FINANSTILSYNET

Discussion paper

Fintech – in the area of tension between financial regulation and new technology

FINANSTILSYNET

Contents

Background

Financial regulation and supervision of corporate compliance do not generally address the technologies deployed by financial companies. Nevertheless, financial regulation is best aligned with existing business models in established financial undertakings. In the past, technological advances were made at a steady pace. In particular, advances tended to be made as upgrades to existing corporate operating platforms. Similarly, the channels whereby companies supply products to customers have increasingly been digitised. However, this has not fundamentally disrupted the interaction between the regulation and those prevailing business models.

Over the last decade, the pace of technological developments in the financial sector has accelerated significantly, both in Denmark and globally. Increasingly, we are also seeing companies with a fundamental technology-based approach, which is beginning to disrupt prevailing business models. Such companies may be providers of social platforms that are starting offer payment services, or small-scale fintech companies offering specific, delimited (unbundled) insurance or pension products.

The focus in the financial sector, and especially among the more technology-based new actors, is not on whether the solutions mesh with the familiar business models and hence financial regulation, but rather on solving specific financial challenges and providing financial services by means that are intuitive and easy for customers to access. In some instances, this makes it difficult to adapt such financial services to current financial regulation since these services may involve digitising the distribution channel for financial products, thereby enabling them to be supplied online or on mobile devices. In other cases, the services involves the use of big data and technologies such as artificial intelligence, machine learning and blockchain.

On the one hand, these trends carries a number of positive effects, such as the potential for increased competition, better and cheaper products for consumers and optimised processes within the companies. On the other hand, the increased use of technology and internet-based business models poses a number of new business and operational risks or exacerbates existing risks.

This raises the obvious question of what role the Danish Financial Supervisory Authority (FSA) should play vis-à-vis this trend. As a regulatory authority in the financial sector, the FSA might in some circumstances promote and encourage the trend in the interest of promoting business digitisation and innovation. In other circumstances, the FSA might seek to curb or even inhibit a trend in the interests of consumer protection or the stability of incumbent financial institutions.

This discussion paper presents four key topics that the FSA expects will determine future developments in this area.

The discussion paper forms the basis for the FSA's fintech conference to be hosted on 4 December 2019 at Docken event centre in Copenhagen.

With this conference, the FSA firstly aims to promote discussion about expectations regarding developments in this area, and secondly, to gain inputs on what the role of the FSA should be in supporting the use of new technologies in the financial sector and how the FSA should address the risks entailed by the evolving trends.

The FSA invites the financial sector, business and industry, consumer representatives, policy-makers, experts and other interested parties to offer their points of view on the topics raised in this paper. The FSA will include these views in the FSA's further analysis of the area.

All contributions and points of view are welcome before, during and after the conference, however, please note that they must reach the FSA by no later than 15 February 2020 at fintech@ftnet.dk

The four key topics for the conference are summarised briefly below, and are then elaborated on individually in the subsequent chapters.

Regulatory sandboxes have been focal in the debate on the role of authorities in the area of fintech. The FSA opened its own version, FT Lab, in February 2018. However, the question is whether regulatory sandboxes are actually the right tool. Do they fulfil the purpose of supporting fintech start-ups and the financial sector's use of technology? To what extent can a sandbox test solutions vis-à-vis the financial regulation?

Open Banking is an example of an area in which the authorities have opted to adapt regulation to a new business model that has emerged as a result of the technological development. Open Banking has the potential to fundamentally alter the way in which banking products are delivered to customers and the terms governing how and where customer relationships are formed. Regulatory developments in this area have only just begun with the implementation of PSD2 in January 2018. What potentials does Open Banking hold? What are the risks and opportunities associated with this business model? Do we need more regulation, and what should the role of the FSA be? What are we expecting to see in this area in Denmark?

Crypto-assets are digital assets linked to blockchain or similar technologies. They could potentially have major impact on a number of financial services in the future, from payments to securities. During 2019, a number of international authorities, such as the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), the Financial Stability Board (FSB) and the Financial Action Task Force (FATF), has addressed this area. How should crypto-assets be dealt with in a regulatory manner? Do they even belong in the financial regulation as we know it?

