Deutsche Bank
Corporate Bank

Regulation driving banking transformation

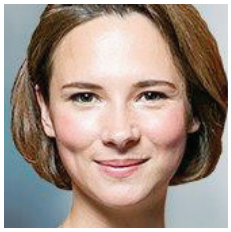
Insights into the key regulatory developments shaping the data economy, FinTech and BigTech companies in the financial industry and crypto-assets

2nd Edition

Contents

Key contributors

Lead contributor



Polina Evstifeeva,
Head of Regulatory Strategy, New Ventures, Corporate Bank, Deutsche Bank

Key contributors

Thomas Nielsen,
Head of New Ventures, Corporate Bank, Deutsche Bank

Luke Templeman,
Research Analyst, Thematic Research, Deutsche Bank

Stuart Davis,
Senior Associate, Co-Chair of Global Blockchain and Cryptocurrency Taskforce, Latham & Watkins

Julian Cunningham-Day,
Partner, Global Co-Head of FinTech & TMT sector, Linklaters

Craig Young,
Chief Information Officer, SWIFT

David Ostojitsch,
Director, Technology and Operations, Association of Financial Markets in Europe (AFME)

Published September 2019

Foreword: Incremental disruption

The disruption enabled by new technologies continues its decisive march into financial services, whether it be in the shape of new players driving new business models, new products, or an increased embrace of the power of Big Data. Ultimately, this affects not only the way financial services are provided, but the fundamental structure of financial markets themselves. The rules have changed. Disruption and innovation today is easier, better, stronger and faster – resulting in 10 times the number of innovators, a tenth of the cost and 100 times the power. As the tectonic plates shift in the financial industry, we cannot stand still – banks need to actively seek and embrace new opportunities such disruption brings

Thomas Nielsen,
Head of New Ventures,
Corporate Bank,
Deutsche Bank

We are living through a technological revolution. I sit writing this foreword in my San Francisco home, video conferencing a colleague in London, while looking over a shared document sent by an instant messaging corporate app from New York. And, let's not forget, I work for a German bank. We live in a world where collaboration across borders and boundaries is now the norm – for me, and many others like me, I can conduct my work equally well regardless of where I am. New technological possibilities for global outreach are having a significant impact on the way companies do business. This is a huge trend for all major industries.

To keep up with the pace of change and disruption, while maintaining a competitive edge, companies need to abandon traditional ways of looking at investment in, and deployment of, technology, and embrace solutions that allow them to adapt to market conditions and change course quickly if required. It is this desire that is driving another major trend, that being the proliferation of the "as-a-service" model: storage-as-a-service; computer-as-a-service; mobile-software-as-a-service; the list goes on. And this trend is broadening its reach, whether it be to payroll-as-a-service or healthcare-as-a-service – with technology aligning around these developments. New entrants are already taking full advantage of this trend, leaving many incumbents to look on with envy at their agility and nimbleness that is a direct result of moving to a pay-as-you-go model.

Filtering down into the banking industry, these macro trends are changing how banks employ people, how they collaborate and, crucially, the services that they offer to their digital native clients.

Changing business, changing markets

There are many exciting paths for us to follow as the financial landscape changes and broadens. Enabling better connection and user experience with clients is one and, over the past year, we have launched several commercial application programming interfaces (APIs) as part of our drive for Open Banking. In April, for instance, we teamed up with global fintech Serrala to launch the first API interface for SEPA instant payments.

Another path is banks entering "non-traditional" banking businesses, which would have been deemed impossible without the technological innovation of recent years. I'm particularly excited about Deutsche Bank's launch of the Yunar app in Germany at the end of last year, which enables users to manage all their customer loyalty cards in a single place on their mobile phone. This is a move towards the "platform economy": it's free, available everywhere and relevant to users' daily lives. The basic version will be continuously developed by incorporating user experience and feedback. Could this be the mobile wallet of tomorrow? Let's see!

Technology is not just disrupting the services and products provided by banks, however. It is changing and challenging the fundamental structures of financial markets themselves.

Everyone likes to talk about cryptocurrencies (although really they are an asset class, not a currency), yet this hubbub has not been matched by substantial action. Facebook's Libra is an interesting development: unlike the majority of cryptocurrencies, the plan is that when it is launched, Libra will be fully backed by a basket of currencies and assets held in the Libra Reserve for every Libra that is created. Pegging a global cryptocurrency to a basket of fiat currencies creates a fascinating challenge for market dynamics: will this flow of crypto-assets be regulated by central banks and governments, or by multi-national companies?

Comments from Facebook co-founder Chris Hughes act as a worthwhile warning: "Move fast and break things — our mantra in Facebook's early days — was an appropriate slogan for a college social network. It's not appropriate for the global monetary system."

I could not agree more: for crypto-assets to be trusted and used, the regulators, central banks and the industry will all need to address the issue in a co-ordinated and aligned fashion. Navigating and embracing such potentially tectonic shifts is never easy – but existing processes and rules are being challenged by changing consumer behaviours. Looking the other way with the hope that this is a fleeting trend is a mistake that financial institutions and regulators cannot afford to make.

Data is the new oil, and clients own the rights to the crude

Another topic that dominates agendas is Big Data, with significant focus on how financial institutions can best commercialise clients' data. But this line of thinking somewhat misses the point. First, banks are no longer the only custodians of clients' financial data and, second, the owners of that data – the clients themselves – need to be invited to the party so that they can influence its use and commercialisation.

While banks have traditionally been the custodians of clients' data, Open Banking initiatives have altered this landscape, mandating that such data should be made available to third-party providers if the client so wishes. Furthermore, we now live in a world where BigTechs have amassed vast amounts of data through their apps and platforms on pretty much everything you and I do in our online lives – and more and more on our offline activities, as well. They know our spending patterns, they know which music we like, who our friends are, our political biases, and they even know our holiday preferences and our driving habits – all available through advanced data analytics.

In some regions, this data has been used to sell financial products to clients (whether this be insurance, money market funds or other services). But do the clients get reimbursed for the use of their data in such a way? Not necessarily. Such use cases are making data a new commodity or a payment tool, if you wish. As clients become increasingly aware of the value of their data, they will want to participate and assume some level of control over its commercialisation for their own benefit.

For our part: yes, we hold data on thousands of clients across the globe, covering not just their cash activities, but also their trade, investment, securities services operations and much, much more. But, even if a business based on commercialising this data stored in our systems became too valuable to ignore, we will have to co-create this proposition with clients and share the fruits of that business accordingly. If data is the new oil, then our clients would likely want to own the rights to the crude in the seabed, and we would become the provider of the drilling platform, the refinery, as well as many other downstream services.

My over-arching opinion on the future is that banks will remain at the heart of financial service provision and the trusted custodian of (financial) data. But we need to consistently challenge our business models and provide additional services that wrap around our core banking offerings, all with a razor-sharp focus on one element: the customer.

1.

Executive summary

The flourishing data economy, the emergence of FinTech and BigTech firms in the traditional banking space and the growth of the crypto-assets market all promise a new era for the financial industry, bringing fresh competition, improved client service and innovative financial products. More fundamentally, these trends could also alter incumbent players' business models and even financial market structure. Regulation will play a key role in shaping the face of this newly emerging landscape, defining the trajectory of change

In the first edition of this paper released last year,[1] we outlined the regulatory environment – and the challenges within it – pertaining to the use of artificial intelligence (AI), open application programming interfaces (APIs), cloud and blockchain. These technologies were selected for their potentially transformative effect on financial services – much of which can be attributed to their ability to enable more effective collection, storage and analysis of the vast and rapid flow of data.

However, the capabilities of these technologies will not be exploited to their full potential without rich and relevant data sets (or Big Data), nor without clients having sufficient trust to share their data with their service providers.

Big Data fuels the so-called "data economy" – the first topic of this year's edition. The data economy is a digital ecosystem where data is collected, analysed and exchanged between governments, companies, or other parties for the purpose of creating value for businesses and individuals. Big Data is the basis upon which advanced analytics operate, which in turn can drive insights and improved client experience, uplifting the provision of financial services. The winners of the data economy will be those that can best bring such benefits to clients, improving their businesses and saving them money. Given the prize at stake – and the cost of falling behind – the importance of data collection, storage and analysis will therefore only rise.

In this respect, data localisation requirements and the confinement of clients' data to individual services providers are a clear hindrance for the financial industry, significantly limiting the depth of data sets for analysis and painting an incomplete picture of clients' needs (which makes crafting bespoke solutions more difficult).

While Open Banking initiatives have helped greater data sharing in the financial industry, they have their limitations: namely they omit from scope data stored with other private companies (for example, platform businesses of BigTech companies) which could otherwise enrich the analytics and, ultimately, the provision of banking services.

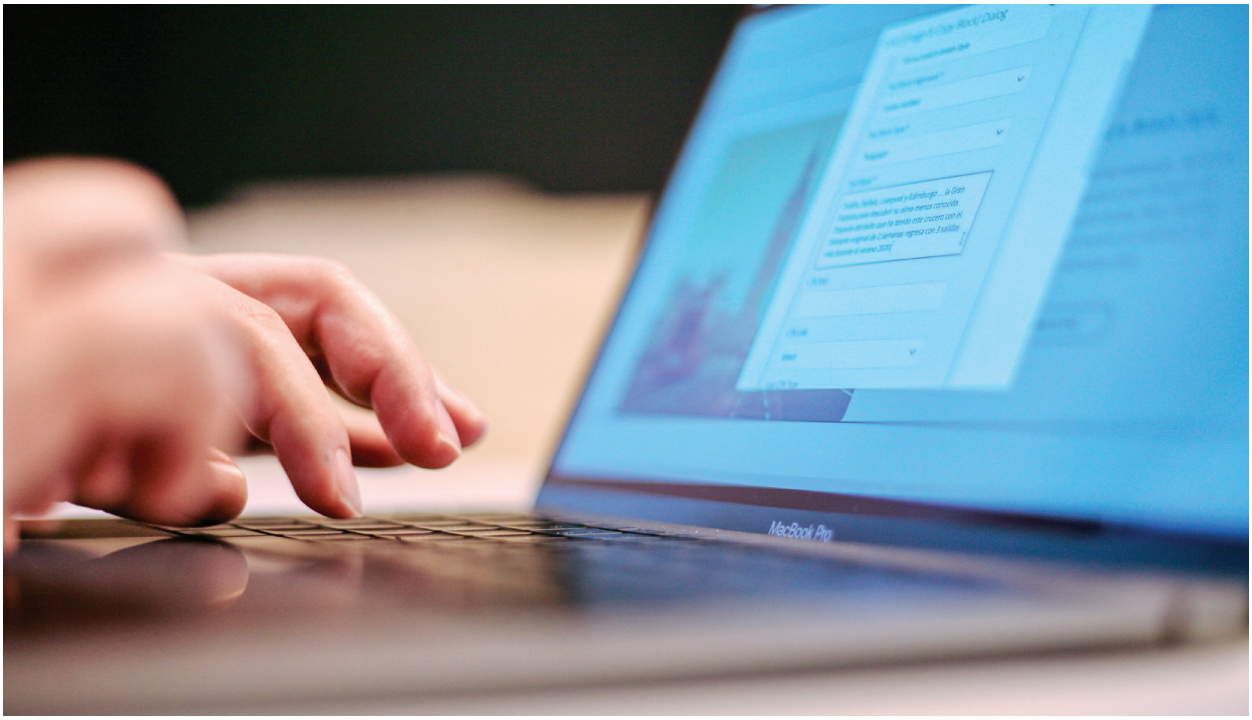
As this issue becomes more prominent and important, regulators will likely face demands to lift such barriers – in a manner that ensures the protection of clients' rights and the security of their data. Marrying the competing demands for further opening-up of data with those for data privacy will require a delicate approach, and the creation of a regulatory environment that builds trust in data sharing and usage.

Arguably, some of the most advanced at consolidating, analysing and using clients' data have emerged from other industries – BigTech companies. As they turn their attention to financial services – using deep pools of customer data to craft bespoke solutions – the industry faces a potential game-changer. With deep pockets and an even deeper understanding of the needs of digital native clients, they raise the bar of what is expected from banking services.

At the same time, this paper highlights that the interaction between BigTechs and incumbent banks runs much deeper than simply competition. They are both mutually reliant on each other for service infrastructure – whether this be payment rails or cloud services, for instance. This interaction plays a precious role in the financial industry, driving competition, innovation and improved client services – all priority areas for regulators. Yet, the very distinct business models employed by BigTechs in financial services (which rely on the "data-network-activity loop") also trigger regulators' vigilance around potential gaps, particularly when it comes to competition and data protection rules.

