Deutsche Bank
Global Transaction Banking

Regulation driving banking transformation

Insights into the key regulatory developments shaping APIs, artificial intelligence, blockchain and cloud

#PositiveImpact

Contents

Foreword 3

1 Executive summary 5

2 Introduction to the global fintech regulatory environment 7

3 Open Banking/Open APIs 9

- 3.1 What is it? 9
- 3.2 What are the benefits? 10
- 3.3 Current regulatory picture 11
- 3.4 Key regulatory challenges and solutions 13
- 3.5 What does the future hold? 15

4 Cloud 16

- 4.1 What is it? 16
- 4.2 What are the benefits? 17
- 4.3 Current regulatory picture 18
- 4.4 Key regulatory challenges and solutions 20
- 4.5 What does the future hold? 22

5 Blockchain 23

- 5.1 What is it? 23
- 5.2 What are the benefits? 23
- 5.3 Current regulatory picture 24
- 5.4 Key regulatory challenges and solutions 24
- 5.5 What does the future hold? 28

6. Artificial Intelligence 30

- 6.1 What is it? 30
- 6.2 What are the benefits? 30
- 6.3 Current regulatory picture 31
- 6.4 Key regulatory challenges and solutions 31
- 6.5 What does the future hold? 34

7 Conclusion 35

8 Contributors 36

9 Glossary 38

Foreword: Re-imagining banking

Technology is fundamentally altering our behaviour. Growing up, I was taught never to get into a car with a stranger. Today, I don't think twice about using an app to actively request a lift from one. The success of Uber, Lyft, Didi and others suggests I am not the only one

Thomas Nielsen, Chief Digital Officer, Global Transaction Banking, Deutsche Bank

Technology provides us with a huge opportunity to change our business models, releasing some control of the component value chain in order to better meet the new needs of clients. If we ignore this opportunity, clients will either force us to change, or worse, vote with their wallets. Disrupt or be disrupted.

Nokia's fall from grace in a relatively short period of time should be a lesson for us all. They created the most successful mobile phone handsets, but it was a monolithic, closed-wall garden – the consumer was limited to the functionality installed on the phone they purchased from Nokia. If I didn't like my phone's digital calendar or email client then, well, tough. Then Apple burst onto the scene and instead of competing with Nokia they changed the rules, and exposed the iPhone's functionality through Application Programming Interfaces (APIs) so that developers could write and deploy applications side-by-side with Apple's own applications. Now, I can choose from multiple calendars and email applications, provided by multiple companies, in the App Store.

This was a tectonic shift in technology, business model and mindset that enabled a US$100bn+ global app economy and turned Apple into one of the most valuable companies on the planet.

This is the promise of Open Banking – banks exposing their platforms and services to their clients, partners, fintechs or even competitors in a safe and secure manner through APIs to create thriving and sprawling ecosystems that produce new and exciting solutions. Post-PSD2, the next frontier for Open Banking will be twofold: commercial APIs in transaction banking – transitioning from retail solutions to high-value, global and complex transactions in a multitude of forms and currencies – and collaboration between banks and regulators to facilitate direct and secure access to data for compliance and regulatory purposes through APIs.

APIs may provide us with the most immediate and obvious opportunities to re-imagine our operations and services, but I am equally excited by the power of blockchain, artificial intelligence (AI) and the public cloud.

At the most basic level, banks take deposits, keep them safe and lend them out. Every bank in every country records this in their own "bank book" – a ledger which acts a single source of truth – which has simply become digitalised over the years. But why just digitalise instead of re-imagining in a globally connected digital world? Blockchain enables us to create a shared digital vault that allows data to be accurately verified and trusted by multiple parties – in a distributed fashion – promoting efficiency, security and speed. The potential use cases are plentiful, touching many areas: from settlement, trade finance and smart contracts, through to payments and regulatory access and reporting.

We also realise that being “data-aware” is no longer good enough. Banks need to be powered by data. This means they must organise, analyse and use data to reshape business models and improve client service. This is the potential of AI, which also could change how we conduct risk management, compliance and fraud detection.

Cloud technology underpins all of this innovation by providing the necessary on-demand and flexible computation power, storage, advanced tools and infrastructure on a global scale. I could go and buy 50,000 servers and build a data centre to be able to run AI analysis over client data. But why do that, and then let it sit idle when not needed, when I instead can adjust the scale of my IT infrastructure freely and instantly using the (public) cloud?

Banks need to place these innovations not just at the heart of their technology strategies, but at the heart of their business strategies. This requires cultural change, bank-wide adoption of new technologies and IT infrastructures, and defined rules for how data is governed and made secure – especially across borders. And all of those strategies must be underpinned by a “secure and compliant” by design approach.

To do this properly, we must also be prepared to disrupt our own businesses. Netflix is a perfect example of the power of disruption. The streaming giant’s original business was built on selling or renting out DVDs, but it took the strategic decision to develop a streaming business alongside it. In hindsight, it seems obvious, but at the time it was radical. They knew that, if successful, streaming would kill their highly lucrative DVD business. It did, of course, but it also created the company we know today.

Ours is, of course, a more closely regulated business that holds more sensitive client information and has a greater impact on the financial system. The intersection of data, technology and business model shift at a global scale – driven primarily by consumers, but also by corporates – offers unprecedented opportunity, but also comes with great responsibilities.

Getting this right is something that can only be done through collaboration with regulators and a wide range of industry groups. We must be responsible. But we need to disrupt, or be disrupted.

1

Executive summary

New technologies have always had the potential to redefine how societies behave, interact and work. But this century's re-definition has nonetheless been remarkable, with humans and businesses operating in a way that would have been unthinkable even just a few decades ago. The age-old business of banking has not been immune to this. Yet there is further change coming

Potentially the most transformative impact of Application Programming Interfaces (APIs), cloud, blockchain and artificial intelligence (AI) lies in the way they allow more effective collection, storage and analysis of the vast and rapid flow of one of the modern global economy's most valuable commodities: data. This, quite rightly, puts cybersecurity and data protection firmly under the regulatory spotlight. We have seen regulators implement global cyber security standards for banks – from strong customer authentication for online payments to fraud monitoring – and rapidly enact data privacy legislations and broader data protection requirements. An emerging area of focus is now the ethical use of client data.

At the same time, regulators understand that barriers to the implementation of these new technologies can hinder banking innovation, competition and the development of new products and better pricing for banking clients. As such, many regulators have thrown their weight behind supporting innovation: you need only look at the multitude of fintech and innovation initiatives that have sprung up globally as evidence of this. It's not just Europe with the European Digital Single Market, it's also the reports on fintech and innovation published this year by India and the US, and transformative initiatives from Australia, Hong Kong and Singapore, which are leading the Asia-Pacific charge.

Contributors to this white paper applaud regulatory efforts to balance innovation and risk management. After all, we are all wrestling with the same challenge. Yet there is broad agreement that there are areas for improvement: the need for acceptance of the new realities created by emerging technologies, and the need for further global regulatory alignment.

Banks are re-imagining their operations, processes and solutions in this new, digital data world. It is important that regulators keep pace with such change.

For instance, legislation relies on traditional means of ensuring data and information security – requiring access to premises where data is stored on cloud for the purpose of physical audits is one example. Re-thinking this approach to rather focus on the advanced distributed platforms and cyber security tools employed by cloud service providers would accelerate the movement of core banking services to cloud.

This paper highlights a number of other areas where we face similar issues – the European Union (EU)'s General Data Protection Regulation (GDPR), as another example, enshrines the "right to be forgotten", potentially hindering the opportunities derived from the immutability of blockchain. Meanwhile, the application of AI brings new complexities to the use of data by banks. Legislation addressing the fact that bank processes need no longer be human-driven would help banks to securely and ethically explore the power of AI.

Global technological solutions require a global regulatory response. Undoubtedly, further regulatory alignment on a global level would greatly support the development of innovative technologies for global business. This is particularly important in the context of data protection and security standards – as long as the rules vary across jurisdictions, technological solutions will be constrained by local boundaries, diluting their potential to transform the industry. If we allow this to happen, we are missing a trick.

This doesn't mean we have to establish a single global standard for regulation, however. We have to be pragmatic. The realistic goal here is attaining a threshold level of alignment across jurisdictions – one that leaves a degree of room for differing standards where complete agreement is unrealistic, but where a broadly similar approach across all jurisdictions would unleash the benefits of global solutions.

Global sandboxes (as envisaged by Global Financial Innovation Network; a collaboration between the UK's Financial Conduct Authority and 11 other financial regulators and related organisations) are one step that could facilitate the move towards globally aligned regulatory solutions. These provide a safe environment for regulators and the industry to identify, learn and uncover the regulatory gaps and barriers at a global level. Given the fast-moving nature of technology and its applications, industry practices should be at the forefront of such collaborative solutions.

We are on the cusp of major change. And forward-thinking regulation stands to be a major catalyst for a thriving and innovative banking industry.

2

Introduction to the global fintech regulatory environment

The emergence of new technology solutions relating to Open APIs, cloud, blockchain and AI – and their uptake by the banking industry – has driven increasing volumes of digital data, and new market players, business models and evolving client expectations

Given the potential of this to significantly transform the banking sector, regulators around the world have taken a closer look – and continue to monitor – the opportunities and risks that technology may bring to the market. New ways of using data, new types of market players and business models, and new cyber threats are among the top items for regulatory focus (see Figure 1).

Figure 1: Fintech: regulators' focus

Area of regulatory focus	Regulatory objectives	Regulatory response
Data usage	– Protect individual privacy – Ensure data is not misused or manipulated – Prevent data leakage – Prevent unethical use of data	– Data protection and data privacy requirements – Advice on ethical aspects of using data
New market players and business models	– Support competition and innovation – Set level playing field for fintech firms and banks – Secure the safety of the financial system as a whole	– Opening client data to fintech firms in a secure manner – Licensing and authorisation of fintech firms – "Same services, same rules" approach – Encouraging responsible innovation – Technology-neutral rules
New cyber threats	– Ensure cyber security and client protection	– Customer awareness – Secure communication – Strong customer authentication – Technical preventive measures – Fraud monitoring and detection

Source: Deutsche Bank

The regulatory response has happened at different speeds globally. Broadly speaking, it is focused on laying the foundations for realising the growth opportunities for emerging technologies while, at the same time, addressing the risks they may bring. Whether it is the EU Digital Single Market initiative, the US Treasury Report on innovation, the Reserve Bank of India Report on innovation, or the New Era of Smart Banking initiative in Hong Kong, it is fair to say that policymakers around the world are focused on promoting innovation by supporting competition and removing barriers to the employment of new technologies which promise to improve digital infrastructure, goods and services.

The next few years will shape the future of financial technology. This is an ongoing process, however, and while there is a strong commitment of regulators to drive innovation, there are still certain regulatory challenges to the immediate uptake of new technologies in the banking industry.

In this paper, we provide a high level overview of the regulations applicable with respect to banks' – and their clients' – use of Open APIs, cloud, blockchain and AI, and assess areas where regulatory and market change could help drive uptake of these technologies by the financial industry.

