Digital finance: Emerging risks in crypto-assets – Regulatory and supervisory challenges in the area of financial services, institutions and markets

European added value assessment

STUDY

EPRS | European Parliamentary Research Service

Author: Jérôme Saulnier with Ilaria Giustacchini
European Added Value Unit
PE 654.177 – September 2020

EN

Digital finance: Emerging risks in crypto-assets – Regulatory and supervisory challenges in the area of financial services, institutions and markets

European added value assessment

European Parliament legislative initiative reports drawn up on the basis of Article 225 of the Treaty on the Functioning of the European Union are automatically accompanied by a European Added Value Assessment (EAVA). Such assessments are aimed at evaluating the potential impacts, and identifying the advantages, of proposals made in legislative initiative reports.

This EAVA accompanies a resolution based on a legislative initiative report prepared by Parliament's Committee on Economic and Monetary Affairs (ECON), presenting recommendations to the European Commission on Digital finance: Emerging risks in crypto-assets – Regulatory and supervisory challenges in the area of financial services, institution and markets.

The main purpose of the EAVA is to identify possible gaps in European Union (EU) legislation. The various policy options to address this gap are then analysed and their potential costs and benefits are assessed.

EPRS | European Parliamentary Research Service

AUTHORS

Jérôme Saulnier with Ilaria Giustacchini, European Added Value Unit, European Added Value Unit, DG EPRS

This paper has been drawn up by the European Added Value Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please email: eprs-europeanaddedvalue@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in September 2020.

PE 654.177
ISBN: 978-92-846-7078-9
DOI: 10.2861/525
CAT: QA-02-20-663-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Background

Digital finance is playing an increasing role in the provision of financial services in the European Union (EU). Rapid progress with digitalisation, data analysis and computing capacities are allowing for a new range of financial services and transactions, contributing to boosting innovation. In particular, the diffusion and the development of crypto-assets enabled by digital financial technology has attracted a lot of attention, as they could offer some potential for economic development and growth if the associated risks are mitigated.

Why should the EU act?

Crypto-assets are diversifying extremely rapidly, in line with the ongoing structural transformation in technology, preferences and usages amongst investors and consumers. Moreover, the international dimension linked to crypto-assets should also be taken into consideration, as crypto-assets are by nature cross-border in their application and infrastructure. These concerns are exacerbated when crypto-assets are not backed by an accountable entity that can be bound by regulation and held responsible for potential breaches of regulation. An important issue when it comes to crypto-assets is therefore also being able to clearly determine exactly what they are and which rules, if any, apply. Some crypto-assets fall under existing EU law, but most of them do not. This can leave investors and consumers exposed to substantial risk.

Given the complexity and the rapidly evolving nature of crypto-assets, there is a need to constantly assess existing legislation to check if it can be effectively applied to this type of asset or if amendments or guidance are needed. So far, no comprehensive and commonly accepted taxonomy of crypto-assets has been established. As a result, there is still a large number of definitions as to what exactly the term crypto-assets encompasses. Also, various classifications of crypto-assets are sometimes difficult to navigate, which contributes to a high level of fragmentation and complexity between Member States and at international level.

This high level of uncertainty and complexity in a rapidly changing environment presents a series of challenges for the legislator dealing with crypto-asset regulation. As highlighted in this study, three areas are particularly pivotal to the future development of crypto-assets and digital finance in Europe and need specific attention at the current juncture. The first is the definition of a common framework for crypto-assets, the second is cyber-resilience and the third concerns the establishment of a comprehensive data strategy.

Description of key findings

To understand whether and which types of crypto-assets fit into existing regulatory classifications, and to assess if and how these need to be amended, it is crucial to agree on common criteria for the categorisation of each crypto-asset and to establish a European framework for markets in crypto-assets, including stablecoins and cryptocurrencies. Such a framework should ensure legal certainty for innovators and investors, while addressing risks to market integrity, risks of market fragmentation and risks of financial instability. It should also be flexible and open, as it may need to be revisited based on future evolutions. Furthermore, the ongoing digital transformation in the financial sector has prompted an increasing focus on the issues of cyber-resilience and on the need to implement a comprehensive data strategy. In this paper we analyse these issues with a view to identifying possible gaps in EU legislation and to evaluating the European added value (EAV) of policy options to address such gaps.

