# REAPING THE BENEFITS OF DLT AND CLOUD

## 1. Lessons learned from DLT applications in the financial sector

### 1.1. Ongoing developments based on DLT in the financial sector

An official noted that there are two main types of impact from new technologies such as Distributed Ledger Technology (DLT). One is existing players trying to integrate these new technologies. Another is the technology enabling new business models.

A regulator explained that developments involving DLT have been monitored by their authority at the international and European levels, for the past three years. There are some very interesting projects underway, such as the European Central Bank (ECB) / Bank of Japan Stella Project looking at DLT with regard to settlement systems; the Monetary Authority of Singapore's Ubin Project aiming to issue Central Bank digital money using DLT; and one by the World Bank together with the Commonwealth Bank of Australia whereby they would issue bonds on DLT. There are also investment firms under MiFID II looking into DLT as a possible technology to offer derivatives through smart contracts.

Initiatives are also being conducted leveraging on DLT platforms in relation to anti-money laundering (AML), combatting the financing of terrorism (CFT) and know your customer (KYC) requirements. KYC apps based on blockchain ecosystems that act as an interface between the customer and banks are being developed, whereby the customer uploads information onto the platform and then banks can get access to it with the customer's consent. Such a system simplifies the process for clients who only have to provide information once and then update it. Clients also may remain the owners of the data throughout the process. This type of platform providing a common database with information on individuals who have caused difficulty to banks in different jurisdictions could also potentially be used by EU policymakers to integrate and strengthen AML/CFT in Europe.

DLT could also be used to simplify and streamline some supervisory processes and improve supervisory convergence in the EU, the regulator suggested. For instance, application processes for a licence under European directives or notification processes could be conducted on a DLT platform developed by the European supervisory authorities (ESAs) that could provide the various authorities concerned with the necessary information.

An industry representative referred to a new asset servicing and reporting platform for credit default swaps developed by their company using DLT and supported by cloud services. A distributed ledger is used for the data storage component, which happens after the processing phase is completed. The original project was to use smart contract software for the processing part of the service but this was not possible in the end, because of the amount of computing power needed to support the smart contract code and the risk of disrupting the existing service. Another issue is that the smart contract technology being used was proprietary code and would have required a relatively complex support ecosystem.

### 1.2. Benefits and challenges associated with DLT

An industry representative considered that the full benefits of the DLT technology have not yet been realised. It has not really delivered on cost savings or provided significant efficiencies so far. Actual maturity and improvement in the technology itself is needed, which is partly an issue for the vendors involved. There also has to be a network because there is a need for multiple players willing to be meaningful members of the network and host nodes. Until there is a critical mass of nodes, the full benefits of this technology cannot be obtained. One other potential benefit of DLT is resiliency, because there is a multi-nodal network where many of the same operations are taking place and the same data is being kept. However, when considering how to comply with recovery times, for example, we are still far from the standards needed for Systemically Important Financial Market Utilities (SIFMU) and securities processing firms e.g. in the US. In addition, for anyone embarking on a journey to implement DLT, an early operational stress testing of the software is essential to check performance and capabilities.

An official noted a calming down of the excitement around DLT, somewhat mirroring what has happened in the past with many other financial or technical innovations. In the end many of these have turned out to be incremental changes that fully integrated into the existing financial ecosystem. This is in part due to the specific market structure and regulatory environment of financial services. Experimentation, including at the Central Bank level, has shown that the technology still has room to mature.

Another official expected more fundamental changes coming from DLT. Although it is still an emerging technology, the fact that some Central Banks such as the Bank of England are considering to use it in their high-value payment system for example is an indication that it could be an important part of financial services in the future. Various other experiments have been conducted by the Bank to evaluate how DLT business models could be integrated into their central bank infrastructure.

Besides the maturity of the technology, an industry representative noted that privacy and how it relates to the governance of the network is a major issue for DLT. Decisions have to be made about what takes place on each particular node being hosted by a network participant. The relevant organisation, their internal policies and procedures, and the applicable laws for the firm's jurisdiction all dictate what can take place on the hosted node. That raises many questions that need to be answered. A paper setting out the key components of an effective governance model for DLT networks has recently been released by their organisation. It suggests in particular that there has to be an identifiable governing body in charge of operating the network.

Convergence or interoperability of blockchain codes is a further challenge that does not appear likely to be solved soon, given that there are still very few significant DLT projects actually in production, the industry speaker believed. At some point, if there is significant adoption of DLT by many firms and they are using these different platforms and languages, it could be a major consideration.

Concerning data privacy another official stated that Europe is in a leading position. GDPR was initially considered as a partly unnecessary constraint, now it is being copied by other jurisdictions such as California. The reality is simply that Europe is ahead in this field and many other jurisdictions are expected to follow.