3

Open Banking/Open APIs

3.1 What is it?

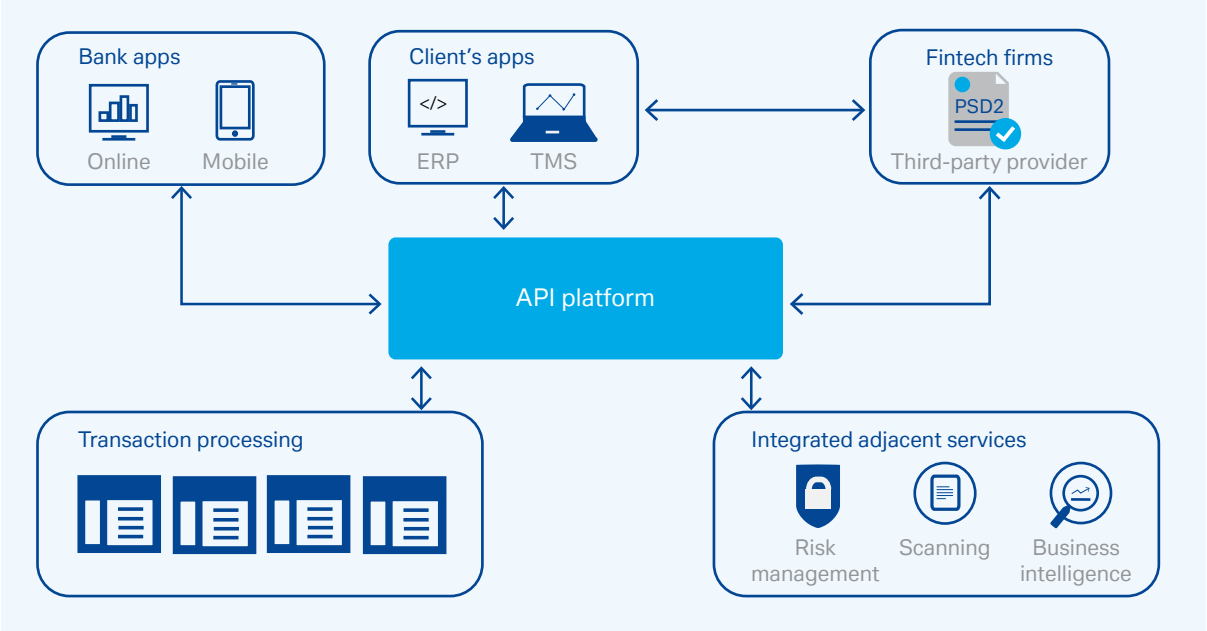
Open Banking is, as the name suggests, the opening up of banks' systems and solutions to third-party providers, or TPPs, facilitating access to customers' payment services and account information in a regulated and secure way. The enabler for Open Banking is APIs.

Industry practitioners seem to agree they are currently on a journey, the object of which is "to provide an easy-to-use, seamless customer experience, with new digital services offered across a broad number of touchpoints." These were the words of John Gibbons, Head of Global Transaction Banking at Deutsche Bank, when announcing Deutsche Bank's acquisition of India-based fintech and API specialist Quantiguous Solutions.[1]

Many banks are, as such, proactively creating and implementing strategies in the Open Banking space (as Deutsche Bank's Thomas Nielsen discussed at EBAday in June 2018[2]), which promise to redefine banks' relationship with customers, in terms of how they engage with them, the services they provide, as well as the channels through which they do so.

Open Banking also redefines how banks view APIs – code that allows one piece of software to talk to another, while hiding the complexity of the underlying functions.[3] APIs have been used by banks for decades, but these have been proprietary and used only for specific internal use cases. Now, banks are exploring how Open APIs can be used to help clients, partners, other financial institutions and fintechs to easily integrate with, and build new solutions around banks' systems and infrastructure (see Figure 2).

Figure 2: Integrated use of Open APIs within banking



Source: Deutsche Bank

> " Open Banking requires banks to embrace new technologies and IT infrastructures, establish defined rules on how data is governed and made secure – especially cross-border – and drive cultural change. Clients want to access information and financial services through one API, not to deal with a wide array of banks using different APIs. This gives us a major opportunity to really transform the client experience for the better "
>
> *Thomas Nielsen, Deutsche Bank*

3.2 What are the benefits?

Those financial institutions that can best unlock the business value of APIs stand to win, and win big. A recent Accenture report suggests €61bn (7%) of the total banking revenue pool in Europe by 2020 will be linked to Open Banking-enabled activities.[4]

This doesn't seem too far-fetched when you cast an eye at other industries. Salesforce.com generates nearly 50 percent of its annual US$3bn in revenue through APIs, while Expedia generates nearly 90 percent of its annual US$2bn in revenue through utilisation of the technology.[5] The "API economy" has arrived.

In short, Open APIs can: reduce payment costs, speed-up settlement times, automate banking services through clients' data workflow and provide the opportunity to develop new products and services.

With respect to the EU's PSD2 (see next section for more detail), many companies are only just beginning to realise the opportunities that this provides to speed-up settlement times and reduce the cost of their payments. Deutsche Bank's payments pilot with the International Air Transport Association (IATA) (see box) is a clear example of the opportunities that this new landscape brings.

Push payments in action: IATA

Deutsche Bank's payments pilot with IATA – the trade association for the world's airlines – will implement a new and much improved solution for internet-based ticket sales to individuals, and is a perfect example of the opportunities that the new API-enabled landscape brings. Via this solution, enabled by Open APIs, Deutsche Bank will collect customer payments for tickets directly from individual consumer accounts, removing the need for them to make credit and debit transactions to the airlines.

Using instant payments supported by SEPA Instant Credit Transfer (SCT Inst), these direct payments can be processed and received in near-real time and airlines can receive funds faster, generating significant working capital and liquidity benefits. Crucially, by removing costly transaction fees and enhancing fraud protection (via two-factor authentication), they can also significantly reduce their costs. The pilot is initially due to be rolled out in Germany in Q4 2018/Q1 2019, and thereafter goes Europe-wide in Q2 2019.

Source: https://www.db.com/newsroom_news/2018/deutsche-bank-pilots-game-changing-payments-solution-with-iata-en-11574.htm

Speaking in an interview on the subject, Vanessa Manning, Head of Liquidity and Investment Solutions at Deutsche Bank, is quick to point out that Open APIs also facilitate the investment of liquidity. She asserts that "once the cash conversion cycle becomes faster and shorter – because of 24/7 payments, APIs for account information, optimal investment decision analytics and movement of AI to accelerate cash conversion cycle through auto-matching – the payment execution and settlement all but disappears."[6]

There is also value in banks using Open APIs to partner with fintechs, as and when required, to build end-to-end solutions. Yet Thomas Nielsen describes how "for them to really add value, they need to be able to integrate into core banking infrastructure".[7] Open APIs – with the appropriate security standards around data transfers in place – therefore promise to transform customer experience and business processes in equal measure.

3.3 Current regulatory picture

There has been broad global acknowledgement by regulators as to the benefits of both Open Banking – as a means of providing a more competitive and innovative financial services landscape – and Open APIs, as an enabler of this. Open Banking regulatory initiatives (see Figure 3 on page 12) therefore have, and will, act as a catalyst for the development of Open APIs – with many initiatives so far focused on the payments and bank account information services.

However, the way in which regulators approach Open Banking varies globally. Not only is there no single view whether it should be mandatory, crucially, we have yet to see consensus regarding API standards, security standards or the certification of TPPs that gain access to customers' information.

In Europe, PSD2 is a major driver of the move towards Open Banking, although its most transformative provisions are yet to come into full effect. From September 2019, they will oblige banks to give TPPs access to customer accounts, with their explicit consent, through a new interface. While not mandated, there seems to be industry consensus that APIs will provide the most secure and effective solution to this.

It is not just Europe, however. In Asia, the Monetary Authority of Singapore (MAS) has been proactive in encouraging financial institutions to develop and share their APIs openly, while similar support for Open Banking has been witnessed in Hong Kong.

Broadly, Asian regulators have promoted Open Banking as a means of driving competition and creating efficiencies, with a strong focus on industry collaboration.

The US Treasury's report, released in July 2018, suggests that it should be the market, and not the government, that lays the foundations of Open Banking.[8] The US Treasury does, therefore, recognise the need to remove legal and regulatory uncertainties that act as barriers to data sharing agreements. Open Banking seems inevitable although it will likely have a different flavour to PSD2.

> " The changing end-to-end value chain that will result from TPP access to account data, needs to be delivered and managed to give regulators confidence that new risks are understood and managed, for example, operational and cyber risk, fraud and financial crime "
>
> *Hamish Thomas, Ernst & Young*

Figure 3: Region-by-region regulatory progress

3.4 Key regulatory challenges and solutions

The challenge of Open API standardisation

Why does it matter?

All of the potential benefits that banks and corporates can potentially seize from an innovative Open Banking environment depend on a minimum level of API standardisation to allow incumbent and new players to compete and collaborate on a level playing field, bringing their customers innovative solutions in a safe and secure manner.

Certainly, standardising Open APIs is crucial to creating a large-scale ecosystem where all participants can run interoperable solutions and mutually benefit from Open APIs. The cost for most banks, corporates and fintech firms to adopt multiple technologies allowing them to connect to different APIs and comply with a number of diverging standards would most likely be prohibitive – hindering the technology's potential to transform processes.

For banking clients, a lack of standardisation would potentially jeopardise the security and efficiency of solutions and ultimately undermine the experience they receive. With safety paramount, a single approach to cyber security within an Open Banking ecosystem – particularly around customer authentication and authorisation procedures – is needed to develop trust, improve security and reduce the risk of fraud.

Latest developments

Broadly speaking, Open API standards are not defined at the regulatory level – which most market participants view as a major barrier to progress – especially in Asia-Pacific where different countries set their own requirements for Open Banking. Similarly, in Europe, PSD2 does not cover the functional and technical details of the dedicated interface that TPPs should use to connect with banks, rather just the scope of what it should deliver.

As a result, market initiatives have emerged to fill in the gap, although they remain local in nature; indeed, the Berlin Group's NextGenPSD2 initiative[9] is the only API standard that was cross-border from its very inception. Noteworthy from the point of view of local collaboration are the CMA Open Banking API (UK), STET API (France), and the API specifications published by the Slovak, Czech and Polish banking associations respectively. In a positive development, the Berlin Group and STET are in advanced convergence discussions and have agreed to full alignment on any future developments. This, thankfully, brings harmonisation of the API landscape more clearly in view.

Many eyes are on standardisation progress in Europe – decisions made will likely have a wide geographical influence on the global move towards Open Banking, setting clear precedents for international standardisation organisations to follow.

Suggested solutions

For these standardisation efforts to progress, Shahrokh Moinian, Global Head of Cash Products, Cash Management, at Deutsche Bank stresses that "market participants should co-operate, adopt best practice and align themselves with developing common global standards" (*see the Deutsche Bank white paper, Unlocking opportunities in the API economy for more information*).[10] The greater the efforts market participants make now to get up to speed on Open API development and to stay abreast of evolving global standards, the more open, competitive and efficient the global market for Open API-facilitated services will become.

Crucially, the steps banks take should go beyond mere regulatory compliance, as they are the first steps into an entirely new world of financial services. While cooperation and alignment are already in progress, more work is needed.

The technologically agnostic requirements for Open APIs, if set by the regulators, would be compatible with the variety of technological solutions for data and platforms adopted by different market participants. Having industry driving the development and implementation of standards should ensure an approach that is agile and sensitive to changes in both technology and market conditions.

Where standards are not forthcoming, we would encourage banks to experiment, as long as with regulatory support and within a secure framework, in order to meet client demands in a timely fashion.

The challenges around TPP access

Why does it matter?