We estimated the EAV through a sectoral growth accounting model for the financial sector and using various scenarios. The scenario which forms the base for the evaluation of the EAV in the financial sector assumes that further legislative effort at EU level is undertaken so that the policy

options identified in the previous part are fully implemented. Under this scenario, the European Commission would introduce targeted amendments to existing financial services legislation to further detail their applicability to crypto-assets. For crypto-assets that currently fall outside the regulatory perimeter, the European Commission would propose a series of legislative measures for crypto-assets issuers and service providers and a bespoke legislative measure on stablecoin issuers. Under this scenario, a series of legislative proposals would strengthen the digital operational resilience of the EU financial sector entities, including their information and communications technology (ICT) security, by streamlining and upgrading existing rules and introducing requirements. Finally, the EU data strategy would be enhanced to allow for consistent, technology-neutral application of existing EU data legislation. Cooperation at international level would be pursued, deepened and reinforced.

The results from our simulations confirm a more dynamic return to economic growth in the European financial sector under this scenario. Potential added value in the sector would increase by €55 billion compared with the baseline scenario. A more prudent scenario indicates a lower bound estimate for the increase of added value of €27 billion. Finally, beyond quantitative results for the financial sector and with a view to broadening the EAVA, a more systemic qualitative EAVA is also performed. In particular, still considering the scenario described above, we evaluate the impact – in terms of potential direct benefits and in terms of risk reduction – which the adoption of a legislative initiative on a framework for crypto-assets, on cyber+resilience and on a data strategy would bring. The results highlight the broader gains that could be expected from well-designed, comprehensive and well-balanced EU legislative action in these areas.

Table of contents

Table of figures

Table of tables

List of abbreviations and acronyms

AIFMD	Alternative Investment Fund Managers Directive
AML/CFT	Anti-money laundering/Combating the financing of terrorism
BCBS	Basel Committee on Banking Supervision
CBDCs	Central bank digital currencies
CRD	Capital Requirements Directive
CFT	Countering the financing of terrorism
CPMI	Committee for Payments and Market Infrastructures
CROE	Cyber resilience oversight expectation
DLT	Distributed ledger technology
EAV	European added value
eIDAS	Regulation on electronic identification and trust services for electronic transactions
EMD2	Electronic Money Directive
ESAs	European supervisory authorities
ESMA	European securities and market authorities
ICT	Information and communication technologies
KYC	Know your customer
FATF	Financial Action Task Force
Fintech	Financial technology
FSB	Financial Stability Board
FSP	Financial service provider
ICOs	Initial coins offerings
IOSCO	International Organization of Securities Commissions
MiFID II	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
NIS	Network and Information Security Directive
SMEs	Small and medium-sized enterprises
B2B	Business-to-business
B2P	Business-to-peer
P2P	Peer-to-peer
PFMIs	Principles for financial market infrastructure
PSD2	Payment Services Directive
RBA	Risk-based approach
ROFIEG	Expert Group on Regulatory Obstacles to Financial Innovation
TIBER-EU	European framework for threat intelligence-based ethical red-teaming
VA	Virtual asset
VASP	Virtual asset service provider

1. Introduction

Digital finance is playing an increasing role in the provision of financial services in the EU. Rapid progress with digitalisation, data analysis and computing capacities allow for a new range of financial services and transactions, contributing to boosting innovation. This financial innovation enabled by digital financial technology (Fintech), has therefore attracted a lot of attention, as it could offer some potential for economic development and growth. As part of the Fintech ecosystem, **crypto-assets** have recently started to expand rapidly and, according to a study by Fidelity, digital assets are gaining in favourability amongst investors. The study, based upon a comprehensive survey of almost 800 institutional investors across the United States of America (USA) and Europe also showed that 36 % of respondents recognise that they are currently invested in digital assets, with 6 out of 10 believing that digital assets have a place in their investment portfolio.