The third transformative trend we assess in this year's paper is the evolution of the crypto-assets market. Although the volumes of initial coin offerings (ICOs) or payments in crypto-assets still pale in comparison to traditional methods of capital-raising or payments facilitation, forward-thinking regulators have already made their moves to provide much-sought-after regulatory clarity to set the path for the market's development.

The extent to which all these trends shape the financial industry will depend on how regulators seek to balance the obvious opportunities against the potential risks. The financial industry should not wait for regulators to show their hand – it will need to adapt to these new realities immediately by leveraging innovative technologies to create bespoke solutions and bring additional value to clients. With high levels of client trust and years of financial service experience, banks are well-placed to take on this challenge.



2.

Data economy

2.1 Introduction

When compact discs replaced the floppy version in the late 1980s, some data scientists considered that the age of "Big Data" had begun. Yet, today, the term is now attached to data sets so large they cannot be captured, stored, managed or analysed using traditional databases[2] – something that would have been unimaginable two decades ago.

Big Data is fuel for the so-called "data economy", a digital ecosystem where data is collected, analysed and exchanged between governments, companies, or other parties for the purpose of creating value for businesses and individuals.[3] In the data economy, data is treated as an asset that has value, and can potentially be traded.

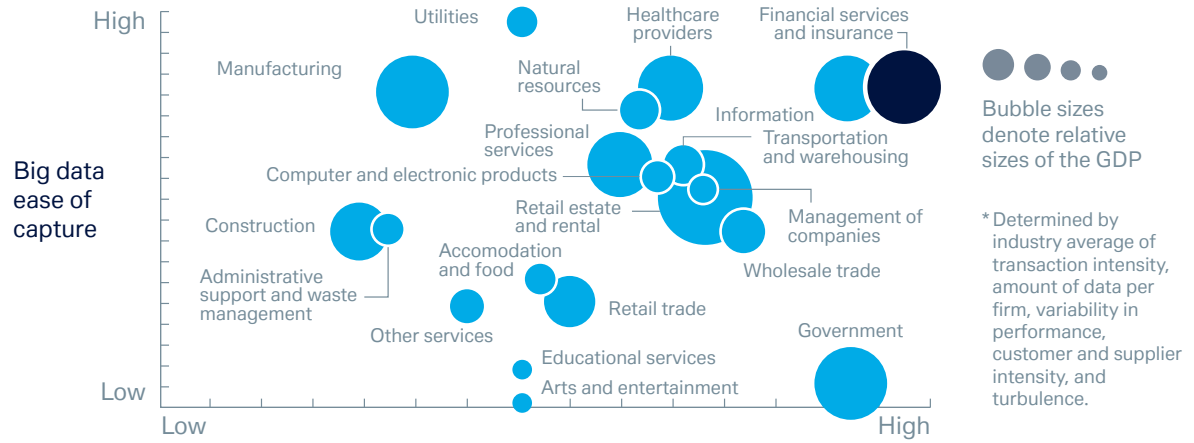
In a perfectly functioning and efficient data economy, data would be allowed to flow freely between parties in order that it can be utilised for the benefit of data subjects (essentially those whose data is being collected, held or processed) in terms of better service provision, or for the benefit of users in terms of profit generation. There would also be mechanisms in place to ensure the safe and compliant use of data, with technological architectures such as data lakes for its collection and storage across geographical boundaries and jurisdictions.

The data economy in the European Union (EU) was valued at €300bn in 2016, equivalent to around 2% of the region's GDP.[4] The European Commission (EC) predicts this could rise to almost €750bn next year, if backed by favourable policy and technology investment.[5] The data economy in the UK alone could be worth almost £100bn in 2025, which would constitute an increase of a third from 2016 values.[6]

In financial services, the benefits that can be derived from the evolving data economy are clear: a better understanding of and response to customers' needs, enhanced cybersecurity and reduced risk (especially around fraud and malicious activity). Indeed, financial services is as well-placed as any industry to benefit from Big Data (see Figure 1), with the Centre for Economics and Business Research (CEBR) valuing this benefit at £7bn a year for the retail and investment banking and insurance industries.[7] A case study on China's financial sector by Boston Consulting Group estimates that AI and Big Data will generate a 38% productivity increase within 10 years, equivalent to a 27% reduction in hours worked.[8]

Figure 1: Impact of Big Data on financial services compared to other industries

Big data and advanced analytics will affect virtually every part of the economy, especially financial services



Source: McKinsey[9]

It is very likely that the winners in the new digital banking landscape will be defined by those that can best collect, manage and analyse data to uplift client service. The ability to do this hinges on three factors: first, the availability of digitised data; second, the use of Big Data analytics empowered by AI and cloud computing power; and, third, the ability to manage data in a secure and compliant way.

In this respect, banks will go head-to-head with BigTech firms that have already made significant moves to harvest data from their non-financial services operations as a shot-in-the-arm for their ambitions in financial services.[10] Clearly, having a more rounded picture of clients' behaviour outside of their financial service use has value in terms of tailoring products and services within it. When combined with the latest technologies to process this data – such as AI and cloud technology – it becomes an even more powerful proposition.

Yet the data economy remains in its nascence, with its long-term success dependent upon the availability of data, where the free flow of data across borders, data sharing, trust and control from both data subjects and data users are crucial elements.

Currently, data sets about the same firm or person are spread across many companies. When a consumer uses banking services to, say, purchase a table or order a dinner, information about these transactions are stored with different companies. None have the full picture. The insights from consolidating data sets across many companies could potentially drive further benefits, such as providing customers with bespoke banking solutions. Furthermore, banks could use a more holistic understanding of clients to inform payments processing and compliance requirements.

> " There are numerous payments-based use cases in a world with more open data. For instance, using data to pre-validate beneficiary account information seamlessly and upfront. The intent is to allow banks to rectify any inaccurate or missing information instantly, thus removing friction in the payment. The second area is case resolution, which helps settle problems of missing regulatory and compliance information. This will free up messages for faster processing and help ensure regulatory issues are corrected on the payment chain"
>
> *Craig Young, Chief Information Officer, SWIFT*

Thus, the continued growth of the data economy relies on data being available for governments, financial institutions, and corporates to access and use. While Open Banking initiatives, driven by regulation, constitute a significant step forwards, governmental or other private companies are not required to similarly disclose their vast data pools – a hindrance to an open data economy.

Further, data will need to not only flow freely between market participants, but also across borders. The inability to move data from one country to another significantly limits the depth of data sets for analysis.

Finally, without trust the data economy will not thrive. Barely a week goes past without news of a corporate data breach, fuelling mistrust of how, and for what purpose, service providers use client data. Only when consumers are confident that the use, analysis and safety of their data will provide benefits without harm, and that their privacy will be protected, will society be in a position to realise the full potential of the data economy.

2.2. Regulatory overview

The success of the global data economy is underpinned by three critical factors: the ability for data to flow unrestricted across borders; the availability of data for re-use by the public and private sector for data subjects' benefit; and trust and control from data subjects that their data is protected (analysed and used in an ethical manner, for example) in order that they are prepared to consent to its sharing.

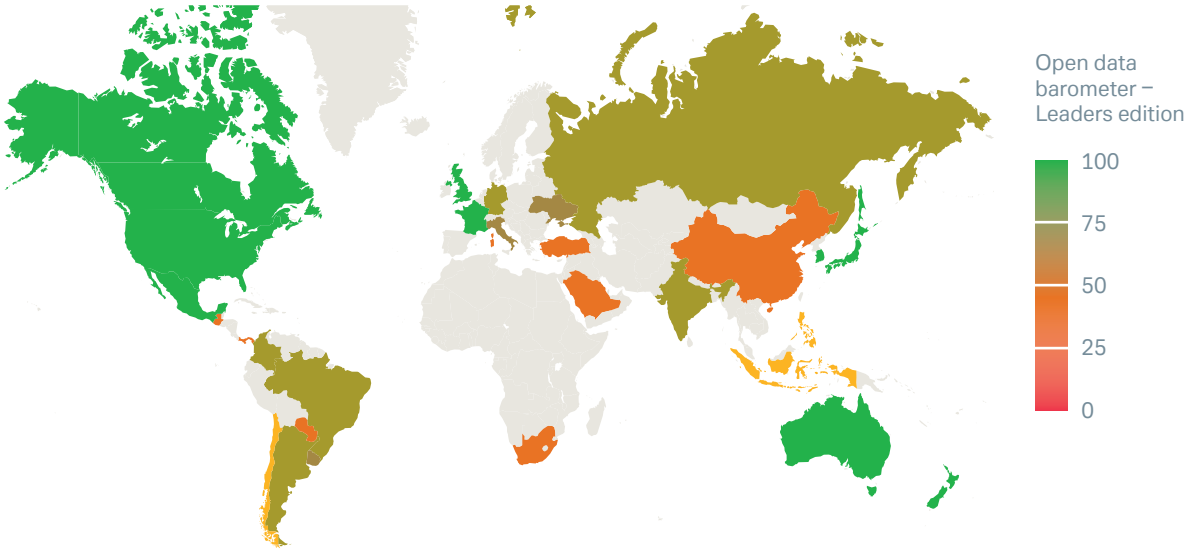
Barriers to the free flow of data globally remain in the form of data localisation requirements. Having said that, in some jurisdictions regulators are working on reducing its impacts by implementing regional solutions and international agreements (see regulatory challenges section for details). By making clients' banking data available to third-party providers (TPPs) via Open Banking initiatives, regulators have provided a boon to data sharing. Indeed, these initiatives have spread across a number of regions from Europe to Asia-Pacific (for more information on Open Banking initiatives globally, please see the first edition of this whitepaper[11]).

When considering the issue of data availability, Australia stands out for the scale of its ambitions, with its Consumer Data Right Act (CDR) set to extend beyond the sharing of just banking data. While CDR will start with banks - the government concluded its consultation on the Open Banking initiative in July 2019[12] – it will ultimately apply to the energy and telecommunication sectors as well.

Building on this broader issue of open data, the EC has led the charge in promoting the opening up of public sector data for use by all, including for commercial reasons. In April 2018, as part of its Digital Single Market strategy, it proposed revisions to the Public Sector Information Directive (PSI Directive) – a legal framework to allow the re-use of public sector information. Adopted on 20 June 2019, once implemented by Member States it will make public sector and publicly funded data re-usable.[13] Further, the EC has also made access to and re-use of private sector data a major cornerstone of a common European data space, working on producing further guidance for private sector data sharing.[14]

The Open Data Barometer[15] — a global measure of how governments are publishing and using open data for accountability, innovation and social impact — suggests that the majority of governments have advanced new and improved open data policies and practices over the past five years. The Barometer places Canada, the UK, the US (which established an Open Data Policy in 2013) and Australia as the most open data economies (see Figure 2).

Figure 2: Level of data openness by country



Source: Open Data Barometer[16]

Policies promoting the opening up of data are somewhat futile, of course, if subjects do not feel comfortable sharing it or participating in its monetisation. In recent years, regulators have made significant strides towards ensuring data protection and inherent controls, especially in Europe, where General Data Protection Regulation (GDPR) has harmonised and augmented data protection regulations. Regarded by some as the global standard for personal data privacy and control, its introduction in 2018 has catalysed similar regulation across the globe.

Yet, the evolution of new technologies and, in particular, the broadening use of AI for Big Data analytics, has brought other areas of regulation under the spotlight. Notably, regulators across various jurisdictions have recently started to consider the idea of "trustworthy" use of AI, which goes beyond just data privacy. The EC's High-Level Expert Group on AI (EC HLEG) produced the Ethics Guidelines for Trustworthy AI in April 2019, following up with policy recommendations in July 2019. Further, the Monetary Authority of Singapore (MAS) also released a set of principles in November 2018 (the FEAT principles) to promote the ethical use of AI and data analytics.[17]

With respect to financial services, the Alan Turing Institute and the Financial Conduct Authority (FCA) have launched a joint year-long project around the industry's use of AI, with a focus on analysing ethical and regulatory questions in order to advise on potential strategies for addressing them – placing particular importance on transparency and explainability of AI.[18]

Going even further in an attempt to take a holistic approach, the UK government announced its intention to develop a National Data Strategy to support the UK in building a world-leading data economy (June 2019).[19] The strategy will help ensure that all citizens and organisations trust the data ecosystem, are sufficiently skilled to operate effectively within it, and are able to access high-quality data when they need it.

It is not just the UK that realises the importance of this debate. The Singapore government has similarly been notable in its efforts to establish a data economy. In May 2019, for instance, the Personal Data Protection Commission (PDPC) introduced a number of initiatives to further drive organisations to shift from compliance to accountability in the management of personal data.[20]

So, while the data economy continues to grow, its success will depend on addressing the remaining challenges relating to data localisation laws, data availability and addressing regulatory gaps for unethical use of data/AI.

2.3. Key regulatory challenges

2.3.1 Data localisation

Why does it matter?

