V. NEW TECHNOLOGIES IN FINANCIAL SERVICES AND PAYMENTS

Issues at stake

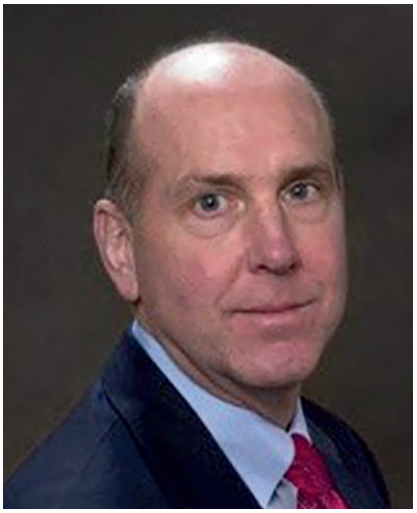
Technology is transforming the provision of financial services and many elements of the current financial system. All financial activities are concerned and can potentially reap the benefits of digitalisation and fintech.

Technologies such as DLT, cloud and AI help to improve existing financial services and processes, increasing their efficiency, agility and transparency, facilitating their cross-border provision and supporting risk management. These technologies also facilitate financial innovation, with the introduction of new services and operating models, enhanced personalisation, the reduction of time to market and the entry of new players into the market. The Covid-19 crisis shows that digitalisation may also be a safety net against operational risks. Furthermore, technologies such as AI and ML facilitate reporting, supervisory processes and support AML and fraud detection.

These new technologies may however pose new challenges in terms of cyber-security, accountability or fair competition and raise issues with regard to appropriate data use, sharing and sovereignty. Their cross-border development in the EU may also be hindered by insufficient harmonisation of legal requirements. This requires taking the necessary steps to ensure the right conditions are in place to take advantage of digitalisation and manage any related risks. Several initiatives are underway at the EU and global levels to address these new challenges, e.g. with the new Digital Finance Strategy proposed by the Commission.

Content

Impacts of digital technologies on financial value chains



Frank Fallon

Vice President Worldwide Financial Services, AWS

Enabling the digital transformation of the European financial services sector

Financial institutions are facing considerable pressure to provide enriched and frictionless customer experiences, while fulfilling their regulatory mandate to ensure that the national and global financial systems that they operate in are secure and resilient. In this context, organisations are seeking alternatives to "business as usual" and legacy technologies. Cloud technology is now at the forefront as financial institutions grapple with these issues. Why? The answer is simple: cloud allows financial services firms to be more agile, protect their customers with enhanced security and get access to the most advanced analytical services, all while reducing costs.

We have seen established organisations ranging from the largest global banks, insurers, asset managers, market infrastructure and financial solution providers take a sharp shift away from the undifferentiated heavy-lifting of managing on-premises data centre infrastructure and embracing the cloud to innovate and enhance resiliency. Indeed, agility, enhanced security and resiliency, and the ability to innovate quickly are today the top drivers for financial firms' cloud programs.

In today's competitive market, financial institutions are looking for ways to differentiate themselves. Leveraging cloud technology provides three key benefits that enable innovation: extracting new insights from traditional and alternative financial data; providing the scalability and agility to respond to market and business changes; and reducing the time and resources needed to manage and maintain technology infrastructure, all while operating with the highest security standards available.

Cloud solutions provide scalability and increased resiliency and security compared to what financial institutions have previously been able to achieve. For AWS, security remains "job zero" and we take active measures to minimise the impact of potential events such as the ongoing COVID-19 crisis, and maintain our security and resiliency through a variety of ways. Our long-standing business continuity plan enables us to respond rapidly in a coordinated manner to potential events and crisis. More broadly, to diffuse the potential for systemic risk in any industry or location, we build our cloud infrastructure in diverse geographic regions with multiple availability zones per region.

Looking ahead, we expect to see increased automation in security through infrastructure and application controls that will help enforce security and compliance policies continuously while reducing human configuration errors. These improvements will allow financial institutions to maintain the data confidentiality and integrity that their customers demand, while maintaining timely and accurate reporting required by industry regulators. As we continue to innovate and roll out more services, financial institutions will see these new services and applications change the way they interact with customers and do business. For European financial services institutions looking to remain competitive in the global market, cloud is undoubtedly an enabler and driver for these organizations to innovate and become more agile.

> *"...agility, enhanced security and resiliency, and the ability to innovate quickly are today the top drivers for financial firms' cloud programs.*

As the European Commission develops its Digital Finance Strategy, ensuring that financial institutions can avail themselves of modern technologies including cloud and machine learning is crucial for the future competitiveness of the sector. For future regulatory initiatives, it remains important for policy makers and regulators to carefully consider an approach that recognises the operational resilience, security and innovation benefits of cloud, and enables firms to make the most of that opportunity. ●

Sophie Heller

Group Chief Operating Officer for Retail Banking & Services,
BNP Paribas

New technologies are fostering new forms of cooperation between industries

First impact of new technologies is on the way the bank is acquiring and serving its clients : Banks are responding to new customer expectations as digital players set new standards, and also to increasing concern for security:

- Choice: customers want to be able to rapidly compare and subscribe to online financial solutions
- Simplicity: customers expect simple & clear journeys
- Personalization: customers expect their Bank to use the huge quantity of data it holds, for their benefit and security : take into account their personal context, demonstrate anticipation, protect them against fraud, and be relevant
- Immediacy: 24/24 7/7 becomes the new normal as well as instant payment ….
- Security : customers expect their bank to protect not only their money but also their data and privacy. This concerns becomes more and more critical as cybercriminality develops along with usage.

Customers positively react to these innovations : More clients are onboarded digitally, most of usual operations such as transfers, card limit management are done digitally - 89% of French people who have downloaded a bank app (55% of French people) check their app at least once a week.

Second, this digital transformation enhances the "human part" of advisors' role while digital channels play a big part in day to day finance management. This shift in advisor role is helped by:

- More time to focus on value-added services as some tasks are handled by customers themselves or drastically eased with RPA or AI for instance,
- A better customer knowledge through real time and comprehensive information
- New platforms for contact management that allow to understand clients requests in natural language and address them to the most relevant available person, independently of its location.

Third, Digital Transformation is about transforming skills, mindset and culture, IT architecture as well as ways of working for everyone from front to back office including functions, it implies for example :

- Fostering an end to end process culture, with a strong focus on operational excellence,
- Developping in big numbers digital and data capabilities across the organization
- Upgrading IT architecture and infrastructure to be able to fully leverage new technologies in particular Cloud and AI.
- Expand Agile ways of working across the whole organization to be able to adapt faster and better to customers' rapidly evolving expectations and have happier teams. It is the necessary shiftfrom product- to customer-oriented organizations so that teams are actually centered on understanding consumers and designing products and services around their needs.

Finally, what goes for the retail banking industry regarding digital transformation is also true for all industries. As each industry becomes centered on delivering an end to end digital experience in a specific set of needs (such as my home, my mobility , my health etc..) , the question of who are you competing or cooperating with, becomes crucial : Big techs, Fintechs but also other incumbents from various ecosystems together such as energy, retail, mobility...

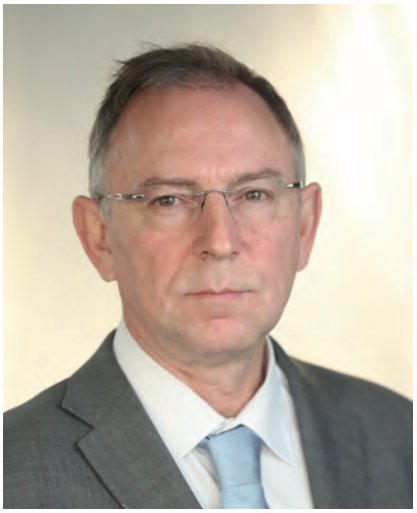
> *New technologies change how customers use services and the nature of the services themselves thanks to new forms of cooperation.*

Retail banks collaborate with Fintechs or integrate GAFA services into theirs (eg Apple Pay or Google Pay). Retail banks have specific competitive advantages:

- Strong banking expertise in all financial areas (consumer finance, investment…) and strong relationship with institutions and corporates
- Loyal customers
- Secure their customers' sensitive data

These advantages, combined with the ones of the players and incumbents from other ecosystems using digital-enabled technologies can create unrivalled propositions for consumers. This is what happened in the mobility ecosystem in Italy for instance, where BNL has created a partnership with Telepass to create a new app allowing consumers to access to all their transportation and shopping services and manage associated payments, all through a single access mobile gateway.

What we see happening for banks is new cooperation acrossindustries in order to design innovative, simple and outstanding new services. ●



Santiago Fernández de Lis

Head of Regulation, Banco Bilbao Vizcaya Argentaria (BBVA)

Competition and innovation in a changing world: a key role for public policy

The steady evolution of financial services can make it easy to forget that the sector has always been shaped by the adoption of new technology. The information and communication innovations of the 20th century brought waves of digitalization: the move from paper to electronic records, credit cards, ATMs, electronic trading, and eventually wider access to internet banking at the turn of the millennium.

But the latest changes in technology have spread more quickly than those before and have transformed more rapidly the economic and social landscape. In the space of little more than a decade some 3 billion people have acquired a smartphone and always-on internet access.

One of the most striking consequences has been the supercharged growth of a new digital platform economy, with the breaking and rebuilding of value chains across almost every industry. And much of the new value has come from being able to capture, analyse and put to use the data generated by the huge increase in digital interactions.

According to an often used metaphor data is the new oil. The metaphor is misguided (among other differences oil is scarce and data grow exponentially), but in any case, data is at the heart of the digital economy and its use - and reuse - will continue to be central to innovation and value creation across industries.

The good news for the financial sector is that new digital channels, data sources and analytical techniques can offer an opportunity to better reach customers and improve services. A more complete picture of customers' needs and behaviours could allow for personalised products and more holistic financial advice. The right datasets could allow credit risk models to be refined, offering the possibility of expanding credit to underserved customers like SMEs, or the development of new green financial products, aimed at helping customers with their transition to a more sustainable economy.

However, to deliver this, firms face the challenge of a new, uneven digital playing field. One where customer relationships are shaped by and channeled through dominant platforms and ecosystems, and where useful data is not always able to flow to where it can deliver the most value for customers.

Public policy has a clear role to play here. And the European Commission has recognised this, with its digital and data strategies and AI white paper published in February 2020 forming key pillars of its support for Europe's digital transformation. The execution of this strategy is now key.

First, the Commission should take robust action to safeguard future digital competition and innovation, with new ex ante rules for significant digital platforms. This should include guaranteeing fair terms of access for other firms, including to hardware functionality, and greater control for users over their data. Individuals and firms should be able to share their platform data easily, securely, in real-time and on a recurrent basis with whom they wish. This would reduce lock-in effects and facilitate data reuse in other sectors.

> *Firms face the challenge of a new, uneven digital playing field.*

Second, the Commission should apply this sharing principle to other valuable personal data such as data from utilities and smart home devices, by implementing its proposal for enhanced personal data portability in the forthcoming Data Act.

PSD2 has enabled this kind of sharing in the financial sector for payments data. And although it is still bedding in, it offers a useful lesson: standardised, dedicated interfaces, such as APIs, are key to secure and effective sharing.

Finally, the EU should focus on supporting the development of AI applications in Europe, as it is essential to a competitive economy. The EU regulatory framework is already comprehensive. Authorities should therefore avoid the risk of over-regulation and concentrate on solving concrete problems, such as clarifying how to meet existing requirements and supervisory expectations on unfair discrimination, explainability and interpretability.

The European financial sector will continue to build on a long history of innovation and adapting to change to deliver value for its customers. The right policy measures now can help to ensure that this is a success. ●

LATEST REGULATORY UPDATE ON

www.eurofi.net

Policy notes written by the Eurofi Secretariat
on recent regulatory developments and
macroeconomic trends impacting the EU financial sector,
including implications of the Covid-19 crisis

Cloud based platforms

Lie Junius

Director of Government Affairs and Public Policy, EMEA, Google Cloud

Solving for better financial services for the European consumers: technology trends and policy considerations

The use of cloud-based technologies is a key pillar of the digital transformation of the economy, driving competitiveness and generating significant economic and social benefits[1].

Trends and benefits

Ultimately, it is the European consumers that stand to benefit the most from cloud-enabled financial services. Innovative financial services providers can create experiences that more closely resemble the best digital ones in other industries.

Today's digitally savvy banks are using the cloud to process vast quantities of information to rapidly construct and sell financial products that differentiate themselves in a highly competitive market. Cloud is reshaping the technology landscape, and it has the potential to transform financial services beyond core infrastructure.

One of the main challenges that the financial industry (and their regulators) is working to address, with the help of cloud, is management of the extremely large volumes of data across the organizational silos and accelerating time to insights.

Also the financial sector can utilise the cloud to become more capable at combating fraud and money laundering. By using more dynamic artificial intelligence (AI) and machine learning (ML) models, rather than static rules-based systems—combined with transactional and behavioral data—banks can now more accurately detect evolving fraud patterns while avoiding costly false positives.

As a recent development, COVID-19 is rapidly changing how financial services institutions serve their customers, empower their workforce with remote work capabilities, and adapt to new market and economic risks.

Challenges to adoption

It is important to take into consideration that most financial institutions across Europe and globally, are at an initial stage of their cloud journey. And the vast majority of initial application of the technology is happening in the area of non-material outsourcing, as confirmed in a recent report by the Financial Stability Board[2].

Whilst financial sector institutions have traditionally been early adopters of the private cloud, they have been relatively slow to migrate to the public cloud due a variety of factors including the complexity of the regulatory landscape and difficulties associated with migrating from legacy infrastructure. These issues are compounded by the concerns over the risk of the vendor lock in, and a variety of perception challenges including around data residency and access. Understanding and navigating change management and upskilling workforces, as well as raising the cloud-specific expertise and trust levels within senior decision makers and board-level stakeholders, are two other critically important factors that cannot be underestimated.