From the legislator's point of view, to understand whether and which types of crypto-assets fit into existing regulatory criteria, or how these need to be amended, it is important to try categorising them. The notion of crypto-assets is fairly new, as in the past digital currencies and tokens have been – and at times continue to be – referred to as: virtual/digital/cryptocurrency, distributed ledger technology (DLT)/virtual assets, or digital financial assets. The European Banking Authority (EBA) defines crypto-assets as 'a type of private financial asset that depend primarily on cryptography and distributed ledger technology as part of their perceived or inherent value'. More largely, public crypto-assets are also under discussion as a number of national authorities are planning or have started trials on central bank digital currencies (CBDCs). The European Central Bank (ECB) for instance has been conducting studies on the possibilities provided for by CBDCs, the ways in which they could be implemented and their implications for the banking system.

Cryptocurrencies such as Bitcoin – which are often the main source of public attention – are thus just the tip of the iceberg of this digital evolution. Crypto-assets are diversifying extremely rapidly, in line with the structural transformation in technology, preferences and usages amongst investors and consumers. Moreover, the international dimension linked to crypto-assets should also be taken into consideration, as crypto-assets are by nature cross-border in their application and infrastructure. As the ECB points out, this ongoing digitalisation of financial systems and services could have large beneficial impacts, particularly when it comes to efficiency gains, reduction of costs, and breadth of reach and diversification of assets.

On the other side, Fintech also brings about some serious challenges, as for example matters of cyber-resilience. Due to the high interconnectedness of financial systems and the risks of spillovers, traditional financial institutions could increasingly be exposed to cyber risks and threats. This could notably happen through service providers or through the outsourcing of part of the related ICT activities to Fintech and BigTech firms that are still lacking the extensive experience and expertise in risk management that represent one of the strengths of more solid traditional financial institutions.[1] In turn, this could also leave investors, businesses and consumers exposed to substantial risks. The ECB Supervisory Board has placed IT-related deficiencies and cyber-crime as one of the biggest challenges facing banks in the next three years,[2] as the magnitude and pervasiveness of the issue is already quite substantial. In 2018, 61 % of companies listed in a European Member States declared to have been victims of cyber-attacks,[3] while a 2020 analysis estimated that without further legislative progress, the value at risk of direct and indirect cyber-attacks in the financial sector could reach US$140 billion per year before 2025. Moreover,

1 X. Vives, Digital Disruption in Banking, *Annual Review of Financial Economics*, 11:243-72, 2019.
2 ECB, ECB Banking Supervision: Risk assessment for 2020, 2019.
3 M. Demertzis, and G.B. Wolff, Hybrid and cyber security threats and the European Union's financial system, Bruegel Policy Contribution No 10, 2019.

cybersecurity problems are linked to data protection and broader data strategies. With increases in the use of crypto-assets and progress in FinTech technologies, the boundaries in data collection, usage and storage would add an additional layer to debates on data protection, as well as ethical use of data.

These concerns are exacerbated when crypto-assets are not backed by an accountable entity that can be bound by regulation and held responsible for potential breaches of regulation. An important issue when it comes to crypto-assets is thus also being able to clearly determine exactly what they are and which rules, if any, apply to them. Some crypto-assets fall under existing EU law, but most of them do not. This high level of uncertainty and complexity in a rapidly changing environment presents a series of challenges for the legislator dealing with crypto-assets regulation. As highlighted in this study, three areas are particularly pivotal to the future development of crypto-assets and digital finance in Europe and need specific attention at the current juncture. The first is the definition of a **common framework for crypto-assets**, the second is **cyber-resilience** and the third concerns the establishment of a comprehensive **data strategy**.