Big tech – Facebook, Apple, Amazon, Google, Tencent with WeChat and Alibaba with Alipay – have so far only gained limited ground in the financial sector, especially in Denmark. However, big tech companies have the capacity to gain market share rapidly and with substantial impact – including in the financial sector. What challenges does this pose? How should the FSA address these challenges and this area generally? How should the supervision with big tech be? Does it pose risks outside the scope of the FSA's competencies?

Regulatory sandboxes

On 1 June 2017, in pursuance of the Government's digitisation strategy for Denmark, the Danish Parliament (Folketinget) decided that the FSA was to establish an *Innovation Hub* for Fintech start-ups along the lines of the UK Financial Conduct Authority's initiative[1].

To that end, the Parliament decided that the FSA should assist in making it more attractive for fintech companies to establish and operate in Denmark. This is to be achieved primarily by providing guidance to start-ups on financial regulation. The FSA is thus required to support the use of new technology in the financial sector, with consideration on growth, financial stability as well as consumers and investors.

In addition, the FSA established a regulatory sandbox, FT Lab, in which companies can test new technologies and business models on real customers together with the FSA. As part of the sandbox testing, companies can obtain authorisation to provide financial services, but under certain restrictions. The FSA determines those restrictions on a case-by-case assessment of the possible risks posed by each company's individual test programme.

While the creation of both the innovation hub and FT lab politically were aimed at supporting start-ups in the financial sector, these initiatives also serve other important purposes: to extend the Danish FSA's insights into new technologies and how they square with Danish financial regulation. In turn, this is intended to enable the FSA to continue to perform corresponding supervision of the financial sector going forward.

In February 2018, the FSA opened for applications for FT Lab. The first-round participants were the companies hiveonline and e-nettet. The focus of the two tests was, respectively, the use of blockchain for payments and the use of machine learning for generating real estate sales price estimates. For both tests, the technologies had not previously been deployed in connection with the regulated activities concerned.

Based on the findings of the first cohort the FSA subsequently adapted FT Lab, and at the time of writing the FSA is reviewing received applications for the second round. The adaptations meant, for example, that FT Lab now accepts applications on an ongoing basis. In other words, the FSA is no longer operating with cohorts and application deadlines. In addition, companies can now test individual components of their business models. This means that they do not need to have a fully developed and coherent business model in order to be accepted for testing in FT Lab.

In addition to fulfilling the purpose of guiding start-ups on financial regulation, FT Lab is also intended to support the use of new technology in the sector. It is the intention that the knowledge amassed from companies that have completed testing in FT Lab, will be made available, as far as possible, to the entire market, for example by means of best-practice documentation or other forms of guidance.

[1] See Appropriation Request No. 80 of 15 May 2017 from the Ministry of Industry, Business and Financial Affairs to the Parliamentary Finance Committee at https://www.ft.dk/samling/20161/aktstykke/Aktstk.80/1756726.pdf.

The outcome of the test of e-nettet exemplifies this. e-nettet and the FSA discussed a machine learning model which the company has developed for estimating the sales price of residential properties in Denmark. Generally, real estate sales price estimation is not subject to financial regulation, but if, for example, a mortgage credit institution were to use those estimates for issuing mortgages, then it would be subject to a number of regulatory requirements. FT Lab tested how companies might document relevant processes and account for the results when they deploy machine learning.

Based on this test in the sandbox , on 10 July 2019, the FSA published a guidance entitled "Best practice when using supervised machine learning"[2]. The paper set out the factors that a financial undertaking should consider, as a minimum, before using machine learning to perform activities that are subject to financial regulation. The paper also describes the documentation of processes, development and results which the FSA expects a financial undertaking to complete. A number of other national authorities, including the FCA in the UK and BaFin in Germany, have published statements and memos, which are well aligned with the Danish FSA's considerations.

In this way, regulatory sandboxes, under controlled conditions, can give the FSA insights into the use of new technologies and business models and their entailed risks. Equally, they give the FSA an opportunity to provide the financial sector with general guidelines based on the experience gained by the sector and the authority in relation to a new technology.