The free flow of data across borders is a fundamental building block for the data economy, enabling the establishment of comprehensive, rich, and – crucially – global data pools. The ability to consolidate data across multiple jurisdictions becomes even more important for financial institutions with global outlooks: only by pooling all client data across geographical jurisdictions can they gain a holistic insight into clients' behaviours and tailor banking products accordingly.

In this case, the existence of data localisation rules – under which both personal and corporate data could fall – are a significant impediment. In some jurisdictions, these restrictions take the form of requirements that explicitly mandate local storage of information through data protection laws; in others they are driven by data security laws, professional secrecy rules and outsourcing rules.

Another issue stemming from data localisation rules is the obstruction to financial institutions adopting a consistent, enterprise-wide and global approach to data storage and management, limiting their ability to benefit from universal technological solutions. Further, this can drive diverse practices relating to information security and governance.

Data localisation rules also could potentially hinder financial institutions providing standardised services on a cross-border basis – and, of course, tailored local solutions could mean higher costs.

Latest developments

In a major step forward, the EU passed regulation concerning the free flow of data allowing companies and public administrations to store and process non-personal data wherever they choose in the EU, with it coming into force in May 2019.[21] However, a number of sector-specific data localisation laws continue to exist in some countries, especially in the area of cloud outsourcing. Germany's financial regulatory authority, BaFin, for instance, has requested the disclosure of the

location of data centres (at least by city), which necessitates storage of data in the cloud in a specific location.[22]

The more comprehensive data localisation laws have appeared outside the EU, however.

> " While some countries impose a blanket ban on the transfer of all data categories, others – such as Australia and South Korea – impose specific restrictions on the transfer of data in very specific sectors (including finance) on grounds of protecting citizens' sensitive data"
>
> *Julian Cunningham-Day, Partner, Linklaters*

In China, there has been a flurry of regulation in recent years seeking to control the export of data to other jurisdictions. The most prominent example is its cybersecurity law which requires network operators to store domestically "personal information" or "important information" collected or generated in China.[23]

In some jurisdictions, there has been the creation of data localisation rules specifically for financial services. For instance, in April 2018 the Reserve Bank of India (RBI) ruled that payment systems providers operating in the country must localise all data relating to their payment systems, including end-to-end transaction details.[24] Other financial services hubs such as Singapore and Hong Kong also place certain restrictions on regulated firms performing offshore processing, by imposing obligations on the firms to seek legal opinions and regulatory undertakings in the offshore locations.

In Europe, organisations can transfer personal data outside of the EU without any further safeguards being necessary, to a country that benefits from a so-called "adequacy decision", which confirms that such countries offer an adequate level of data protection (Japan, Canada, Switzerland or New Zealand, for example).

International efforts are also being made to break down barriers in certain areas (such as the Global Forum on Transparency and Exchange of Information for Tax Purposes, and the Financial Action Task Force).

> " There are some precedents for mitigating the impact of data localisation restrictions, whether this be via a relaxation of professional secrecy laws (seen in Luxembourg and elsewhere via international pressure and court action, such as impact of IRS claims on Swiss secrecy rules), creation of regulatory safe harbours for data pooling by banks (the Patriot Act in the US and state-sponsored financial information units in various markets such as India, for instance) or the removal of export authorisation requirements pursuant to GDPR (in Germany, Italy and Luxembourg)"
>
> *Julian Cunningham-Day, Partner, Linklaters*

Potential solutions

Although some degree of regulatory convergence and interoperability is achievable through adequacy decisions or trade agreements, there are limited ways in which countries are managing to work around the more generic localisation rules. Technological solutions therefore hold much appeal.

> " Most banks with operations in countries with data localisation rules are setting up mirrored data storage facilities to enable the bank's local entities to offer their local regulators access to domestic data"
>
> *Julian Cunningham-Day, Partner, Linklaters*

When it comes to storing data in the cloud, as one example, cloud service providers have devised technological solutions to meet localisation requirements. For instance, they offer their global footprint of data centres in order to store data within domestic borders while still maintaining a single solution for accessing and analysing data.

2.3.2 Data availability

Why does it matter?

The data economy lives or dies by the availability of data. In the financial industry, deeper and richer data pools mean greater input for analysis by AI, deeper insights and more accurate understanding of client needs, fuelling tailored banking products and, ultimately, better service.

Such enhanced service provision is not possible, however, if data exists in silos with no regulation existing to make it available for use by not only the company that stores such data, but also other companies that could re-use it to benefit the subjects of data. This issue becomes particularly pertinent in instances where data sets about the same client (whether an individual or a firm) are spread across various institutions. Consolidation of such data sets becomes highly problematic, given that there is currently no single regulatory tool across the industries that requires the holders of client data to disclose it. Above all, this harms data subjects, which miss the opportunity to receive benefits from enriched analytics showing a holistic view of their true needs.

While there are a few solutions in the arsenal of regulators, none of these currently provide a universal approach to enabling the subjects of data to transfer all data sets about them from one institution to another. Instead, regulations have only gone so far as to establish frameworks for mandatory disclosure of specific information by designated companies.

For instance, data portability rules embedded within data protection laws (such as GDPR) enable individuals to request receipt of their personal data, and to transmit it between organisations (the data controllers). However, as data privacy rules only apply to personal data, portability requirements do not extend to data on individuals that does not fall within that definition, nor to company data (only in a restricted number of countries do these rules extend to other forms of data). The lack of common standards further hinders efficient data portability.

Another regulatory tool, Open Banking, constitutes a step in the right direction, but has its limitations too. As the requirement to disclose clients' banking data (subject to their consent) to TPPs extends to banks only, it leaves data stored with other institutions outside of the requirement. In particular, such rules do not extend to governmental or non-bank private companies (for example, platform businesses of BigTech companies) that hold huge data sets which, if shared, could provide significant insights that could benefit the provision of banking service to clients. In addition, by only mandating banks – and not other companies providing only selected banking services – to open-up data, Open Banking potentially creates an uneven playing field.

Latest developments

Calls from regulators and government bodies for greater data availability have grown louder over the course of 2019. The EC has recommended data availability to support innovation,[25] while the PDPC of Singapore has been consulting on data portability and data innovation provisions as part of its ongoing review of its data protection act.[26]

A few other interesting initiatives of note are the plan by the Hesse state government in Germany to create a data-pooling platform in Frankfurt (to strengthen Frankfurt's position as a financial centre of innovation) and the plan to create an open platform in the UK in order to boost access to finance for small-to-medium-sized enterprises (SMEs) – mentioned in the Bank of England's (BoE's) response to the Future of Finance report.[27]

Data availability and data sharing were also mentioned by the UK's Digital Competition Expert Panel as a means for ensuring the country's competition framework is fit to face the economic challenges posed by digital markets[28].In a similar vein, Germany has also created a new advisory body – the Commission Competition Law 4.0 – tasked with proposing reforms to competition law to better support digital innovation and associated changes in market structures.

Potential solutions

Data portability measures driven by privacy policies go some way to establishing the degree to which data subjects can share their data. Extending data portability requirements to data on firms and non-

personal data on individuals would be one way forward. Complementary to this could be to apply Open Banking frameworks to mandate other institutions (private or public) to disclose the data on their clients (subject to client consent). Not only would this allow companies to generate insights for better banking services, it would also firmly place the control over data in the hands of the subjects (the clients).

While industry-led initiatives can hit the ground running far quicker, they are limited in what they can do given that they require voluntary participation. As we have witnessed with Open Banking, regulatory initiatives may take longer to implement, but constitute a much more powerful tool, introducing legally binding obligations that provide an efficient solution for secure data sharing.

With the need for further regulatory developments, however, there is a way to go before such solutions are implemented and break-down existing data sharing barriers.

2.3.3 Liability for unethical use of data/AI

Why does it matter?

Access to data allows companies to use it as a basis for further analysis – often using AI. But unless clients feel comfortable that their data is going to be used to their benefit in an ethical and trustworthy way, they will not feel confident sharing it. As AI technology develops at breakneck speed, and crunches an increasingly vast amount of Big Data, it is inevitable that disputes will arise. Therefore, clearly defining the liability for unethical use of clients' data is crucial for fostering trust in AI analytics.

Some liability for the unethical use of data is already covered by existing regulation (such as data protection, consumer protection, and competition/trade laws). However, given that AI remains a relatively new phenomenon, there is an emerging concern that clients' data (whether customers' or businesses') may be used for AI analytics in a way that would be considered unethical. And while such use may not contravene existing regulation or laws, it can still be harmful for subjects of data (such as unfair, deceptive practices, or unjust bias in AI systems' decisions).

Defining liability, even where guiding regulation exists, is made challenging by a number of factors.

Many companies are moving away from expensive proprietary technology development towards the use of applications available as a service. AI is no different. Yet, when AI is outsourced, you could very easily end up with extremely complex supply chains, which muddies the water when it comes to making the assessment of liability.

The global nature of AI adds an additional layer of complexity. As data sets for AI analytics are collected and analysed across the world, the liability could be defined by the laws of multiple countries. Whereas country-specific liability for breaches of data protection rules would normally be linked to the entity in charge of data processing within its borders, some rules (particularly privacy rules in Asia and South America) can apply extra-territorially.

This means that the liability position can vary greatly between jurisdictions, making it complex for subjects of data to understand the potential protections they can rely upon when it comes to unethical use of their data. This also creates some challenges for the firms employing AI solutions.

> " The lack of harmonisation in the approach to the regulation of AI makes it hard for firms to adopt effective global standards and to quantify their risk of rolling out AI innovations internationally"
>
> *Julian Cunningham-Day, Partner, Linklaters*

Latest developments

Regulators across various jurisdictions have taken a particular interest in moving beyond existing regulations (such as data privacy) in order to ensure trustworthy use of AI.

In particular, the EC HLEG produced the Ethics Guidelines for Trustworthy AI in April 2019,[29] providing guidance around the definition and principles for the trustworthy use of AI – a first step towards defining a firm framework.

This trend is happening globally. In Singapore, MAS released a set of principles in November 2018 to promote fairness, ethics, accountability and transparency (FEAT) in the use of AI and data analytics.[30] Similarly, the UK established the Centre for Data Ethics and Innovation in March 2019 – an independent advisory body set up and tasked by the UK Government – to investigate and advise on maximising the benefits of data-driven technologies.[31]

Following the development of guidelines for trustworthy AI, regulators in Europe are now considering whether there are policy gaps that need to be addressed. The HLEG's second deliverable – "AI policy and investment recommendations for Trustworthy AI", published in June[32] – suggests considering if there is a need for wide-ranging policy adjustments. These span all the way from civil liability considerations (ensuring adequate compensation in case of harm, including potential introduction of mandatory insurance) to ensuring that criminal liability can be attributed for unethical use of AI. The recommendations also suggest considering whether there is sufficient protection against cybersecurity risks posed by AI system, and the adequacy of enforcement mechanisms against discriminatory outcomes.

The HLEG also specifically suggests considering the "volume of data or incumbency data advantage", including, for example, anti-competitive behaviour, or abuse of dominant position.

Regulatory initiatives around the ethical use of data and AI remain in their nascence, however, with little-to-no mandatory requirements. Although the HLEG's second deliverable is a positive step, their role is only to provide recommendations – it will be the regulators, of course, that will decide if and how they apply them.

Potential solutions

When a new technology emerges it brings the temptation to introduce specific regulation to mitigate the risks it might potentially bring with it.

Yet technology often moves on before the regulation is formed. To ensure the rule making is an efficient process, before any legislation is implemented, there should be a proper impact assessment of possible scenarios.

For this reason, at the initial stage it is more effective to stick to principles-based, technology-agnostic regulation which in the future could then form more specific guidance and targeted enforcement – allowing flexibility as the risks continue to be better understood.

2.4 The road ahead

The rapid transformation towards a data economy shows no signs of abating. Far from it in fact: appetite for data collection is burgeoning while technology development focused on driving data insights continues at pace across industries.

This is particularly noticeable in banking, where we expect the competition for data, use of AI and cloud solutions to continue on its upwards trajectory. With new market entrants putting data at the core of their businesses, banks will continue to explore how they can best use Big Data and advanced technologies to provide bespoke services to clients in order to maintain a competitive edge.

A growing ability to consolidate data from various sources – which could be driven by technological innovation or more readily available data across jurisdictions – would be a game-changer. Open Banking initiatives which require banks to share certain clients' data with TPPs should be considered only the start of the journey. There are many miles ahead. Empowering banks and other companies to use data sets held by firms across various industries should be the next milestone for regulators – and one which would greatly enrich data analysis.

With data localisation rules remaining a barrier for the meantime, financial institutions will seek technological solutions that allow them to make the most of the data they store across the globe, while maintaining compliance with requirements across jurisdictions. However, given that such solutions only partially address the issue, the pressure will remain on regulators to establish the necessary legal rails to enable data to flow freely across borders.

