Andreas Dombret: Digitalisation – repercussions for banks and their supervisors

Speech by Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the 16th Norddeutscher Bankentag "Digitalisation – (r)evolution in the banking industry" at Leuphana University Lüneburg, Lündeburg, 8 June 2016.

* * *

Professor Baxmann

Ladies and gentlemen

People love simple stories. There is evidence to show that we find it easier to follow a speech and memorise its contents if we quickly pick up the thread and the message that is being conveyed.

The picture isn't much different where the digitalisation of the financial sector is concerned. Digitalisation is often portrayed as a huge opportunity, as a grave threat, as the first step into a world without banks or as a decades-long gradual process of evolution. But if you ask me, we need to suppress the urge to only ever want to tell, or have ears for, just one of these narratives. We will only be able to grasp what digitalisation means for the banking sector if we are willing to view it with very different sets of eyes and acknowledge the existence of highly disparate aspects. Bearing this in mind, my speech today here at Leuphana University will seek to paint a nuanced picture that does justice to the genesis and growth of digitalisation and how it will impact on banks and their supervisors.

1. General digitalisation trends

Ladies and gentlemen, technical innovation isn't exactly a novelty in the banking sector. As you will know, credit institutions were often among the early adopters of information technology in their administrative operations, at the customer interface or in trading. Hardly a day goes by without digitalisation grabbing the headlines, and that's probably because it's come to be seen as a force that will shake the structure and internal functional make-up of the banking industry to its core, just as it has done in other industries.

But it's not just the technical capabilities of digitalisation that make it so special; the social upheaval it is expected to trigger – and already has done – also makes it something to be reckoned with. There is already evidence aplenty of this phenomenon worldwide. Even in Germany, which isn't a pioneer in this regard, most bank customers now usually conduct their banking affairs online, and mobile banking is also on the rise there. There are already some institutions which use smartphones as the sole channel for their entire service package. As habits change and technical innovations emerge, so, too, will people expect the banking industry to evolve and adapt. There is also a growing desire among customers to use bank services whenever they want, however they want.

Researchers and policymakers have launched a variety of initiatives in an effort to categorise technological advances and uses and to quantify the impact on the economy and society. Yet we need to keep in mind that there's very little, if anything, we can say with any certainty about how financial technologies ("fintechs") will evolve going forward. After all, the sky's the limit for technology – many ideas are refined and tweaked, others are discarded. Whether or not an application is worth pursuing depends in part on how well it goes down with customers, and many other developments in the market. For me, any attempt to realistically predict whether an innovative app will stand the test of time is a little like trying to predict how climate change will impact on the Lüneburg Heath bird population ten years from now.

That being said, it does no harm to say that digitalisation has unleashed an irreversible process. Few of us these days shed a tear over the demise of analogue photography,

typewriters or credit transfer slips. And that's why all stakeholders in the banking industry would be well advised to embrace digital change, and do so sooner rather than later. I would now like to explore the challenges faced by two of the parties mainly affected by the advent of digitalisation: supervised credit institutions, and the financial supervisors and standard-setters themselves.

2. Digitalisation – a challenge for traditional banks

Ladies and gentlemen, speaking as a banking supervisor, I would boil the challenges facing credit institutions down to a straightforward formula. The jury is still out on whether banks can cope with the wave of innovations and remain both profitable and safe in the brave new digital era.

Remaining profitable is a tall order for a number of reasons. First, the competitive landscape in the digital era is a more colourful, more global and faster-moving place. Fintech companies touting groundbreaking, IT-based business ideas are making inroads into the market. In 2014, fintech start-ups attracted a total of more than US$12 billion in funding worldwide.[1] The hyped-up exuberance seen in the last few years and the spectre of new competitors carving up the banking business between them may appear to have given way to a period of sounding out which business ideas stand to be feasible, there's no getting around one simple fact. The influx of new rivals, combined with the advent of more efficient technology and a more discerning customer base, hasn't exactly eased the pressure on the sector as a whole to consolidate.

Second, many forward-looking ideas still need to show what they're made of. The entrepreneurial balancing act, as it were, is to get to the bottom of developments early on and put together a broadly balanced business franchise.

Blockchain technology, an innovation that has repeatedly grabbed the headlines, illustrates this challenge well. Its potential for slashing costs, boosting efficiency and streamlining turnaround times, it is said, is immense. This projection comes as no surprise, seeing as blockchain does indeed promise to revolutionise ledgers and settlement processes by making accounts for financial transactions available to all parties simultaneously as original documents, so to speak, and virtually in real time. Blockchain technology thus has the potential to drive down costs, reduce processing times and possibly even boost the accuracy of not just payments, but securities trading and complex contracts as well. On the other hand, blockchain applications are not a trivial matter in either technological or legal terms.

Whether or not this technology, on balance, is worth it for a value chain in the banking industry thus hinges on a large number of concrete questions. The particular challenge for institutions lies in the fact that successful blockchain applications and other innovations could, thanks to network effects, potentially quickly become the new standard.