In the debate regarding the rationale for FT Lab, some stakeholders pointed out that the outcomes of regulatory sandbox testing primarily benefit the participating companies. Therefore, it is essential that the experience gained in FT Lab is shared with the entire market in a format that benefits as many companies as possible. As stated, the FSA's experiences from FT lab's first round provided the basis for "Best practice when using supervised machine learning". However, the sandbox testing of the company hiveonline did not generate any new knowledge on a scale that merited dissemination in specific recommendations to the sector.

Questions:

1. Is a regulatory sandbox like FT Lab the right tool?

2. Does a regulatory sandbox give start-ups the intended access to necessary guidance?

3. Does a regulatory sandbox adequately support the use of new technologies in the financial sector?

4. To what extent can a regulatory sandbox test solutions vis-à-vis financial regulation?

[2] Cf. https://www.finanstilsynet.dk/Nyheder-og-Presse/Pressemeddelelser/2019/Machine_learning_10719.

5. Regulatory sandboxes provide an opportunity for the FSA to examine closely new technologies and business models. Equally, they give the participating companies insights into which requirements they are subject to and how to comply with them. How do we ensure that other segments in the market also benefit from these insights, and how can we best communicatet hose insights?

6. Does a regulatory sandbox primarily benefit either new start-ups or incumbents, both types of financial undertaking, or is it in fact only the FSA that stands to benefit?

7. If it only benefits one part of the sector, what adjustments are needed in order to diffuse those benefits sector wide?

8. How might FT Lab be designed to maximise its value to the market as a whole?

Open Banking

The revised EU Payment Services Directive, PSD2, implemented in the Danish Payments Act ("Lov om betalinger") entered into force in January 2018. The last delegated acts entered into force in September 2019. The new rules require banks and others who offers payment accounts to their clients to open their payment infrastructure to third parties that can execute transactions (payment initiation services) and retrieve payment data (account data services) on behalf of those clients from their payment accounts. This must be accomplished by the banks making functional and well-documented technical interfaces (APIs) available to the third parties.

API is an acronym for Application Programming Interface, which is a software interface. An API allows different programs to communicate with each other. Basically, an API enables data to be exchanged regardless of the application in use at either end; in this case between the bank's and the third-party's applications. In popular terms, API is analogous with the means of 'plugging into' a bank. With an open API, parts of an infrastructure are made accessible to others so that they can integrate with the infrastructure and develop products and services on top of it. This means that APIs enable third parties to develop services and products for customers on top of the solutions already offered by the banks. Initially, the simplest solutions might consist of a new payment solution for online purchasing based on bank-to-bank transfers or a budget app allowing users to gain an overview of their finances based on data from their account(s) with one or more banks. However, the scope of what companies potentially can build on top of banks infrastructures is very broad.

APIs are part of an ongoing trend, not only within the financial sector, but in society at large, where consumers and companies are increasingly gaining access to and ownership of their own data, which has formerly been retained by third parties.

In the financial sector, this has resulted in a growing number of banks voluntarily opening up their infrastructure and data to business partners. This trend is known as *Open Banking.* Open Banking has the potential to go beyond the APIs required by PSD2 as it enables third parties to develop new solutions for customers on top of the existing financial infrastructure

in areas other than payment services. For example in relation to investments, pensions or mortgage credit. As such, the ultimate consequence of this is that banks come to serve as platforms upon which third parties – either in cooperation or in competition with the banks – develop new products and services.

On the one hand, Open Banking promises more competition and better and cheaper solutions for customers. Many banks have created innovation and partnership units, and some foreign banks have fully embraced Open Banking, basing their entire business on open APIs. In these cases, the bank typically provides the underlying financial activity, such as transacting a payment or setting up a deposit account, while the partner provides the technology that makes it possible to provide the end users with a more user-friendly and smart interface.

On the other hand, Open Banking also raises a number of concerns and significantly alters the overall risk exposure. Among other things, the development of open APIs introduces new operational and IT risks. How do we ensure that APIs do not affect the stability of other services offered? That APIs do not simply provide easy access for criminals to payment infrastructure and facilitate fraud and money laundering? And how do APIs provide for sufficient protection of consumer data?