To shed light on these issues, we start this study by describing the current state of play and the underlying organisation of the crypto-assets market. We recall how DLT is designed, how the crypto-assets market is structured and its current significance in the financial sector. In a second part, we describe the main current regulatory issues in the crypto-assets market. In the third part, we define more precisely the scope and policy context of this assessment. In the fourth part, we further explain why EU action is needed, by identifying the gaps in the existing EU regulatory and legislative framework. In the fifth part, we present the main policy options under discussion to address the existing gaps. Finally, in the last part, we conduct a thorough comparative economic analysis of the EAVA of the policy options identified.

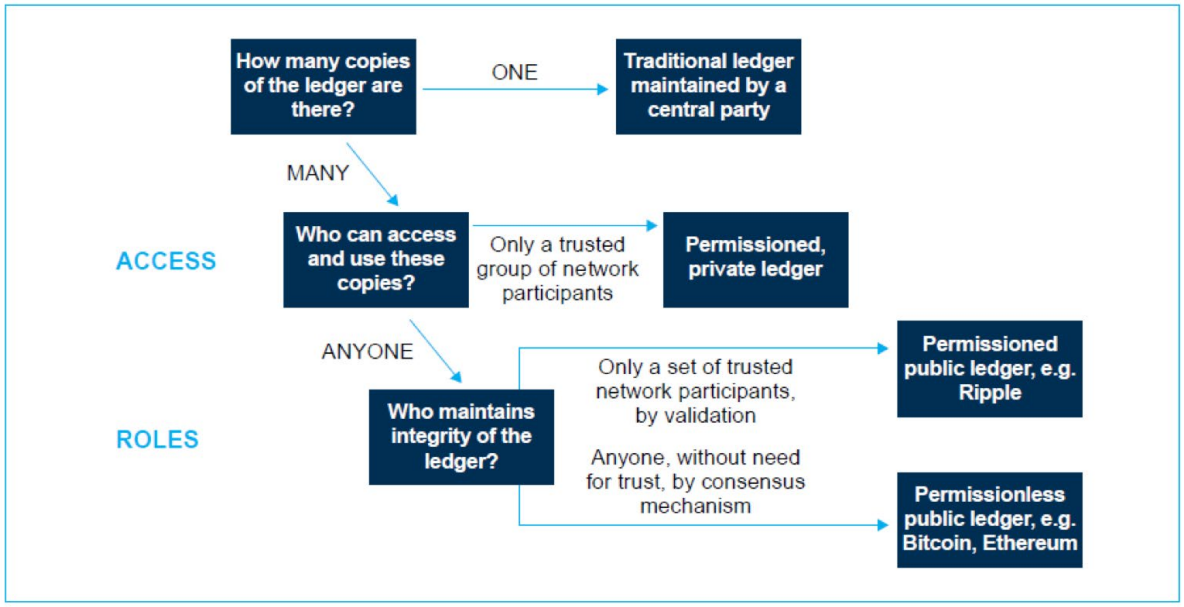
2. Description of digital finance services and market organisation

Ongoing rapid progress in computing capacities, digital technologies and artificial intelligence (AI) have started to significantly transform the traditional provision of financial services. As a result, the development of digital finance is increasing across all areas of the financial sector, notably payments and financial infrastructures, consumer and SME lending, insurance, investment management, and venture financing. The development of crypto-assets currently represents one of the Fintech innovation frontiers with extremely rapid and complex underlying evolutionary processes.

2.1. Understanding the role of DLT in the crypto-assets market

Issuance of crypto-assets and asset tokenisation are direct applications of DLT such as blockchain. The recent emergence of DLT has the potential to structurally transform the functioning of financial markets, as it could facilitate the exchange of value without the need for a central authority or intermediary (e.g. governments or banks). If properly regulated, such disintermediation offers the prospect for large efficiency gains in the financial sector. Distributed ledger (DL) can be open (permissionless) or permissioned (see Figure 1). Bitcoin and Ethereum are the most prominent examples of completely permissionless blockchains, where network participants can join or leave the network at will, without being pre-approved or vetted by any entity. All that is needed to join the network and add transactions to the ledger is a computer with the relevant software. There is no central owner and identical copies of the ledger are distributed to all network participants.