Nevertheless, adoption of public cloud services has gradually increased over the past few years, as financial institutions have realized the business and security benefits of making the shift, and many initial concerns were eased by the cloud service providers' stronger compliance programmes. Banks like Lloyds, Deutsche Börse Group, HSBC are accelerating their cloud innovation, in partnership with Google Cloud.

> *Cloud adoption in finance is accelerating, but further efforts are needed to raise trust and understanding of security and operational resilience of the cloud.*

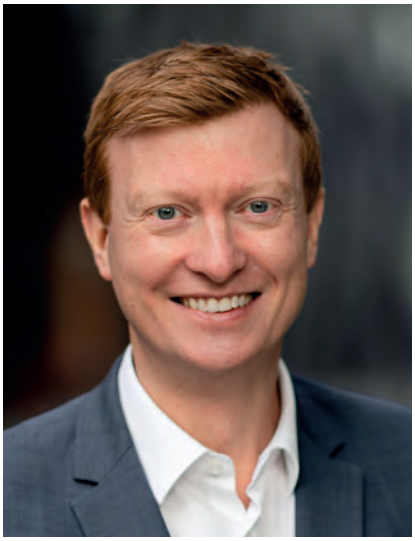
Security and operational resilience of public cloud

The adoption of public cloud technology can augment security. Recent research from McKinsey[3] concludes that organisations expect to double their public cloud adoption due to the growing understanding that cloud platforms' security capabilities have surpassed those available on premises.

Similarly, cloud providers that develop and offer to their customers highly redundant and resilient systems by design, are well prepared to cater for the business continuity and disaster recovery needs of the financial institutions.

Application of multi-cloud strategies also supports financial institutions in addressing vendor lock-in concerns and enhancing operational resiliency capabilities. ●

1. Deloitte: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf
2. https://www.fsb.org/wp-content/uploads/P091219-2.pdf
3. McKinsey. Making a Secure Transition to the Public Cloud: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Making%20a%20secure%20transition/Making-a-secure-transition-to-the-public-cloud-full-report.ashx



Kaj-Martin Georgsen

Head of Corporate Responsibility & Public Affairs, DNB Bank ASA

A future-proof, customer-centric banking system needs to tap into the cloud

Reaping the benefits of cloud computing is a prerequisite for providing customers with the services they expect in 2020. Banks and regulators need to work closely together to address the requirements for both security, competition and competitiveness.

Physical data centres and other physical IT infrastructure represent are costly, inefficient and often redundant: Since they need to be scaled for peak demand, much capacity will remain idle for most of the year. The result: sunk investment and high maintenance costs.

In realizing this redundant capacity could be leased off to others, Amazon kicked off the cloud revolution which has swept the world of IT in during the last decade, including, to an increasing extent over the last few years, financial institutions.

For banks, in the face of new competition for the end-the benefits of cloud computing are numerous. Moving data and service into public clouds enables us to build new solutions more quickly and deploy at greater scale while reducing costs. At DNB, our P2P payments app Vipps was one of our first major venture into the public cloud in 2016. We haven't looked back since.

Cloud infrastructure allow us to source single-purpose functionality from third parties into both backend and customer-facing applications almost instantly, enabling a more agile development approach.

Third-party solutions from smallish fintech partners provide the APIs behind our PSD2 integrations, the voice authentication we are piloting in our call centres, the face recognition for our ID app and the invoice scanner in our mobile bank.

Between these specialized applications and the underlying infrastructure services, today we rely on more than 50 cloud services that allow us greater speed, flexibility and security.

This migration into the cloud does not come without risks. Having fewer companies provide a deeper stack of services inevitably means concentration risks, which regulators are increasingly focusing on. Lock-in effects pose real risks to competition and vendor diversity.

> *Regulators, cloud providers and financial institutions need to work closely together ...*

Regulatory authorities are right to be vigilant about these new risks. DNB have maintained a close dialog with our chief regulators, the Norwegian FSA and the Bank of Norway. Our thinking has evolved on both sides of the table as we have gained more experience with the upsides and possible downsides of outsourcing systems of varying degrees of criticality.

Fortunately, thinking has evolved among the cloud providers we work with, too. Thanks to close dialogue with our national regulators and some of the major U.S.-based service providers, we have secured a greater degree of transparency and audit rights than seemed possible a few years ago.

Cloud providers that barely had a national presence in many EU countries, are engaging with both clients and regulators in Europe, and display a better understanding of European concerns about issues such as privacy, competition and security.

Certification and licensing regimes might be useful in certain scenarios, but current rules e.g. for payment providers means licensing regimes are already in place. Taking a risk-based approach, regulators should focus on the main platforms than entail systemic risk, as well as those that provide core financial services.

Applying stringent licensing requirements for all suppliers means erecting barriers to entry for new actors as well as many of our current providers, many of whom are precisely the kind of small, tech-savvy start-ups we should be encouraging.

In seeking to mitigate the risks of the cloud through regulatory measures, EU legislators and regulators need to be careful not to throw the baby out with the bath water. Regulators, cloud providers and financial institutions need to work closely together to ensure the European financial industry is able benefit from the power of the cloud. ●

Slaven Smojver

Director, Information Systems Supervision Department, Croatian National Bank

Use of cloud services: opportunities are clear but challenges still abound

Cloud services undoubtedly offer numerous opportunities to financial institutions. Some of the more important ones are greater efficiency in cost management, flexibility in the provisioning of computing resources and the ability to use modern technology stacks. However, the financial institutions' perception of risks related to the use of cloud services and regulatory scrutiny have stymied wider adoption.

Croatian banks have taken a cautious approach toward implementing cloud services and until now have primarily focused on the collaboration and support tools. The complexity of the cloud service providers' (CSPs) infrastructure, long supply chains and the opaqueness of their internal control mechanisms have made risk assessments quite challenging, particularly in relation to the regulatory requirements.

Recognition that small errors in the configuration of cloud environments can have an outsized negative effect (e.g. public disclosure of personal and financial data), uneasiness about CSPs' use of client's data and the need for new threat models also negatively influence information security assessments. Information asymmetry and differences in size between the dominant CSPs and their smaller clients (such as Croatian banks) further exacerbate challenges for risk assessment and relationship management.

The European Banking Authority (EBA) has defined regulatory expectations related to the use of cloud services in the banking sector in the Recommendations on outsourcing to cloud service providers and Guidelines on outsourcing arrangements. These documents recognize the use of cloud services as outsourcing. Major CSPs have recently enabled the addition of financial services addendums to their standard contracts that, as they claim, fulfil regulatory expectations. However, hurdles in the exercise of audit rights, vagueness of the shared responsibility model and uneasiness about vendor lock-in and geopolitical risks still impede a wider adoption of cloud services.

> *The financial institutions' perception of risks related to the use of cloud services and regulatory scrutiny have stymied wider adoption.*

Various developments that might mitigate some of the risks are under way. The European Commission's FinTech Action plan recognizes the need for the development of standard contractual clauses for cloud outsourcing. These would alleviate some of the issues but require further development. The initiatives such as the Gaia-X Project might reduce vendor lock-in and geopolitical risks but are still in the early phases of development.

The EBA's Guidelines on outsourcing arrangements mandate that institutions should provide competent authorities with a register of all outsourcing arrangements, which – in turn – might enable the identification of systemic risks. It is reasonable to assume that a well-thought-out framework for independent, standardized, continuous and in-depth assessment of the adequacy of CSPs control environments and the related certification and accreditation regimes would go a long way in mitigating many of the identified risks and challenges. ●

Alban Schmutz

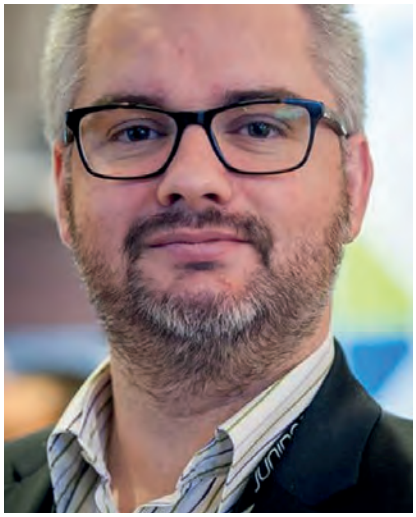
VP Strategic Development & Public Affairs of OVHcloud and Chairman of CISPE - Cloud Infrastructure Service Providers in Europe

Towards a European framework on cloud for financial services

Banks are essential to our economies. Indeed, their continued strength together with the sovereignty of our financial infrastructures are essential for Europe's success. Who controls IT infrastructure today has become a major geostrategic question. At the same time, for the financial sector it has become key to have the ability to use massively the cloud to take advantage of greater efficiency, innovation and competitiveness.

Ongoing discussions on technological sovereignty over 5G infrastructures or on more localised production of pharmaceuticals, exacerbated by the Covid-19 emergency, remind us that the ability to control our critical infrastructure and supply chains is vital for the EU and our future.

This is why a Europe-wide framework applicable in all Member States ▶



▶ is essential. This should first deal with the reversibility and portability of infrastructure and applications to allow a rapid change of provider and easy data portability. The freedom of the financial sector to leave cloud providers quickly and seamlessly, without harming production constraints, is a key element of this sovereignty.

Second, a European framework on cloud for financial services should encompass and make explicit the necessary privacy requirement under the GDPR, particular transparency in data storage and processing locations, to ensure we are working through shared European values.

Third, such a framework has to be future proof, ideally anticipating upcoming legislation of relevance, such as the EU's Revised Payment Services Directive and other European laws that affect the ability of the financial sector to develop new value-added services that benefit companies and citizens alike. For this to succeed, a collective effort and broad public consultation is necessary.

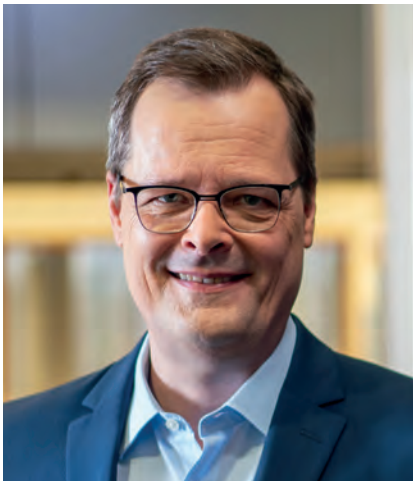
> *Designing a robust time-to-market solution to deliver that new framework is of the utmost importance.*

The association of Cloud Infrastructure Service Providers in Europe (CISPE) is already engaging beyond financial services with European and Member State authorities to address the above challenges and to create the right environment to support businesses and customers. For example, CISPE co-chaired, together with the European association of CIOs (EuroCIO), the Working Group on a Reversibility Code for Cloud infrastructure services, which the European Commission facilitated.

Since the financial sector is a regulated sector, co-ordinated efforts between cloud service providers, European banks and EU authorities are paramount to identify the right regulatory framework. This will, in turn, foster the much-needed developments in the cloud industry, AI and other enabling technologies that are required as we move forward.

Designing a robust time-to-market solution to deliver that new framework is of the utmost importance. This is why setting up a round table between cloud service providers and European banks in close co-operation with EU authorities is very much needed to underpin the financial industry's resilience and enhance the growth potential of European economies. ●

Is AI use growing in the financial sector?



Joachim Wuermeling

Member of the Executive Board, Deutsche Bundesbank

How can AI change banking and what will this mean for supervision?

Artificial Intelligence and Machine Learning (AI/ML) will fundamentally change the financial sector in the medium term. AI/ML may undermine one of the foundations of banking business: banks' privileged access to their customers' financial and risk information. In that respect, AI is comparable to financial innovation in the nineties: Whereas derivative instruments have made local risk globally tradeable, AI/ML makes banks' specific local information substitutable and therefore globally accessible and processable.

At the same time, AI/ML offers many opportunities to banks as well as to their new competitors: it enables the financial industry to exploit masses of information in order to improve their risk management and decision-making processes. Therefore, banks are encouraged to use AI/ML where this leads to improved service to their clients and better risk management, or, in a word: more effective and efficient banking operations.

However, a lesson from the past is that innovation unfolds its benefits only if its major implications are well understood. By construction, in AI systems there exists a strong nonlinear relationship between their input and output. This, along with tremendously increased computing power, is what makes them successful: a huge amount of data can be processed quickly, and its inherent information extracted. However, this feature also marks the flip side of the coin: it is hard to understand their "reasoning". Morever, the sheer amount of data utilised raises ethical questions about its rightful usage.

The application of AI/ML can create considerable risks for banks as well. It is often difficult to know (i) how reliable the inferred relationship between input and output is and (ii) which causality exists between them. This is called the explanatory gap of AI. There are many situations where the explanatory gap does not matter. In those cases, all we need to know is that AI works as expected, and that, if it stops working as expected, this can be detected and fixed quickly. In such cases, we will not need specific regulatory safeguards.

Supervisors have a task when the outcome of an AI/ML method is critical for the functioning of internal controls, for compliance with external requirements or for banks' relationship with their customers or counterparties. In these cases, banks have to fulfil requirements for their AI/ML methods similar to those for any other quantitative model used in risk management: sound modelling practices, reliable processes surrounding the methods, rigid and effective validation, and appropriate management of the inherent model risk.

In a nutshell, the supervisory approach should be to look first at the scope of application of an AI/ML system. If an AI/ML application turns out to have a severe impact on informed decision-making, sound risk management, or otherwise a bank's fundamental functions, supervisory action will clearly be required. The aim is to keep operational risk reasonably contained.