One of the fundamental aspects of Open Banking is that it opens the gates for other market participants to access client data that was traditionally the preserve of banks. Yet, for this to work in practice, it must be underpinned by a significant level of trust and security. This means accountability of those accessing bank data in order to maintain cybersecurity and avoid misuse, leakage or fraud. It also means banks being able to ensure that a party accessing client data or initiating payments is duly authorised to do so, and having an audit trail of when data has been accessed or changed.

Having a reliable register or certification – updated in real-time and allowing for automated transmission of data – which allows real-time verification that a party accessing client data or initiating payments is licensed for such activity, is therefore essential.

Latest developments

While EU TPPs are subject to authorisation – the European Banking Authority (EBA) will maintain a centralised register.

PRETA's Open Banking Europe directory[11] is also expected to provide a repository where all third-party providers may list their contact information. So far, 30 financial institutions and industry service providers have joined. Mastercard has also announced it is developing a pan-EU directory service which will include fraud monitoring, a dispute resolution services and a connectivity hub. Meanwhile, ETSI completed a standard for EU qualified certificates as defined in the eIDAS regulation in May 2018 that meets secure communication requirements under PSD2.

In Asia, the Hong Kong Monetary Authority (HKMA) consultation on Open Banking considered three potential approaches to TPP certification: bilateral – where banks carry out their own risk assessment and due diligence on any bilateral engagement with a TPP; central certification entity – where a central body is funded and formed with agreement by all the banks involved to certify TPPs; or bilateral with common baseline – where a set of risk-based and due diligence baseline criteria is developed and agreed by banks.[12] Based on the discussions held, and feedback received, during the consultation exercise, the bilateral arrangement with a common baseline was the preferred option.

Suggested solution

The most reliable solution for TPP certification would clearly be certification by the regulator (as in Europe), ensuring that certification carries weight and is an enforceable requirement. As a result, it would generate trust in API-enabled solutions and increase their competitiveness.

As the number of transactions and payment services initiated through TPPs grows over the coming years, any register used to record their details must be real-time, in order to be at all times reliable and trusted.

It is not clear whether certification and central registers will happen across all jurisdictions globally, however. In the meantime, private enterprises are developing their own registers; their usefulness has yet to be tested in practice.

3.5 What does the future hold?

Despite the significant hype, we conclude that Open Banking is only at the nascent stage of its development – with the focus currently on regulatory compliance in locations where it is mandatory (such as PSD2 in Europe). We must go well beyond compliance to reap the full benefits on offer. Positively, we already see signs of the industry transitioning to the next stage, where banks see the opportunities provided by this innovative ecosystem and proactively open up their data and platforms to competitors and their products.

The spread of Open Banking globally is underpinned by the support of regulators, which are removing barriers to entry and suggesting or requiring that banks open up their data securely to TPPs. Regulators, like industry, see the potential Open Banking can bring for retail and corporate clients in terms of competition and innovation, as well as providing a more collaborative market ecosystem.

Moving to a more open environment, defined by greater standardisation and collaboration, would constitute a major leap forward. Yet we can – and should – go further. Speaking on a panel at EBAday, Deutsche Bank's Thomas Nielsen and Nordea's Claus Richter outlined that the next step on the journey towards true Open Banking should see all parties leverage and monetise each other's data and products (a business model adopted by YouTube, for instance).[13]

The ultimate goal would see the creation of an ecosystem value chain that moves beyond offering just traditional banking products, similar to Amazon's business model.

But let's not get ahead of ourselves. Successfully progressing through each stage of openness will be impossible without first addressing the early challenges we witness. This boils down to two crucial issues: first, the need to have standardised Open APIs and, second, the ability to have a reliable certification by the regulator and source of information for identification of third-parties that are accessing client data.

Addressing these challenges should be spear-headed by the industry experts in order that we generate a secure and structured framework where all players can commit to Open Banking strategies.

4

Cloud

4.1 What is it?

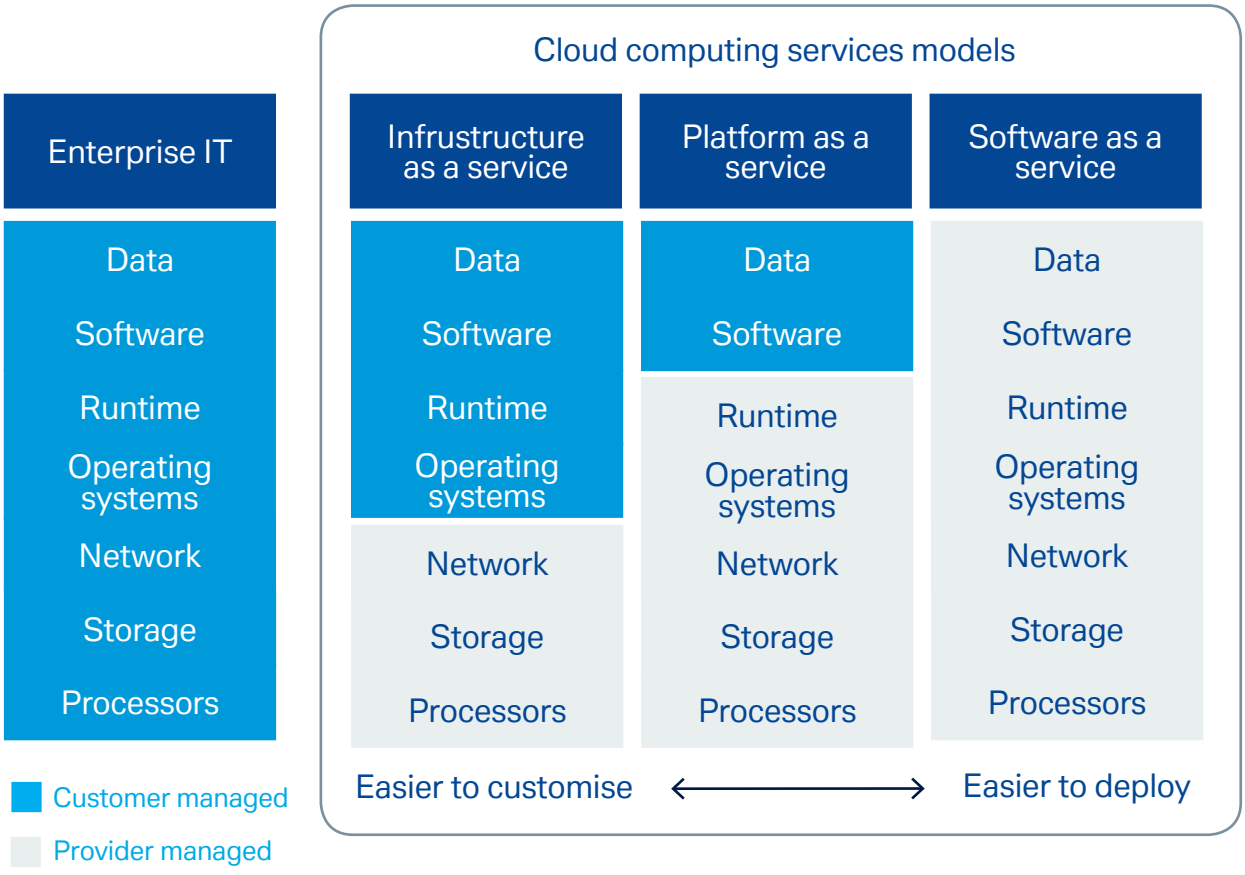
The US National Institute of Standards and Technology defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released.[14]

Cloud computing is not new to financial services: banks have been using private clouds for decades. There are many cloud computing service models that are currently available (see Figure 4). Yet most banks continue to approach the use of public cloud with a healthy dose of caution and scepticism, focusing instead on establishing their own private clouds, and relying on their own IT infrastructure.

The IDC Cloud Tracker expects the finance industry to spend US$4bn on cloud technology in 2018 (compared to US$3.23bn in 2017) – yet this pales in comparison to other industries. Healthcare providers, for instance, are expected to spend over US$10bn on cloud this year.[15]

While the EBA states that banks therefore remain in the "exploratory stage" of implementing cloud, many are now looking at the possibility of migrating core systems from private to public clouds, signifying a significant leap forward.

Figure 4: Cloud computing service models compared to enterprise IT



Source: US Treasury Report on Nonbank Financials, Fintech, and Innovation (page 46)

4.2 What are the benefits?

By providing near-unlimited hardware and software resources on a global and pay-as-you-go basis, cloud computing drives down costs, enables innovation and creates the flexibility to respond to change. Banks can scale-up and scale-down their IT infrastructure as required – escaping the encumbrances of their legacy IT systems and avoiding regular and expensive upgrade work.

As Thomas Nielsen explained for the purpose of this paper, the computing capacity opened up by a cloud environment provides the perfect building blocks for other technology innovations – APIs, blockchain and AI – which require "global computing power and capacity beyond the infrastructure of most banks". The combination of big data and potentially unlimited computing power, for instance, will allow banks to develop systems capable of providing better insight into clients' behaviour – and make better informed decisions.

Cloud Service Providers (CSPs) can also add value in a cloud environment. With respect to cyber security, CSPs can provide the most up-to-date security, reliably and on a cost-effective utility-based model. CSPs also offer a whole host of analytical tools for users to take advantage of. Indeed, cloud is increasingly becoming a platform to democratise access to AI technology to allow all businesses, large and small, and public sector institutions to innovate with the help of state-of-the-art technology, without further investment into complex research.

Given the obvious benefits, the question is: why has cloud uptake by financial institutions been so sluggish? A recent US Treasury report asserts that there are many reasons for this, although the report highlights "the criticality of such functions and the difficulty of transitioning away from legacy IT systems."[16]

On 3 July 2018, the EBA concurred with this perspective in a report on "the impact of fintech on incumbent credit institutions' business models".[17] It observed that while many banks have already altered existing processes to account for technology such as mobile banking and biometrics, they are still in the "exploratory stage" of implementing the "second wave" of technologies comprising cloud, big data, AI and blockchain.

The importance of these functions, and the data they hold and use, is clearly central to the issue. Traditionally, banks have been reluctant to embrace cloud computing on security grounds say the majority of CSPs that contributed to this paper, although Google also stated that "perceptions towards cloud technology are rapidly changing as businesses and public sector organisations increasingly recognise the potential of cloud to tackle security concerns."[18]

Certainly, the major CSPs have invested heavily in securing their infrastructure with many hundreds of engineers dedicated to security and privacy. Microsoft asserts that this means that "you can extend your security perimeter across your modern digital landscape, and be better poised to protect yourself in an increasingly hostile environment". In addition, it suggests that, "with a traditional security approach a breach can remain undetected

> " Perceptions towards cloud technology are rapidly changing as businesses and public sector organisations increasingly recognise the potential of cloud to tackle security concerns "
>
> *Nicholas Bramble, Google*

> " Cloud computing, has been one of the most disruptive forces in the technology industry over the past decade – driving down costs, generating flexibility and, crucially, providing the building blocks for other technologies to operate to their full potential. At the same time, public clouds and multi-cloud environments have allowed customers to choose their optimum combination of providers and services "
>
> *Thomas Nielsen, Deutsche Bank*

for a long period and cause significant harm to a business", whereas its approach is to "assume we are always breached, utilising advanced threat detection and continuous monitoring to ensure early detection and containment of all breaches".[19]

As security fears soften, we may be approaching a new era for cloud utilisation in the financial services sector. A report by the Asia Cloud Computing Association (ACCA) suggests that, as the technology proves its worth and security, "the migration of core systems to the cloud will be the next frontier of cloud adoption".[20] The report states that many will do this to ease the burden on their IT budgets as the pressure to innovate increases and costs of upgrading legacy core systems rise in step. Regulators' recognition of the suitability of cloud adoption, and the availability of successful case studies, will spur this trend, says the ACCA.