## 2. Lessons learned from the use of cloud computing services in the financial sector

### 2.1. Benefits of cloud services

The benefits of using cloud services go beyond savings, an industry representative explained. Cloud allows for the digital transformation of financial services firms with a significant reduction of the investment needed to build IT infrastructure and of the time and money for running it, as well as increased scalability and accelerated go-to-market to satisfy new customers' demands, hence enriching customer experiences and increasing security. Cloud service providers offer standard building blocks that firms can leverage in a standard way for their services in a pay-as-you-go way. There is no longer a need to spend millions of pounds of capex-intensive investment to just test an idea. If the idea works, an organisation can productionise it quickly. Over the last 10 years, it has been observed that over 90% of start-ups no longer build their own on-premise infrastructure, and in the last 7 or 8 years many different financial institutions have also been attracted to that way of operating. The speaker mentioned a large sovereign wealth fund that recently moved from an outsourced environment and established its own cloud services unit. That helped them to improve their agility through self-provisioning of elastic resources, increased performance and a higher pace of innovation.

An official believed that cloud is becoming a strategic and commercial imperative that company management needs to consider because of the flexibility and agility it offers, the ability to adapt business models in real time and the potential to react to customers' needs as they evolve. This is true in a number of sectors including financial services. Cloud helps to improve significantly time to market, and makes financial services markets much more competitive and healthier. Cloud that uses best-in-class technologies also offers significant resilience benefits for institutions struggling to maintain ageing legacy systems, which can pose challenges for operational resilience. Cloud may also offer effective cyber defences.

An industry representative agreed that resiliency benefits are important when considering how to leverage cloud providers. This is true for financial institutions but also for market infrastructures that are starting to move forward with their cloud strategy.

### 2.2. Implementation process

An industry representative explained that the approach for implementing cloud services is similar for retail and wholesale financial services. The baseline is security, followed by durability, then availability and then speed of the service. The journey is somewhat different for every financial organisation but there are some common characteristics. Many firms start with non-critical services and just want to test an idea. If that idea works, they then productionise it in a very secure and available way.

This is a major change from the traditional way of delivering projects based on a waterfall delivery model. Traditional projects often involved hundreds of people in siloed technology areas and took months if not years to deliver, going through a process of handing product and work units from one team to another. There is now a shift to small technical teams that have all the skills they need within the team, a practice which is widely known as development and operations (devops). It enables the team to take an idea and programmatically configure everything that is needed to test that idea and to then bring it to market. That does require an operating model change, and thoughtfulness of segregation of duty within the team and how to oversee it.

### 2.3. Market concentration issues

An industry representative mentioned that in conversations with financial organisations, the question is no longer about whether cloud is necessary but how to implement it. Gartner published a study last year stating that by 2020, 40% of financial institutions around the world will be using cloud.

An official agreed that moving towards the cloud seems inevitable economically, but raised the question of how the high concentration in the cloud service sector should be addressed by the public authorities. One question is whether the legal view of outsourcing tasks and not responsibilities used in traditional outsourcing arrangements remains relevant with such a concentrated cloud sector. Another is whether this concentration can be dealt with only using regulatory tools or if competitive tools should be deployed.

Another official considered that from a financial stability perspective, the fact that the cloud market is extremely concentrated cannot be ignored. The top four providers account for about 65% of the EU market, which speaks to the fundamental economics of cloud provision, which are that it is a scale business. Such market structures however raise financial stability concerns that have to be thought through, and financial services firms and cloud service providers must be worked with collaboratively to consider how to capture the benefits of cloud whilst also protecting the economy and society from the potential risks. In addition, given the very persuasive benefits of cloud technology, a very wide adoption can be anticipated, not just in financial services but in every area of the economy, which may require a cross-sector approach.

Regarding the use of competition tools, central banks such as the Bank of England are not competition authorities. Its first and foremost responsibility is to protect the safety and soundness of the financial institutions supervised and financial stability in the markets. It does have a secondary objective to promote competition in the markets it oversees, but in doing so its tools are less competition than financial supervision tools. These latter tools involve a close monitoring of changes in market structures and their implications for financial stability to avoid markets being locked into certain critical providers. Secondly, supervisors interact with firms using cloud and conduct on-site inspections of cloud service providers, which requires changing both the supervisory mindset and skill set.