At the same time, the competitive situation is changing between banks as well as between banks and third parties, now that it is possible to access data and initiate payments from accounts controlled by other entities. The customer relationship itself may be transformed when the customer is no longer interacting with the bank itself (meaning the provider of the underlying financial service), but with a third-party provider positioned on top of the infrastructure.

The new rules on payments – and Open Banking more generally – will result in – and have already resulted in – a number of new players in the financial sector who, to a greater extent than banks, base their business models on customer data. This raises the question of how companies can best inform consumers and encourage them to make prudent choices concerning the use of their data. How can we jointly ensure that consumers are aware of who they are sharing their data with, what their data are used for and the consequences of this ?

In addition, a number of questions arise concerning the role of regulatory authorities in relation to Open Banking in general. To what extent should the authorities promote or prohibit financial undertakings from developing APIs that can do more than the APIs required by PSD2?

The FSA has several possible courses of action in its supervision of compliance with the new rules in PSD2. On the one hand, the authorisation rules that apply to new third-party providers could be interpreted restrictively, and the FSA could impose strict requirements regarding the development of APIs. This would counter some of the new risks in that it would restrict access to data and features accessible through APIs. Similarly, the FSA could restrict the number of new third-party providers. However, such restrictions would also disincentivise the development of new products and services.

Alternatively, supervision could be oriented towards proactive support for the development of more and better APIs that will give potential third-party providers even better opportunities for developing innovative new services. One way of achieving this would be for the FSA to engage more actively in the development of banks' APIs. One option would be to establish collaborative forums between third party providers and banks along the lines of those set up in the Netherlands and the UK. This could facilitate the development of new and improved products and services for consumers and companies. It would also serve to strengthen Denmark's position alongside benchmark countries in developing a state-of-the-art banking infrastructure.

However, this course of action poses a number of risks and concerns regarding the aspect of competition . If the number and diversity of products available through open APIs are allowed to go beyond payments, the complexity will increase. This will in turn increase the operational risks. At the same time, we will need even better consumer protection. Finally, consideration must be given to how we ensure a level playing field between the banks and the new third party providers.

In Denmark, we have a tradition for creating solutions to large-scale IT development projects jointly within the financial sector. This, for example, is the mindset behind Denmark's common payment infrastructure. However, development of the open APIs has not been accomplished in the same concerted manner. The advantage of this is that the various banks and data centres have been able to develop APIs tailored to their particular setup and ambitions. A drawback to this is that it might potentially result in a fragmented market.

Other countries, such as the UK, France, Czech Republic and Poland have taken the initiative to develop a national API standard at sector level. In some cases, these initiatives have also involved the national authorities. Do we have a similar need in Denmark, and if so, does it go beyond the APIs developed on the basis of PSD2?

Questions:

9. What are the risks and opportunities associated with Open Banking?

10. Have the new rules inPSD2 had the intended effect? If not, how do we achieve that?

11. Do we need more regulation, and what should the role of the FSA be?

12. Do we need API standardisation in Denmark? If so, which body should be responsible for this?

13. What are the implications of Open Banking for the financial market of the future?

Crypto-assets

The first bitcoin transaction was completed in January 2009. Since then, interest in bitcoin, and in blockchain as the underlying technology, has only increased. The authorities have to

a great extent followed developments in this area from a distance. In 2013 and 2014, the FSA, Danmarks Nationalbank (the central bank og Denmark) and the Danish Customs and Tax Administration issued guidances and official statements on bitcoin and other virtual currencies. At the same time, the FSA emphasised that bitcoin and similar virtual currencies are not subject to financial regulation, and warned consumers against the risks posed from trading these currencies.

Since 2013, the market has undergone tremendous development. Businesses of all sizes are now seeking to use the technology behind bitcoin for a number of purposes other than for simply supporting a decentralised means of payment. This means that interest in blockchain today is more concentrated around other usages, such as raising capital or registering ownership of assets, rather than virtual currencies such as bitcoin. This has also rendered the original concept of virtual currencies obsolete, which has been replaced by the concept of crypto-assets. Crypto-assets denotes digital assets, the value of which depends primarily on the use of asymmetric cryptography and distributed ledger technology (DLT).