4.3 Current regulatory picture

Moving banking services to the cloud does, of course, not relieve a financial institution of its responsibilities with respect to confidentiality, integrity and availability of data. Financial institutions' cloud arrangements are subject to both cybersecurity and data protection regulations, as well as banking-specific outsourcing rules – requirements which must be ensured through proper contracts, monitoring and auditing of cloud services providers (as prescribed by the regulators).

Financial regulators' outsourcing guidelines therefore have a key role to play in shaping this environment, and can determine the extent to which financial institutions can benefit from cloud computing technology.

Speaking for the purpose of this paper, Noémie Papp, from the European Banking Federation (EBF), comments, "success will clearly need a harmonised approach to such issues as chain outsourcing, which provides the right balance between security and innovation. Certainly, the variation by national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers."[21]

In Europe, the EBA recommendations on cloud outsourcing seek to make financial institutions responsible for the activities of their outsourced cloud provider, and require them to closely supervise this.[22] Similarly, in Asia, a number of regulators have moved towards clarifying rules and guidelines to aid firms in achieving compliance in their outsourcing activities; notably in Hong Kong and Singapore.

Laurence Van der Loo from Asia Securities Industry & Financial Markets Association (ASIFMA), highlights however that in Asia "there are significant regulatory challenges when rolling it out across large parts of Asia. A number of Asian countries – including China, India and Indonesia – have restrictive data regulations that prohibit offshore data storage and processing. As long as these are in place, this will strictly limit cloud use."[23]

> " Public clouds are global by nature for reasons of elasticity, reliability and availability. Differing regulations by country or region, which are sometimes conflicting, make it difficult for CSPs to comply "
>
> *Olivier Colinet, Ernst & Young*

Uncertainties over financial supervisory authorities' expectations remain in some jurisdictions due, in particular, to the absence of harmonisation of national rules and different interpretations of outsourcing rules. There are a number of areas where there is an uneasy fit between what the regulators demand of financial institutions and what information or control is realistically available to them regarding the cloud services they receive.

The US Treasury report makes the point that "the large number of [US] regulators involved with allowing the use of cloud in financial services can present administrative burdens, as well as challenges with inconsistent requirements".[24]

Figure 5: Region-by-region regulatory progress

Cloud

Europe

The EBA Recommendations on outsourcing to Cloud Service Providers

December 2017

Establishes the security measures and controls for using cloud, e.g. access and audit rights, security of data and systems, location of data and processing

The European Commission (EC) FinTech action plan

March 2018

Mentions a number of actions, including the proposal for a regulation on a framework for the free flow of non-personal data in the EU, which aims to remove unjustified data localisation restrictions (e.g. relevant to the use of cloud)

EC will encourage and facilitate the development of standard contractual clauses for cloud outsourcing by financial institutions, building on the cross-sectorial cloud stakeholder efforts already facilitated by the Commission, and ensuring financial sector involvement in this process

Australia

Secure Cloud Strategy

1 February 2018

This strategy replaces the 2014 Australian Government Cloud Computing Policy and focuses on what will make it easier for government agencies to use cloud services.

The strategy outlines a number of ways to help build understanding of cloud and confidence in using it, as well as growing the skills to transform old systems

US

The US Treasury report on Nonbank Financials, Fintech, and Innovation

July 2018

US Treasury recommends that federal financial regulators modernise their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud.

US Treasury also recommends that a cloud and financial services working group be established among financial regulators so that cloud policies can benefit from deep and sustained understanding by regulatory authorities

India

Recommendations on Cloud Services By TRAI

August 2017

Aims to strike an appropriate balance between innovation and the business needs of this rapidly evolving sector and the protection of interests of consumers of cloud services.

Recommends an overarching and comprehensive data protection law covering all sectors, including a legal framework to protect the data being collected, stored and processed in the cloud

Singapore

MAS Guidelines on outsourcing

July 2016

Sets out MAS' stance on cloud computing and gives clarity on its positive posture towards financial institutions' use of cloud services.

Establishes the rules for data use, confidentiality and security, resilience and business continuity, as well as the rules around due diligence, audit and monitoring and control of services

4.4 Key regulatory challenges

The challenge of data location requirements

Why does it matter?

Data hosted by a CSP can reside in multiple geographical regions as directed by the client. While technology has developed – and sentiment changed – the traditional belief that data can only be secured if close-to-hand persists in the form of data location and restrictions applicable when moving data abroad. As the Information Technology and Innovation Foundation notes, "dozens of countries have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country's borders."[25]

In particular, a number of Asian countries – including China, India and Indonesia – have restrictive data regulations that prohibit offshore data storage and processing. Data privacy laws, especially GDPR, in Europe set certain requirements for data transfer outside of the region. CSPs tend to offer universal solutions, GDPR requirements will need to be embedded in these solutions – irrelevant of whether banks intend to store personal data or not.

> " It is the customer's choice how they design and deploy an application in the cloud, however we provide architectural blueprints and technical expertise to guide them in best utilising our resiliency and data protection features. We commit that data will only ever reside in the storage locations that clients specify, and we offer geo-redundancy features to support in-country data sovereignty requirements"
>
> *Andrew Dapre, Microsoft*

The impact of data location requirements is an area of contention among market participants. Some suggest that as long as these are in place, they will strictly limit cloud use, as companies' servers must remain within the borders of the country in which they are located. The recent US Treasury report notes that data localisation can "have unintended and harmful effects on competition, innovation, and economic growth".[26]

Others argue that restrictions are only prohibitive if the CSP does not have a global footprint of data centres, allowing for data to be stored within domestic borders and enabling it to work within data regulations. They argue that having such a footprint negates the issue: a bank could store its data in Germany, yet access it on screen and run applications using it via the cloud in Australia, without the data ever having to cross borders "physically".

Nonetheless, experience suggests that it does provide a challenge for banks and their legal and compliance teams, requiring significant resource.

Latest developments

The European Commission's proposal for a framework for the free flow of non-personal data (cited in its FinTech Action plan[27]) is a step in the right direction when it comes to removing a key barrier relating to unjustified data localisation restrictions.

In a similar vein, the recent US Treasury report suggests that concerns about data security and access can be better addressed through technology, enhanced security controls, contractual arrangements, and bilateral or multi-jurisdictional agreements.[28] This is a helpful, and forward-thinking, approach.

> " As more advanced security technologies and privacy solutions become available, regulators will likely retreat from old-school data localisation requirements and instead identify new best practices – including redundant geographic storage of data and the usage of distributed security solutions such as sharing and obfuscation to safeguard the security of data in the cloud "
>
> *Nicholas Bramble, Google*

The ACCA's report notes progress in this respect, although points to continuing data localisation issues in Indonesia – where regulation has been passed mandating that firms keep disaster recovery resources and personal and transaction data within Indonesian borders – and Malaysia, where new draft outsourcing guidelines have data localisation requirements. India, also, will ask all payment service operators – as well as their service providers and third-party vendors – to store their payments data within Indian borders by 5 October 2018, for the regulator's unrestricted access.[29]

Suggested solutions

Globally, it is of course difficult to achieve harmonisation without a single rule book that applies to everyone. This requires internationally-recognised and harmonised high level principles for data management, and guidance on how these apply specifically to CSP arrangements. Industry led initiatives – including both cloud users and providers – in co-ordination with the regulators, with principles reviewed on an ongoing basis, could be swiftly amended in line with market practice and developments.

Some degree of regulatory convergence and interoperability is achievable through trade agreements, notes Google in an interview for this paper. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership includes clear prohibitions on data localisation as well as a requirement that parties allow "the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a service supplier".

The challenge of access and audit rights

Why does it matter?

Current regulation (notably in Europe) requires financial institutions to not only know where their data is physically located, but to be able to access and audit it. When using cloud services, however, the user's data is physically located on a server within the CSP's network.

In Asia, ambiguity surrounding the scope and frequency of audit rights can therefore cause difficulties when these rights are being negotiated, says the ACCA. Agreeing on the scope of such rights could be challenging because the CSP may be reluctant to grant full and wide-ranging access (sometimes for fear of undermining their confidentiality and security policies). This therefore poses a problem for financial institutions seeking to make the most of cloud services.

While an understanding by CSPs of the issues – and a willingness to be flexible – undoubtedly softens the problem, banks' experiences point to this issue being one that can slow negotiations, and restrict uptake for some without the necessary legal resources to cope.

> " Given a CSP has many clients, compliance with regulatory requirements to maintain physical access audit rights might be a challenge – how would a CSP support broad rights of access and audit in practice for thousands or millions of their clients? At the very least, differing interpretations of these regulations can complicate and slow negotiations between banks and CSPs "
>
> *Polina Evstifeeva, Deutsche Bank*

Further, these regulatory issues may have implications for a bank's relationship with a CSP that outsources some of its operations. In Europe, the EBA's cloud outsourcing recommendations mandate that banks must not only ensure that their CSPs fulfil all regulatory requirements, but that any subcontractors of those CSPs do also. Access and audit rights therefore have to be cascaded down in a CSP chain to any subcontractor – which could include a significant number of entities.

This poses a number of challenges. Banks have little control over the nature of a CSP's whole outsourcing chain, especially given the dynamic nature of the cloud environment and the fact they use a complex infrastructure based on multi-tier supply chains. They are therefore heavily reliant on CSPs to share the necessary information, and implement contracts with their supply chain to ensure this is done.

Latest developments

The EBA's report on outsourcing may provide a way forward, recognising alternative solutions to on-site audits: pooled audits; third-party certification; third-party or internal audit reports made available by CSPs. That said, this brings new concerns relating to the risk to business operations from multiple parallel regulatory requests to CSPs or potentially duplicative requests.

The ACCA's report notes that a number of its region's regulators have also moved towards clarifying rules and guidelines to aid firms in achieving compliance in their outsourcing activities. However, it provides a note of warning for Malaysia: if its outsourcing guidelines are finalised in their current draft form[30], they will mandate that financial institutions must have the rights to access a CSP's premise, and will stipulate maximum periods for outsourcing agreements. This will limit scalability, and constitute a step backwards.

Suggested solutions

Principally, we welcome the EBA's alternative suggestions for audit rights. However, we suspect that while pooled audits may work in some cases, they may not in others (indeed, UK Finance, responding to the EBA paper, described them as "prohibitively difficult to arrange" in some instances[31]). It is therefore important that the EBA continues to engage with cloud stakeholders to consider alternative approaches to satisfy these contractual requirements, while removing potential burdens and duplication, and maintaining risk controls.

Other potential solutions could include the regulator-driven shared assessments of CSPs (on behalf of a consortium of financial institutions) or the wider use of industry certifications (such as ISO) as an alternative to direct oversight. Alternatively, self-regulation of CSPs – subject to standards which they set in consultation with financial regulators – could be another way forward, guaranteeing legal certainty and facilitating the adoption of cloud-based solutions by financial institutions.

One particularly interesting approach relates to the intersection between public cloud, APIs and blockchain. It is possible to imagine a world where local regulators will be able to audit data and transactions related to their particular jurisdiction through a set of "self-service" APIs that relies on local storage and distributed trust.