The current approach of supervisors is to put the responsibility of cloud arrangements on regulated financial institutions, the official confirmed, as for other outsourced services. This situation is being further investigated by the authorities and specific guidelines have been published by the European Banking Authority (EBA)[1] on the use of cloud and outsourcing arrangements, but no threshold has been defined yet for policy intervention. In June 2019 the Bank of England issued a commitment to update its policy on critical outsourcing arrangements, particularly cloud. It will include clear expectations for financial firms about how they can use the cloud and expectations around risk management, incorporating the EBA guidelines on the use of such arrangements. Ways to promote and participate in international collaborations should also be considered, to make sure that cloud can be used in a resilient and safe way across borders and to avoid fragmentation, given that many financial institutions and cloud service providers are international.

Answering a question about whether cloud providers should be considered as critical infrastructures, an official was not sure that a conclusive answer could be provided at this juncture. Cloud services are only one aspect of critical services that need to be assessed more broadly. Another official considered that there needs to be supervisory metrics to assess the level of concentration and these do exist. The degree of criticality goes together with the benefits that cloud provides and that is being watched closely. However, any policy response should strive to harness those benefits rather than stifling innovation.

## 3. Regulatory and supervisory approach to DLT and cloud services

### 3.1. More specifically related to DLT

An official noted that regarding technology the role of financial regulators is notably to avoid the emergence of risks and maintain a level playing field. The impact of innovations should not come to the detriment of markets and speed-to-market should not be pursued ignoring risks. This may require some specificities in the supervisory or oversight approach.

When assessing new business models, for example those that may emerge with DLT, it appears that some are designed in a way that is fully compatible with the existing regulatory framework and others try to test the boundaries of existing regulation. Addressing this from a regulatory standpoint requires technology neutrality. For example if an arrangement is designed to perform transfers of values it is likely a payment system and should be regulated as such, irrespective of whether it uses DLT or tokens, or some other innovative feature. A more functional approach to regulation should be considered, going beyond the traditional prudential focus on entities. These are already long-established concepts in central bank oversight that looks at particular services, schemes, arrangements and operators.

In terms of rules and standards, the European Commission is assessing whether the existing financial acquis is posing obstacles to the implementation of new technologies in the financial sector, as part of the fintech action plan. Attention is notably given to privacy and data management issues in this context. At the international level a review of the global principles for financial market infrastructures (PFMIs issued by CPMI-IOSCO) has concluded that they are technology neutral, with perhaps the exception of the need to have a central responsible entity within a DLT network. The combined result of work conducted at International and European levels should allow for the provision of a technology neutral and risk sensitive regulatory environment to foster and support innovation based on new technologies.

Interoperability concerns still need addressing, the official considered. Otherwise there will be silos and fragmentation in the implementation of DLT, resulting in frictions and costs, that will then take much time to overcome. There is a particular role to be played jointly by the industry and the regulators in this respect to ensure a sufficient harmonisation of rules and technical standards.

### 3.2. More specifically related to cloud services

An official explained that there needs to be continual adaptation of how technology applications are supervised in order to ensure operational resilience. Supervisors are already assessing this thoroughly, but they need to address those questions in a more specific way and become quicker at resolving some of the concerns.

Another official agreed that supervision needs to evolve with the increasing use of technology. The starting point in the central bank oversight domain is perhaps easier to adapt to cloud services than for prudential supervisory frameworks, because it already uses the notion of critical service provision in addition to outsourcing. Due to the emergence of a number of new services, a very intensive mapping exercise has been undertaken across the European infrastructure to evaluate the degree of critical service provision in the financial sector. Numerous critical service providers were identified, with different degrees of criticality, showing that Europe is a very complex picture when it comes to infrastructures.

The existing oversight policy framework for critical service providers is being reviewed in the Eurosystem. A first question is the degree of provision of critical services by a single provider that may constitute systemic relevance and what this may imply for the user of the critical services. A second point relates to the way evidence of compliance with regulatory requirements is provided by the users of critical services, given that many infrastructures and institutions rely on the same critical service providers. Each individual institution may provide some evidence, or there could perhaps be a more streamlined and collective process. A third aspect relates to the extent to which an institution or infrastructure relies exclusively on cloud service provisions, and whether there is a need to have alternative, non-cloud based mechanism in the case of emergencies. A last point concerns the implications of cyber-resilience. In the Eurosystem, cyber-resilience oversight expectations have recently been issued, which impose increasingly stringent standards on overseen entities. When the overseen entities rely on third parties, there is a question of how to ensure that there is sufficient compliance with these requirements and how supervisors can be provided with evidence of this.

A regulator believed that supervisory approaches should evolve in a digital environment. More money should perhaps go into supervisory technology that could allow more automated approaches for checks. The cloud and related analytical tools provided by cloud service providers could also potentially be used more by financial supervisors to access the data of licensed entities and carry out checks.

An industry representative concluded that it is crucial that the right balance be found to ensure that risks are mitigated while encouraging innovation and growth. This notably requires taking into account the needs and concerns of market participants.

[1] https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf