytics and artificial intelligence can significantly improve market surveillance capabilities.

That said, the nature of FinTech innovation is such that non-financial companies may enter this market, some of whom may not have any experience of regulated environments. As such, any regulatory framework needs to ensure appropriate consistency between such firms and traditional regulated entities. This is not only to safeguard a level playing field, but also to ensure adequate and effective investor protection and systems resilience – including the safeguarding of personal data and other privacy issues.

SECTION 4: BALANCING GREATER DATA SHARING AND TRANSPARENCY WITH DATA SECURITY AND PROTECTION NEEDS

GENERAL:

4.1. How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

The WFE membership did not raise any specific response to this question.

STORING AND SHARING FINANCIAL INFORMATION THROUGH A RELIABLE TOOL:

4.2. To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

Blockchains provide a secure way of storing and managing information through the use of cryptography and systemically embedded economic incentives for network maintaining entities.

However, there are potential challenges to consider and overcome, particularly regarding data protection / privacy. These are discussed in the response to Q4.4 below.

4.3. Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

The WFE membership did not raise any specific response to this question.

4.4. What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

Whilst blockchains provide a secure way of storing and managing information through the use of cryptography and systemically embedded economic incentives for network maintaining entities, DLT may be a challenge regarding personal data protection because:

- Blockchains are decentralized and distributed so it would be difficult to identify the entity responsible for controlling and processing the data and how they are doing it/what they are doing with it. That said, currently entities that process personal data can be centralised - although this in itself can create a single point of failure with, for example, risk of data being stolen through hacking of systems;

- You cannot change or delete information contained on a blockchain including personal data as transactions are not reversible;

- Whilst we acknowledge (and at this point support the fact) there is no specific legislation relating to DLT (given it is a change in technology, not necessarily activity), it is difficult to pinpoint the jurisdiction in which data in a blockchain is being processed, and therefore what data protection laws may be relevant.

Therefore it is of utmost importance that DLT-based networks are designed in a way that protects privacy when necessary without hampering the technology's benefits. The extent of the privacy issues depends on the type of information that is stored on the blockchain and on the governance of the system.

THE POWER OF BIG DATA TO LOWER INFORMATION BARRIERS FOR SMES AND OTHER USERS:

4.5. How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

The WFE membership did not raise any specific response to this question.

4.6. How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

The WFE membership did not raise any specific response to this question.

SECURITY:

4.7. What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

As a general point, we consider the provisions and principles within the CPMI-IOSCO guidance, alongside that in other commonly-referred to global standards (such as NIST, ISO, etc), and industry-developed standards of best practice like those produced by WFE in April 2017, continue to be relevant and appropriate. Given the global nature of markets and FinTech applications, any specific additional thinking should consider the global aspect to ensure continued high standards and consistency globally and across the industry.

Further, we caution that regulators should ensure any general FinTech technical or regulatory standards are consistent with other related existing rules, for example on cyber security and data protection.

FinTech's innate technology may mean non-financial companies enter this market, some of whom may not have any experience of regulated environments or existing regulatory standards (for cyber security, or other). As such, any regulatory framework needs to ensure appropriate consistency between such firms and traditional regulated entities not only to safeguard a level playing field but also to ensure adequate and effective systems resilience and investor protection – including the safeguarding of personal data and other privacy issues.

In relation to cyber risk specifically, as with all technological systems, DLT remains susceptible to unlawful intrusion and cyber-crime, but it is important in this context to distinguish permission-based distributed ledgers applied in the context of securities markets from the underlying permission-less peer-to-peer network upon which Bitcoin and other virtual currencies are operated. We believe that there are security benefits derived from the cryptographic encryption techniques employed within DLT, but market participants and regulators must work together to ensure the implementation of best practice standards on resilience and security within a DLT environment.

4.8. What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

Cyber threat information sharing is a challenging area. While STIX and TAXII initially promised to make the structured exchange of threat information easier and automated, in practice these standards have not gained great traction. Further, the way in which threat information is described varies in quality, and as such some WFE members observe that organisations often tend to rely on trusted vendors as their primary sources. Lastly when threats crystallise, it if often the case that the organisation will be primarily focussed on addressing the threat rather than sharing details - particularly where the outcome may still be uncertain.

Without a reasonable degree of automation and a central authority for quality control it is hard to see how this will become more than an ad-hoc, after-the-event activity for major common issues, with some minor levels of sharing where organisations have sufficient resources and are motivated to do so for wider reasons, as using the current models and tools does not scale well.

4.9. What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

Centrally coordinated activities can bring value to participants and it seems reasonable to consider that "Red Teaming" activities will become a standard part of the testing toolkit as they allow organisations to check that the detection and response controls they have in place are working appropriately.

It is possible the emergence of crowdsourced Penetration Testing companies (e.g. Synack) may change this dynamic, allowing more of a continuous assurance approach (at least for the external facing applications and perimeter). This may also be driven in the longer term (5-10 years) by the emergence of Artificial Intelligence attackers which would demand faster reactions to threats and vulnerabilities than is currently possible.

Generally speaking, the case for coordination is relatively strong given the geographically independent nature of the threats. However, any specific additional EU thinking should consider the wider global aspect to ensure continued high standards and consistency globally and across the industry, and to prevent undue duplication of efforts.

OTHER POTENTIAL APPLICATIONS OF FINTECH GOING FORWARD:

4.10. What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing? Are there any regulatory requirements impeding them?

The WFE membership did not raise any specific response to this question.

Nandini Sukumar
CEO, World Federation of Exchanges