4.5 What does the future hold?

> " The more transparency from the CSPs on their sub-contractors and their respective certifications, the more comfortable corporations from all industries will be in adopting cloud across their full application suite "
>
> *Olivier Colinet, Ernst & Young*

The potential of cloud computing is huge, evidenced by its transformative impact in other markets, where it has allowed companies to increase efficiencies, lower costs and improve time to market.

As the EBA's fintech report reveals, banks have been reticent to follow suit, and that a potential migration to the cloud could increase Information and Communication technology (ICT) change risk in the event of reliance on complex legacy infrastructure. Issues related to the jurisdictional location of data are another area for focus. Yet these barriers are rapidly falling, with many banks now exploring how they can move even their core operations to cloud infrastructure.[32]

Many firms have also come to see cloud as a way of improving security, rather than endangering it. Indeed, we can now accept that cloud providers often implement and manage industry-leading security controls – their business and reputation depend on it.

For regulation to be an enabler of change, it must evolve at pace and remain relevant to today's digital world – data in the cloud is a different species to data on paper. Auditing the premises where such data is stored, therefore, arguably does little to provide increased controls and security over intangible data existing on huge servers in data processing centres across the globe.

Re-assessment of perceptions of how data is best managed and made secure is therefore crucial if banks are to work with CSPs to employ cloud widely to the benefit of their clients.

5

Blockchain

5.1 What is it?

Blockchain works by creating blocks of record (location of goods, for instance), that are built upon by further blocks – once agreed by all participants. This creates a chain of related blocks that are all irrefutable: a blockchain (see Figure 6 below).

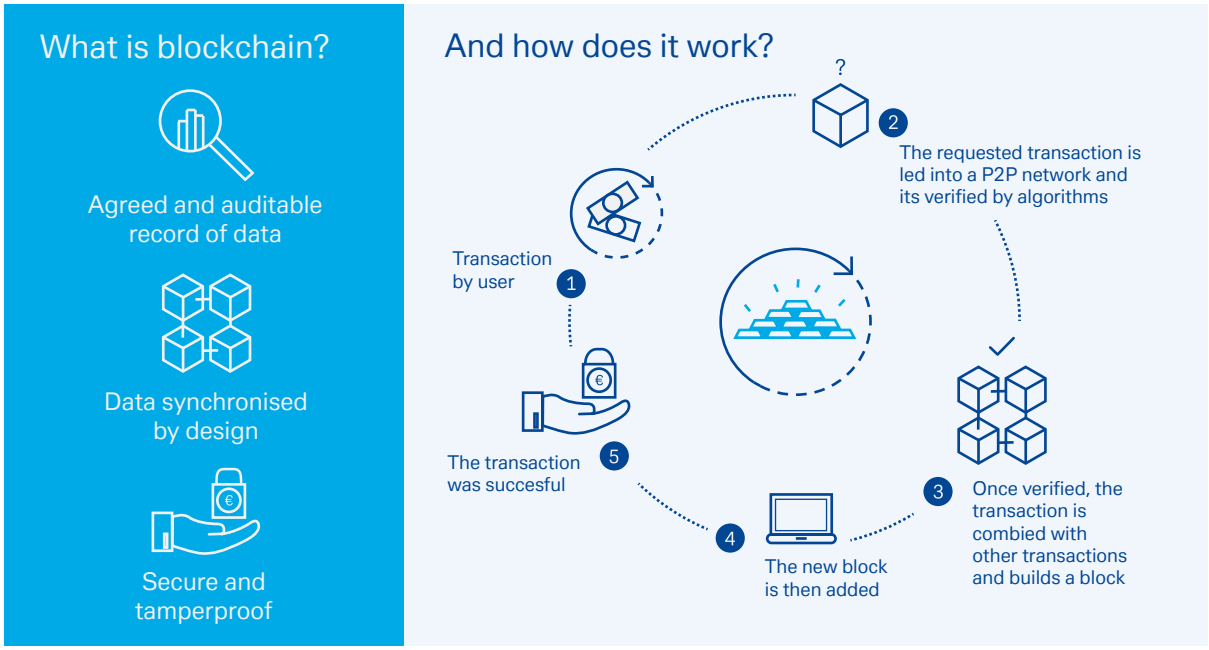
Blockchain first garnered public attention in a 2008 document explaining Bitcoin.[33] Now, global spending on blockchain solutions is forecast to reach US$11.7bn in 2022, according to the International Data Corporation.[34] Much of this is due to the almost endless use cases for blockchain, with consortia, projects and tests springing up almost monthly across capital markets, international payments, trade finance, supply chain management and regulatory compliance.

It is not just the banks looking to seize the opportunities, however. Many corporate projects have already moved from theory to reality: examples include Ornua's letter of credit (LC), Marubeni's LC in the trade chain and a third pilot that has significant implications for the entire container shipping industry (Maersk and IBM).[35]

5.2 What are the benefits?

Make no bones about it: blockchain is disruptive. But it may lead to faster end-to-end processing, improved transparency, enhanced assessment of operational and financial risks, and reduced costs. Some eye-catching estimates put this saving of banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance at US$15–20bn a year by 2022.[36]

Figure 6: Explaining a blockchain



Source: Deutsche Bank

There is broad consensus that custody and clearing could be revolutionised by the technology. In most markets, financial market infrastructures are entrusted by their participants with updating and preserving the integrity of a centralised ledger – yet blockchain could completely re-shape this way of operating, and radically change how assets are maintained and stored, obligations are discharged, contracts enforced, and risks managed.

> " Blockchain can reduce the costs associated with labour-intensive non-STP, contracting and documentation management – while providing greater accuracy and lower levels of risks. Firms can also record the ownership of assets and 'performance history'; allowing them to present their own signature 'golden record' audit trail to regulators and clients for traceability purposes "
>
> *Anthony Kirby, Ernst & Young*

Trade finance is another area prime for transformation. Here, blockchain could reduce processing times and reduce costs and inefficiencies associated with paper-based transaction processing, while ensuring transparency, security, and trust – and even deploy so-called "smart contracts". As Daniel Schmand, Global Head of Trade Finance at Deutsche Bank and Chairman of ICC Banking Commission, comments in the 2017 ICC Banking Commission report, 'Rethinking Trade and Finance'[37], "the elimination of paper from trade finance transaction processing could reduce processing time by two hours per transaction and reduce compliance costs by 30%".[38] Concurring, Bain & Company estimates that, if applied correctly, blockchain could reduce trade finance costs by between 50–80%.[39] There are many bank projects striving towards this goal, with the most notable being the we.trade and Marco Polo initiatives.

The Utility Settlement Coin (USC) concept, a digital cash model aimed at facilitating payment and settlement for institutional financial markets, is another project gathering pace in transaction banking.[40]

Critical mass will not come easily, however – Deutsche Bank's Thomas Nielsen warns that as many as 90% of blockchain projects will fail (although the winners will be truly transformative).[41] What is needed? First, standards, protocols and market best practices all need to evolve in tandem. Many of the solutions are being developed as hypothetical use cases or most viable propositions without the operational process, risk systems or compliance experience to underpin them. Anthony Kirby from Ernst & Young adds that "firms will need to handle migration issues including how to develop solutions in parallel with legacy market infrastructures and evolving technologies such as the Cloud, AI, RPA and smart contracts."[42]

> " Long-term, we foresee blockchain having a significant impact on transaction banking services; driving not just new products and services but re-shaping business models of banks and our clients "
>
> *Anja Bedford, Deutsche Bank*

5.3 Current regulatory picture

Blockchain use cases focus on existing – and hence already regulated – bank services and processes. Many different types of regulation and law remain applicable to a blockchain environment: civil law governs basic ownership rights and creation of contracts, whereas banking regulation decrees how the industry processes securities transactions, payments, client data and how it ensures cyber resilience and security.

At the same time, the regulators are currently assessing blockchain use cases and its potential impact on the banking industry (see Figure 7), with the goal of creating a framework of legal certainty around the emerging applications.

Globally, the Financial Stability Board (FSB) has considered the implications of blockchain, and continues to work alongside the Committee on Payments and Market Infrastructures (CPMI) to identify key issues that market participants and policymakers need to address. The CPMI released a report that focuses on the potential impact of blockchain on payments, clearing and settlement in February 2017, which confirmed the need for a legal framework, while calling for robust governance structures and data controls.[43]

In Europe, the European Parliament's Draft Resolution on blockchain recommends the creation of a strategic plan for building blockchain-based infrastructure among EU Institutions for public sector modernisation – potentially putting blockchain at the heart of a trusted transactional ecosystem and enabling cross-border transactions between Member States.[44] The EU Blockchain Observatory and Forum (which was launched by the European Commission in February 2018) should help drive further engagement in this field.

The regulatory landscape in Asia-Pacific is dominated by the progress made towards assimilating the technology into innovative solutions while mitigating the risks of cyber-crime in Japan, Hong Kong, Singapore, Australia and China. Laurence Van der Loo from ASIFMA highlights that Asia "throws up a number of major challenges, the most significant being its historic fragmentation: apart from China and India, Asia is a collection of relatively small markets, each with its own law and regulators, and despite some recent efforts to increase co-operation and harmonisation between regulatory regimes, expanding business from one Asian country into another tends to be costly and time-consuming".[45]

5.4 Key regulatory challenges and solutions

The challenge of data privacy regulation

Why does it matter?

The core features of blockchain from which its benefits are derived – namely being decentralised, immutable and transparent – are potentially at odds with global data protection laws, which focus on the importance of allowing personal data to be removed or edited. This creates an impediment for developing workable use cases for the technology.

More broadly, different jurisdictions define data, its use and the necessary means of protection in markedly different ways. In practice, this restricts the free flow of data across borders and makes it impossible for one single solution to be employed in all markets. The result: fragmented global solutions and sub-optimal results for banks and their clients.

Latest developments

Europe ushered in GDPR in May 2018 – making these data challenges yet more pronounced. Firstly, GDPR was crafted around the implicit assumption that data is collected, stored and processed in a central database, not a decentralised ledger. Secondly, as highlighted by the EU Blockchain Observatory and Forum, "blockchains are, generally speaking, constantly growing, append-only databases, to which information can only be added, not removed," while GDPR "explicitly gives individuals the right to have their data amended…or erased."[46]

There are further areas for concern. GDPR is very clear, for instance, on the need for a "data controller" that is responsible for data use and protection – something that is difficult to ascertain in an open, permissionless blockchain. Further, it stipulates that data can only be transferred to third parties outside the EU if the location in question offers equivalent levels of protection. Using blockchain, it is impossible to selectively limit where the data goes. Worryingly, many privacy laws echo this approach, such as India's draft data protection bill.[47]

Suggested solutions

With respect to GDPR, there are potential solutions that the industry should consider and test. When it comes to the immutability of records, for instance, Latham & Watkins suggests that clients should consider storing personal data off-chain and simply maintaining a record/signpost to such data on the chain. The law firm also puts forward that clients should be cognisant of the basis for

Figure 7: Region-by-region regulatory progress

Blockchain

Europe

The European Commission (EC) FinTech action plan

March 2018

The EC will continue to appraise legal, governance and scalability issues and support interoperability and standardisation efforts, including further evaluating cases of blockchain use and its applications in the context of the Next Generation Internet

The EU Blockchain Observatory and Forum launched in February 2018 will be used to monitor trends and developments, pooling expertise to address sectoral and cross-sectoral issues and exploring joint solutions and cross-border cases of blockchain use