Therefore, both supervisors and banks face challenges and opportunities alike. Supervisors have to adjust their approaches and skills to escort the introduction of AI/ML in banking. Banks have to give supervisors sound explanations of what their AI/ML systems actually do, as well as to what end. ●

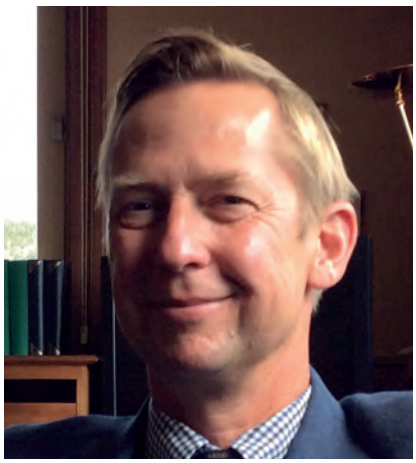
Pēteris Zilgalvis

J.D., Head of Unit, Digital Innovation and Blockchain, DG Communications Networks, Content and Technology & Co-Chair, FinTech Task Force, European Commission

The European approach to Artificial Intelligence in Fintech: current efforts and ambitions

There are prominent synergies between Artificial Intelligence (AI) and the financial services sector as emerging technologies rapidly extend their impact on the financial industry. This reality is reflected in and addressed by the European Commission's new Digital Strategy (2020), the European Data Strategy (2020), the White Paper On Artificial Intelligence - A European approach to excellence and trust (2020), the SME Strategy (2020), the eIDAS Regulation, Payment Services Directive 2 as well as non-legislative financial services initiatives such as the FinTech Action Plan (2018).

In the financial sector, AI solutions are already being used to enable personalisation of financial services and products, ▶



better anti-fraud protection, and faster and more reliable credit assessment. The 2020 Digital Strategy lays out the ambition to create a new regulatory and policy framework for digital finance addressing crypto assets, cyber resilience, as well as a strategy for an integrated pan-European digital payment infrastructure. These efforts are part of a broader EU objective to deepen the Single Market for digital financial services and promoting a data-driven financial sector in the EU, in which AI will play a critical role.

Europe is well-positioned to tap into the potential of AI by capitalising on Europe's competitive industrial and professional markets, including financial services, and its digital innovation and research capacities. At the same time, building an ecosystem of trust is essential. A European approach to AI should ensure that machine-based learning technologies are human-centric, ethical, sustainable and respect fundamental rights and values.

It is important to recognize that while AI can do much good, including by providing better access to finance, reduce costs, and increase efficiency, it can also have negative impacts. It is therefore imperative to mitigate unintended consequences, in particular the risks of data bias, which may arise in the financial services and other sectors. The integrity of the data is paramount, as is the design of AI applications with fundamental rights protections in mind (especially personal data and privacy protection, and non-discrimination).

The Commission is addressing these challenges through a variety of efforts and initiatives, including providing guidance in its AI strategy (2018), Coordinated Plan with the Member States, the Guidelines on Trustworthy AI published by the High-Level Expert Group (2019), and most recently the Commission White Paper on Artificial Intelligence (2020).

For any future EU regulatory framework on AI it will be important that it strikes the right balance. It would need to be effective to ensure the protection of fundamental rights and consumer protection, while encouraging innovation and investment in AI and not imposing a disproportionate burden on developers or business.

A relevant approach in ensuring the protection of fundamental rights and consumer protection is that of regulatory sandboxes. In the SME Strategy for a Digital and Sustainable Europe, it was stated, 'The Commission will encourage Member States to develop proposals for regulatory sandboxes by launching a pilot.' Regulatory sandboxes in the financial services area give opportunities to firms to live test applications, pursuant based on a specific testing plan agreed and monitored by a dedicated function of the competent authority, such as innovative financial products, financial services or business models. Another pertinent and related approach is that of innovation hubs. Innovation hubs provide a dedicated point of contact for firms to ask questions to competent authorities on FinTech related issues and to seek non-binding guidance on regulatory and supervisory expectations, including licensing requirements.

As foreseen in the FinTech Action Plan, the Commission has set up a EU Fintech Lab. The EU FinTech Lab provides a regulators forum to discuss regulatory and supervisory issues regarding new technological applications that are on the market with experts. The Lab has met four times so far (1x cloud, 2x artificial intelligence, 1x RegTech/SupTech), the last time in December 2019 (on AI). ●

Patrick Montagner

First Deputy General Secretary,
Autorité de Contrôle Prudentiel
et de Résolution (ACPR)

Promoting responsible innovation in finance through AI multipronged evaluation

Increasing technicity

Supervisors' technical expertise needs to follow market innovations in AI. Ideally, it would mirror - both in breadth and in depth - the tradecraft of those implementing the systems: just like supervisors hired statisticians to master the intricacies of internal models developed for banks by quants, their staff should include AI experts.

We propose grounding AI evaluation on four pillars: performance (minimizing prediction errors), fairness (yielding decisions, which do not discriminate against individuals or groups), stability over time, and explainability. The latter is particularly prevalent nowadays due to the regulatory context but also as an ethical duty. This implies being able to "open the black box" enclosing any algorithm whose output directly impacts individuals. Thus, the supervisory method itself should evolve: supervision must become more technically-oriented and cross-disciplinary.

As for fairness, the world we live in is full of biases. Those biases are by definition reflected in – and often reinforced by – ML algorithms. The emerging research domain of bias mitigation aims to alleviate discriminatory and unethical outcomes from their output. At any rate, algorithms and data must be evaluated hand-in-hand. Hence, a proposed dual approach to empirical evaluation of AI, based on challenger models and benchmark datasets, will be subjected by the ACPR to feedback from a public consultation.

AI supervision has much to gain from defining methodological best practices, which would cover the entire lifecycle of AI, from data preprocessing and model selection through industrialization to stability issues.

Promoting responsible innovation

On the other hand, the speed of AI adoption in finance should not be overstated: few ML (Machine Learning) algorithms are in production, and those few are rarely the more advanced kind, especially in highly regulated domains or client-facing tasks. Reasons for excessive caution in AI implementation include its operational and compliance risks. ▶

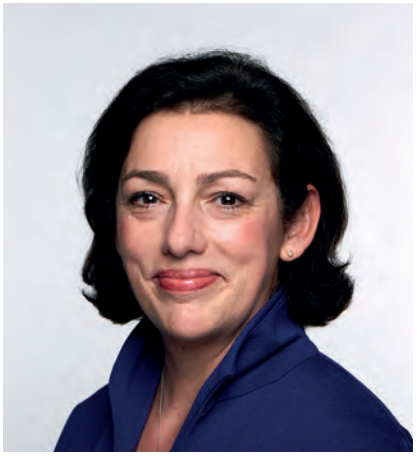
Indeed, as AI strives by nature towards autonomy, the most prevalent threat beyond generic cybersecurity and ML-specific threats is a loss of control, whether by dearth of skills or inappropriate oversight.

Supervisors should thus encourage the positive effects of its widespread usage. Hence one of our key missions: to foster responsible innovation – in other words remove undue obstacles and ensure proper interpretation of the regulation, while also ensuring proper risk management and customer protection.

Co-designing supervisory technology

ACPR SupTech strategy builds around mastering AI technology, which enables us to dialogue with the marketplace, anticipate emerging risks, and enhance our own methods and technologies.

We rely heavily on networking for this: bilateral exchanges with national, European, or international authorities and working groups. Such dialogue may result in proposals for regulatory amendments, but also in more technical deliverables, such as data exchange protocols or software code sharing: for example, pseudonymization (a common GDPR requirement) benefits from all financial supervisors contributing their country- and language-specific expertise. ●



Nausicaa Delfas

Executive Director of International, UK Financial Conduct Authority

AI – managing the future for firms and regulators

Artificial intelligence (AI) has increasingly been used in financial services over recent years. At the FCA, we are considering how we can design a regulatory framework that ensures sufficient oversight, manages the trade-offs firms may need to make, and allows consumers to benefit from the efficiencies AI can bring.

An optimal regime should avoid being tied down to specific technologies. We believe that an outcomes-based and principles-based approach is more conducive to regulating areas that are rapidly evolving. Few of our rules are technology-specific. Detailed and overly prescriptive rules run the risk of becoming quickly out of date and of stifling desirable innovation which can benefit markets and consumers.

Accountability is key when we consider how firms should manage their application of AI. We believe human beings should remain responsible, and accountable, for the technology they use. In the UK, our Senior Managers and Certification Regime is designed to achieve this. But what does accountability look like in the world of AI deployment? As AI technology applications become increasingly advanced and complex, there may be fewer experts who truly understand them. There is also a risk of growing divergence between the experts and senior managers. Senior managers will need to address this.

Effective accountability should support more transparent and explainable use of AI. The use of AI may force firms and regulators to make new types of trade-offs. For example, it can allow more data to be considered in a consumer's credit application, or help provide consumers with products suited to their needs, but it can also incorporate errors and amplify biases. Firms should manage such risks effectively and be clear with consumers about how their data are used. We are currently running a research project with the Alan Turing Institute in the UK to consider how AI could improve outcomes for consumers and support regulatory initiatives.

Machine learning and other AI applications can also be used by malicious actors; for example, to facilitate cyberattacks or financial crimes that spread quickly, are difficult to detect, and cause damage. Firms need to ensure that they are operationally resilient, are vigilant against financial crimes, and can prevent, respond to, and recover from such incidents. Some firms are already using machine learning to combat cyberattacks and money laundering.

The FCA is exploring how we can utilise machine learning to support us in carrying out conduct and prudential regulation. We are investing to become an even more data-driven regulator, enhancing our ability to monitor, predict and respond to firm and market issues. With the Bank of England, we are also setting up a joint AI Forum to gather industry views and share information on safe adoption and usage of AI in financial services and in regulation.

We remain committed to working with international regulators and standard-setting bodies to support an approach to AI that promotes the interests of consumers and is fit for purpose in a fast-changing world. ●

Bruno Scaroni

Group Strategy & Business Accelerator Director, Assicurazioni Generali SpA

Promoting responsible Artificial Intelligence in insurance

As a representative of Assicurazioni Generali, I recently had the privilege of participating in the Geneva Association Working Group on how to promote the responsible adoption of Artificial Intelligence in the industry. I would refer to them as those intelligent systems that automize routine tasks or assist human decision-making along the entire value chain. Such systems may combine new types of learning algorithms with the analysis of data from new types of data sources, such as online media data and IoT data. Natural language processing is surely an AI revolution for the industry: it enables intelligent systems to 'talk' and interact with humans, and Insurers are increasingly using chatbots that can identify and respond to ordinary customer queries that are available 24/7.

While working in Europ Assistance some years ago, we pioneered the use of natural language processing for the delivery of Motor Assistance and towing services in Europe: by establishing a chatbot to manage ordinary assistance request calls, we succeeded ▶

▶ in improving customer service and responsiveness of the call center operations, whilst preserving operational efficiency. Computer Vision technology is also an AI application that can materially improve how Insurers manage claims with faster and more accurate responses: intelligent systems can detect and recognize objects in pictures, extract related information and provide guidance on the claims management. Such an approach is present tense in some markets, especially in the Motor Other Damage servicing.

In addition to such cases, intelligent systems can detect patterns and correlations in complex data in ways never thought possible before, and set the basis for analytical tasks such as classification, regression and clustering that are crucial in the insurance business model. Compared to traditional modelling that generally relies on linear models, intelligent systems have the potential to provide more complex non-linear relationships between variables and consequently better risk modelling. The Geneva Association working group identified three socio-economic benefits of AI:

- Expand the scope of risk pooling, by extending coverages to new and previously uninsured customer segments, and by widening the range of risks for which insurance is available
- Reduce the cost of risk pooling, by decreasing the cost of the value chain through automation of specific activities, reduction of moral hazards and adverse selection
- Mitigate and prevent risks by better modelling and enabling predictive capabilities that can avoid or reduce losses.

However, in all contexts AI is based on data, and data represents the key factor that allows intelligent systems to consequently progress. Insurers need to master data and earn customer trust to utilize their data in to maximize the benefits of AI. To gain such trust is crucial to clarify AI benefits, provide undisputed value to customers and manage data responsibly. In order to achieve customer confidence and reap maximum benefits from AI, Insurers should adopt clear guidelines on how to implant intelligent systems in their value chain, and how to appropriately make use of its capabilities. In conclusion, Internal guidelines and policies play an important role in raising the awareness of the benefit–risk trade-offs in the use of AI in insurance.

From a regulatory perspective, the definition of ethical principles for the use of such technologies can be a key initial step in supporting both technological progress and the industry evolution. Such principles would also be guiding stars for other technologies that will arise in the future, and pose similar benefit-risk trade-offs. (Reference: The Geneva Association - Promoting Responsible Artificial Intelligence in Insurance, January 2020). ●

Diana Paredes

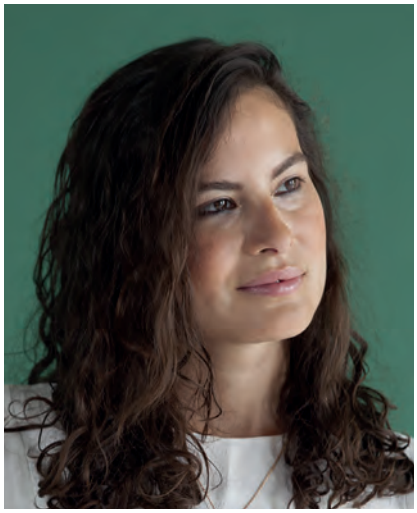
Chief Executive Officer & Co-Founder, Suade Labs

Basel IV, Common Data Standards and Artificial Intelligence

Artificial intelligence (AI) and machine learning (ML) in the RegTech industry are disrupting regulatory compliance. By creating a common data standard, RegTech companies can leverage AI and ML tools to perform analysis on standardised data to spot discrepancies faster and more accurately. Where regulation was previously a cost centre for financial institutions, compliance functions can now create value by cutting costs and producing highly accurate data that financial institutions can then use to make strategic business decisions. Institutions that employ such software are already enjoying cost savings, whilst investors, the public and supervisors can benefit from standardised, highly accurate regulatory submissions.

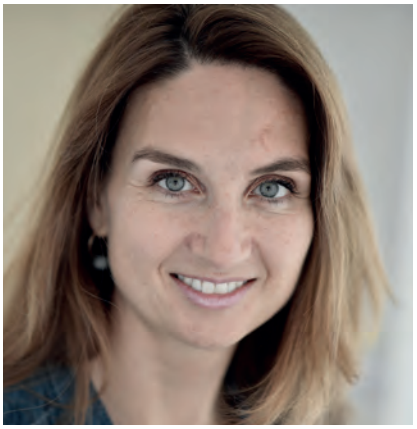
The Basel Accords provide a good example of the benefits of standardisation in regulation and compliance. With Basel III, the Basel Committee on Banking Supervision (BCBS) introduced new capital, liquidity, and leverage requirements following the financial crisis of 2007/2008. For most financial institutions, this meant significant added expenses on consultants, manual processes, and contractors who were hired to cope with regulatory demands. The manual processes and disparity among contractors' approaches resulted in discrepancies in compliance with Basel III among financial institutions. To address this, the BCBS introduced Basel IV in 2017 to restrict the use of internal models for calculating capital at financial institutions. Standardisation was the ultimate objective.