As the data economy lives or dies by the availability of data, the value of that data will continue to rise. This will give significant clout to the subjects of that data: the clients themselves. They will decide who they empower with their data, and how – and at what value – they want to be compensated doing so.

This makes the establishment of the necessary legal tools to facilitate clients sharing their data a key focus for regulators and companies going forward. This will see the benefits of greater data portability explored more and more in the finance industry as a tool that enables clients to share their data in order to benefit from enhanced financial services.

At the same time, new technologies such as AI are transforming how data is utilised, which potentially brings new and unexpected risks specific to the technology. This places the issue of trust at the heart of the debate: only if clients have trust that AI systems for data analytics are built, governed and used in a trustworthy way, with the necessary legal protections in case something goes wrong, will they share the necessary data to fuel the data economy.

While regulators will continue their work in assessing how best to ensure the trustworthy and ethical use of data, avoid data privacy breaches and anti-competitive behaviours, it will be down to individual industries to retain the trust of clients when it comes to data use. In this respect, the banking industry's long legacy of trust puts it in good stead.

3.

FinTech and BigTech companies in the financial industry

3.1 Introduction

Corporate history shows that most industries experience long periods of calm before being suddenly and swiftly disrupted by new technology. There are few better examples than what is currently happening to the finance industry with the rising prominence of FinTechs, and the emerging role of large established technology companies, or BigTechs. Whether in the form of delivering services and technology infrastructure to banks, or financial services to clients, the penetration of FinTechs and BigTechs in financial markets has been remarkable.

FinTech	FinTech firms focus on technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.
BigTech	BigTech firms are large technology companies that expand into the direct provision of financial services or of products very similar to financial products.

Source: FSB report on FinTech and market structure in financial services[33]

According to KPMG, global investment in FinTech companies reached an astounding US$111.8bn last year,[34] with the size of FinTechs growing in step.

The impact of FinTechs and BigTechs on the financial industry is most visible in the area of collaboration with incumbent financial services providers. In fact, KPMG reports that one quarter of banks already partner with BigTechs, and another quarter plan to do so in the near future; while over half already partner with FinTech start-ups.[35]

Bank-FinTech partnerships are particularly prominent in the field of payments: Deutsche Bank, for instance, last year took a stake in payments technology start-up ModoPayments to provide new digital payment functionalities and extend its payments ability into non-bank platforms such as Alipay, Paypal, M-Pesa and WeChat.[36]

In the supply chain finance (SCF) space, it is not unusual for banks to outsource the administration and onboarding of suppliers to a platform provider while retaining the KYC element and providing their balance sheets for financing.[37]

Cooperation also takes place with respect to data storage and analytics. In particular, the increasing use of cloud services and AI platforms are two of the most prominent ways in which FinTech and BigTech firms have become enmeshed with the financial industry, making them vital to certain banking operations. The BoE's "Future of finance" report cites Finastra data that suggests 30% of financial institutions in the UK and 33% in the US have begun the process of moving their payments or collaboration workflows to the cloud, while institutions in Singapore lead the way at 42%.[38]

By providing near-unlimited hardware and software resources on a global and pay-as-you-go basis, cloud computing is driving down costs and creating greater flexibility to respond to change. This allows technology infrastructure to be scaled up and down as required, and drive new products to market.

> " As more and more banks shift to the cloud, they're looking for partners on many fronts – not only to help provide frictionless payments but also to help enable and strengthen the security of those networks"
>
> *Craig Young, Chief Information Officer, SWIFT*

This service dependence is reciprocal, of course. Even though some of the largest BigTech companies (such as Facebook, Google and Amazon) offer financial services, including payments, money market funds, and credit, they still require the services of traditional banks to help facilitate this (unless, of course, they are a licensed bank themselves).

While collaboration is one storyline, another is competition. Many FinTechs and BigTechs have established strong footholds in niche markets by "unbundling" traditional financial services – relying on regulatory frameworks that allow the provision of certain banking services without the need for a full banking license. In this respect, FinTech firms – of which there are many examples – have typically focused on areas such as platforms for peer-to-peer lending, payments and digital wallets solutions. BigTechs have also targeted payments business – with Google Pay, Amazon Pay, Apple Pay and payments on Facebook Messenger all being good examples – although there are signs that they may continue to broaden their sights within financial markets in future (take Facebook's Libra initiative for instance).

According to the European Banking Authority (EBA), payment and settlement business lines of banks are most affected by FinTechs' activities.[39] Indeed, in the UK, today, 45% of lending to UK-based companies comes from market-based finance, compared with 37% in 2006, according to the BoE.[40] Echoing this, PwC estimates that FinTechs are contesting nearly a quarter of banking revenues – and expects similar trends to play out across the insurance and wealth management segments.[41]

In time, BigTechs may prove equally as disruptive as FinTechs, although in a different way. The BoE's "Future of finance" report notes that currently BigTech firms are only dipping their toes in financial waters; the implications if they dive in could be profound.[42] As opposed to FinTechs, most BigTechs have significant balance sheet strength and access to an extensive client base – allowing them to bolster their core product offering with add-on financial services. It is also worth noting that BigTechs often do not play by the same "rules" as incumbents – they challenge and at times ignore established workflows, in order to force tectonic shifts in business models. This creates a new trend in terms of how clients interact with the financial industry.

To get a feel for this, you only need to look at the retail banking space, where BigTechs are already starting to provide financial services to clients, often wrapped within their more traditional business offering. Over 33 million users have made a purchase via a "Pay with Amazon" button, for instance.[43] In Asia, the world's largest financial service firm, China's Ant Financial, an affiliate of technology Alibaba group, now has over one billion clients – without a single bank branch.[44] Alipay, the online payment platform of Ant Financial, conducts over a third of all Chinese electronic payments, while WeChat Pay, which falls under the Tencent umbrella, accounts for 15% of the same market.[45]

The financial industry will almost certainly be affected in other ways too: it is interesting to see, for instance, how increased choice has already raised clients' expectations, particularly for fast, intuitive and digitally-enabled financial products.

> " It is worth considering how customer expectations have changed — especially in areas such as the demand for fast frictionless payments — as a by-product of competition, technological innovation, the larger role of cloud computing and open banking. While we can see much disruption, I also think it's creating a number of new opportunities for businesses to drive value for customers and put a new focus on challenges, such as trust, safety, and security"
>
> *Craig Young, Chief Information Officer, SWIFT*

The benefits of this evolving landscape of collaboration, reciprocal service dependency and competition go beyond merely greater efficiency and convenience. Competition promotes the drive towards digitalisation in the industry and spurs innovation – as such, the creation of new types of products and uplifted client experience may be the most valuable outcome. For the most part it is a virtuous circle: what is good for the client is good for the industry.

3.2 Regulatory overview

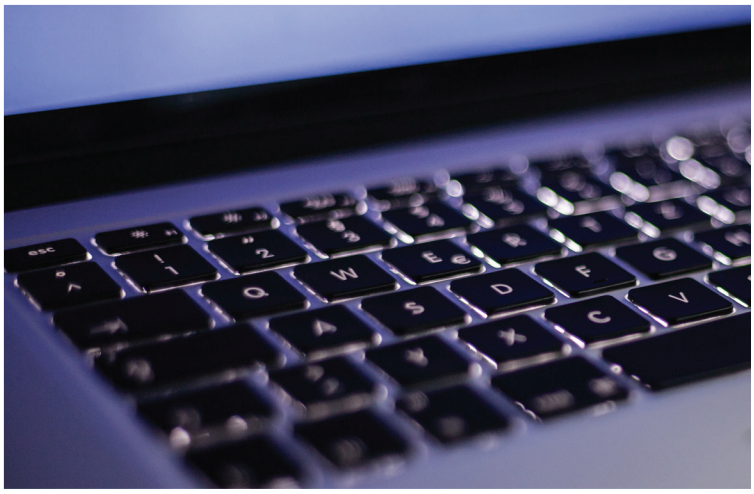
The emergence of FinTech and BigTech in financial services has not gone unnoticed by regulators and little wonder – these new entrants bring numerous potential transformations for financial markets. In support of this, authorities in key geographies have all announced clear intentions to drive innovation: in Europe it is the FinTech Action plan,[46] in the US it is the Treasury Report on "Nonbank Financials, Fintech and Innovation",[47] and in Asia it is both the RBI's "Report of the Working Group on FinTech and Digital Banking"[48] and the New Era of Smart Banking initiative in Hong Kong.[49]

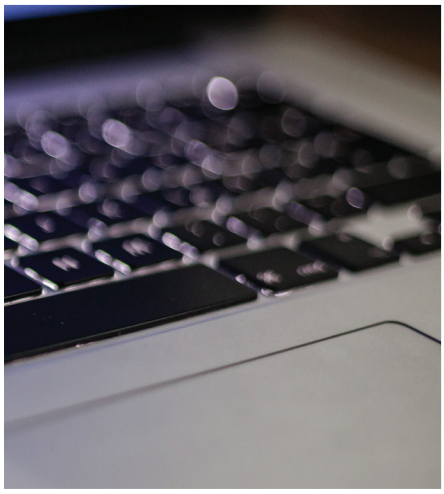
Meanwhile, regulators have also introduced a range of licensing regimes to allow the provision of selected financial services by FinTechs without a need for a full banking license. These include licences and authorisation for such activities as European "Reg-lite" activities (such as credit broking), e-money issuance, and platform businesses.

At the same time, the global spread of Open Banking initiatives has moved certain FinTech activities from unregulated to regulated; TPPs under Payment Services Directive 2 (PSD2), for instance. Several jurisdictions have also put in place a regulatory framework specifically for FinTech credit through new forms of licences for FinTech platforms.[50]

With the new types of FinTech activities emerging in the market, we should not expect this movement to slow over the coming years. A Basel Committee on Banking Supervision (BCBS) survey, cited by the FSB, indicated that "nearly half the regulatory authorities surveyed are considering new regulations or guidance related to Fintech services."[51] These regulations are likely to be very targeted, however.

> " I don't think there will be much more regulatory focus on existing FinTech areas, such as licensing, which are more or less fit for purpose. Instead, the focus will very quickly shift to the issue of crypto-assets and ICOs, and the types of products and firms existing in that space"
>
> *David Ostojitsch, Director, AFME*





The European Securities and Markets Authority (ESMA), in its report on licensing of FinTech business models,[52] suggests that "the primary area where regulatory gaps and issues have been identified by national competent authorities (NCAs) and where FinTech firms do not fit neatly within the existing rules is related to crypto- assets, ICOs and distributed ledger technology (DLT)". The report concludes that this will need to be monitored, assessing whether adaptations to the EU legislative framework are required given emerging innovation.

Special licensing regimes are just one of the tools regulators have at their disposal to promote FinTech innovation. Other tools include innovation hubs, which bring FinTechs together with regulatory experts that provide guidance on FinTech-related issues,[53] and regulatory sandboxes, which create an environment for firms to test innovative financial products, services or business models.[54] These are proving popular approaches: to support innovation in cross-border solutions, for instance, a group of international organisations (including regulators) established the world's first international sandbox – the Global Financial Innovation Network (GFIN) – in January 2019.[55]

While regulators are upbeat in terms of their plans for fostering further innovation in financial services through supporting new participants, they are also vigilant to potential risks driven by certain imbalances or gaps in the current regulatory frameworks applicable to FinTechs and BigTechs.

The list of regulatory and supervisory responses to such risks lengthens by the month. The European Banking Authority report on the impact of FinTech on incumbent credit institutions' business models (July 2018),[56] the FSB report on "FinTech and market structure in financial services" (February 2019),[57] and the chapter in the report of the Bank for International Settlements (BIS) on "Big Tech in finance: opportunities and risks",[58] all consider the interaction models of banks and FinTechs, and more broadly examine the drivers and implications of the growth of FinTech and BigTech in finance.

In general, the influence is seen as positive by the regulators, driving innovation and new solutions, with the impact on financial stability deemed to be negligible at present. That said, as BigTechs begin to play a bigger role in the financial industry (through provision of cloud services to banks or financial services to retail or corporate clients, for example), this assessment could rapidly change.

Some regulators have already voiced a number of emerging competition concerns. Notably, in Europe, the EC released a report on "Competition policy for the digital era".[59] They suggest, among other things,

that there might be a need to provide more guidance to firms on what constitutes pro-competitive data pooling and where a dominant firm could be expected to provide data access, potentially under some form of data portability. Greater data availability was also one of the proposals put forward by the UK's Digital Competition Expert Panel for ensuring the country's competition framework is fit for purpose in the context of the digital areas.[60]

3.3 Regulatory challenges

3.3.1 Introduction of new business models

Why does it matter?