Hong Kong

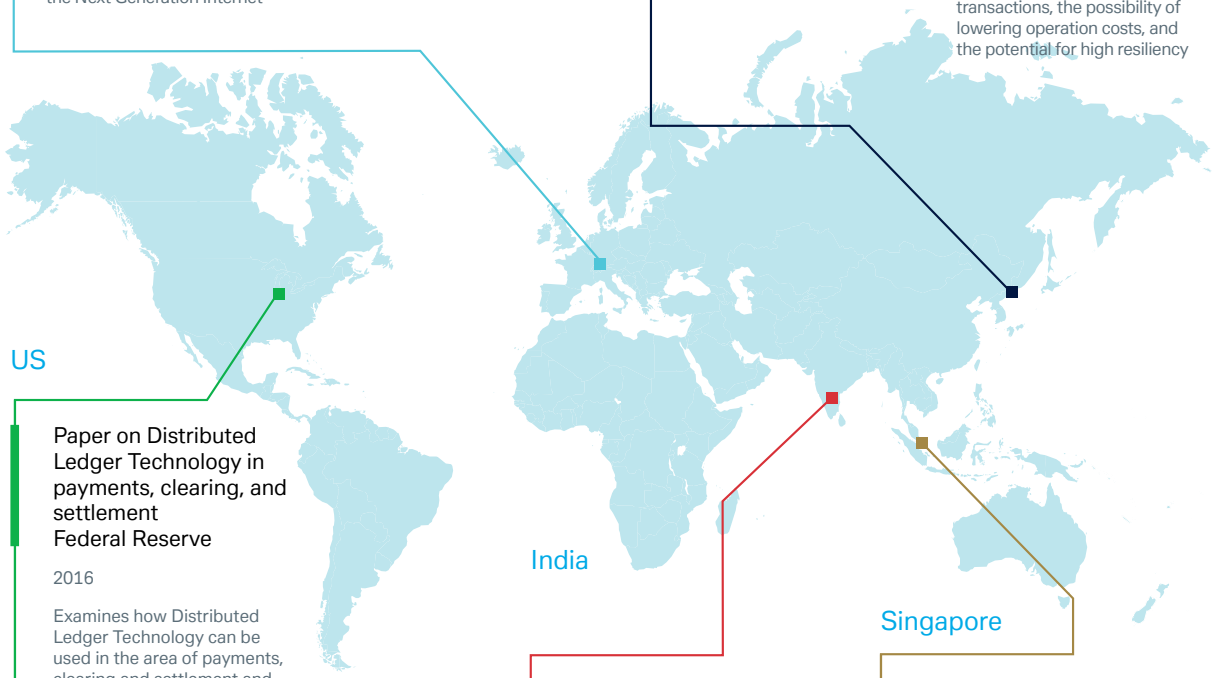
HKMA and ASTRI's white paper on Distributed Ledger Technology

First paper published in 2016, Second paper published in 2017

Analyses governance, potential application, risk-management, and regulatory compliance of Distributed Ledger Technology

Produces initial findings of the proof-of-concept work carried out on Distributed Ledger Technology applications, e.g. trade finance and digital identify management.

Suggests that Distributed Ledger Technology has the potential to bring new opportunities to the banking and payment industries, based on such key strengths as the ability to achieve complete traceability of records and transactions, the possibility of lowering operation costs, and the potential for high resiliency



US

Paper on Distributed Ledger Technology in payments, clearing, and settlement Federal Reserve

2016

Examines how Distributed Ledger Technology can be used in the area of payments, clearing and settlement and identifies both the opportunities and challenges facing its long-term implementation and adoption.

Notes that a number of challenges to development and adoption remain, including in how issues around business cases, technological hurdles, legal considerations, and risk management considerations are addressed.

Concludes that understanding the potential range of Distributed Ledger Technology adoption and its link to changing the financial market structure is an area for future research

India

Report on FinTech and Digital banking, commissioned by Reserve Bank of India

November 2017

This report is focused on reviewing and reorienting appropriately the regulatory framework in response to the dynamics of rapidly evolving fintech. Blockchain is one of the topics covered in the report.

Concludes that if widely adopted, blockchain can pose new challenges for regulation; constant monitoring of developments in the application of the blockchain to financial services and systems is prudent given the significant potential of the technology

Singapore

Project Ubin: Central Bank Digital Money using Distributed Ledger Technology

November 2016

Project Ubin is a collaborative project with the industry to explore the use of Distributed Ledger Technology for clearing and settlement of payments and securities.

It aims to help MAS and the industry better understand the technology and the Distributed Ledger Technology potential benefits it may bring through practical experimentation

processing of personal data and the impact this has on the need to satisfy certain data subject rights, such as the right to be forgotten and the right of data portability, which, on the face of it, appear irreconcilable with blockchain.[48]

The EU Blockchain Observatory and Forum also adds a note of optimism on this issue, suggesting that "GDPR and blockchain at heart share the objective of data sovereignty, so blockchain could become a tool to achieve this objective."[49] Blockchain could in theory make it easier for platforms and applications to have this compliance "baked in" to the code, supporting data protection by design.

The challenge of conflicts of law

Why does it matter?

Cross-border transactions are an area where blockchain offers significant potential, but the issue of determining which jurisdiction and law should apply is a challenging one when different blockchain nodes may be in different jurisdictions. The answer to this conundrum depends on a vastly complex set of rules known as conflicts of law.

According to the European Commission, "When securities are exchanged across borders, it's not always easy for investors, credit providers and other market participants to know which national law applies to these transactions"[50] – which means ownership rights cannot be determined with legal certainty.

This issue has been exacerbated by the disparity of approaches, to date, by central bank and national competent authorities. Ernst & Young suggests that, practically, this may result in different blockchain ecosystems being created, starting with domains such as trade finance and supply chain management where arrangements are generally standardised under English Common Law.[51]

Perhaps worse, we may end up with multiple copies of shared ledgers operating on different technology platforms with different database environments, leading to time-consuming and expensive reconciliation – exactly what the technology is looking to circumvent.

Latest developments

In March 2018, the European Commission proposed the adoption of common conflict of laws rules on the third-party effects of assignments of securities claims, suggesting that, as a rule, the law of the country where the assignor has its habitual residence will govern the third-party effects of the assignment of claims.

By introducing legal certainty, the Commission believed that the new measures would contribute to promote cross-border investment, enhance access to cheaper credit and contribute to market integration. The Commission's proposal was accompanied by a more recent communication in March 2018 clarifying the conflict of law rules for securities and covering the third-party effects of the transfer of financial instruments.

Suggested solutions

If it is to realise potential, blockchain transactions should involve global participants, activities and instruments with different nodes of the blockchain being located in different jurisdictions – so it is imperative that they can interoperate at will under as common a legal framework as possible. This will only be achievable via global co-ordination on regulation that takes into accounts the specifics of blockchain.

Macro-approaches such as organising a G20-style response (or getting the FSB to opine) are therefore positive – as is the European Commission's work – although these have hinged on the central banks reaching agreements in areas of common concern, such as resilience/robustness of blockchain architectures and the treatment of data privacy. It is important that such agreement is met.

> " The direction of travel is increasingly one of collaboration between central banks and competent authorities in order to forestall the complications arising from conflicts of law when applied to blockchain "
>
> *Anthony Kirby, Ernst & Young*

The challenge of securities law

Why does it matter?

Central Securities Depositories Regulation (CSDR)[52] – which applies to European Central Securities Depositaries (CSDs), their participants, and to securities settlement systems in the EU – mandates that the ultimate record of ownership of securities is to be a CSD. This requires all newly issued securities in Europe to be immobilised or dematerialised as a book-entry of a CSD by 2023, and all existing securities to follow suit by 2025. Only allowing CSDs to issue or process securities transactions clearly restricts the use of blockchain for this purpose.

Suggested solution

Latham & Watkins suggests that, rather than being incompatible with CSDR, blockchain could form part of a hybrid model in which the CSD operates a blockchain platform itself which performs the book entry role and is the ultimate version of title, or the CSD continues to perform this role off-chain, with the third-party blockchain platform accessing those records held by the CSD via an API.

However, in order to be able to use the blockchain for the purposes of issuance of securities, it would be beneficial to have specific rules recognising the creation of securities on the blockchain, and the creation, maintenance and transfer of rights to those on-chain securities or, alternatively, clear guidelines as to how existing securities laws and regulations should be interpreted in the context of blockchain.

Clearly, in order to be able to use the blockchain for the purposes of issuance of securities, there should be rules recognising the creation of securities in blockchain, and execution rights to securities.

> " Part of the promise of blockchain solutions for financial markets is the possible disintermediation of some of the entities involved in the current financial market infrastructure in order to increase market efficiency and to save costs, through the creation of an ultimate record of ownership of securities and financial instruments. But, if European law mandates that the ultimate record of ownership of securities is a CSD, is that not completely incompatible with blockchain and the purpose of it? The answer is: not quite"
>
> *Stuart Davis, Latham & Watkins*

5.5 What does the future hold?

Blockchain is set to become a fixture in a number of critical bank processes over the coming years, with the EBA's FinTech report highlighting smart contracts in trade finance and customer due diligence as key areas of advancement.[53]

Though blockchain has been widely hailed as a revolutionary technology, the implementation of a truly cross-border solution will face the same regulatory issues as any other sophisticated cross-border arrangement.

As an inherently global technology, it therefore requires cross-border regulatory solutions – something that remains highly challenging to achieve due to the need to unite authorities from numerous jurisdictions behind a single policy. As with all regulation pertaining to technology, we stress the need for technology-neutrality – regulating the applications and outcomes of blockchain, rather than the technology itself.

Noémie Papp from the EBF comments that "it's widely accepted that regulation should also be neutral regarding technological developments and business models" and adds that the EBF considers that improvements are needed in current legislation, and regulatory requirements must be proportionate to ensure the current framework does not hamper technological growth nor

competitiveness. Ultimately, she adds, "regulation will not be a barrier if it is adapted to the digital reality and the needs of all users – but regulatory bodies should wait to see the direction of the technology and allow business models to grow, instead of being too prescriptive now as to how the individual technologies can be used".[54]

That said, blockchain also has unique properties in terms of both security and data management, which promise to work in harmony with regulations. The best approach to regulating blockchain-based solutions will take advantage of these – using blockchain as a means of raising standards and broadening approaches to both security and data sovereignty.

With an open dialogue across all industry participants (as driven by the Blockchain Observatory and Forum), it should be possible to create a stable and sound environment for the development of secure blockchain solutions. Developing the regulations on the basis of an understanding of its use cases, issues and trends is a powerful way of designing the rules that would be truly supportive of the technology and its employment by the industry.

6

Artificial Intelligence

6.1 What is it?

AI can be viewed as the ability for technology to "understand" and "learn". However, it is a broad and complex term that is often misused or misunderstood.

AI and machine-learning techniques have been used in capital markets for over 50 years. While originally limited to highly specialised applications that required deep technical expertise, the technology has evolved considerably in line with developments in computing capabilities and increased investment in the technology.[55]

Over the last five years, AI (in all its forms) has gained increased attention, with applications identified across many industries. By mid-2017, it was estimated that there were already over 400 recognised AI companies operating across Europe, with projections suggesting the AI industry could increase the region's overall economic growth (GDP) by US$2.5trn over the next 10 years.[56] The banking sector, is set to be one of the most significant beneficiaries of this development, with McKinsey estimating it will boost revenues by US$200–300bn.[57]

AI does not exist in a vacuum, however – and nor could it. The adoption of this technology is dependent on the availability of large quantities of data, as well as new high-performance computing and networking – cloud being a prime example.