The RegTech industry can help financial institutions capitalise on increased standardisation in financial regulation. It can transform financial institutions' disparate data through a common data standard into an easily machine-readable format. AI and ML advancements can then use this data to produce the highly accurate regulatory submissions that the BCBS were after with the introduction of Basel IV. The



RegTech industry's ability to leverage AI and ML is the best way of achieving uniformly high standards in capital, liquidity, and leverage, and ensuring a stable and secure financial services industry that is effectively supervised. Those financial institutions that entrust their compliance to the RegTech industry can set precedent for RegTech innovation and compliance in the years to come. ●

Leveraging DLT in the securities market



Natasha Cazenave

Managing Director, Head of Policy and International Affairs, Autorité des Marchés Financiers (AMF)

How can the EU take full benefit from the development of blockchains and smart contracts?

With distributed ledger technologies and smart contracts, we are moving to the next level of Internet: the "Internet of Value". What the Internet has made possible for information transfers now seems possible for value transfers, i.e.: virtually free, almost instantaneous, anytime, cross-border, secure exchanges of any type of value: virtual currencies, loyalty points, coupons for future services, representation of physical goods. In recent months, we noticed a growing interest in the representation and transfer of securities.

DLT present a number of benefits for the competitiveness and integration of EU securities markets. On the issuance side, digitalisation or "tokenisation" could reduce the total cost of the transaction and facilitate the exchange of illiquid assets. It could also allow the emergence of new asset classes and facilitates cross-border trading. On the secondary market side, the use of DLTs and self-executing contracts (smart contracts) eliminates the need for reconciliation, which can reduce back office costs by a factor of up to 3. Finally, the direct publication of financial information on the blockchain network makes it possible to carry out almost instantaneous transactions between two counterparties compared to the two business days required for traditional settlement. Automation of back-office processes (settlement, cash flow payments, etc.) would also be possible for repurchase agreements, margin calls on derivatives and the exercise of options, thanks to the use of smart contracts.

As a regulator, it is our duty to be aware of these changes and possibilities and to ensure that our regulatory frameworks remain appropriate. These frameworks must allow us to manage risks and protect users effectively, without losing the benefits of innovation. Against that background, the AMF examined the legal obstacles to the development of security tokens that mainly stem from EU regulation and presented its analysis in a recent paper[1].

To overcome these obstacles, we recommend the creation of an « EU digital lab » allowing national competent authorities (NCAs) to remove, in return for appropriate safeguards, certain requirements imposed by European regulations and identified as incompatible with the blockchain environment, provided that the entity benefiting from this exemption respects the key principles of the regulations and that it is subject to increased oversight by its NCA. The AMF also published a position to clarify the notion of trading platforms and bulletin boards.

Where tokens do not qualify as financial instruments, pending the creation of an EU framework, the French "PACTE law" adopted in 2019 introduced in France an optional visa regime for fundraising in crypto-assets (ICOs) and an optional license regime for digital assets service providers (DASPs) supplemented by a mandatory regime that imposes to DASPs due diligence in the fight against money laundering and the financing of terrorism. Only crypto-assets that are not considered as financial instruments are eligible to these regimes. The creation of these new regimes and interaction with numerous professionals for two years before the law was passed has helped us improve greatly our understanding and develop specific and more tailored requirements. As for the implementation, the AMF gave its first optional visa for an ICO in December 2019, and some players have expressed interest in the DASP optional framework. The two first DASP registrations were granted mid-March. It is too soon to learn all the lessons, but we are convinced that only a bespoke, flexible and attractive framework can work at this stage for the European Union. ●

1. See : https://www.amf-france.org/en/news-publications/news/legal-analysis-application-financial-regulations-security-tokens-and-precisions-bulletin-board

Glen Fernandes

Group Strategy, Euroclear

Embracing the DLT (r?)evolution

Over the past years, DLT has emerged as an important piece of technology that promises to transform capital markets by delivering a real-time, transparent, Peer-to-Peer(P2P) and inclusive experience. It enables a real-time view of activity and positions across a business network. Making it possible to detect, assess and react faster to threats and opportunities. Participants can share and trust in a single source of truth, increasing transparency and reducing reconciliation. Because of its distributed nature, participants can directly hold and transfer value in a P2P manner, but still retain the possibility to be serviced by a third party without mediation of information or network. This allows for greater direct inclusion to capital markets.

Inspired by this promise, a number of the DLT based PoCs have now moved to a project phase and aim to go live soon. Post Trade FMIs & intermediaries also fully acknowledge this transformative potential. Hence, they have not been a passive observer and have already launched dozens of projects with DLT or invested in FinTechs for use cases related to issuance, settlement, asset servicing, funds distribution, collateral management etc.
The journey for most industry initiatives, however has been a very long and arduous one and the path to mass adoption ▶

▶ is not yet obvious. It is clear that the mere use of DLT is no longer a sufficient condition to expect success.

"Will DLT introduce additional risks and costs?" or "Will it deliver benefits materially beyond what we have today?" are questions that often get asked, but the answers are not obvious. For example, DLT instant settlement does reduce counterparty risks but also increases liquidity costs with no netting and pre-funding before trade-execution. Similarly, decentralization brings with it significant governance and legal risks. And participating on a DLT network isn't cheap. Not everyone can afford the node setup, licensing fees, upskilling efforts etc.

So when seen in context of EU capital markets that have gone through an era of transformation to deliver market-wide efficiencies, lower risks, greater legal certainty and interoperability, the material benefits in return for undertaking such costs and risks are not always apparent.

Meanwhile market actors assess whether such goals of efficiency, transparency etc. could be more easily achieved using other new technologies such as AI, Robotics, API and Cloud.

While such questions will possibly get ironed out over time by lowering costs, skilling more staff, etc. what certainly is required at this stage is greater legal and regulatory certainty. An EU-wide legal classification and a technology neutral regulatory framework is thus an important first step to support market adoption. Moreover, it is important that regulators take a "substance over form" approach leveraging existing safe & robust regulatory and risk frameworks, but applying them proportionally to allow innovation to thrive.

> *The path to industry-wide adoption of DLT isn't yet obvious. How can regulators and market actors help the industry embrace in its future evolution?*

Such logical supportive steps from both public authorities & market actors will help the markets embrace the DLT evolution rather than impede its radical revolution. FMIs, given their decades experience in driving safety and efficiency and their committed experimentation will certainly be key enablers in this journey. ●

Andrew Douglas

Managing Director Public Affairs and Regulatory Relationships, Europe & Asia, The Depository Trust & Clearing Corporation (DTCC)

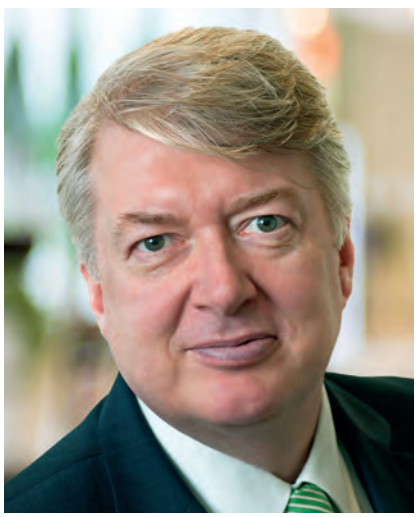
Slow down to speed up: DLT reaches potential through collaboration and standardisation

The technology adoption life cycle – often referred to as an S-curve – has four stages – innovation, syndication, diffusion and substitution – and there is also usually a period of hype early on, when a new technology is introduced.

Distributed ledger technology (DLT) is sitting firmly in the syndication phase, during which technology is demonstrated and a small portion is commercialised, with the potential for immediate utilisation. True to a typical technology life cycle, DLT did experience the intense hype phase, however recently, the industry has taken a more considered position as to how it may benefit financial services. That said, for DLT to be accepted more widely in financial markets, certain areas need to be addressed.

> *The industry needs a standardised approach to security to ensure the integrity and availability of an organisation's DLT operations.*

A key issue is security. As addressed in our recent whitepaper, Security of DLT Networks, the industry must develop a comprehensive and standardised approach to security to ensure the confidentiality, integrity and availability of an organisation's DLT operations. There is no 'one size fits all' approach but there is an optimal model: the development of a reliable and comprehensive industry-approved framework. A critical component of this framework is the development of industry standards,



which enables interoperability between multiple DLT implementations and therefore reduces risk and cost for market participants by preventing a fragmented industry eco-system.

DLT standards would also facilitate the sharing of information between market participants and vendors, which would improve understanding of the benefits and risks of the technology, knowledge ▶

likely to the speed up adoption. Standards can help with other critical security issues such as data governance, which often delays the implementation of new technologies such as DLT. Via the development and adoption of a principles-based framework, firms are better able to identify potential weaknesses in their DLT projects. Further, a universally accepted framework will provide regulators with a consistent approach to assessing the potential strengths and weaknesses of different DLT implementations.

Effective and efficient collaboration between relevant stakeholders - clients, regulators and vendors - is another benefit of developing standards that is critical to the successful implementation of DLT. For example, it is important that the industry collaborates with policymakers to ensure that the case is well-made around how new technology implementation can safely serve the public, as well as the clients and the industry.

Regulators and policymakers must consult and collaborate on new technologies, such as DLT, at the global level to better understand how the technology can improve the functioning of financial markets without putting safety at risk. Standard setting bodies (SSBs), such as the Financial Stability Board and IOSCO, have an important role to play in that process.

Now that the initial excitement about DLT has died down, it remains clear that the technology holds potential value for the industry. Benefits include, processing efficiencies, operational capacity and scalability, as well as maintenance of data integrity. In order to realise this value, there must be a standardised approach to DLT security via a comprehensive framework most effectively achieved through collaboration between the industry, market infrastructures, policymakers and vendors. ●

Morten Bech

Head of Secretariat,
Bank for International Settlements (BIS)

Tokenised securities and the future of settlement

Distributed, "tokenised" securities could be the future

For years, financial authorities have warned the general public about cryptoassets' severe price volatility and consequential lack of safety. Yet the underlying distributed ledger technology (DLT) could have useful applications. Although cryptoassets and stablecoins focus on creating new types of money and means of payment, another area being explored is for securities and their settlement (Bech et al (2020)).

Today, most securities are book entries, with their ownership electronically recorded at some entities. The most common setup is an indirect holding system, where an intermediary (such as a custodian bank) holds securities on behalf of its clients with central securities depositories (CSDs). This arrangement, where securities are transferred through "book entries" across accounts at a CSD and intermediaries, minimises the management of information by CSDs, yet also fragments ultimate ownership records. This can add complexities and costs for end users.

The technology underlying cryptoassets could help through "tokenisation". A number of projects around the world are transforming securities into digital tokens – representations of value not recorded in accounts. This would mean that, in the future, equities and bonds could exist on distributed ledgers held across flat networks of owners. This could make ownership records more transparent and settlement much faster.

Yet tokenisation is not that simple

If this sounds too good to be true, it is. Not only are there technological challenges to tokenising securities, but serious trade-offs in the management of risks. Although ownership records can be distributed with DLT and some functions automated with "smart contracts", transactions still need to be validated and updated by all parties, rather than centralising these processes at CSDs and big intermediaries. Intermediaries do not just play a purely operational role either; they smooth trade flows and provide credit, making settlement more efficient overall.

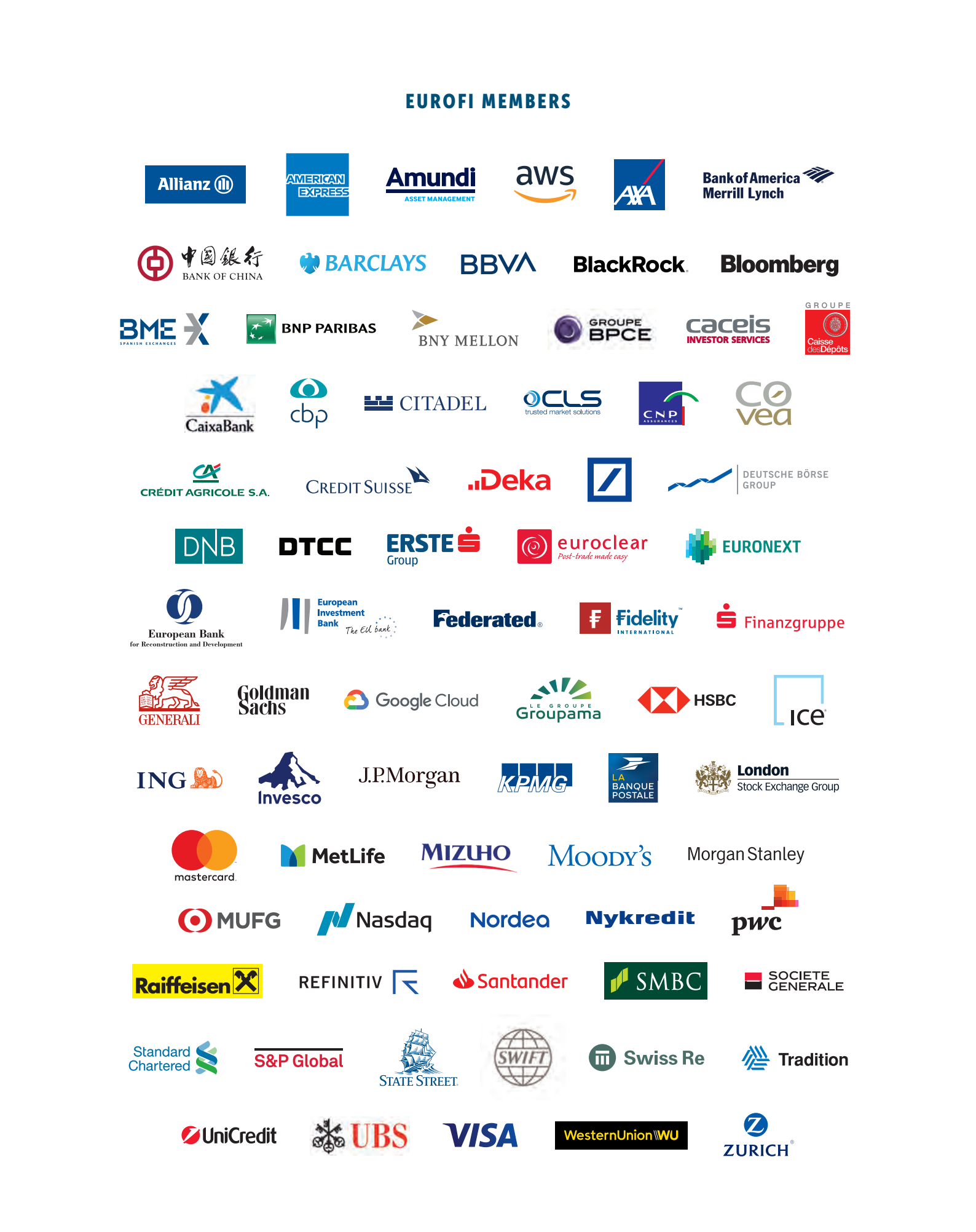
Faster settlement is not without its challenges, or costs. A traditional settlement cycle (eg T+1 or T+2) allows more participants to trade and reduces the amount of securities that market-makers need to store in inventories. Faster settlement could also increase the likelihood of trades not settling, resulting in time and effort resolving disputes about failed settlements.