By adding financial service provision to their more traditional product offerings, BigTech firms (particularly platform providers) have had a noticeable impact on financial markets and gained market share. Yet, while BigTechs may provide traditional banking services to clients (in areas such as payments and lending), they have very distinct, and often unique, business models.

In particular, there is an emerging view that the effects of the "data-network activities loop",[61] which uniquely underpins BigTech's business models, could potentially bring new risks for the users of their platforms and for the market more broadly. The concern centres on whether the current regulatory environment accounts for such business models; or if there rather is a regulatory gap open to exploitation when it comes to competition and data protection. Clearly, such a gap would result in an uneven playing field in the financial markets playing out negatively for customers.

Recent developments

BigTechs' expansion into financial services has driven regulators to more deeply analyse the specifics of their business models in order to assess the potential impact on the financial industry and its clients.

For instance, the FSB report on FinTech and market structure in financial services notes that BigTechs' competitiveness hinges on their ability to access and process data – a crucial commodity for their service.[62] In many cases, an observed phenomenon is customers providing personal data in exchange for receiving the services offered by BigTech firms, instead of paying fees (as mentioned by the FSB).[63] This data is then used by BigTech firms for cross-selling for their other business lines.

The BIS chapter on BigTech in finance goes further along this line of thinking and suggests that the uniqueness of business models of BigTech platforms is underpinned by data analytics, network externalities and interwoven activities (termed "DNA" by the BIS)[64] which drives a "data-network activities loop".[65] Within this, each of the elements reinforce each other: a user's benefit from participating on one side of a platform (for example, as a seller on an e-commerce platform) increases with the number of users on the other side (buyers); this then generates more data which can be analysed to enhance existing services and attract further users. By offering financial services (such as payments and lending) BigTechs can further reinforce the loop.

While recognising that BigTechs' DNA can lower the barriers to provision of financial services and as such enhance financial inclusion, the BIS stresses that this may come at the expense of increased risk, such as anti-competitive use of data, or biases caused by sophisticated algorithms used to process personal data.

In alignment with this view, the FSB report suggests that there is a risk that "while BigTech firms could represent a source of increased competition for incumbent financial institutions, in some scenarios, their participation may not result in a more competitive market over the longer term", as it is evidenced in China where two firms account for 94% of the overall mobile payments market.[66]

Similar concerns have been echoed by the EC in its report, "Competition policy for the digital era",[67] which was published in April 2019 and assesses the risks to competition across different industries that could be posed by dominant digital platforms and ecosystems. Data bottlenecks are identified as something that, if not cleared, could impede effective competition. The EC thus indicates that "mandated data access may sometimes be needed".

> " The regulatory focus will increasingly turn to BigTechs and their use of data. And at that point it will become about the concentration and the transparency of it. An important development here would be the adoption of the Digital Services Act, which will introduce the liability rules when it comes to operation of digital platforms. Generally, the regulators need to make sure the competitive landscape is maintained and that there is a level playing field between new entrants and existing players"
>
> *David Ostojitsch, Director, AFME*

Reflecting on the new phenomena of BigTech business models, BIS concludes that the entry of BigTechs into financial services may require a far more comprehensive and coordinated response from regulators across industries, assessing aspects relating to competition, data privacy, as well as financial services considerations.

Potential solutions

First things first: regulators will need to understand whether current regulatory mechanisms are effective and armed with the tools that enable necessary safeguards against the potential risks posed by emerging business models.

Yet given the complex and cross-sectoral nature of the new phenomenon, it will require efforts and collaborative work from different regulatory bodies. At the national level, this will require the alignment between competition authorities, financial regulators and data protection supervisors, given the interdependencies of potential effects of this trend, and that altered policy in one area might have a knock-on effect elsewhere. The same goes for cross-border co-ordination, which is going to be another important focus given the global nature of many BigTech firms.

Above all, if innovation and competition are to be supported, there should be a well-balanced use of policy tools by regulators focused on these endeavours.

3.3.2 Financial stability

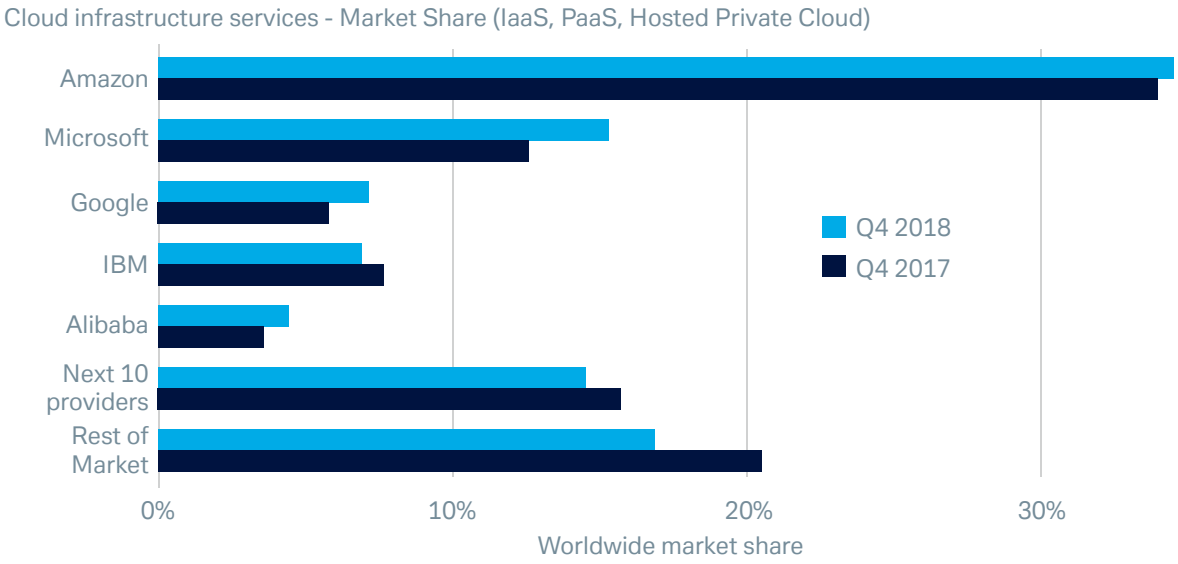
Why does it matter?

It is widely recognised that the move to the cloud brings great benefits to financial institutions and their clients, with enhanced cyber resilience perhaps the most significant of these (see the previous edition of this whitepaper for more information[68]).

Regulators around the world have implemented a number of outsourcing guidelines with the aim of ensuring controls over external service and cloud providers are maintained to the same standard and high level of security as those over banks' own operations. Without doubt, this goes some way towards ensuring the resilience and stability of the market.

As the market matures, there are an increasing number of financial institutions relying on cloud providers for their core business operations. Given that the cloud services market is dominated by a few large firms (see Figure 3)[69], this raises concerns with regulators about the dependence on a small number of critical suppliers,[70] which potentially makes them significant market participants and infrastructures within the EU financial sector. Such a concentration of business with a select number of cloud providers increases the inter-connectedness in the financial system, potentially making them a single point of failure if one were to be subject to a serious breach.[71]

Figure 3: Market share in cloud infrastructure services



Source: Synergy Research Group

Recent developments

Regulators continue to review cloud outsourcing requirements to take account of market changes and acknowledge concerns about the criticality of cloud providers to the financial industry as a whole.

Particular attention from the likes of the BCBS and International Organization of Securities Commissions (IOSCO) is being devoted to the issue of third-party dependencies. In alignment with this, the EBA has also raised concerns around the concentration risk at the industry level.[72]

The FSB Financial Innovation Network (FIN) plans to further explore third-party dependencies in cloud services and single-point-of-failure risks (including, lock-in risk and cross-border issues).[73]

Echoing these plans, the European Supervisory Authorities (ESAs), in their joint advice to the EC on ICT risk management, advised the Commission to consider establishing an oversight framework for monitoring critical service providers to the extent that their activities may impact financial institutions.[74]

Potential solutions

As regulators worldwide assess the need to adjust existing regulatory frameworks to address the concentration and growing inter-connectedness of cloud providers with financial markets, there is a risk that new regulatory requirements – if implemented without proper analysis of the potential impacts – could have unintentional negative impacts on the financial industry.

One the one hand, regulators need to ensure that the financial markets are not threatened by new types of risks – meaning ensuring the existence of all necessary regulatory tools ready for immediate reaction in case such risks were to emerge.

At the same time, it is crucial that the introduction of any regulation is aligned with that concerning the provision of cloud services to other industries, so as not to impact market competition and choice for financial institutions. The worst-case scenario would be that regulatory changes make the provision of cloud services to financial institutions less attractive to cloud providers when compared to other industries, affecting their appetite for that line of business.

> " It's not impossible that some of the BigTechs could consider exiting financial services long-term. Alternatively, they may scale-back. Either way, there would be some kind of knock-on effect for the banks"
>
> *David Ostojitsch, Director, AFME*

To avoid such unintended consequences, it is therefore crucial that any adoption of new rules is preceded by a proper consideration of the emerging risks against the efficiency of the existing rules. Giving a full and thorough consideration of the probability of a BigTech failure, especially given how important cyber security and contingency are for BigTech cloud providers, would be a good area to start.

Lastly, considering the cross-border nature of cloud services, international alignment will be crucial to ensuring a level playing field, where financial institutions in all jurisdictions can have equal access to the best cloud services.

3.4 The road ahead

The role of FinTech and BigTech in the financial industry will only gather momentum. The interactions between incumbent banks and new entrants will continue to deepen, driving further innovation in the banking sector and enhanced services to clients.

Recognising the benefits this trend brings to the financial industry, regulators across the globe have a keen interest in supporting it. Frameworks provisioned by regulators, such as innovation hubs and regulatory sandboxes, will move the needle and act as an accelerator for bringing innovative solutions to the market.

While unleashing the upside of innovation, regulators will also have the downside firmly on their radar: particularly the growing dependency between the financial market and new entrants, with cloud services being watched the closest. Given the increasing concern that the supply of these services will be concentrated with just a few large cloud providers, issues surrounding financial stability and the potential development of a new single point of failure will lead the discussion.

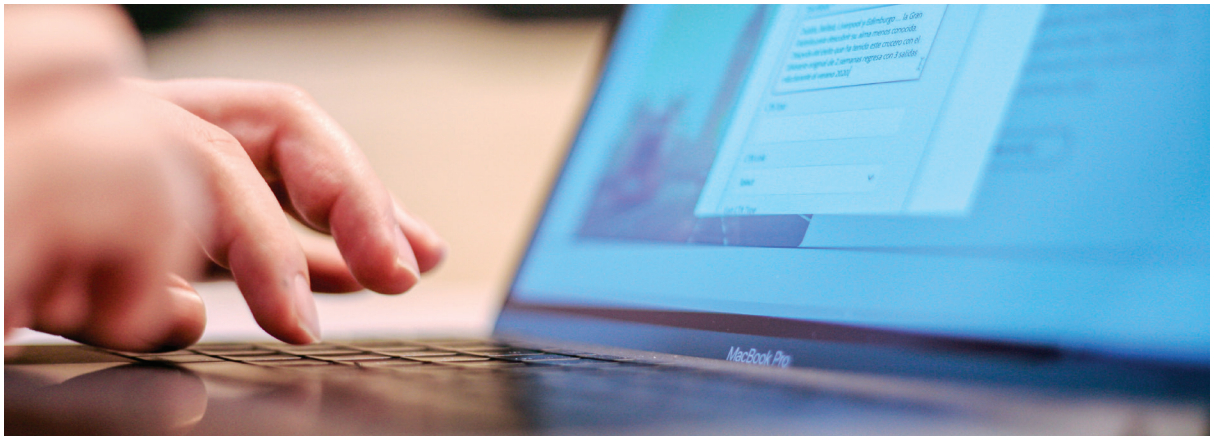
Yet, dependencies will grow in both directions. Just as banks will increasingly turn to technology specialists to provide solutions to underpin their operations, so FinTech and BigTech will remain dependent on incumbents, with traditional bank accounts and payment systems remaining at the core of how they build their financial products offering.

This spirit of collaboration will clearly not stop the lure of competition. BigTechs will continue to target niche banking services in payments, or lending for retail and SME clients – using this add-on to

enhance the potential of their main business activities. FinTech firms too will go ahead enjoying the benefits of licensing frameworks allowing the provision of selected financial services without a full banking license. This will be further supported by evolving regulatory licensing regimes that facilitate a move away from "one-shop, one-stop" banking services in favour of partial (or unbundled) products and services – something that will allow FinTechs and BigTechs to pick-and-choose offerings that best suit their business proposition.

There are numerous ways in which the growing presence of new entrants in the financial industry will play out. And policy makers at the national and global level have already carried out research into the subject, exploring various outcomes of the interactions currently being observed. As the picture continues to take shape, the regulators' vigilance will grow, paying close attention to the impacts these developments would have on financial stability, competition and clients' protection.