6.2 What are the benefits?

AI offers a range of benefits to market participants – from better client experience, efficient risk management, and compliance (including reporting and identifying illicit behaviour) through to operational efficiency (including the reduction of transaction breaks).

As has been well-documented, banking clients' expectations are changing along with technological development, and they now expect even more personalised services. AI can perform analysis of client data to determine client needs – using the insights gleaned to offer more tailored products and services, as well as automated and predictive resolution of service issues.[58] For instance, a bank algorithm could identify when a corporate client has surplus liquidity in a low-yielding account and recommend a fixed-term deposit or money-market fund that would offer better returns.

For banks, this not only means a chance to provide a better, more tailored service to their clients, but also potentially to recommend other products in the bank's catalogue that can add value. Breaking down the silos of data, and creating more dynamic ways of accessing it, will make banks the standout financial service providers in an increasingly fragmented industry. On the client side, it's equally advantageous – promising a higher level of service and optimised treasury functions.

The use of AI stands to generate considerable cost savings for banks (as outlined in an FSB report[59]) – reducing the amount of time required to carry out complex administrative functions, while simultaneously performing them more accurately and increasing operational efficiency. In a paper on the potential of AI, Accenture states that optimal efficiencies are likely to be seen first in back-office functions, where robotic process automation (RPA) is already having a significant impact.[60]

It also promises earlier and more accurate estimation of risks, determining normal behaviour patterns and flagging outlier transactions – for instance, with respect to anti-money laundering (AML) and know-your customer (KYC) compliance – as well as identifying cybersecurity risks.

6.3 Current regulatory picture

As an existing technology and via its underlying processes, AI already falls under current regulations, including data privacy regulations, to a large extent – and does not need much by way of further regulatory scrutiny. It also accords with the generally accepted principle that regulation is technology-agnostic and should capture activities and outcomes – which remain largely unchanged – and not technologies.

That said, assessing the key risks associated with AI, its control principles and the question of ethics are hot topics for global regulators. In November 2017, the FSB called for "monitoring" of the uses of AI in order to maintain financial stability, outlining the importance of assessing the implementation of relevant data privacy, conduct risk and cybersecurity protocols. Similarly, the US has established an AI congress advisory committee[61] to assess the technology, while there have been numerous developments in Europe.

The EC's European Group on Ethics in Science and New Technologies (EGE) has put ethics at the centre of the debate, calling for the launch of a process that paves the way towards a common, internationally recognised ethical and legal framework for the design, production, use and governance of AI. In Asia, MAS, echoing this trend, announced in April 2018 that it was working with key stakeholders to develop a guide for promoting the responsible and ethical use of AI and data analytics by financial institutions.[62]

6.4 Key regulatory challenges and solutions

The challenge of finding the right method of regulation

Why does it matter?

When existing financial services regulations were created, AI was not sophisticated enough for widespread industry use. That has clearly changed, and it now can – or does – perform tasks a human simply could not. This becomes difficult when you consider the current rules still regulate AI in the same way they would a human. This can be stifling for the development of new AI-driven products and solutions, restricting employment of AI solutions by the banks.

Finding the right method for regulating AI, however, is inherently difficult, and must find the right balance between specificity – applying precise rules with clear applications – and flexibility, since all regulation risks sliding into obsolescence, especially with technology evolving at such an exponential rate. With the same consideration in mind, regulators must also balance the demands for quality, comprehensiveness and consistency with that of speed.

Suggested solutions

While technology continues to change, the objectives and outcomes it fuels in the financial services industry stay the same. Consequently, regulating AI will be a matter of refining the rules in place, taking into account the specifics of data processing that AI facilitates.

This will require extensive consultation with the wider financial services industry – taking in financial industry, and technology vendors. Regulators, together with the market, should conduct a regulatory impact assessment to identify the exact areas where new rules could hinder progress, and where regulatory changes are required.

There have already been promising steps in this direction (such as the EC's review of the current financial services regulatory framework, to determine its future fitness for emerging technologies such as AI[63]).

Mandatory stress testing of algorithms will most likely be an important component in any new regulatory package – and should certainly stand as industry best practice. Sandboxing – using statistical models to synthesise how scenarios would play out under different forms of regulation – creates a safe space to explore important questions, such as how AI solutions would react to extremely high client demand, or how they treat anomalies.

Figure 8: Region-by-region regulatory/government incentive updates

AI

Europe

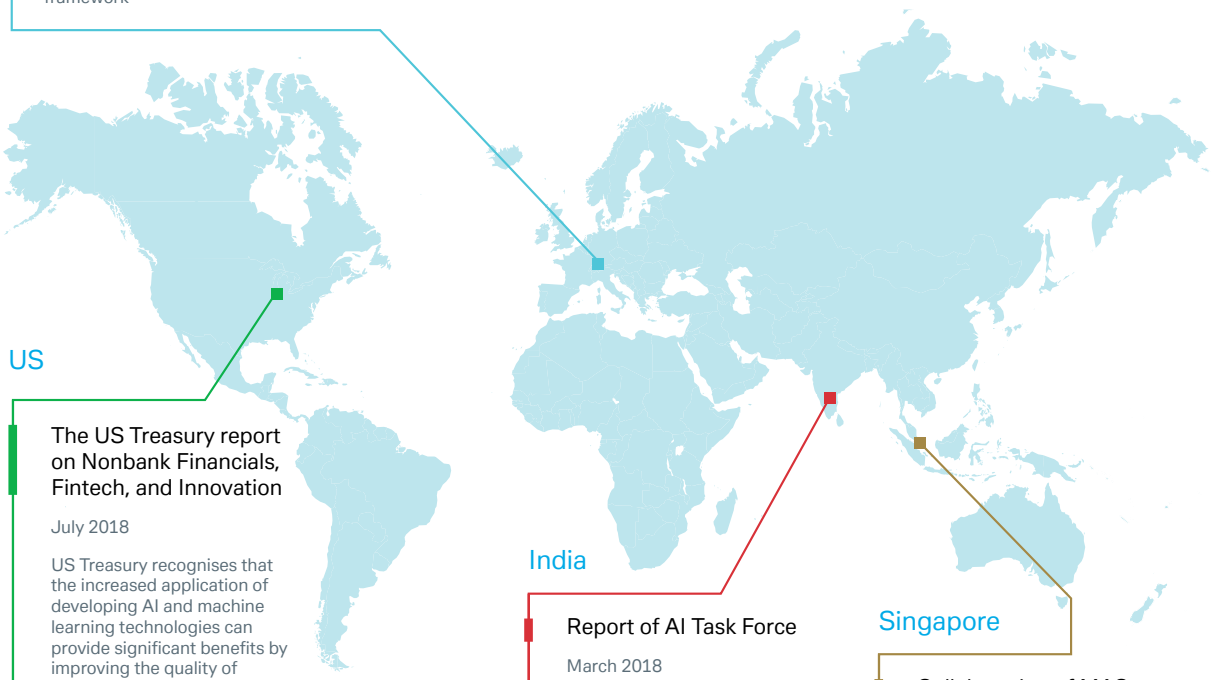
EC communication on Artificial Intelligence for Europe

March 2018

Sets out a European initiative on AI, which aims to boost the EU's technological and industrial capacity and AI uptake across the economy, prepare for socio-economic changes and ensure an appropriate ethical and legal framework

Recognises a need for a solid European framework which promotes innovation and respects the Union's values and fundamental rights as well as ethical principles such as accountability and transparency.

The EC will work with Member States on a coordinated plan on AI with the view to agree this plan by the end of 2018



US

The US Treasury report on Nonbank Financials, Fintech, and Innovation

July 2018

US Treasury recognises that the increased application of developing AI and machine learning technologies can provide significant benefits by improving the quality of financial services for households and businesses and supplying a source of competitive strength for US firms.

Treasury believes that regulators should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial services companies as the technologies develop

India

Report of AI Task Force

March 2018

Names fintech as one of ten key domains where AI could be an enabler of social and economic development for India.

Anticipates that the use of AI in fintech will help and expand the existing efforts of India Stack, helping to provide assistance to small and medium enterprises and help for risk assessment.

Identifies challenges and the key enablers for AI development and commercialisation in the fintech sector, mentioning the availability of data and open APIs

Singapore

Collaboration of MAS, EDB, IMDA, and IBF to accelerate the adoption of AI

May 2018

Aims to foster a thriving AI ecosystem comprising financial institutions, research institutions, and AI solution providers.

The agencies will work towards a conducive environment that supports and expands the adoption of AI and data analytics in Singapore.

It will encompass three key prongs: developing AI products, matching users and solution providers, and strengthening AI capabilities

The challenge of data privacy and ethics

Why does it matter?

A bank is, of course, bound by a code of ethics in using personal data, and maintaining customer trust is paramount. However, Accenture reports that banking customers are largely inclined to allow banks access to their financial data – so long as it results in an improved service.[64] Indeed, the Accenture report cites a survey in which almost two-thirds of banking consumers in North America said they would be comfortable letting their bank do this.[65] That said, there are limitations to what customers will accept, especially when it comes to obtaining information from social media sources.

The FSB report suggests that it is necessary to consider how the output of customer analysis should be protected, ensuring the anonymity of individual consumers while facilitating the safe and efficient use of big data for better services.[66]

Part of the problem, however, is that AI is currently advancing more rapidly than the process of finding answers to these questions – along with a host of other challenging ethical, legal and societal challenges. These include whether banking clients have the right to know whether they are dealing with a human or with an AI artefact, and whether there should be limits to what AI systems can suggest to a client, based on the data it holds.

Latest developments

The EC's EGE has called for the launch of a process that paves the way towards a common, internationally recognised ethical and legal framework for the design, production, use and governance of AI. The EGE has laid out the EU's ethical principles and democratic prerequisites for AI, which includes responsibility and rule of law and accountability. This includes protections against risks stemming from 'autonomous' systems that could infringe human rights, such as safety and privacy.

In Asia, Singapore established an advisory council formed of tech companies and AI users in 2018. The council will collaborate with stakeholders and regulators, such as MAS, to develop a governance code for the ethical use of artificial intelligence and personal data. Backed by a five-year research programme from the government, its code will be based on the aim of ensuring all decisions made using AI are explainable, transparent and fair.

Some of the most prominent initiatives towards the formulation of ethical principles regarding AI have stemmed from industry, such as the Institute of Electrical and Electronics Engineers' policy paper and Google's DeepMind.

Suggested solutions

We are approaching a stage where we need a set of fundamental ethical principles and democratic prerequisites that can guide binding law (or the interpretation of it). Yet current efforts represent a patchwork of disparate initiatives – meaning there is, as the EGE notes, a need for a greater deal of conversation between those in, and perhaps outside, the industry to truly understand the ethical implications of autonomous technology.

Data privacy must also form a central part of these conversations, with regulators needing to find a balance between imposing rigorous standards in terms of how data is shared and used (which should always be transparent to the data owners), and leaving adequate room to realise the full benefits of AI analysis.

Any outcome must be consistent globally, however. A situation where AI developers or users can "race to the bottom" – re-locating in countries with lower ethical or data privacy standards – would be harmful for all. That said, allowing the debate to be dominated by certain regions, disciplines, demographics or industry actors risks excluding a wider set of societal interests and perspectives.