Distributed ledger technology (DLT)

No formal definition of DLT exists. In general terms, DLT may be described as a set of technical solutions that in combination facilitate a decentralised and cryptographically secure registry (ledger) of data that are securely distributed to – and processed by – a network of disparate network participants. The ledger may contain all kinds of data such as transaction data, proprietor records and identity data. The ledger may also contain more complex data such as software. By using DLT, the decentralised ledger, unlike traditional centralised equivalents, does not have to be operated by a trusted third party. For example, the ledger may be operated by all its users jointly. In this way, everyone has access to the data without anyone necessarily owning it.

Although both knowledge of crypto-assets and DLT and their uptake have increased significantly in recent years, so far, the most widely adopted notion of crypto-assets has been influenced by the original understanding of bitcoin. At the same time, the majority of business models that emerged in the period following the launch of bitcoin were attempts to emulate bitcoin. The common aim of these business models was to create a product that would serve as a virtual and decentralised means of payment on the internet – just like bitcoin. The general perception has typically been and to some extent persists that the design of bitcoins primarily made them suitable for money laundering. Solutions based on blockchain are therefore often viewed with some scepticism. This is unfortunate bearing in mind that the technology can be used to solve legitimate problems in the financial sector.

The underlying blockchain technology has evolved significantly over the past 2-3 years. Whereas it was originally simply a decentralised registry of transactions, today's blockchain technology may comprise and execute more complex software applications. This innovation has meant that companies in the financial sector are now able to use existing business models, but based on blockchain technology. At present, this applies to activities such as money remittance, e-money issuance, digitisation of rights by tokenization, crowdfunding through Initial Coin Offerings (ICOs) and insurance policies taken out and administered by means of smart contracts (a kind of "intelligent" and digitally-accessible contracts that use algorithms

to decode the terms of the contract and automatically monitor whether those terms are met).

Initial Coin Offerings (ICO)
The concept of ICO refers to when a company seeking to raise capital offers its own crypto-asset for the public to buy. Purchasing crypto-assets may grant various rights, including shares in the company, profit rights, managerial powers or rights to the company's future goods or services.

This entails a need to determine whether such new business models fall within or outside the scope of current financial regulation, especially given that many of these business models are reminiscent of products or activities that are currently regulated. For example, a token issued on a blockchain that grants the holder the right to receive a percentage of a profit or turnover is similar to a share certificate or other proof of ownership.

In other words, DLT allows companies to transfer a number of existing activities they currently offer via centralised platforms and registries to a decentralised platform, which gives the individual stakeholders better options for trading amongst themselves without costly intermediaries. Using encryption and distribution of data between network participants, DLT provides a means of carrying out secure transactions and exchanging data among multiple parties who are not necessarily known to each other. In this way, the technology eliminates the challenge of asymmetrical information (the situation where a party holds information which other parties do not), which results in full clarity as to who owns what. The need for a financial undertaking as 'middleman' is thus reduced, given that one of the customary roles of financial undertakings is precisely to ensure that this is effected securely and credibly.

A number of international companies are also testing whether blockchain and crypto-assets can be used to facilitate inter-bank procedures for cross-border payments. This might involve the use of so-called stablecoins, meaning cryptocurrencies the value of which is linked to real assets such as dollars or euros. In this way, the parties avoid using the conventional correspondent bank setup, which is both costly and complicated. Instead of a payer transferring money through a bank to a payee, the transferor exchanges an amount into a cryptocurrency, which is then transferred to the payee and immediately converted into money in the agreed currency.

Fintech companies have, for example, already succeeded in significantly reducing the cost of international money transfers through the use of crypto assets. Equally, the prediction is that DLT will be an integral element in future database infrastructures across sectors. More and more financial institutions are exploring how they can use DLT to either create tomorrow's financial services or provide yesterday's in a more efficient way.

On the other hand, DLT and crypto-assets pose challenges for both authorities and financial undertakings. In particular, the decentralisation of services puts the regulatory framework to the test. The increasing trend in favour of decentralised platforms makes it difficult to identify who, in practice, is to ensure compliance with regulatory requirements (and who can subsequently be penalised for non-compliance). This is because it can be difficult to identify a natural or legal person as the originator of a given activity. The challenge arises because

current financial regulation is aimed at the specific undertaking that performs regulated activities.