But no matter how this all unfolds, the focus of the financial industry will remain on clients; ensuring that banking products maintain pace with innovation and the evolving (often demanding) client expectations. Clients will therefore be the ultimate winners.



4.

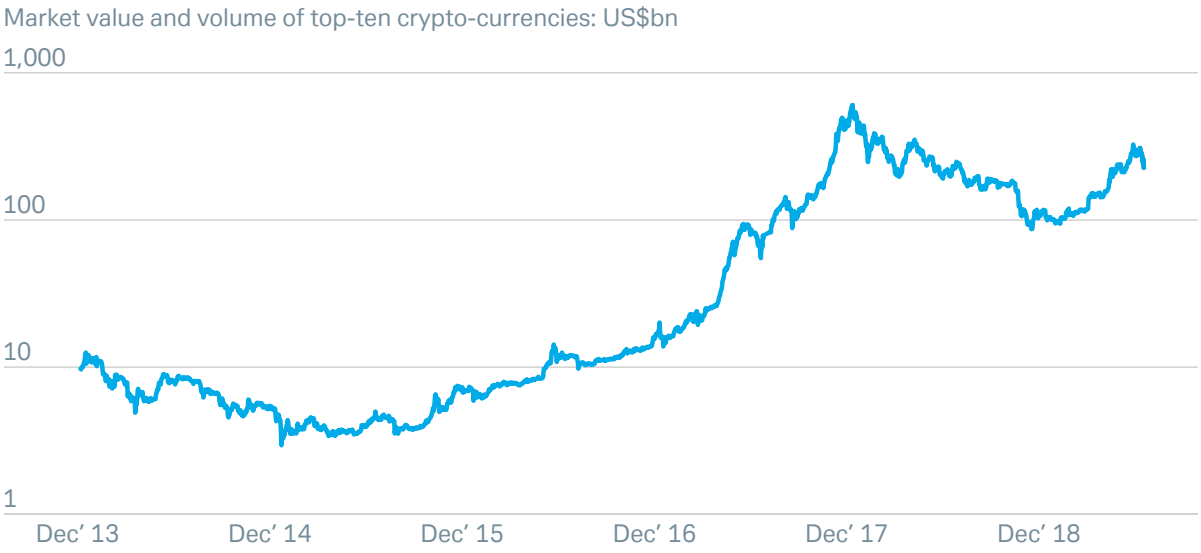
Crypto-assets

4.1 Introduction

What are crypto-assets?	There is no single agreed definition of crypto-assets. For the sake of simplicity, this paper generally uses the umbrella term of "crypto-assets" to define cryptographically secured digital representations of value or contractual rights that are powered by forms of distributed ledger technology (DLT) and can be stored, transferred or traded electronically.[75]
What are cryptocurrencies?	Cryptocurrency is a type of crypto-asset, which typically does not provide rights, but is used as a mean of exchange – for example, to enable the buying or selling of a good provided by someone other than the issuer of the cryptocurrency, or for investment purposes or for the storage of value.[76]

There has been much speculation as to the role and impact of crypto-assets in the finance industry – no surprise given that there are now more than 2,000 crypto-assets[77] and the top ten cryptocurrencies have a market capitalisation of nearly US$230bn (as at July 2019), a twentyfold increase since December 2013 (see Figures 4 and 5).[78]

Figure 4: Market capitalisation and transactions of the top 10 cryptocurrencies



Source: Coinmarketcap.com[79]

Figure 5: The top 10 cryptocurrencies by market capitalisation (US$bn)

Bitcoin	168.8
Ethereum	22.5
XRP	13.2
Litecoin	5.7
Bitcoin Cash	5.2
Tether	4.0
EOS	3.5
Binance Coin	3.0
Bitcoin SV	2.2
Stellar	1.7
TOTAL	229.8

Source: Coinmarketcap.com at 18 July 2019

This speculation proposes numerous scenarios. One of the most oft-cited is the idea that, if domestic cash and electronic payment instruments gave way to cryptocurrencies for retail payment transactions, there could be tangible consequences for monetary policy and economic activity. The ability of central banks to control inflation is linked to their management of the supply of money. Yet, the decentralised nature of global cryptocurrencies places them outside of the control of national central banks – the supply of bitcoin, for instance, is governed by algorithms that release according to a strict implementation.

This means that, if such cryptocurrencies become widely established as a payment tool, central banks would be forced to factor them into their monetary policy decisions – yet without the necessary mechanisms to influence their supply, this could undermine the effectiveness of monetary policy. Similarly, the supply of a cryptocurrency created by a private company could mean that company ultimately having an impact on the overall "money supply", leaving domestic economic performance dependent upon the flows of such cryptocurrency. For instance, if launched, Facebook's Libra would be a practical test of this scenario: a potentially global payment tool used by people in their everyday lives which would be managed by a non-governmental organisation.

On a more positive note, crypto-assets have the potential to support innovation and drive efficiency, with another scenario seeing crypto-assets fostering greater financial inclusion, particularly in emerging markets. High barriers to entry of traditional capital-raising methods exclude many small firms that are unable to meet the criteria. Crypto-assets could present an alternative mean of capital raising, bringing into scope a broader universe of potential investors and opening-up financing to more businesses and individuals.

Yet the reality is that while ICOs have grown in popularity – some of the largest blockchain start-ups obtained as much of 87% (or US$3.3bn) of funding from ICOs in the first quarter of 2018[80] – volumes remain low when compared to more traditional methods.

Crypto-assets are yet to experience widespread adoption for payments too. There are still fewer than 600 independent retailers in the UK that will even accept the most popular, bitcoin, for

instance.[81] The slow speed of transaction processing appears to be one of the main reasons behind sluggish uptake. BitPay, the world's biggest bitcoin payment processor, reported just over US$1bn in transactions last year, which pales in comparison to Visa, which processed US$11tn worth of transactions in the same period.[82]

There are numerous other practical challenges to the greater acceptance of crypto-assets. Price volatility and high conversion fees (from fiat currency into cryptocurrency) are one set. The associated cyber-security risk, with the potential for hacking and theft, is another. Indeed, there have been a few high-profile incidents already: in May 2019, one of the most popular crypto-exchanges, Binance, announced that hackers had exploited a security lapse and stole US$40m worth of bitcoin (the company's insurance fund covered the losses).[83] In total, about US$1.7bn worth of cryptocurrency was stolen from exchanges or scammed from investors last year.[84]

Separately, crypto account holders can potentially face unprecedented risks, incomparable to any other asset class. For example, in Canada, customers of failed crypto-exchange QuadrigaCX lost access to their assets in January 2019 after the chief executive passed away without leaving the passwords to the digital keys.[85]

While regulators have made a significant effort to greater clarify the regulatory environment for crypto-assets, uncertainty and gaps remain. Inevitably, this has left many market participants adopting a "wait-and-see" strategy.

4.2 Regulatory overview

Crypto-assets' reputation amongst investors, as well as their portrayal in the press, has tended to seesaw between over-enthusiasm and outright denunciation. The situation has not been helped by lack of clear guidance when it comes to legal status of these assets, protections available to investors in crypto-assets and requirements related to Anti- Money Laundering (AML) and Know-Your-Customer (KYC). However, this is now changing.

In the past few years, regulators have been largely focused on raising awareness around potentially adverse effects and threats associated with crypto-assets. There are numerous examples of this globally: ESMA issuing a statement on the risks posed by ICOs in November 2017,[86] the US Securities and Exchange Commission (SEC) releasing a statement warning that investors in crypto-assets should be "wary" in December 2017,[87] a speech by MAS on "The Good, The Bad, and The Ugly" of crypto-assets in March 2018,[88] and the FSB report on financial stability implications of crypto-assets from October 2018.[89]

However, more recent regulatory reports and guidance have shifted the conversation, potentially catalysing a major change in the industry's perception of crypto-assets.

Recognition by governments that crypto-assets can be used to support innovation is broadening. The UK's Cryptoassets Taskforce suggests that, when used for capital raising, crypto-assets can: support innovation and competition; improve efficiency; address financing gaps; and build new investor bases.[90] In the US, the SEC has noted that ICOs "can be effective ways for entrepreneurs and others to raise funding."[91] Meanwhile in Japan, the Financial Services Agency has encouraged innovation by allowing the virtual currency industry to self-regulate.

In Europe, ESMA and the EBA produced two separate reports in January 2019 bringing much sought-after clarity as to the regulatory rules in securities and payments applicable to certain types of crypto-assets. Both reports indicated gaps in the current regulatory framework, while also creating an expectation that they will be addressed within the coming years. In individual European countries there have also been a number of important developments (such as in Gibraltar, Malta and Germany – to name but a few).

In the UK, the regulatory position is becoming much clearer too, aided by the UK Cryptoassets Taskforce report,[92] the guidance from the FCA on the regulatory status of crypto-assets[93] and the transposition of AMLD V (following consultation by HM Treasury)[94] as well as guidance from HMRC on the application of corporate tax rules to crypto-assets.[95] Together, these steps may go a long way towards reducing the uncertainty concerning regulation of crypto-assets in the UK.

The US position on crypto-assets can be seen as welcoming, providing they are compliant with applicable laws and regulations (notably securities laws for investment tokens). In April 2019, the SEC released a framework for assessing whether a blockchain-issued token constitutes an investment contract, and hence subject to securities laws.[96]

To casual observers, these developments may appear insignificant. But, they may have far-reaching effects. Regulatory uncertainty has been one of the biggest barriers to widespread uptake of crypto-assets by the markets – removing this will allow the industry to undertake proper due diligence on crypto-assets, driving a more accurate assessment of the various risks and legal rights associated with investment.

At the same time, even though these initiatives provide considerably more solid foundations, it is recognised that there are numerous topics to be addressed consistently at a global level to make crypto-assets a cross-border success. The classification, and therefore legal treatment, of crypto-assets and professional activities associated with it tops the list. In May 2019, the FSB produced a report outlining the potential gaps in regulatory approaches to crypto-assets globally, with work continuing at numerous global organisations (such as the BCBS, the Committee for Payments and Market Infrastructures and the Financial Action Task Force (FATF)).[97]

Once defined at a global level, it would be up to national regulators to implement respective recommendations and standards into national laws. Although this certainly constitutes a move in the right direction towards global alignment, practice shows that without a strong commitment from national authorities, the road towards harmonisation can be long and arduous.

4.3 Key regulatory challenges

4.3.1 Classification of crypto as an asset class

Why does it matter?

It is fair to say that the complexity and speed of change within the crypto-asset market has given regulators plenty of food for thought.

Fundamentally, many are genuinely new kinds of digital assets that do not fit straightforwardly into regulators' traditional asset definitions. While some might show one or more features of a traditional asset class (such as a share or e-money), others do not.

This poses a number of practical challenges: the definition of asset class informs the legal rights attributable to it and the legal protections the asset owner can rely on, which form the cornerstones upon which investment decisions are made. Also, this would be particularly important for investment funds which face strict rules on the types of asset classes in which they can invest.

Latest developments

Some jurisdictions – such as China – have negated this issue by introducing bans on ICOs, while others – such as the US – have opted for expansive definitions of financial instruments that serve to bring crypto-assets under the scope of existing regulation. Other jurisdictions, notably Malta and Gibraltar, have gone further, building specific regimes which effectively allow the regulator to rubber-stamp cryptocurrency businesses.

In Europe, as well as other jurisdictions, regulators have made attempts to define the regulatory perimeter and which types of crypto-assets fall in and outside of this. While a sensible approach, it is the nuances of the definitions that perhaps cause most challenges for investors, issuers and intermediaries operating within the crypto-assets space.

Crypto-assets, according to recent guidance from European regulators EBA and ESMA, may – depending on their characteristics – be defined as "electronic money" or "financial instruments" and as such fall under existing payments or securities regulation respectively.

In the field of payments, the EBA report explains which crypto-assets qualify as "electronic money" and fall within all respective rules provided to such asset class under the electronic money directive (EMD2) and under PSD2.[98]

Working hand in hand with EBA, ESMA's report[99] explains that crypto-assets can qualify as transferable securities or other types of "financial instruments" under the Markets in Financial Instruments Directive (MiFID). If so, a full set of EU securities market rules would apply, including the Prospectus Directive, the Transparency Directive, MiFID II, the Market Abuse Directive, the Short Selling Regulation, the Central Securities Depositories Regulation and the Settlement Finality Directive.Unfortunately, however, a crypto-asset may just as easily fall outside of the definition of a financial instrument under MiFID – and here is where a key challenge arises.