> *"The more open and interoperable a tokenised securities system can be, the better.*

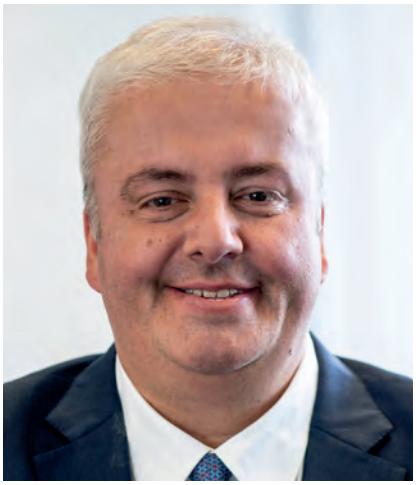
And the future is likely to see a transition, not a big bang

Tokens and DLT offer a number of benefits for securities, but they come with costs. It is therefore very unlikely that a large-scale coordinated move will take place any time soon, or simultaneously. Therefore, as new assets and securities become tokenised, they will need to interoperate with existing account-based cash and securities systems. The more open and interoperable a tokenised securities system can be, the better. ●

EUROFI MEMBERS



Data sharing and sovereignty issues



Burkhard Balz

Member of the Executive Board, Deutsche Bundesbank

Effective data sharing requires data sovereignty

We have recently discovered a new world: the digital world. This entails both great potential and great risk at the same time. On the one hand, the combination of increasing amounts of data and advancing technical possibilities leads to added value in the use of personal data. This includes, for example, discounts on products and seemingly free usage of digital products. On the other hand, there are risks of becoming dependent on data companies, losing our data sovereignty, and facing monopolistic market structures. These dangers arise in particular due to the growing role of platforms.

The recently emerged platform economy, with its small number of large and often global network companies, warrants special attention in this regard. Personal data in combination with machine learning may be used to gain the upper hand. For instance, data could be used not only to assess a potential borrower's creditworthiness, but also to identify the highest rate that they would be willing to pay. It is even more concerning that this discrimination may not necessarily be intentional. A sophisticated algorithm may be biased by finding an underlying cause.

In order to protect the right to informational self-determination, regulators have introduced a variety of rules. The most prominent of these, the GDPR, sets out a legal framework for data protection. Its major achievements are the required express consent for the collection and usage of data as well as the right to demand the deletion of personal data. However, the practical implementation of these provisions presents a number of challenges. Therefore, in order to achieve full data sovereignty, further steps may be necessary. Developing a user-friendly technical tool that allows users to conveniently control the usage of their own personal data could be one potential solution. Based on a secure and neutral data infrastructure, the data owner would maintain the right to decide independently on the use of their data and would be able to fully or partially share their data with companies or authorities for a designated period of time. This would potentially ensure that data access and usage can be tracked and controlled effectively and that property rights, such as deletion of data, can be exercised with ease. Such a facility would not block data sharing; instead, it would facilitate it under fair conditions and therefore help to increase competition.

Beside this new digital world, existing market structures appear to be disrupted. Data is collected at near-zero marginal cost, which means that new services are easily scalable. Once sufficient scale has been achieved and a captive ecosystem established, potential competitors have little chance to catch up. This restricts innovation and competition. A legal framework is necessary to create a level playing field. PSD2 has successfully established such a framework for financial institutions. Banks have to share their data with certified companies if this has been authorised by the customer. In order to create a level playing field for data sharing in other markets as well as between different markets, a legal framework analogous to the PSD2 model should be established at the European level. ●

Carsten Hess

Head of Digital Policy, Banco Santander

Five principles for an innovative European data economy

For the EU's economy to remain competitive on the global stage, Europeans need to turn the necessary digital transformation of its traditional industries into a global advantage.In Santander we support the EU Commission's plan to create a 'data agile economy' where data and fair rules around its sharing and usage are key to create a more innovative digital economy.

However, we believe it is critical to accelerate on an open cross-sectorial data framework that, while empowering users and putting them in the centre to control the data they generate, would contribute to developing a level playing field in all sectors. We strongly support the vision of a single European data space where personal (and non-personal) data is secure and where businesses (including SMEs) also have easy access to industrial data. While empowering users and putting them in the center, opening cross-sectorial data would also multiply the opportunities for disruptive innovation and contribute to developing a level playing field in all sectors and with platforms that leverage in data from diverse markets and contexts. We therefore support the horizontal ambition of the EU's data strategy.

When it comes to banking, more data, and especially data that is uncorrelated ▶

▶ with the traditional one, can help improving services in the benefit of customers and trigger innovation, just as it happened some years ago with PSD2. Non-financial data has a huge potential to improve banks' predictions and thus enable customers access to finance. It will also trigger similar levels of innovation outside the financial space.

In order to create these conditions for success, we propose a set of five principles creating a data agile economy by contributing to opening-up data across sectors in a way that individuals and business users can benefit in fair manner. Those principles will also help providing choice within a secure framework to make their choice to share data from all sectors with their chosen providers.

1. Give control to the user by creating a framework that is consumer centric. People and businesses, as owners of their data must be in control and decide freely with whom and for what purpose they share it.
2. Create the right conditions for the secure transmission of data. APIs are the preferred method for this as they are safe, efficient and provide access to data on an immediate & ongoing basis. In addition, access can also be easily stopped whenever the user decides to.
3. Clarify the different nature of data to be shared. Users are the owners of their raw & observed data; but companies building "value" around the data need to be able to retain this value. Elaborated or inferred data should not be mandatory shared.
4. The data regulatory framework should enable greater access to data improving services to the benefits of users. The focus of any future data sharing framework should be put on the revision of the online intermediation services regulation, since this is where most amount of data lies.
5. A fair cross-sector approach is also needed to ensure maximum benefits to our society. No mandatory data sharing should be triggered in a sector (banking) where players from other sectors also compete but don't have similar requirements. ●

Tsvetelina Penkova

MEP, Committee on the Internal Market and Consumer Protection, European Parliament

The EU towards data sharing economy

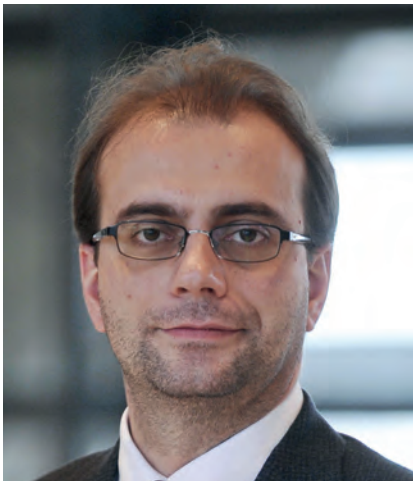
Globally, there are deeper and deeper concerns regarding the market dominance of tech giants. There is a continuing and ever increasing corporate concentration, where governments have explored different measures, from breaking up tech giants to creating public alternatives to exercise strict controls and transparency. In Europe, a number of measures to tackle competition have been adopted, non-exhaustively in industries like telecoms or energy, however, when it comes to the 'Big Tech', experience has shown that ex-post measures like fines imposed by the European Commission have neither restored fair competition, nor avoided growing market dominance. This is a reason why, in the Group of the Progressive Alliance of the Socialists and Democrats in the European Parliament, we call for a review of the EU competition rules, which should take into account the future competition in the digital economy, including market-dominance driven predatory pricing strategies, and which should allow for preventive measures to tackle uncompetitive behavior and guarantee a level-playing field.

> *"Taxes should be paid where the profits are generated.*

Such companies are accumulating huge amount of data and often prevent others, including the data subjects, from accessing and using it. GDPR and the ePrivacy directive provide users with the right to access and use their data but there is often a lack of tools and standards to do so in a practical way. The European Commission is trying to address these issues, i.e. through data interoperability and governance, in their newly published European strategy for data. As much as this strategy brings revolutionary initiatives like common sectorial data spaces, also for the finance sector, it brings a number of questions and challenges. What would be the incentives for companies to share data, especially rare or important data? What data could be shared? Is there a price for this data? The Commission believes that there is a merit in thinking about extending the approach taken in PSD2 to other sectors, thus extending open banking to open

finance. This brings additional questions with regards to the scope and application. In any case, the experience with the PSD2 can serve to future debates on the need for a standardised approach for sharing data and a high level of trust among actors.

Finally, we are also of the view that the way added value is created through digitalization and tax regulations should be adapted accordingly. While huge profits are global, some companies optimise their profits in only a few tax advantageous countries. This is unfair to both the consumers and the competition. Taxes should be paid where the profits are generated. ●



Sébastien Raspiller

Head of Department, French Treasury, Ministry of Economy and Finance, France

A sustainable European data ecosystem at the service of the financial sector

The EU financial area could only stand out from the crowd with a well-protected, well-regulated, well-advised while highly open, sovereign data ecosystem.

When it comes to financial data, the GDPR is broad in scope and also has a large set of sector-specific requirements in terms of security. Some of them (e.g. from payment cards) are undeniably considered "highly" personal given their criticality and the GDPR provides for some ex-ante measures such as the conduct of a data protection impact assessment in the case of personal data processing likely to generate risks for consumers.

Whether sectoral or not, a safe and secure environment for data and high-value information is at the heart of the Single Market concerns. Initiatives ranging from e-IDAS regulation and EBA Regulatory Technical Standards (RTS) to the trades secret European directive allow for a common area of data where citizen's rights are preserved, consumers are highly-protected and the non-EU investors or suppliers are truly welcome as long as the EU requirements are fulfilled.

The core EU values could be undermined or weakened notably by an increasing reliance on systemic non-EU third-party providers of crucial services such as data (including cloud computing) or even cybersecurity and algorithms This raises the question of the supervision of non-financial players and the robust assessment of the systemic risks linked to their use as much as taking into account intertwined public policy objectives such as financial stability, fair competition and its implications for the free flow of data, portability, personal and non-personal data business models.

The cross-borders nature of data also hampers information and data sharing through the creation of determined circles of trust that are essential to build a sovereign European data ecosystem, but eminently remains a puzzle hard to solve. At the meantime, conflicts of sovereignty could occur regarding sensitive data location such as computer vulnerability data (e.g. bug bounties platforms) or highly personal ones and non-EU domination of certain activities (e.g. security standards, sovereign rating agencies) with a serious lack of European counter-models, that is damaging not only in terms of international outreach but also for the full control of our critical infrastructures.

However, it is clear that transboundary and cross-sectoral issues require both EU and international responses and enhanced synergies between public and private players in correspondence with EU rules and values. A well-designed common European financial data space and a high-reaching European Strategy for data (European Commission) would be a promising step ahead in that sense. ●

Kostas Botopoulos

Advisor to the Governor of the Bank of Greece & Former Chair, Hellenic Capital Markets Authority

Data restrictions in times of emergency

The extraordinary times we are living in because of the outburst of the coronavirus pandemic have an impact on nearly every aspect of private and public life. This is also true for the field of data protection: instead of debating on data sharing and the impact of technology on European financial markets, as we were supposed to be doing in Zagreb, we are suddenly confronted with two completely different, and much more problematic, sets of issues: on the one hand the very survival of the European financial markets, and on the other the legality and legitimacy of restrictions of data protection which are already taking place all over Europe in the effort to combat and contain the pandemic. Leaving aside the economic consequences, which would perhaps merit a special Eurofi conference once the nightmare is over, I would like to highlight some of the legal and operational aspects related to data restrictions.

The data-protection framework in the EU is comprised by three sets of principles: constitutional provisions in some member states (for example, Art 9A of the Greek Constitution), the "horizontal" GDPR provisions and relevant national legislation enacted on the basis of the GDPR. All three sets of provisions enshrine a robust protection of privacy and personal data but also cater for exceptions. The principles of legality and proportionality

apply in the constitutional framework, be it on the national level (Art 25 of the Greek Constitution) or through the EU Charter of Fundamental Rights. In the EU we have, since 2018, the GDPR, as ▶

complemented by relevant provisions of Directive 2002/58 on the protection of privacy in electronic communications. Art 6, 1, e (and also whereas no 46) of the GDPR provides for exemptions from consensual processing for the protection of vital public interests (among which health is first and foremost), whilst Art 9,2, i specifically mentions health issues as providing an exemption whereby even sensitive data (such as health data) may be processed without consent. This does not mean, however, that said processing may be done in contravention of the fundamental principles laid down in Art 5 of the GDPR: legality, limitation of goal, minimization, exactitude, limitation of storage, confidentiality.