In other words, technology can have a disruptive impact on individual business models. That is why it is advisable to confront technological and societal change proactively and to develop a strategy.

Quite apart from this, the banking industry should also use the opportunity presented by digitalisation to become more profitable than before. Digitalisation must on no account be reduced to a zero-sum game in which players aim to divide up a cake without changing its overall size. Costs can be cut significantly in the medium term, and fees justified by innovative services.

But whether it's a multi-channel bank, a purely smartphone-based bank or a niche institution: as a banking supervisor, it is not my place to evaluate business models and strategies. Nor do I wish to have the final say on how banks can and must be as innovative as fintechs. That is

[1] Accenture (2015): The future of fintech and banking: digitally disrupted or reimagined?

up to the market, at the end of the day. But supervisors have an interest in sustainably profitable institutions. If they don't have a strategy relating to the digital age, however, institutions do not have a sustainable position as far as I'm concerned. The entire business organisation, from the IT architecture to long-term staff management, hinges on the digital strategy. Digitalisation therefore has to be addressed by senior management as a matter of priority.

The flipside of digitalisation is the security and reliability of banking business. Here is where digitalisation disrupts the story, if not beforehand. Operational risk in IT is becoming increasingly important, and the digitalisation of banking has transformed financial crime. A large number of reasons can motivate cyber attacks, which range from simple attacks by amateurs to meticulously planned attacks with an economic or political background. At the same time, new hacking methods are spreading through the net at lightning speed and are constantly evolving. A global study conducted in 2015 revealed that 61% of CEOs believe that cyber risks present a key threat.[2] Financial institutions were therefore ranked first out of all sectors in 2014 as the main purchasers of insurance against cyber risks, with average limits of US$57 million.[3]

Banking supervisors have been bringing IT risk and cyber risk more into focus for many years now, for precisely these reasons. After all, their importance can't be estimated highly enough. In the digital age, trust in banks is particularly synonymous with trust in IT. Hence, IT and cyber security remain one of the priorities for the Single Supervisory Mechanism in 2016.

As financial supervisors, we therefore call on credit institutions explicitly to manage their IT and cyber risks just as diligently as they would the traditional risks in banking business. An end-to-end system of cyber defences cannot be created from the bottom up by the IT department – I am certain it is, at its roots, a management task. And it is crucial, not just for the institutions, to evolve in tandem with these developments. I would therefore like to turn my attention now to banking supervision.

3. Banking supervision must evolve in tandem with developments ...

Naturally, supervisors cannot provide an exact prescription for IT and cyber security, as IT applications and the cyber environment are so changeable these days that technical details become outdated extremely quickly. Moreover, there is no one-size-fits-all solution for the multitude of different institution types and sizes. In the end, we should face up to the fact that there is often no perfect defence against individual threats either. So, instead of absolute cyber security, the focus is shifting towards the concept of resilience to cyber risk and the best possible balance between the costs and benefits of various security measures.

That is why German banking supervisors have formulated risk management principles for the institutions we oversee, creating fixed terms of reference, despite rapid developments. There are, of course, specific elements, such as those for cyber defences, that form part of a checklist for all institutions: (1) Network plans with appropriate and (2) multi-level security areas, (3) contingency plans and (4) a well-conceived update management system.

Cyber defences, in particular, shine a light on the fact that security requires more than just a well-functioning first line of defence in the enterprise. Defence against cyber risks is by no means trivial; it actually requires a great deal of foresight and ingenuity. The threats are constantly evolving. And people – whether customers or staff – are often the weak link in the

---

[2] PwC (2015): A marketplace without boundaries? Responding to disruption. 18th Annual Global CEO Survey.

[3] The figure relates to the total limits of cyber insurance policies purchased in 2014 by enterprises with turnover of at least US$1 billion. Source: Marsh (2015): Benchmarking trends: As cyber concerns broaden, insurance purchases rise.A Turner (2015), Between Debt and the Devil: Money, Credit, and Fixing Global Finance, Princeton University Press

security chain, including at banks and savings banks. Ultimately, this calls for intelligent risk management, above and beyond the technical measures. Long-term cyber security thus requires responses to new, and sometimes unknown, circumstances, which simultaneously ensure that the institution reliably fulfils the tasks it is entrusted with. Because after all, and how can it be otherwise: enterprises and organisations are constantly evolving and growing.

Managing the various responsibilities is therefore of paramount importance. This also involves breaking through the responsibility "firewall", where no one is willing to assume responsibility for the many interlinked aspects of cyber risk. Banks often outsource sections of their IT provision, such as servers and software. The cloud is playing an ever greater role, as we all know. But ultimately, banks retain responsibility for any malfunctioning. As a supervisor, I am therefore calling on institutions to be fully aware of what's at stake and to have a plan as to how they intend to tackle risks. Finally, a security culture must be set up and pursued, anchoring the awareness and willingness to act responsibly in the digital bank, above and beyond individual business units.