> " The onus is on issuers and any intermediaries to decide whether a crypto asset is regulated. For example, if you are issuing a security token, you might fall within scope of the Prospectus Rules – and it is a criminal offence not to comply with them. If you are intermediating a security, then you might be carrying out the regulated activities of dealing, arranging or safeguarding, or if you are running a trading platform, you might need to be regulated as an operator of a multilateral trading facility (MTF; a European regulatory term for a type of regulated financial trading venue). For e-money issuers, that's also a licensable activity under EMD2 and if you are a payment service provider, you will need to be licensed under PSD2. And it's been very difficult because regulatory requirements underpinning these regimes typically are not drafted to deal with these types of assets"
>
> *Stuart Davis, Senior Associate, Latham & Watkins*

Even though certain crypto-assets may fall under the microscope of MiFID, the interpretation (and transposition into national laws) of MiFID rules by member states may be different, leading to a disparity in regulatory classification of a number of existing crypto-assets (as found in a survey of EU NCAs conducted by ESMA last year).[100]

On a practical level, this means that the same crypto-asset can be classified as a share in one European country – and be subject to the regulatory regime attributable to shares (e.g. legal rights certified by shares, issuance of shares, investor protections) – while falling outside of the regulatory perimeter in another. Not only does this create the potential for regulatory arbitrage, it also limits the ability of issuers and investors to benefit from a single European capital market.

Although the US has taken a similar approach focusing on classification of crypto-assets,[101] it faces the same question – how will this classification correlate with the classification under European law, and thus what will it take for issuers and investors to benefit from listing of crypto-assets (financial instruments) in the US and Europe?

Another set of challenges arise for those crypto-assets that do not fit into any regulated asset class category. ESMA concludes that "there are a wide range of crypto-assets being issued and only a fraction of them are likely to qualify as MiFID financial instruments",[102] whereas the EBA states that a "significant portion of activities involving crypto-assets do not fall within the scope of current EU financial services law (but may fall within the scope of national laws)".[103] The FCA adds that certain crypto-assets (such as so-called "utility tokens") are likely to fall outside the regulatory perimeters provided for electronic money or financial instruments.

This creates a practical regulatory challenge: outside of the existing regulatory perimeter there are no rules that would give clear guidance around issuance of such crypto-assets, nor rules that would provide similar protections for investments into them as provided for financial instruments, for instance.

While this does not hinder investment in, or use of, such crypto-assets completely, the inability to assess the regulatory and legal risks will cut the appetite of many, and potentially cut off a substantial number of traditional investors with deep pockets.

Potential solutions

Crypto-assets, due to the nature of their underlying technology (blockchain), might have specifics which are different from traditional financial instruments or e-money. Yet, any new regulations should attempt to create a level playing field for all financial instruments or e-money regardless of whether they are issued as crypto-asset or in another form. For instance, requirements designed specifically for crypto-assets (such as additional information requirements or restricted sale to retail investors for blockchain-based financial instruments) should address only new risks (if any) attributable specifically to crypto-assets, bearing in mind that any differences may potentially drive a misconstrued perception that a financial instrument issued on a blockchain is riskier than one issued on another medium.

Extending the existing rules to crypto-assets that do not fall within the perimeter is another approach.

And, finally, it is crucial that all of this is coordinated at a global – or at the very least, regional – level.

> " It is very difficult for institutional businesses to provide a full cross-border crypto-asset service: without further harmonisation, in the EU alone you need to comply with 28 different regimes. That would be extremely complicated and time-consuming"
>
> *Stuart Davis, Senior Associate, Latham & Watkins*

Aware of this, ESMA has expressed concern around bespoke regimes of some member states, claiming that it hinders the establishment of a "homogeneous framework across the EU"[104] – a framework which would set the path forward for the European crypto-assets market.

The UK Cryptoassets Taskforce also considers that an internationally coordinated approach would help mitigate risks to UK consumers – many of whom invest in crypto-assets through firms based outside the UK. This issue is one that would affect all countries, of course, and not just the UK.[105]

Together, these steps may go a long way towards increasing certainty and global alignment of regulating crypto-assets, which could potentially open them up to more mainstream investors.

4.3.2 Investor protection

Why does it matter?

Fraudulent activity and cybercrime occur frequently with respect to crypto-assets. In the UK alone there were 203 reports of crypto-asset scams between June-July 2018, with victims reportedly losing over £2m in total (according to data from Action Fraud, the national fraud and cyber-crime reporting centre).[106] Evidence also suggests there is a particularly significant risk of fraudulent activity associated with ICOs: one study suggests a quarter of ICOs could potentially be fraudulent,[107] with many cases of issuers not delivering the anticipated product or service.

This raises specific concerns relating to investor protection, notably around: difficulties in assessing crypto-assets' fundamental value; the buying of unsuitable products; and the buying of products while being unaware of the associated risks.

By clarifying the different types of crypto-assets, regulators have partially addressed this issue. As explained in the previous section, those assets that fall within the existing regulatory perimeter of a known asset class can benefit from the respective protections provided by law: risk disclosures requirements; appropriate risk management; segregation of assets; conflicts of interest rules; advertising rules; compensation schemes; and complaints handling procedures.[108]

The challenge however comes for those crypto-assets which fall outside of the protections afforded to financial instruments or e-money. In these instances, the investor cannot rely on these protections to be guaranteed by law and thus be available to them in case something goes wrong – naturally, this increases risk. The same issue would arise in the event of bankruptcy or the hacking of a crypto-asset service provider.

Latest developments

In addition to the broad reports from ESMA and EBA, discussed earlier, some jurisdictions within Europe have devised their own solutions.

In the UK, the regulatory position is becoming much clearer and may well be fully settled by 2020. The regulators plan a consultation in 2019 to further explore this issue and assess whether an extension of the regulatory perimeter is required to cover crypto-assets that do not fall within the securities or payments regulations.[109] Subject to the outcomes of this consultation, it stands ready to legislate to redefine and expand the perimeter if necessary.

Potential solutions

Bringing regulatory clarity and setting mandatory compliance rules is one way of fostering investor protection. Another way is to adopt voluntary disclosure and code of ethics type regimes. In France, for example, the PACTE draft bill was adopted on 11 April 2019 – once enacted, the law will mean that an ICO issuer can sign up to a voluntary regime, agreeing to comply with principles set by the regulator around issues such as disclosure and obligations to investors.[110]

This may also be a solution for misalignment of regulatory frameworks globally – establishing such a voluntary regime at the international level could be a significant step forward for the whole industry.

4.3.3 AML and KYC

Why does it matter?

When it comes to AML obligations of providers of crypto-asset services, a key issue centres on customer due diligence and proving a client's source of wealth, or origin of its assets. This requirement derives from the general rules within the Anti-Money Laundering Directive (AMLD).

However, there are a number of challenges when applied to crypto-assets. First, crypto-assets on permissionless networks are by nature anonymous. While public addresses and associated transactions can be tracked in the network, the address cannot be easily linked to anyone's personal identity.

Second, there are a multitude of ways in which crypto-assets can be bought or transferred. Not all of these are through structured exchanges with strict KYC processes; some are completely decentralised, with no central source of control and oversight, and are simply executed via smart contracts.

Using these exchanges, an investor could receive crypto-assets into its wallet and would find it challenging to prove the source of those funds. That provides a significant problem if that same investor were then to try and sell them on a cryptocurrency exchange which was required to prove the source of wealth of clients.

Latest developments

This is a worry that is seemingly coming to fruition. In February 2019, the FATF released a set of new draft recommendations on performing due diligence in relation to crypto-assets.[111] Crucially, this brings into play a so-called "Travel Rule".

> " The "Travel Rule" requires exchanges to pass customer information to each other when transferring crypto-assets. The FATF's guidance will require the implementation of additional systems and controls at crypto exchanges and it remains unclear how all participants will comply. In particular, it is not currently clear how crypto exchanges should validate the customer information they receive, and it is not clear how the rules will apply in the context of decentralised exchanges"
>
> *Stuart Davis, Senior Associate, Latham & Watkins*

At European level, AMLD has been recently expanded in scope by AMLD V to cover cryptocurrency exchanges and custodial wallet providers (including the services in relation to crypto-assets that fall outside the regulatory perimeter).[112]

Potential solutions

Effectively, the only solution would be for cryptocurrency exchanges to only on-board clients who can prove that they have only performed transactions on other exchanges that verify all of their users from an AML/KYC perspective. However, investors with a long track-record in crypto-assets will likely have at one point in time traded on decentralised exchanges where no AML or KYC ever took place.

> " This could exclude some substantial holders of crypto-assets from the system. Early adopters of cryptocurrencies, some of whom have amassed significant crypto-assets, would - in the early days of Bitcoin - likely have been trading on decentralised exchanges in a time when AML/KYC standards for crypto exchanges were very different to those in place today"
>
> *Stuart Davis, Senior Associate, Latham & Watkins*

4.4 The road ahead

Without a marked change in regulatory direction, it appears unlikely that we will see a widespread uptake of crypto-assets any time soon.

This is a particularly pressing issue for the type of crypto-assets that strive to become an alternative global payment method. The key barrier remains the lack of alignment across jurisdictions – while in one region a crypto-asset could be treated as payment token, or electronic money, in another the same asset would be prohibited from circulation. But, even assuming greater regulatory alignment is achieved, crypto-assets will still need to be able to scale-up like traditional payment tools and be plugged into existing infrastructure to be considered a solid option for global payments.

These issues will likely restrict crypto-assets as a payment tool to a niche phenomenon for now. Yet, this is not to downplay the potential transformative impact that crypto-assets (representing financial instruments) might bring to securities markets. In Europe, for instance, there has already been major regulatory progress to clarify in which instances a crypto-asset should be treated as a financial instrument – defining the applicable rules when it comes to its issuance and circulation, including the protections that the investors in such crypto-assets can enjoy.

Such certainty brings comfort to investors and financial institutions that might want to purchase or otherwise deal with crypto-assets representing financial instruments. While the ability to list and trade such crypto-assets in numerous countries is similarly undermined by regulatory asymmetries between various jurisdictions, this issue is not too dissimilar to that faced when dealing with traditional securities.

The long-term benefits of crypto-assets remain compelling. Yet, though some jurisdictions are moving in the right direction, the regulatory certainty enjoyed by traditional assets is still not a reality for all types of crypto-assets. This makes dealing in them subject to uncertain risks. Additional steps need to be taken not only by the regulators, but the industry itself. We are therefore only at the beginning of the journey.

5.

Full list of contributors

Polina Evstifeeva, Head of Regulatory Strategy, New Ventures, Corporate Bank, Deutsche Bank

Thomas Nielsen, Head of New Ventures, Corporate Bank, Deutsche Bank

Luke Templeman, Research Analyst, Thematic Research, Deutsche Bank

Stuart Davis, Senior Associate, Co-Chair of Global Blockchain and Cryptocurrency Taskforce, Latham & Watkins

Julian Cunningham-Day, Partner, Global Co-Head of FinTech & TMT sector, Linklaters

Craig Young, Chief Information Officer, SWIFT

David Ostojitsch, Director, Technology and Operations, Association of Financial Markets in Europe (AFME)

Danil Nemirovsky, Senior Engineer, New Ventures, Corporate Bank, Deutsche Bank

James Longstaff, Strategic Intelligence, COO, Deutsche Bank

Jordan Robertson, Strategic Intelligence, COO, Deutsche Bank

References

[1] "Regulation driving banking transformation", Deutsche Bank, October 2018, see https://cib.db.com/insights-and-initiatives/flow/regulation-driving-banking-transformation.htm

[2] "Big Data: how it can become a differentiator", Deutsche Bank, see https://cib.db.com/docs_new/GTB_Big_Data_Whitepaper_(DB0324)_v2.pdf

[3] "The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization", IBM, see https://www.ibm.com/downloads/cas/4JROLDQ7

[4] "Final results of the European Data Market study measuring the size and trends of the EU data economy", European Commission, 2 May 2017, see *https://ec.europa.eu/digital-single-market/en/news/final-resultseuropean-data-market-study-measuring-size-and-trends-eu-data-economy*

[5] "Final results of the European Data Market study measuring the size and trends of the EU data economy", European Commission, 2 May 2017, see *https://ec.europa.eu/digital-single-market/en/news/final-resultseuropean-data-market-study-measuring-size-and-trends-eu-data-economy*

[6] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/%20future-of-finance*

[7] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.pdf?la=en&hash=59CEFAEF01C71AA551E7182262E933A699E952FC*

[8] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.pdf?la=en&hash=59CEFAEF01C71AA551E7182262E933A699E952FC*

[9] Beyond the buzz: Harnessing machine learning in payments, Mckinsey & Company, see *https://www.mckinsey.com/industries/financial-services/our-insights/beyond-the-buzz-harnessing-machine-learning-in-payments*