6.5 What does the future hold?

While the public consciousness still entertains futuristic images of AI, there are a number of more grounded and practical applications that are already at an advanced stage. According to McKinsey, corporate payments –including B2C, C2B and B2B transactions – generate more transaction data than any other area of banking.[67] This has led financial service providers to explore a raft of use cases – from analysing transactions and value chains, selling curated data sets and providing automated advice based on client data, to detecting fraudulent transactions.

While these new capabilities pave the way for an exciting future, the same regulations that have previously governed financial services remain in place. This might create conditions where new capabilities, such as automated advisory services, are not accounted for by existing regulations.

Where the old regulations are no longer fit for the purpose of governing services augmented or revolutionised by AI, their update, if any, should take into account for specifics of AI new capabilities. However, this need not be a rushed process. Rather, regulations will need to evolve naturally as use cases arise, and regulatory authorities will need to work together to ensure they agree a common approach.

This will take time, but it is crucial to develop common legislation that covers the applications of AI as they emerge, rather than drafting pre-emptive legislation before there is a clear need. In this respect, the EBF advises that "future regulation should work to explain how AI should be used, conceptually, rather than being specific about the exact procedure, algorithms and data (and require reporting of these)".[68]

Likewise, it is important that this legislation is drawn up with all jurisdictions broadly aligned. Only then can we create an open and level playing field that enables players around the world to build and fund innovative new solutions powered by AI.

However, it is important to accept that AI brings new risks – whether it be the technology performing prohibited actions without control, or rogue employees training it to perform a prohibited action that cannot be traced back to the bad actor – which means that security must remain paramount at all times. We should therefore ensure that AI solutions operate under similar control environments to those governing human activity (albeit at higher velocity), and that we maintain tight controls over their algorithms and programming.

7

Conclusion

This paper, and the conversations that have taken place with a wide range of industry experts to produce it, make one thing clear: the financial services industry will be transformed by technology. The extent to which this will happen, and the extent to which all participants experience the benefits, will depend on a wide range of factors. Regulation is almost certainly one of the most important

Regulation has so far proven both an enabler and a challenge to transformation in global transaction banking. But, we conclude that conducive and forward-thinking regulation stands to be a major catalyst for a thriving and innovative banking industry. For this to be realised, we trust that the regulatory approach is:

1 Globally aligned – while cross-border solutions are, admittedly, challenging to achieve, global technology solutions will depend on them. Global sandboxes are the first step in this direction, yet it is important that regulators continue with this momentum.

2 Technology-neutral – as with all regulation pertaining to technology, we stress the need for technology-neutrality, regulating the applications and outcomes, rather than the technology itself.

3 Digitally relevant – while technology-neutral, regulation must remain relevant in today's digital world.

4 Embracing of new solutions – when cybersecurity solutions are provided by CSPs, it is important that market-leading solutions that can provide significant benefits to clients are accounted for.

5 Industry-led – the optimal approach when addressing issues such as API standards, for instance, would be for the industry to lead developments, with support from the regulators.

8

List of contributors

Thomas Nielsen, Chief Digital Officer, Global Transaction Banking, Deutsche Bank

Polina Evstifeeva, Head of Regulatory Strategy, GTB Chief Digital Office, Deutsche Bank

Anja Bedford, Blockchain/ DLT Product Owner, GTB Chief Digital Office, Deutsche Bank

Noémie Papp, Head of Digital & Retail, EBF

Laurence Van der Loo, Senior Manager, CEO Office, Lead on Fintech Practice, ASIFMA

Nicholas Bramble, Senior Policy Specialist, Google

Andrew Dapre, EMEA Lead Financial Services, Microsoft

Dr. Anthony W. Kirby, Associate Partner, Regulatory & Risk Management - Regulatory Intelligence, Ernst & Young

Hamish Thomas, Partner, Head of Banking Technology and Payments, Ernst & Young

Olivier Colinet, Partner and Head of Cloud, Ernst & Young

Stuart Davis, Senior Associate, Financial Institutions Group, Latham & Watkins

Vanessa Manning, Head of Liquidity and Investment Solutions, Deutsche Bank

Shahrokh Moinian, Global Head of Cash Products, Cash Management, Deutsche Bank

9

Glossary

Application Programming Interfaces (APIs)	A set of subroutine definitions, communication protocols, and tools for building software
Artificial intelligence (AI)	Intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans
Asia Securities Industry & Financial Markets Association (ASIFMA)	An independent, regional trade association with over 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers
Blockchain	A growing list of records, called blocks, which are linked using cryptography
EU Blockchain Observatory and Forum	Created as a European Parliament pilot project, the EU Blockchain Observatory and Forum is being run under the aegis of the European Commission. It aims to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU
Cloud	A network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer
European Banking Authority (EBA)	An independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector
European Banking Federation (EBF)	The voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 3,500 banks
European Commission	An institution of the European Union, responsible for proposing legislation, implementing decisions, upholding the EU treaties and managing the day-to-day business of the EU
Financial Stability Board (FSB)	An international body that monitors and makes recommendations about the global financial system
General Data Protection Regulation (GDPR)	A regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area
Hong Kong Monetary Authority (HKMA)	Hong Kong's currency board and de facto central bank. It is a government authority
Monetary Authority of Singapore (MAS)	Singapore's central bank and financial regulatory authority

Open Banking	The use of Open APIs that enable third party developers to build applications and services around the financial institution
PRETA	Created in 2013 to develop and innovate market competitive services in digital payment and identity solutions
Payment Services Directive 2 (PSD2)	An EU Directive, administered by the European Commission to regulate payment services and payment service providers throughout the EU and European Economic Area
Sandbox	A testing environment
Third-party provider (TPP)	An authorised online service provider that has been introduced as part of Open Banking
Unified Payment Interface (UPI)	An instant real-time payment system developed by National Payments Corporation of India facilitating inter-bank transactions.

References

[1]https://www.db.com/newsroom_news/2018/deutsche-bank-acquires-india-based-fintech-start-up-quantiguous-solutions-to-accelerate-the-bank-s-open-banking--en-11578.htm

[2]https://www.finextra.com/videoarticle/1843/accelerating-the-open-banking-strategy

[3]https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc1/Open-API.pdf

[4]https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-71/Accenture-Brave-New-World-Open-Banking.pdf#zoom=50

[5]https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/apis-three-steps-to-unlock-the-data-economy039s-most-promising-new-go-to-market-channel

[6]http://cib.db.com/docs_new/TMI260_P8-14_Cover.pdf

[7]Taken from an interview with Thomas Nielsen for the purposes of this paper

[8]https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[9]https://www.berlin-group.org/

[10]http://cib.db.com/news-and-events/news/unlocking-opportunities-in-the-api-economy.htm

[11]https://www.openbankingeurope.eu/

[12]https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20180111e1.pdf

[13]http://www.cib.db.com/insights-and-initiatives/flow/the-new-payment-paradigm.htm

[14]http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[15]https://www.idc.com/getdoc.jsp?containerId=prUS43354417

[16]https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[17]https://www.eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf

[18]Taken from an interview with Nicholas Bramble at Google for the purpose of this paper

[19]Taken from an interview with Andrew Dapre, EMEA Lead Financial Services, Microsoft

[20]http://www.asiacloudcomputing.org/images/research/acca-fsi2018_report_final.pdf

[21]Taken from an interview with Noémie Papp, Head of Digital & Retail, EBF, for the purpose of this paper

[22]https://www.eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8fb2f1e

[23]Taken from an interview with Laurence Van der Loo, Senior Manager, CEO Office, ASIFMA, for the purpose of this paper

[24]https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[25]http://www2.itif.org/2017-cross-border-data-flows.pdf

[26]https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[27]https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

[28]https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[29]http://www.asiacloudcomputing.org/images/research/acca-fsi2018_report_final.pdf

[30]http://www.asiacloudcomputing.org/images/research/acca-fsi2018_report_final.pdf

[31]https://www.ukfinance.org.uk/wp-content/uploads/2017/08/UK-Finance-response-EBA-cloud-consultation-final.pdf

[32]https://www.eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf

[33]https://www.bitcoin.com/bitcoin.pdf

[34]https://www.businesswire.com/news/home/20180719005018/en/Worldwide-Spending-Blockchain-Forecast-Reach-11.7-Billion

[35]http://www.cib.db.com/insights-and-initiatives/flow/trade_finance_and_the_blockchain_three_essential_case_studies.htm

[36]https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf

[37]https://iccwbo.org/publication/2017-rethinking-trade-finance/

[38]http://cib.db.com/insights-and-initiatives/flow/emerging_technology_revolution.htm

[39]http://www.bain.com/Images/BAIN_BRIEF_Wolf_in_Sheeps_Clothing_Disruption_in%20_Transaction_Banking.pdf

[40]https://www.db.com/newsroom_news/2016/medien/utility-settlement-coin-concept-on-blockchain-gathers-pace-en-11661.htm

[41]Taken from an interview with Thomas Nielsen, Chief Digital Officer, Global Transaction Banking, Deutsche Bank for the purpose of this paper

[42]Taken from an interview with Dr. Anthony W. Kirby, Associate Partner, Regulatory & Risk Management - Regulatory Intelligence, Ernst & Young for the purpose of this paper

[43]https://www.bis.org/cpmi/publ/d157.pdf (page 1)

[44]http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-619.045%2B01%2BDOC%2BPDF%2BV0%2F%2FEN

[45]Taken from an interview with Laurence Van der Loo, Senior Manager, CEO Office, ASIFMA, for the purpose of this paper

[46]https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf

[47]http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

[48]Taken from an interview with Stuart Davis, Latham & Watkins, for the purpose of this paper

[49]https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf

[50]https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/securities-and-claims-ownership_en

[51]Taken from an interview with Dr. Anthony W. Kirby, Associate Partner, Regulatory & Risk Management - Regulatory Intelligence, Ernst & Young for the purpose of this paper

[52]https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/central-securities-depositories-csds_en

[53]https://www.eba.europa.eu/documents/10180/2270909/Report+on+prudential+risks+and+opportunities+arising+for+institutions+from+FinTech.pdf

[54]Taken from an interview with Noémie Papp, Head of Digital & Retail, EBF, for the purpose of this paper

[55]https://medium.com/cityai/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-build-in-europe-bd17a3d499b

[56]https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

[57]https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20ai%20frontier%20applications%20and%20value%20of%20deep%20learning/mgi_notes-from-ai-frontier_discussion-paper.ashx

[58]Taken from an interview with Stuart Davis, Latham & Watkins, for the purpose of this paper

[59]http://www.fsb.org/wp-content/uploads/P011117.pdf

[60]https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-68/Accenture-Redefine-Banking.pdf

[61]https://www.congress.gov/bill/115th-congress/house-bill/4625/text

[62]http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-and-financial-industry-to-develop-guidance-on-responsible-use-of-data-analytics.aspx

[63]http://ec.europa.eu/finance/consultations/2015/financial-regulatory-framework-review/docs/consultation-document_en.pdf

[64]https://www.accenture.com/t00010101T000000Z__w__/gb-en/_acnmedia/PDF-68/Accenture-Redefine-Banking.pdf

[65]https://www.accenture.com/t20160609T222453__w__/us-en/_acnmedia/PDF-22/Accenture-2016-North-America-Consumer-Digital-Banking-Survey.pdf

[66]http://www.fsb.org/wp-content/uploads/P011117.pdf

[67]https://www.mckinsey.com/industries/financial-services/our-insights/technology-innovations-driving-change-in-transaction-banking

[68]Taken from an interview with Noémie Papp, Head of Digital & Retail, EBF, for the purpose of this paper

www.db.com/gtb
gtb.marketing@db.com