Consequently, measures taken by public authorities, such as compulsory data gathering, processing and exchange of data between member states and authorities, would be admitted if based on a specific legal act setting out the conditions and the duration of the emergency (in the case of Greece it took the form of a so-called "act of legislative content", a presidential decree ratified by the Parliament on a later stage and used only in exceptional and urgent circumstances) and respect of above DGPR core principles.

Private sector entities, usually regulated by the relevant national legislation such as Law 4624/2019 in Greece, can, in principle, also impose restrictions on data protection, based on a specific national legal base and respecting the core GDPR principles. Statistical use, such as the one made by some member-states but also requested from the Commission, is also permitted under the proportionality and anonymization conditions. For every processing act the possibility of judicial action against measures considered as contravening the core protection principles should be guaranteed by member states. On all those issues, the European Data Protection Board rendered a public statement on the 19th of March 20120. Obviously, full protection, sovereignty, and even use of technology are secondary in times of such emergency. Even in such times, however, the European state of law remains in place. ●

Benjamin Angel

Director for Direct taxation, Tax coordination, Economic analysis and Evaluation, DG Taxation and Customs Union, European Commission

New challenges lay ahead, prompted by financial innovation

Recent scandals have put the financial sector under scrutiny by legislators. For the last decade, the fight against tax evasion and avoidance has been a priority for governments around the world. From the strengthening of anti-money laundering requirements to the automatic exchange of financial account information for tax purposes, financial institutions were called upon to strengthen their procedures and share customer information with the authorities.

In 2016, for the first time, EU financial intermediaries were required to collect and report customer information to the tax authorities. The alignment of the Directive on Administrative Cooperation to the OECD common reporting standard ensured the minimisation of the potential burden for EU financial institutions. This Directive was recently amended and will require that intermediaries, including financial intermediaries, report aggressive tax planning schemes.

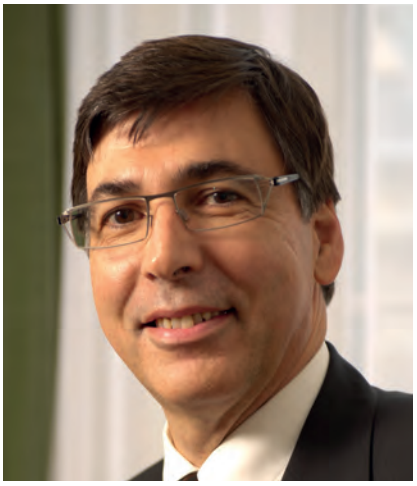
However, new challenges lay ahead, prompted by financial innovation. Innovative financial technologies and products bring efficiency gains but also new demands for the industry and legislators. Due diligence and customer identification obligations set forth in legislation still rely mainly on traditional requirements, while technologies such as electronic signatures and seals or even biometric data sensors recognition are being considered by the industry. In this context, the regulatory framework will need to remain fit for purpose while both governments and financial institutions must ensure the protection of clients' data and its security.

New financial products such as virtual assets are now under the scrutiny of legislators. What started as a minor alternative means of payment has now been taken up by key market players, often outside the boundaries of the financial industry. Such "outsiders" are not subject to as stringent regulatory framework as the financial sector, which may lead to a biased playing field. The financial sector will need to reinvent itself while ensuring it keeps its competitiveness in an ever-changing environment. At the same time, as it evolves from simple low-value payments into a means of investment and storage of value, virtual assets are relevant for taxation purposes as well as other areas such as the fight against money laundering.

Lastly, a comprehensive review of the taxation of Multinational enterprises is ongoing within the OECD. It remains unclear how and to what extent it will affect the taxation of the financial sector. The latest draft notes that most financial services are supplied to commercial customers and therefore not within scope, but only goes so far as to say that there is a "compelling case" for consumer-facing services to be excluded, on the basis that they are already subject to heavy regulations.

Any legislative action must foster innovation in the EU, or at the very least not impede it. The way forward must keep up with innovation and new financial realities, while relying on the synergies between the different legal frameworks. A "whole-of-government" approach is the only way to avoid the duplication of procedures and avoid unnecessary costs for governments and economic operators. Action in the area of taxation, anti-money laundering and financial regulation needs to be consistent and mutually reinforcing. ●

Stablecoins and crypto-assets



Denis Beau

First Deputy Governor, Banque de France

Crypto-assets, acknowledging the potential benefits, tackling the actual challenges

In the past 10 years, a new class of assets has emerged, the so-called crypto-assets. If the first generation, like the Bitcoin, was essentially of speculative nature, we are now seeing a number of market initiatives, still building on the potential offered by the DLT technology but based on mechanisms designed to ensure the stability of their value, and for this reason generally referred to as stablecoins.

These initiatives are diverse in their nature and features, but aim at bringing improvements in payments. Some intend inter alia to make cross-payments quicker and cheaper and to improve financial inclusion – and progress is indisputably needed there. Others tend to pave the way for faster settlements between financial intermediaries. As such, the various projects must be looked at with lucidity and technological neutrality.

At the same time, we must be fully aware of the challenges they raise. The stablecoins indeed form settlement assets that may compete against commercial and central bank money at the center of our payment systems. As many central bankers have stressed, today's crypto-assets do not satisfactorily offer the qualities expected from a settlement asset to be used interchangeably with commercial bank and central bank money. This highlights the misleading nature of the name of "crypto-currency".

From that perspective, as pointed out by the G7 in its October 2019 report under the French presidency, stablecoins of potential large size and reach may not only pose risks in terms of legal certainty, money laundering and terrorist financing, consumer and investor protection, but also raise additional challenges to competition policy, financial and monetary stability.

The preferred response should be to establish appropriate regulations to reconcile the need to address risks and the preservation of the potential for technological innovation offered by crypto-assets. This has to be done according to the "same business, same risk, same rule" principle so that a risk-based and proportionate regulation and oversight be applied to stablecoins.

We need proper regulation and oversight to make them part of the solution, not part of the problem. At global level, the Financial Stability Board has been mandated to assess potential regulatory and supervisory gaps and to suggest a potential way forward to handle them.

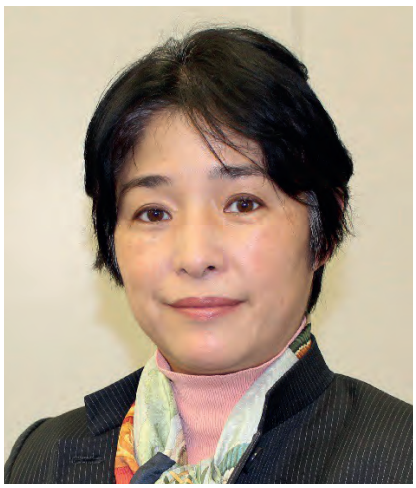
This does not mean that the sole response from the public authorities should be defensive. Where innovation helps the financial system function more efficiently, it must be supported, as central banks have kept doing since decades. The private sector, to the extent that it does bring improvements without inducing unaddressed new risks, is of course best placed here, be it for front-end or back-end payment solutions. Central banks have also a role to play, as issuers of the reference settlement asset and operators of critical payments infrastructures. This is why Banque de France will experiment a wholesale Central bank digital currency, with a view to fooding Eurosystem thoughts. This is why also it fully supports - and actively contributes to - the G20 roadmap on the improvement of cross-border payments. ●

Yuko Kawai

General Manager for Europe,
Bank of Japan

Covid-19, digitalization of payments, and the crypto assets

The outbreak of Covid-19 and subsequent lockdown of many societies have reinforced the necessity to promote digitalization in payments. Today, as of the end of March 2020, one-third of the global population is said to be under some sort of lockdowns, and any payments using physical measures are subject to significant constraints. Some retailers try to avoid touching banknotes and coins. Bank checks are subject to the delivery constraints. Furthermore, even for the electronic remittance by corporations and financial institutions, physical security measures such as token devices, or a dedicated computer terminal with an exclusive IP address, which are kept or installed in the office premises, prohibit the parties from making remittance once their employees are suddenly required to work from home. I believe that people who felt inconvenience will look for the digital solutions. ▶



▶ Should we consider the crypto assets, including the stable coins, in our new regime? Why not. Once such time comes, we will need to use every piece of wisdom to recover from the consequence of this pandemic. If the decentralized and digital encryption features, which are common in many crypto assets/coins, can serve the purpose of elimination of physical devices with good security, it is worth pursuing.

Having said that, I also would like to pay attention to the risks. The obvious challenges to crypto assets are the cyber security, AML checks, and the backstops when things go wrong. Also, the stableness of the stable coin may be questioned during the severe market turmoil. In fact, some of so-called stable coins experienced unusual value fluctuations in March 2020 amid the spike of the volatility in financial markets. These issues also lead to the question about the consumer protections.

Also, if we assume the wider usage of stable coins operated outside of the banking system, it may reduce the presence of the banks, then we will need to consider who will replace the functions banks are currently providing. For example, under the current crisis, in order for the financial compensations to support curtailing the social contacts, or, in later days, to support the recovery of damaged economic sectors, data to identify the most needed recipients and the swift and effective measures to remit money to them are vital. The substantial part of this financial support is expected to take the form of loans, the traditional bank products. In countries where digital neo money platforms are already in full broom, these functions maybe supplemented by them, but I myself am not sure whether the currently suggested stable coin frameworks will function in a similar manner.

As discussed above, I believe the current crisis will make us think more about the digitalization of payments, which may include the crypto assets, but the risks and points of governance will not change in crisis from the peaceful time. I hope that the discussion about the crypto assets, or more specifically about the embedded decentralization and digital encryption technologies will help us to improve the efficiency of the incumbent payment system as well. ●

Nicole Sandler

Regulatory Policy Lead, Barclays

Stablecoins – refining the regulatory landscape of crypto-assets

Blockchain and crypto-assets have changed the way people think about money, and this technology is a focus area for policymakers globally. To date there exist over 2000 different types of crypto-assets, with no precise definition of what these are, rather there are a variety of terms that describe more or less overlapping phenomena. The understanding in regulatory terms of what we are dealing with is varied, with some current classifications, commonly used by EU policymakers ie exchange/payment, security and utility tokens, being too broad and requiring further clarification based on a token's characteristics.

Today, the United Nations recognises 180 currencies worldwide from the US dollar to the British Pound to the European Euro, and more, with these currencies being used to buy goods and services. The value of most of these currencies is subject to minor changes on a daily basis, for instance a pint of milk will standardly cost £1 in the supermarket and one does not have to worry that it will be £2 on any day that same month. However, one of the criticisms of a number of cryptocurrencies (a sub-type of crypto-assets) as a means of payment, is the volatility in price fluctuations – the same pint of milk could cost anywhere between 20p - £10 in a given week.

'Stablecoins', another subset of crypto-assets, have characteristics that distinguish them from the categories mentioned above, most notably their stabilisation functionality with underlying or reference asset - what that underlying or reference asset may be varies from coin to coin. To date, the key distinctions among stablecoins have been the governance and the mechanisms for maintaining stability. However, it is important to flag that there are many different types of so-called stablecoins with some being neither stable nor a coin. That aside, the main benefit generally associated with stablecoins, is that depending on how and what they are pegged to, they may not be subject to the extreme price volatility that other crypto-assets are affected by.

In addition, they could potentially offer decentralisation, and in some cases global reach, with the ability to help the unbanked. These reasons are why this class of crypto-assets are seen by some as an attractive means of payment. Whilst there are a lot of discussions about the use of stablecoins, particularly from a policy perspective, the majority of industry participants are not yet launching anything in this space, primarily because of the lack of regulatory clarity on how such assets should be treated. Whilst there are benefits which warrant further discussion, this does not mean they are free from risks.

These include (i) risks to consumer protection, data privacy and financial stability, (ii) they could promote illicit activities, (iii) threats to weaker currencies and (iv) banks may lose their place as intermediaries if they lose deposits to stablecoin providers. The current financial markets uncertainty (brought upon by the COVID-19 crisis) has the potential for changing habits across all society in looking for technological 'safe havens'. While this may hasten some of the debate and support for certain crypto-assets, this still needs to be a measured and strategic response.

It is important that given the cross-border nature of many types of crypto-assets, that the industry and policymakers work together across jurisdictions to have agreed definitions and regulations to minimise the risks and maximise the benefits. Further, it is essential that the approach policymakers take is a uniform one that applies the principle of 'same activity, same risk, same regulation' in order to avoid fragmentation and allow market participants to benefit from scaling effects. ●

Pan-European retail payments

Ulrich Bindseil

Director General, DG Market Infrastructure & Payments, European Central Bank (ECB)

Key requirements for a future-proof European retail payments market

The transformation of the retail payment landscape is driven by technological progress, legislative and regulatory action and cross-industry initiatives led by large global digital firms. Keeping step with these developments puts established banks and payment service providers increasingly under pressure.

In Europe, the payments industry is at risk of losing its economic edge. Whereas a fair level of progress has been achieved at the back-end of the retail payments chain with harmonised SEPA standards and pan-European settlement, the customer front-end, in particular for point-of-sale and online payments, remains fragmented along national borders. This predominance of country-specific solutions hinders competition and stifles innovation at the pan-European level.

In addition, a growing dependence on non-European global players creates the risk that the European payments market will become susceptible to external disruption. Furthermore, global service providers with market power may not necessarily act in the best interest of European stakeholders.

The only effective remedy to this situation is the development of an industry-led, pan-European retail payment solution that facilitates instant, secure and inexpensive payments – both online and in brick and mortar stores. With the aim of fostering pan-European market initiatives for retail payments at the point of interaction (POI), the Eurosystem has put forward a payments strategy that provides conceptual vision as well as high-level guidance to the market. Market initiatives aiming to deliver pan-European retail payment solutions would have to fulfil five key objectives.

First, customers should be able to make POI payments throughout the entire European Union just as efficiently and safely as in their home country. To this end, pan-European reach with wide merchant acceptance is required.

Second, to achieve a high degree of customer acceptance, such a solution needs to be designed in a way that enables an easy, flexible, secure and user-friendly payment experience for both consumers and merchants. It should be flexible enough to allow the use of different payment instruments, initiation channels and technologies.