[10] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[11] "Regulation driving banking transformation", Deutsche Bank, October 2018, see *https://cib.db.com/insights-and-initiatives/flow/regulation-driving-banking-transformation.htm*

[12] "Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking", Australian government, see *https://treasury.gov.au/consultation/c2018-t329327*

[13] "Open data", European Commission, see *https://ec.europa.eu/digital-single-market/en/open-data*

[14] "Guidance on private sector data sharing", European Commission, see *https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing*

[15] "Open data barometer", see *https://opendatabarometer.org/leadersedition/report/#findings*

[16] "Open data barometer", see *https://opendatabarometer.org/leadersedition/report/#findings*

[17] "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", Monetary Authority of Singapore, 12 November 2018, see *https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT*

[18] "New collaboration with the FCA on ethical and regulatory issues concerning the use of AI in the financial sector", The Alan Turing Institute, see *https://www.turing.ac.uk/news/new-collaboration-fca-ethical-and-regulatory-issues-concerning-use-ai-financial-sector*

[19] "National Data Strategy open call for evidence", UK government, 10 June 2019, see *https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence*

[20] "Personal Data Protection Commission introduces three initiatives to strengthen accountability among organisations and encourage data innovation", Personal Data Protection Commission, 22 May 2019, see *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2019/2019-05-22-Media-Release-on-Guide-to-Active-Enforcement-and-Data-Portability-Public-Consult.pdf*

[21] "Free flow of non-personal data", European Commission, see *https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data*

[22] "Cloud computing: Compliance with the supervisory requirements regarding rights of information and audit and ability to monitor", BaFin, 7 May 2018, see *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1804_Cloud_Computing_en.html*

[23] "Overview of China's Cybersecurity Law", KPMG, February 2017, see *https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf*

[24] "Storage of Payment System Data", Reserve Bank of India, see *https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130*

[25] "Competition policy for the digital era", European Commission, see *http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*

[26] "Public consultation on review of the Personal Data Protection Act 2012 – proposed data portability and data innovation provisions", Personal Data Protection Commission, 22 May 2019, see *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Public-Consultation-Paper-on-Data-Portability-and-Data-Innovation-Provisions-(220519).pdf*

[27] "New economy, new finance, new Bank", Bank of England, see *https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report.pdf?la=en&hash=34D2FA7879CBF3A1296A0BE8DCFA5976E6E26CF0*

[28] "Unlocking digital competition, Report of the Digital Competition Expert Panel", UK HM Treasury, 13 March 2019, see *https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel*

[29] "Ethics guidelines for trustworthy AI", European Commission, 8 April 2019, see *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*

[30] "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", Monetary Authority of Singapore, 12 November 2018, see *https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT*

[31] "Centre for Data Ethics and Innovation 2-year strategy", Centre for Data Ethics and Innovation, March 2019, see *https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-cdei-2-year-strategy*

[32] "Policy and investment recommendations for trustworthy Artificial Intelligence", European Commission, 26 June 2019, see *https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence*

[33] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[34] "The Pulse of Fintech 2018 H2", KPMG, see *https://home.kpmg/xx/en/home/insights/2019/01/the-pulse-of-Fintech-2018-h2-infographics.html*

[35] "Forging the future", KPMG, 2017, see *https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/10/forging-the-future-global-fintech-study.pdf*

[36] "Deutsche Bank takes stake in payments technology start-up Modo", Deutsche Bank, 23 August 2019, see *https://www.db.com/newsroom_news/2018/deutsche-bank-takes-stake-in-payments-technology-start-up-modo-en-11663.htm*

[37] "Payables Finance: a guide to working capital optimisation", Deutsche Bank, September 2019, see *https://cib.db.com/insights-and-initiatives/white-papers/payables-finance-a-guide-to-working-capital-optimisation.htm*

[38] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[39] EBA report on the impact of fintech on incumbent credit institutions', Business models, July 2018, see *https://eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf*

[40] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[41] "Redrawing the lines: FinTech's growing influence on Financial Services", PwC, 2017 *https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf*

[42] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[43] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[44] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[45] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[46] "FinTech action plan: For a more competitive and innovative European financial sector", European Commission, 8 March 2018, see *https://ec.europa.eu/info/publications/180308-action-plan-fintech_en*

[47] "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation", US Department of the Treasury, July 2018, see *https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf*

[48] "Report of the Working Group on FinTech and Digital Banking", Reserve Bank of India, November 2017, see *https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF*

[49] "A New Era of Smart Banking", Hong Kong Monetary Authority", 29 September 2017, see *https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml*

[50] "FinTech credit: Market structure, business models and financial stability implications", Financial Stability Board, 22 May 2017, see *http://www.fsb.org/wp-content/uploads/CGFS-FSB-Report-on-FinTech-Credit.pdf*

[51] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[52] ESMA report on the licensing of FinTech business models: *https://www.esma.europa.eu/press-news/esma-news/esma-publishes-report-licencing-fintech-firms-across-europe*

[53] "FinTech: Regulatory sandboxes and innovation hubs" European Banking Authority, see *https://eba.europa.eu/documents/10180/2545547/JC+2018+74+Joint+Report+on+Regulatory+Sandboxes+and+Innovation+Hubs.pdf*

[54] "FinTech: Regulatory sandboxes and innovation hubs" European Banking Authority, see *https://eba.europa.eu/documents/10180/2545547/JC+2018+74+Joint+Report+on+Regulatory+Sandboxes+and+Innovation+Hubs.pdf*

[55] "Global Financial Innovation Network (GFIN)", Financial Conduct Authority, see *https://www.fca.org.uk/firms/global-financial-innovation-network*

[56] "EBA report on the impact of FinTech on incumbent credit institutions' business models", European Banking Authority, 3 July 2018, see *https://eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf*

[57] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[58] "Big tech in finance: opportunities and risks", BIS, 30 June 2019, see *https://www.bis.org/publ/arpdf/ar2019e3.pdf*

[59] Competition policy for the digital era", European Commission, see *https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*

[60] "Unlocking digital competition, Report of the Digital Competition Expert Panel", UK HM Treasury, 13 March 2019, see *https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel*

[61] "Big tech in finance: opportunities and risks", BIS, see *https://www.bis.org/publ/arpdf/ar2019e3.pdf*

[62] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[63] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[64] "Big tech in finance: opportunities and risks", BIS, 30 June 2019, see *https://www.bis.org/publ/arpdf/ar2019e3.pdf*

[65] "Big tech in finance: opportunities and risks", BIS, 30 June 2019, see *https://www.bis.org/publ/arpdf/ar2019e3.pdf*

[66] Competition policy for the digital era", European Commission, see *http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*

[67] FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[68] "Regulation driving banking transformation", Deutsche Bank, October 2018, see *https://cib.db.com/insights-and-initiatives/flow/regulation-driving-banking-transformation.htm*

[69] "Fourth Quarter Growth in Cloud Services Tops off a Banner Year for Cloud Providers", Synergy Group, 5 February 2019, see *https://www.srgresearch.com/articles/fourth-quarter-growth-cloud-services-tops-banner-year-cloud-providers*

[70] "Future of finance", Bank of England, June 2019, see *https://www.bankofengland.co.uk/report/2019/future-of-finance*

[71] "Joint Advice of the European Supervisory Authorities", 10 April 2019, see *https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf*

[72] "Recommendations on outsourcing to cloud service providers", European Banking Authority, 20 December 2017, see *https://eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf*

[73] "FinTech and market structure in financial services", Financial Stability Board, 14 February 2019, see *https://www.fsb.org/wp-content/uploads/P140219.pdf*

[74] "Joint Advice of the European Supervisory Authorities", 10 April 2019, see *https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf*

[75] "Guidance on Cryptoassets", Financial Conduct Authority, January 2019, see *https://www.fca.org.uk/publication/consultation/cp19-03.pdf*

[76] "Report with advice for the European Commission on cryptoassets", European Banking Authority, 9 January 2019, see *https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf*

[77] "Advice: Initial Coin Offerings and Crypto-Assets", European Securities and Markets Authority, 9 January 2019, see *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*

[78] See *https://coinmarketcap.com/*

[79] See *https://coinmarketcap.com/charts/*

[80] "Cryptocurrencies and tokens", ING, September 2018, see *https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf*

[81] "Guidance on Cryptoassets", Financial Conduct Authority, January 2019, see *https://www.fca.org.uk/publication/consultation/cp19-03.pdf*

[82] "BitPay Sees Record Year for Revenue in 2018, with $1 Billion in Transactions", BusinessWire, 16 January 2019, see *https://www.businesswire.com/news/home/20190116005701/en/BitPay-Sees-Record-Year-Revenue-2018-1*

[83] "Binance hackers shift stolen bitcoin, identity still unclear: researchers", Reuters, 9 May 2019, *https://uk.reuters.com/article/us-crypto-currencies-binance/binance-hackers-shift-stolen-bitcoin-identity-still-unclear-researchers-idUKKCN1SF230*

[84] "Cryptocurrency thefts, scams hit $1.7 billion in 2018: report", Reuters, 29 January 2019, see *https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-thefts-scams-hit-1-7-billion-in-2018-report-idUSKCN1PN1SQ*

[85] "Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins", Bloomberg, 4 February 2019, see *https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem*

[86] "ESMA highlights ICO risks for investors and firms", European Securities and Markets Authority. 13 November 2017, see *https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms*

[87] "Statement on Cryptocurrencies and Initial Coin Offerings", US Securities and Exchange Commission, 11 December 2017, see *https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11*

[88] "Crypto Tokens: The Good, The Bad, and The Ugly", Monetary Authority of Singapore, 15 March 2018, see *https://www.mas.gov.sg/news/speeches/2018/crypto-tokens-the-good-the-bad-and-the-ugly*

[89] "Crypto-asset markets: Potential channels for future financial stability implications", Financial Stability Board, 10 October 2018, see *https://www.fsb.org/wp-content/uploads/P101018.pdf*

[90] "Cryptoassets Taskforce: Final report", FCA and Bank of England, October 2018, see *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*

[91] "Statement on Cryptocurrencies and Initial Coin Offerings", US Securities and Exchange Commission, 11 December 2017, see *https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11*

[92] "Cryptoassets Taskforce: Final report", FCA and Bank of England, October 2018, see *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*

[93] "PS19/22: Guidance on Cryptoassets", Financial Conduct Authority, 1 August 2019, see *https://www.fca.org.uk/publications/policy-statements/ps19-22-guidance-cryptoassets*

[94] "Cryptoassets Taskforce: Final report", FCA and Bank of England, October 2018, see *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*

[95] "Tax on cryptoassets", UK government, see *https://www.gov.uk/government/publications/tax-on-cryptoassets*

[96] "Framework for "Investment Contract" Analysis of Digital Assets", US Securities and Exchange Commission, see *https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets*

[97] "Crypto-assets: Work underway, regulatory approaches and potential gaps", Financial Stability Board, 31 May 2019, see *https://www.fsb.org/2019/05/crypto-assets-work-underway-regulatory-approaches-and-potential-gaps/*

[98] "Report with advice for the European Commission on cryptoassets", European Banking Authority, 9 January 2019, see *https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf*

[99] "Advice: Initial Coin Offerings and Crypto Assets", European Securities and Markets Authority, 9 January 2019, see *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*

[100] "Advice: Initial Coin Offerings and Crypto Assets", European Securities and Markets Authority, 9 January 2019, see *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*

[101] "Spotlight on Initial Coin Offerings (ICOs)", US Securities and Exchange Commission, see *https://www.sec.gov/ICO*

[102] "Report with advice for the European Commission on cryptoassets", European Banking Authority, 9 January 2019, see *https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf*

[103] "Advice: Initial Coin Offerings and Crypto Assets", European Securities and Markets Authority, 9 January 2019, see *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*

[104] "Advice: Initial Coin Offerings and Crypto Assets", European Securities and Markets Authority, 9 January 2019, see *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*

[105] "Cryptoassets Taskforce: Final report", FCA and Bank of England, October 2018, see *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*

[106] "Police grapple with rise in cryptocurrency fraud", Financial Times, 10 August 2018, see *https://www.ft.com/content/f5583d68-9c9e-11e8-9702-5946bae86e6d*

[107] "Cryptocurrencies: looking beyond the hype", Bank of International Settlements, see *https://www.bis.org/publ/arpdf/ar2018e5.pdf*

[108] "Report with advice for the European Commission on cryptoassets", European Banking Authority, 9 January 2019, see *https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf*

[109] "Cryptoassets Taskforce: Final report", FCA and Bank of England, October 2018, see *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*

[110] "Towards a new regime for crypto-assets in France", AMF, 15 April 2019, see *https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France*

[111] "Public Statement – Mitigating Risks from Virtual Assets", FATF, *http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html?mkt_*

[112] See *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN*

www.db.com/flow
corporate.bank@db.com