Traditionally, money remittance has been offered by companies run by natural persons who offer to do the transferring, which means that there is a central service provider identifiable to customers and authorities. The company that offers money remittance has an address, registered owners, a management, etc., whereas these are not always identifiable for a great many decentralised services. This is often because the services do not have an address, registered owners or a management, this being exactly the decentralised aspect. These services or platforms often consist solely of a piece of autonomous software (for example, a 'smart contract') that has been uploaded to a blockchain or otherwise made available online. The question in the future will be how this new type of platform can and should be regulated. Should the programmer who encoded and uploaded a software application be held liable analogously with a company offering a service? How might a smart contract be subject to supervision and enforcement if it is no longer in the programmer's control once it has been released for use?

The use of crypto-assets for value transfers also poses potential challenges in preventing money laundering and terrorist financing. Masking and anonymisation of value transfers and transaction data is becoming readily available, and there are no key operators who can be required to be perform know your customer procedures.. This lack of transparency has meant that crypto-assets to some extent have been exploited for illegal purposes. Europol estimates that between three and four billion Euros were money-laundered through crypto-assets in Europe in 2018[3].

In an attempt to curb this, the EU, with its fifth anti-money laundering directive (AMLD5), decided that in future, anti-money laundering regulation should extend to "providers of currency exchange services between virtual currencies and fiat currencies" and "custodian wallet providers". This means that as of 10 January 2020, providers of currency exchange services between virtual currencies and fiat currencies and custodian wallet providers are required to apply for the FSA's authorisation to provide these two types of services. This means that the providers must comply with the requirements of the Danish anti-money laundering act, including the fit and proper rules. These two types of services have been included in the anti-money laundering regulation because they are the primary interfaces between the crypto-asset market and the traditional financial market. Concurrently with the implementation of AMLD5, various authorities under the auspices of international organisations are seeking to further strengthen the regulation of service providers, whose services are linked to crypto-assets. This will entail, among other things, that providers of exchanging services between various virtual currencies in the future also will be subject to the anti-money laundering act.

In addition to the above mentioned issues, there are a number of risks associated with crypto-asset trading that consumers especially are exposed to. This includes absent or insufficient investor information. Particularly in the case of ICOs, which often fall outside the scope of the financial regulation, a lack of investor information may pose a problem. The reason for this

[3] "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", p. 17 (www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf).

is that ICOs are generally not subject to the same documentation requirements as, for example, securities offerings in a regulated market that requires the offeror to publish a prospectus. Similarly, there have been several cases of fraud/scams in which the information accompanying an ICO proved to be misrepresentations. In these cases, crypto-assets were put up for sale in order to take advantage of the attention and risk appetite associated with ICOs, but without any intention of realising the business plan published in connection with the issuing.

Against this backdrop, a number of questions arise as to how the authorities should address the situation and how the prevailing legislation should be interpreted in relation to crypto-assets.

Questions:

14. How might crypto-assets transform current financial services? Should the FSA support this transformation?

15. Is it possible to effectively regulate activities involving crypto-assets and the assets themselves by means of the current regulation?

16. Does Denmark need specific regulation of crypto-assets? Or do we only need clarification of which rules apply to activities involving crypto-assets within the prevailing financial regulation?

Big tech

Major technology companies such as Google, Amazon, Facebook and Apple from the US and Tencent with WeChat and Alibaba with Alipay from China have grown significantly over the past two decades. Today, they are key elements in the daily lives of many citizens and companies. The business model of many big tech companies is largely based on collecting data on user behaviour. In this sense, the users have 'paid' with their data to gain access to the services available on the digital platforms.

The companies use this data for optimising their platforms and offering new services, which in turn generate more data on the users. Big tech companies have thereby created a self-reinforcing *feedback loop*, in which more and more data on users is being generated, which in turn is used to retain them on the platforms. Revenue for big tech companies has mainly been linked to these data, for example by them offering other companies targeted marketing to specific segments of their platform's users.