Third, a new European payments solution must comply with all relevant legal and regulatory requirements. To boost consumer confidence, it should provide the highest levels of fraud prevention and offer consumer protection with robust complaint and refund procedures.

Fourth, it should aim to foster European identity by using a common brand and logo. A European governance structure would enable European payment stakeholders to have direct influence on the strategic direction and business models.

Fifth, to reinforce economies of scale and domestic adoption and to keep step with other global solutions, a new European solution should also be accessible to merchants based outside the EU.

European stakeholders are invited to step up their collaboration and act together. ●

Stéphanie Yon-Courtin

Vice-Chair & MEP, Committee on Economic and Monetary Affairs, European Parliament

The pan-European payments market: innovative competition and protective autonomy

A pan-European market for payments is at the heart of the EU promises to consumers and businesses. It should at the same time allow for innovation through competition on a level playing field and build autonomous capacity in the EU in light of growing global fragmentation and economic stimulus needs post-COVID crisis.

Decisive EU action to open competition in the retail payment space, in particular thanks to open finance pioneered in the Payment Service Directive (PSD2), has brought about innovation to the benefit of European consumers. Digital services offered by innovative players – for example on international transfers or currency conversion – have eased the daily ▶

lives of citizens travelling across the European continent and abroad. Through price transparency, consumers have been empowered to start a new dialogue with incumbent providers on payment services and associated charges. Consumers can also rely on price regulation when transparency is not enough to ensure they receive a fair treatment.

> *A pan-European market for payments is at the heart of the EU promises to consumers and businesses.*

This welcome innovation should however not be at the expense of the protection guaranteed to all EU citizens. The EU rulebook on anti-money laundering, security, privacy, and consumer protection should be respected with the same level of ambition when the nature of services is comparable, regardless of the provider and with an equal level of protection across the EU. When exploring new payments solutions, we should also remain mindful of citizens that are less digital literate and that could encounter accessibility challenges.

European businesses have also benefited from the gradual buildup of an efficient payment system for the single market. The Single Euro Payments Area (SEPA) and the most recent TARGET Instant Payment Settlement (TIPS) have already shown the benefits of EU action to accelerate C2C, C2B and B2B transactions within the Eurozone. Cryptocurrencies could further smooth payment operations in the future. Enhanced individual portability of data access and reuse could also fuel innovative business models at all levels of the payment value chain.

European autonomy should be the cornerstone of all future EU initiatives, to preserve European sovereignty in the current crisis context. We need more action to reduce the knock-on effects of dependency on non-European card schemes, in order to preserve the independence of our foreign policy decisions and of our ability to finance economic recovery.

Similarly, the emergence of new actors, including BigTechs, in the payment and currency areas begs the question of the powers for European regulators to control the impact of these new ventures on the European economy, as we grow more reliant on access to digital services in our day-to-day lives.

The European Renaissance will require pan-European payment systems bringing innovative solutions for consumers and businesses. These new infrastructures and services will ensure that Europe remains autonomous in the wake of post-COVID recovery and with the disruption of economic models that digital innovation creates. ●

Burkhard Balz

Member of the Executive Board, Deutsche Bundesbank

Forming a competitive European payments market that benefits society at large

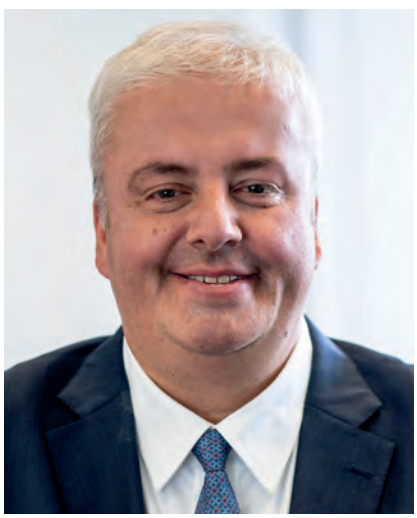
Cashless payments are becoming ever more common place. In the EU, around 140 billion non-cash transactions were processed in 2018, up 8.8% on the year. Market intelligence is projecting further annual expansion rates of 8.5% up until 2022 and expecting associated revenues to grow by around 6% p.a. through to 2028.The bulk of global revenues is generated by card payments, which currently account for 62%.

However, incumbent banks appear to be capturing less of the revenue growth than their rivals. The last few years have seen digital banking and smartphone banks burst onto the scene and global technology firms, BigTechs, make inroads into the payments and banking space. These firms can leverage their platforms and capitalise on extensive network, scale and scope effects to enhance their market power. Considerable changes in user preferences are fuelling this development.

> *Now it's time to make a pan-European payment solution a reality.*

While consumers undoubtedly value the convenience of global platforms, there are some challenges for European societies as a whole. Platform economies tend to favour monopolies, so as BigTechs gain ever greater shares of the payments and banking business, the contestability and competitiveness of European markets will diminish.

Furthermore, banks face the risk of being disintermediated by platform solutions as they lose their direct links with their customers. Consequently, they might end up as mere commodity suppliers of back-end banking infrastructure and regulatory compliance on behalf of digital solutions.



So their margins and revenues are at stake. In addition, European providers usually manage payments and other banking segments as a profit centre activity. That means putting a price tag on account-providing and payment services. For most platform models, though, it's the data analytics that tend to be monetised. Given the above-mentioned monopolistic tendencies, consumers should continue to be able to choose whether they wish to depend on data-driven models or accept a fair price for using services that ▶

▶ minimise the collection and use of their data.

Against this backdrop, European authorities are calling for a compelling pan-European payment solution that addresses these challenges. National central banks on the continent have responded by defining five key objectives that this solution would need to satisfy: 1) pan-European reach and uniform customer experience; 2) convenience and cost efficiency; 3) safety and security; 4) European identity and governance; and 5) global acceptance in the long term.

Now it's time for European market players to make this solution a reality. A number of building blocks, like instant payments and the necessary infrastructure, are already being rolled out. Others, such as standardised request-to-pay and confirmation messaging, as well as common security mechanisms, are still lacking. Moreover, European providers need assurance that payments can remain an attractive business. Also, it is crucial for them to have a level playing field with their new rivals, like in terms of having reasonable access to technical interfaces such as NFC. Ultimately, though, the industry will need to forge a compelling solution for all the different payment situations – one that will be to the taste of European consumers. Otherwise, consumers might ultimately turn away. ●

Carlos Carriedo

Senior Vice President & General Manager, Global Commercial Services Europe, American Express

European retail payments – the EU's defining moment

In the last decade, Europe has been a global pioneer and a standard-setter in terms of payments. The second Payment Services Directive ("PSD2") in particular has been one of the most revolutionising pieces of legislation in decades, especially when it comes to boosting innovation. Implementing all of its estimable objectives, however, has proven harder to achieve than many would have thought, and these shortcomings provide valuable lessons for the future.

Indeed, Europe's future as a world leader in this area is anything but certain. Today, the region is part of a highly connected world, where physical borders matter less than ever. When shopping online, today's consumers want limitless options. They expect to be able to buy from any EU Member State, Asia or the United States, with no or few restrictions. All the evidence suggests that these expectations are even more pronounced among millennials, who pay little heed to the provenance of the goods or services they select. They just want the best online service they can get.

These generational changes imply both risks and opportunities for companies, regardless if they are European or non-European. One thing, however, is certain: companies which can match consumer expectations with global market realities, while providing the seamless and fast service consumers want, and the security they demand, are the ones that will succeed.

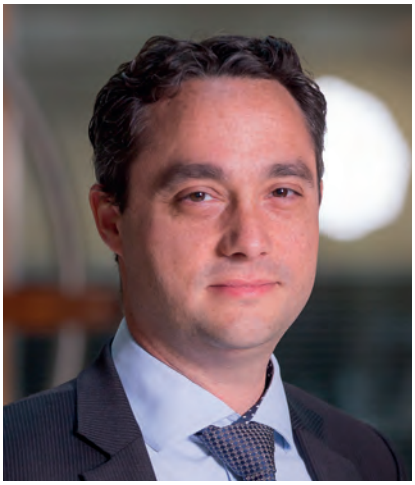
Yet over the last two years, the EU has advocated for a pan-European solution in the payments market, with many policymakers calling for more investment in domestic solutions. On the face of it, a pan-European scheme would increase competition and provide consumers with a new choice in an otherwise duopolistic card payments' market. This increase in choice is something we would welcome. However, in a world where consumers wish to shop globally, any domestic or regional solution must be able to meet their needs by offering not just speed and reliability, but true global interoperability. Without this, no amount of political support will be enough to ensure a new, home-grown European scheme can succeed.

While considering the development of pan-European solutions, we believe there are also other paths the EU could, and should, consider to increase competition even further. For instance, PSD2 - as well as PSD1 - focused on measures that sought to encourage competition, by facilitating the entry of non-bank players to the market. The EU should assess how to replicate similar measures, for instance by broadening the scope of open banking to open finance, bring into scope the full range of financial services – from insurance to savings and pensions products – that European consumers and small businesses crave.

> *"Any domestic or regional solution must be able to meet their needs by offering not just speed and reliability, but true global interoperability.*

By the same token, it is incumbent on the EU to address the shortcomings of existing pieces of legislation, most notably the Interchange Fee Regulation (IFR). That Regulation, too, was intended to boost competition, but instead reinforced the existing duopoly by focusing almost entirely on price reduction – a savings which has yet to be truly passed on to consumers. Any future review should bring back genuine competition to the heart of the IFR, by making it easier for new and small players to enter and to thrive.

The stakes could hardly be higher. For whatever path is finally chosen, it will have the potential either to secure or to scupper the EU's place as a global competitor. ●



Roeland van der Stappen

Head of Regulatory Affairs,
Europe, Visa Europe

European retail payments at a crossroads

We are at crossroads in the payment and banking sector, driven together on one side by innovators and disruptors in the FinTech world and governments and regulators who see an opportunity to put the consumer in control of their money and financial data.

Open finance is where they converge, all centered on putting consumers in control of their money and their financial data. This opens the banking market to new players, services and possibilities while giving consumers more choice than ever imagined.

Europe is at the leading edge of that change. European regulation, such as the revised Payment Services Directive (PSD2), through a focus on open access and standard-setting, has paved the way for open finance to flourish and created new opportunities for innovations that consumers need and want to adopt.

Importantly, the design of the PSD2 regulation has enabled businesses to innovate in an unfettered and consistent way across the single market. It has allowed consumers to benefit from the best of what the world has to offer, and empowered consumers to make that choice for themselves.

In a world that is moving fast and digital, Europeans continue to have high expectations for security, reliability, control and protection. They want choice and simplicity as they manage their financial lives.

When we think about the future of payments, we should stay grounded in consumers' expressed needs and on enabling choice to maintain a level playing field and continued innovation, without prescribing operational solutions and technology.

There are also inherent trade-offs if infrastructure is local or regionalized rather than global. International payment networks offer some of the highest levels of cyber –and operational resilience.

The ability to route data through multiple data center around the world, with instant fail-over capabilities, contribute to best-in-class operational resilience. At the same time, access to global data for cyber threat analysis allows for the detection of fraud/scams outside of Europe in order to react faster to threats to European citizens.

> *When we think about the future of payments, we should stay grounded in consumers' expressed needs and on enabling choice to maintain a level playing field and continued innovation, without prescribing operational solutions and technology.*

If Europe wants to stay ahead in payment innovation and encourage the emergence of FinTech players, it is better to promote innovation and set common and open standards that facilitate change, rather than build new European-only infrastructure.

This approach would support operational and cyber resilience, while expanding the opportunities for competition, growth and innovation – which drives the best results for consumers. This will be ever more important as we move towards open finance. ●

Mikael Svensson

Head of Public Policy, Europe,
Government Affairs and Public Relations,
Mastercard Europe

Increasing competition in the European payments market

Over the past years, the European retail payments market has gone through significant transformation. Thanks to technological innovations, consumers and merchants now have a wide range of payment methods they can choose from. The change in consumer habits, in particular the growth in cross-border and online commerce, has changed the dynamics of payments and how they enable new and different shopping experiences that benefit the consumer and the retailer.

In addition to these consumer- and technology-driven developments, Europe has been at the forefront of regulation to boost electronic payments, reduce end-users' costs, prevent fraud and disable barriers for new players entering the market. The EU Interchange Fee Regulation and 2nd Payment ▶

Services Directive (PSD2), which are inherently linked, are still having a huge impact on the market and the full effects are yet to be seen. Indeed, Europe is the region with the lowest payment acceptance costs in the world and the PSD2 continues to drive further competition in the European payments market. As the PSD2 opens the payments market to new entrants, it also leads to greater choice for consumers and businesses by enabling them to use third-party providers to manage their finances and initiate payments on their behalf.

Even if most in-store transactions in Europe are still conducted with cash, the increased competition has resulted in consumers having access to multiple payment methods including cards, cash, mobile phone payments, payments through wearables, such as watches or wristbands, voice-enabled devices or other new payment methods that use (often instant) credit transfers directly from their bank accounts. With the increased use of smartphones and apps, further growth of innovative payment methods is expected.

> *Legal certainty is paramount for new and existing players to develop innovative solutions that meet consumers' and businesses' needs.*

New alternatives also mean that consumers and retailers use multiple payment methods depending on the situation they are in. This leads to payment service providers increasingly competing for consumers to use their payment solution at the point of sale, in store, or online. Innovation, convenience and safety are fundamental in this.

As the effects of existing regulation are further unfolding, one can expect these trends to continue. Also, digital wallets are expected to be used more broadly by consumers. Instant payments, often enabled by third parties, QR codes or Near Field Communication (NFC) will also offer new alternatives. These trends mean that the market for retail payments is likely to continue to deliver good outcomes in terms of efficiency, innovation and choice in the future, provided that the right regulatory framework is in place.

Legal certainty is paramount for new and existing players to develop innovative solutions that meet consumers' and businesses' needs. Further legislation should therefore only be considered once the full effects of existing rules and regulation are known and a need for further regulation has been identified. This is the best way that innovation and competition continue to flourish in this sector across Europe. ●

Dr. Joachim Schmalzl

Executive Member of the Board, Deutscher Sparkassen- und Giroverband (DSGV)

Payments in Europe - set the course now!