4. ... but not reinvent the wheel

In light of the rapidly changing environmental conditions – and by these I mean new technologies, new behavioural patterns, new competitors and new dangers – the question arises for many as to whether the current regulatory approach will still be viable in future. In my opinion, this question is the logical consequence of a superficial perception of technology, on the one hand, and banking on the other.

We associate technologies with positive characteristics such as the 24-hour availability of the internet, the transparency of comparison websites, the convenience of smartphone apps and the seemingly free services of many online providers. However, I think it is very important that we also take a look at the downsides. Indeed, technology remains error-prone and obeys economic incentives. Indeed, the manipulated issuing practices of an American loan brokerage platform have come to light just recently. And then there are self-regulating or self-supervising financial technologies such as distributed ledgers, whereby genuine bookings are confirmed by countless numbers of computers carrying out thousands of crosschecks on the bookkeeping of other computers. While these technologies may significantly reduce the likelihood of errors and fraud, they do not eliminate it altogether. Faith in a thoroughly better technology-based world therefore seems to me to be a further expression of the yearning for simple realities and narratives that I mentioned at the outset.

Technology does not, therefore, obviate the need for a critical view from the outside. It is my firm belief that the state cannot, and must not, withdraw from its surveillance function. Moreover, technology does not in any way alter the fundamental tasks and risks that justify the existence of both banks and banking supervisors. The financial system needs monetary policy intermediaries, as well as agents that enable essential services such as lending, deposits and payments. The existence of banks is therefore intrinsically linked to the mechanics of our economic and financial system. And, what's more, key aspects of the financial sector such as risk taking cannot be left to computers because financial decisions are, by their very nature, associated with uncertainty. Therefore, both banks and their supervisors will retain their significance in a digital financial market order.

Neither the systematic favouring of new technologies, nor discrimination against them, can be justified from a regulatory perspective. In my view, what we need instead is a regulatory regime that treats technology neutrally and intervenes at the very moment instruments and institutions produce disproportionate risks. The principle of "same business, same risk, same rules" – to which international regulation already subscribes – will therefore remain the guiding principle now and in future.

There is therefore no need to reinvent the wheel as far as regulation is concerned. The risk-oriented supervisory approach in Germany continues to provide the proper foundation and also

has the necessary supervisory tools at its disposal to take action, for example, against illicit unlicensed innovative financial products and services.

The task today, and in future, therefore consists in consistently applying this risk-oriented approach to new developments and business models. For which financial instruments is automated investment advice or robo-advice really to be classified as advisory business within the meaning of the German Banking Act? Where should the line be drawn between third-party brokerage activities and proprietary lending or proprietary deposit-taking? Here we need to scrutinise grey areas of the law, which in effect can only be assessed on the basis of individual, specific business models of financial start-ups. The many enquiries that fintechs are sending to authorities therefore currently represent a demanding and time-consuming task for supervisors in Germany. This procedure is, by the way, far from new. It has been the case for decades that financial innovations are examined in great detail as part of individual audits and evaluated for the presence of risks that might be subject to supervision requirements.

If we wish to be consistent in terms of our risk orientation, we need to look beyond the existing and functioning supervisory apparatus and keep an eye on possible new risks that could endanger the stability of the financial system. In this context, we will probably need to take a closer look, in particular, at data protection and consumer protection in the coming years.

What about the competitive framework in the digital financial sector? Our regulatory objective should consist in establishing a framework in which the risks taken are defined as the measure of fair competition between all market participants. The debate on the level playing field is being distorted by comparing unregulated and regulated competitors without taking into consideration the financial risks involved. Regulatory and supervisory requirements are seen by institutions as one-sided cost factors and by unlicensed fintechs as barriers to entry. But from the regulatory perspective, the competitive framework should serve neither of them, but instead the economy as a whole.

With regard to the regulatory view of digitalisation, I would, in conclusion, like to make one more remark on the relationship between supporting innovation and ensuring stability. Both objectives are, without a doubt, desirable from an economic standpoint. But while it may appear necessary for banks and savings banks to be simultaneously innovative and reliable, from the perspective of law enforcers and rule makers the various tasks should be clearly separated, where possible institutionally, in order to avoid conflicts of interest.

5. Conclusion

The way one assesses digitalisation in the financial sector depends to a large extent on the pair of glasses one is looking through and the hat one is wearing.

- For banks, it represents a mandate and an opportunity to remain profitable and secure. Each institution requires a carefully balanced, yet clear, digital strategy.
- Supervisors are faced with the challenge of ensuring, amidst a changing environment, that confidence in institutions is always maintained. This means keeping pace with developments and requiring entrepreneurial responsibility wherever significant risks arise.
- Regulators should, however, take care not to reinvent the wheel given the advent of new competitors and new technologies. Specific business models and innovations should be regulated precisely where they produce risks for the financial system.

If all aspects of digitalisation are sufficiently taken into account, I am confident that the history of digitalisation of the financial sector will, in a few years' time, be extolled as a success story by all parties involved.

Thank you very much for your attention. I am now happy to take your questions.