However, the vast volume of data on the users of the platforms can also be used to offer various financial services. The range of these, which are linked to the other services on the platforms, supports the feedback loop and ties platform users even more closely to the given platform.

Payment services was the first area traditionally offered by the financial sector to be targeted by big tech. PayPal (originally owned by eBay) started offering electronic payments in the

early 2000s. In China, Alipay, which is affiliated with the Alibaba e-commerce platform, is currently the largest electronic payment service provider. The area of payment services exemplifies how a financial service can channel users into the big tech companies' data-generating feedback loop. If the platform offers to manage the payments for users trading with each other, it retains those users on the platform. Meanwhile, the platform gains access to even more data on the users, namely the transactions. This also means that the need to make money from the management of payments itself is lesser for big tech than for more conventional financial undertakings that provide payment services. The business model is based on tying the user to the platform, thereby generating more data - not necessarily on earning a fee on each transaction.

Over the past 5-10 years, big tech companies have started to move into other financial areas beyond payments. There are examples of big tech targeting segments such as money market funds, insurance and credit. These areas can to some extent be seen as the next step in the big tech expansion of their platforms and user retention.

When a platform offers to mediate user payments, it stands to amass very large transaction volumes, which it has to manage for the short period of time elapsing from when the purchaser transfers the money and until the seller receives it. One result of this has been that Yu'E Bao, a money market fund affiliated with Alipay, is now managing assets worth in excess of DKK 1,000 billion, making it the largest money market fund in the world.

Companies can also use the increasing insight into user behaviour and transactions on a platform to offer loan financing. Amazon, for example, offers loans to small businesses through the company Amazon Lending. These customers are typically sellers of goods and services on Amazon's platform. This has generated vast volumes of data on the companies, which Amazon has been able to use to continually credit-rate them and predict when they would require liquidity.

The above mentioned services are all provided on the basis of a data availability that more conventional financial undertakings do not have. At the same time, this raises a number of both legislative and supervisory issues.

On the one hand, big tech companies are providing user-friendly, targeted and smart solutions that meet customers’ demand. In countries outside Denmark, by virtue of the structure of their platforms, they can boost financial inclusion by extending financial services to individuals who traditionally have not been eligible for a bank account, e.g. due to their private financial circumstances, geography or a lack of financial infrastructure.

Access to vast volumes of data and the increasing maturity of technologies such as artificial intelligence and machine learning enable big tech companies to analyse liquidity requirements and creditworthiness, which may be significantly more accurate than ratings based on the information traditionally available to financial institutions.

All of this promotes increased efficiency and better and cheaper financial products and services.

On the other hand, all of this entails new types of risks and potential new competitive problems, which in turn, could result in economic distortions (market failures).

The platforms offered by big tech companies could become so dominant that they actually limit the competitiveness they initially facilitated. This is mainly because the value to the users of those platforms comes from the (many) other users already using those platforms, also known as 'network effects'. The entry barriers to the markets dominated by big tech companies can thus become very substantial, as new players find it difficult to achieve the same user bases. Once users have engaged on the platform, the company has a vested interest in ensuring that users choose and use those products and services that generate the highest revenue and activity on that platform. Big tech platforms thus have the potential to create data monopolies.

Moreover, access to high volumes of data on consumers and companies (merchants) can provide a great deal of insight into their shopping/trading patterns and preferences. This insight can help consumers make better choices. However, it can also be abused to exploit consumers' cognitive biases in a way that has not been possible before. This presents a number of concerns about how to best ensure consumer protection in a world where data volumes are growing.

Level playing field is a focal aim of financial regulation. Legislators and public authorities must ensure that the payment services regulation is consistent, whether the services are offered by Facebook or a bank, and that insurance policies meet the same requirements, whether offered by Amazon or an insurance company. This raises a number of questions about how big tech companies are in fact subject to the same regulation as established financial institutions.

Questions:

17. How do we ensure a level playing field between big tech and conventional financial companies?

18. Is it a concern that big tech companies have access to data on their users' behaviour that other financial companies do not have access to?

19. Does Denmark need special regulation, e.g. competition or data protection rules, or supervisory measures to ensure the necessary consumer protection as data-driven platforms move into the financial sector?