The increasing momentum in the payment transactions sector has accelerated significantly in recent months. But what are the drivers that have caused payments - an area which might previously have been considered boring - to reach the attention of decision-makers in the banking industry? The answer to this is complex: the rapid technical development seen over the last few years has been a global driver, enabling an increasing number of new services in this area and leading to dramatic changes in existing payment offers and the processes behind them.

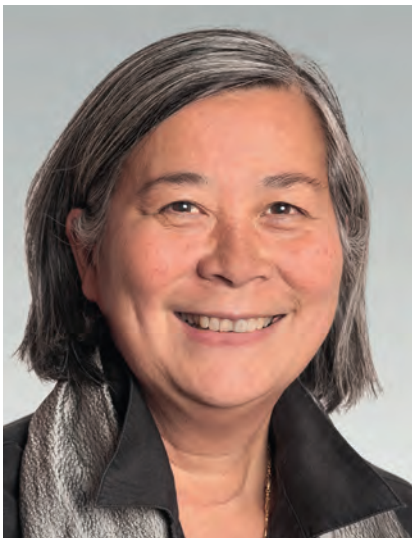
Closely linked to this are the entirely new customer requirements and the resultant offers in the area of payments and additional payment services, for example in the area of data usage. Whereas payment business was previously the domain of banks or bank-related service providers, there are now a large number of providers in the market which are outside the banking sphere and which just a few years ago played only a minor role. These not only damage the banks' position as payment service providers, but also their important role as account managers, because third-party providers will foreseeably expand their services, which are currently still based on payments, to other lucrative business areas. This gives the subject a completely different, existential dimension in addition to the purely financial consideration: the anxious question that arises for the banks is whether they will continue to be the account-holding entity for customers in future, and thus the first port of call for financial services, or whether they will be displaced to a secondary role.

> *The German Savings Banks Finance Group wishes to play an active role in shaping European payment transactions.*

How should European banks respond to this development? Certainly not with "business as usual" as this is sure to lead very predictably and quickly to the situation described above. Despite the recent political and economic challenges, Europe is a strong continent - if it acts in a concerted, consistent and focused manner. And this is particularly true for the payments sector. Why not join forces and put all our weight behind this? With almost 513 million inhabitants, around 697.5 million current accounts and more than 112 billion payment transactions annually, the European Union has the potential to shape the European payments market with a focus on European requirements and to offer customers modern and exciting payment services. The Savings Banks Finance Group has already completed ▶

valuable preliminary work in this area. For example, instant payments were implemented very early and consistently in the Group, currently enabling around 10 million transactions (incoming and outgoing payments, as at the beginning of April) to be processed each month. In addition to this, a highly customer-oriented P2P process has been developed on the basis of instant payments to serve as the basis for further expansion stages, e.g. for P2B transactions. A further focus of activities is the provision and expansion of convenient smartphone-based POS payment solutions, whether based on credit cards or on the German debit card payment scheme girocard.

The German Savings Banks Finance Group, as the market leader for payments in Germany, wishes to play an active role in shaping European payment transactions and is therefore intensively involved in the work of the European Payments Initiative (EPI). The aim must be to create uniform payment scheme throughout Europe with the potential for innovation in all customer-relevant use cases, based on sustainable business models. This is the only way to create a successful counter-model to internationally operating and financially strong players. ●



Narinda You

Head of Strategy & Market Regulation, Credit Agricole Payment Services

Emerging payment means a myth or a reality?

Payments are and will be executed through payment accounts. These accounts were a bank monopoly but with PSD2 some new players appeared on the market under the status of Payment institutions.

These new Payment service providers are still relying on bank payment means but they could develop a certain kind of intermediation with the growth of e-money transactions in market places organised by large merchants for instance.

Banks should pay attention to this evolution because it could weaken their intermediation role and limit them to mere payment account handling considered more as a commodity than real services.

The customers be they on payee or payer side believe that their payment services are secured by their banks. They do not always realise that when using new "payment solutions" they are not in the same trust environment.

Banks have invested for decades to protect their customer data and to secure their processes.

They are under scrutiny of multiple authorities and overseers. They have the ability to monitor and report whilst it is not always the case of new players.

As the reputation and financial risks will be borne by banks they have to understand these new ecosystems, the user experience, the easiness and the immediacy that seem to become the new normal.

They also will have to examine very carefully their new clients needs: to activate/de-activate, to increase/decrease the payments amounts authorised, temporarily/permanently, specific counterparts or not, etc. It is then our responsibility to allow them to do so in the limits of our risk analysis and appetite.

On the merchant side, it is crucial for banks to be able to provide information with the right level of protection and security to allow them to develop their business and mitigate their fraud rate.

The mean of payment is not important per se. What will make the difference is whether one or the other offers more easiness and benefits to both payer and payee.

It is important too to be able to rely on sustainable providers offering security and availability.

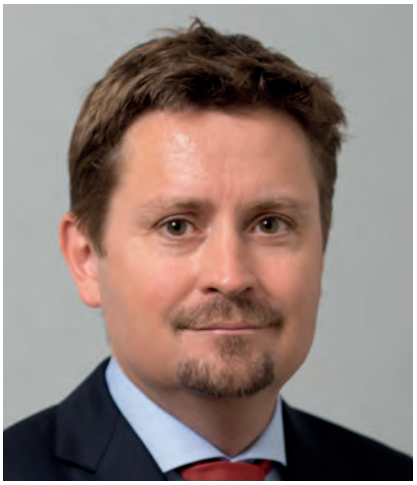
It is the ambition of 20 large banks in Europe to deliver such an end-to-end pan-European payment solution that would bundle a card (plastic) and a wallet (digital card or payment account based) relying on an interbank settlement through SCT Inst which is a genuine European scheme. The key factors of success reside in the attractiveness of the solution, the speed of adoption and deployment.

> *"The crisis we experience today should intensify the work because this project could be a strategic move in the European payment policy.*

It is crucial to maintain the momentum of the EPI Project (European Payment Initiative) that necessitated nearly one year of discussions among banks but also with the other stakeholders such as the international card schemes, the non-bank acquirers and some processors and manufacturers ... and of course the regulators at national and European level.

The crisis we experience today should not slow down but, on the contrary, intensify the work because this project becomes more relevant than ever and could be a strategic move in the European payment policy. ●

Ensuring operational resilience with increasing digitalisation



Morten Bech

Head of Secretariat, CPMI,
Bank for International Settlements (BIS)

Avoiding a cyber mess

"Don't put all your eggs in one basket" is good advice for life, and for operational resilience too. The job of concentrating functions and risk in the financial system needs to be handled with care, and maximum resilience. Decades of work on financial market infrastructures have strengthened business continuity arrangements to ensure continuity of services through fires, floods and power outages, and pandemics. The eggs are safe in the basket.

Cyber risk has made keeping our eggs safe a far more complex and challenging task. Now, replicating data for a seamless failover to a backup site could help spread compromised data across all systems. It might not be obvious that any irregularities are even malicious until it is too late to share information. Outsourcing critical services might help better distribute operational risk, but if everyone uses a common service provider, then an issue can quickly become systemic. Cyber scrambled egg is a risk.

The CPMI's strategy to avoid the omelette is to "protect the core and secure the periphery". The core of the financial system comprises the financial market infrastructures that are covered by the CPMI- IOSCO Guidance on cyber resilience for financial market infrastructures, which led the way for standard setters in this field. Yet cyber defence cannot be boiled down to a pass-or-fail test; improving it requires a cooperative approach. A CPMI-IOSCO roundtable that brought together the 22 largest global and regional FMIs and their supervisors identified three key challenges that need a common solution: (i) data integrity, (ii) information-sharing and (iii) third-party service providers.

International industry-led working groups were set up to tackle each of these challenges. This is the first time this type of cooperative approach has been adopted. Each group has a tough challenge. For data integrity, or how to recover if underlying data are corrupted, there are a number of possible avenues to explore, including contingency arrangements, segregated ledgers and frequent reconciliations. For information-sharing, common protocols exist to share financial events, but operational incidents are still segregated by type of FMI, market and jurisdiction. Setting expectations and developing a practical arrangement for alerting on international operational incidents could enable faster and better-informed responses. Third-party services (eg cloud) can benefit from cooperation by users, provide a clearer view of risk management practices at the common service provider and avoid duplicating third-party risk assessments.

So, although the challenges are tough, financial authorities, infrastructure and their members all have an incentive to cooperate and avoid a cyber crisis. Working together now, to strengthen common operational resilience, can ensure we avoid scrambling our cyber eggs. If we fail to do this, we will all end up with egg on our face. ●

Simon Chard

Partner, Operational Resilience Lead, PwC

Standardised regulatory requirements can improve operational resilience

Everyone is talking about operational resilience. With a fast moving COVID-19 that may become the ultimate stress test, right in the middle of regulatory consultations across Europe, it's the key topic for firms. There is no shortage of policy areas to focus on to make both individual firms and the wider financial system more resilient. We covered a number of them in depth in our report "Operational Resilience: Time to Act" with theCityUK. In this article, I'd like to focus on four areas identified by the European Commission in their consultation: ICT and security risk management and incident reporting requirements, digital operational resilience testing and third party oversight.

The current state of ICT and security management requirements in Europe is inconsistent across sectors. While I don't believe anyone needs to be convinced that improved, consistent standards for risk and resilience across Europe would lead to ▶

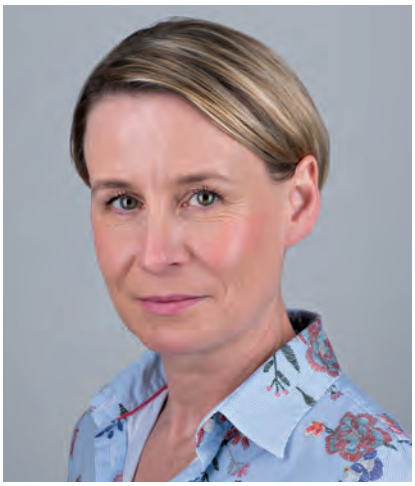
an uplift in practices, let's talk benefits. Operational resilience is an outcome, not a process, function or methodology. So benefits must be evident from any initiative taken. For firms, having one standard means a level playing field in Europe, and clarity about what is expected for service chains which cross borders into different regulatory territories. For customers, improved management of risks means more reliable services and improved trust in financial institutions.

It goes without saying that even with the best risk management in the world, failure is inevitable. Industry-recognised standards on the timeliness and nature of reported incidents would enable customers to make decisions based on the relative resilience of firms. Increased consistency and transparency of reporting can also accelerate industry-wide detection of emerging systemic risks and help regulators and firms in their responses.

This understanding of emerging risks should be used to drive digital operational resilience testing. While almost all firms adhere to an operational testing regime, there is again currently no standardised framework. While such a framework may increase costs, if applied with appropriate proportionality, it could not only give firms more confidence in their own ICT and security estate but also that of other firms in their supply chain. For customers, improved and consistent testing will lead to greater confidence in the security and privacy of their assets.

Thinking about supply chains leads us to the final policy area: third party oversight. Third party failure is one of the most common causes of outages, so how well third parties are managed can clearly have a critical impact on the resilience of financial firms and markets. A common framework to manage third parties would not only reduce systemic risk by uplifting standards but also allow firms to leverage this framework to demand more of their suppliers via increased audit rights and participation in scenario stress tests.

Harmonisation of requirements across sectors in Europe can clearly be beneficial not just for customers but for firms and markets. While Brexit may create challenges for European harmonisation, we shouldn't lose sight of the fact that financial services routinely cross borders and therefore greater standardisation with shared global norms will surely be a good thing. ●



Nicola Russell

Director, Global Operational Resilience, HSBC Scotland

Operational resilience as an outcome

Technology to enable digitalisation and innovation has been a priority for financial firms as well as for financial services policy makers for some years now. However, as the financial sector becomes more digital, attention is beginning to turn in earnest to the risks posed by a greater use of technology. A renewed conversation is needed about how firms, and the financial system in general, can become more operationally resilient in the face of rapid technological change to the sector and the economy more generally.

Good risk management provides a strong foundation upon which to build resilience. While regulations for ICT risk and cyber security have existed for years, there has been an uptick in the amount of new regulation in these areas with more on the way. While necessary in the short term, eventually we will reach a point where more risk management offers diminishing returns for improving resilience. We must instead remain focused on achieving resilience as an outcome and not be distracted by a compliance driven exercise more concerned about ticking a box.

A focus on outcomes allows firms the flexibility they need to keep up with a shifting operational environment. The threat landscape for digitally-enabled businesses continues to change and the system is growing more complex, in part to deal with the expectations of consumers enabled by legislation like PSD2. This continuous change will make prescriptive regulation increasingly ineffective; for instance, a mandated risk control measure that was vital one year may be obsolete the next as the technology and threats evolve. In contrast, a focus on outcomes, monitored and enforced through supervision, allows firms to continuously innovate in risk management and resilience while ensuring that regulatory policy objectives are still achieved.

So what does the future of operational resilience look like for both firms and policy makers? All market participants including regulators, firms and policy makers have a shared motivation to ensure the financial system and its participants can continue to withstand, and operate through, disruption. As stakeholders in the financial system we must all recognise this common goal and develop more collaborative ways of working together toward that outcome if sustainable progress is to be made.

For firms, with the threats, system complexity and use of technology increasing, operational resilience must become more holistic. Firms are already shifting their focus to ensuring that they can continue to provide what is important for their customers, the market and their own operations in the event of disruption. That means ensuring the resilience of the systems, people and processes that support these services from top to bottom.

For policy makers, there is a need to step back and consider the macro context. Fragmentation has been an issue in financial regulation for over a decade. International bodies such as the FSB and BCBS have worked to address this and they will need to do the same in the area of operational regulation. Europe has a part to play in that effort. Finally, time is needed – time for current regulation to embed and begin to make a difference, and time for a new approach suited to the future financial services system to evolve. ●