Figure 1 – DL taxonomy



Source: UK Government Office for Science, 2016.

In permissioned DL, members are pre-selected by an owner or an administrator of a ledger, who controls network access and sets the rules of the ledger. This solves a number of concerns governments and regulators have about permissionless distributed ledgers, such as identity verification of network members, whom to license and regulate, and legal ownership of the ledger. On the downside, it also reduces a chief advantage of permissionless blockchains: the ability to function without the need for any single entity to play a coordinating role, which necessarily requires other participants to trust this entity. However, even in permissioned DL, in general there is no administrator for the execution of transactions.

Financial businesses are so far showing more limited interest in open, permissionless blockchains, due to the difficulty of complying with existing regulatory and compliance frameworks. Financial sector concerns mainly relate to the open access and the difficulty of identity verification in permissionless systems. Financial businesses are, however, making significant investment in researching permissioned DL as a technological solution to reduce costs and increase efficiency. Typically, DL offers a number of potential advantages over traditional centralised and other types of shared ledgers, including decentralisation and disintermediation, greater transparency and easier auditability, gains in speed and efficiency due to automation and programmability. That being said, the technology may also pose new risks and challenges. The most commonly cited risks related to DLT concern scalability, interoperability, operational security and cyber security, identity verification, data privacy, transaction disputes, and challenges in developing a legal and regulatory framework for DLT implementation.

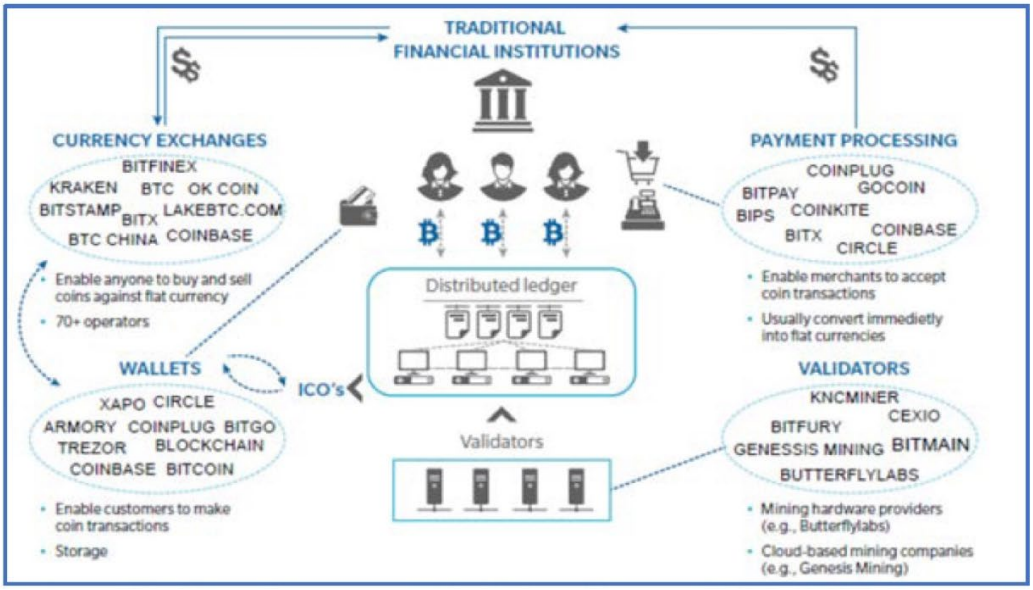
Ultimately, it should be understood that DLT is a technology under constant development and evolution. For instance, while in theory a distinction is made between open and permission DL systems, in practice the situation is one of a continuum with fully open, permissionless blockchains such as Bitcoin at one end of the spectrum and permissioned blockchains hosted by private entities at the other, while precise features vary greatly from platform to platform. This further challenges the harnessing of potential benefits by the financial sector, while increasing potential risks and complicating the establishment of comprehensive and stable taxonomy and legislation.

2.2. Types of crypto-assets, market organisation and actors

In theory, any asset can be tokenised and rights to such assets can be represented on a DL. While a lot of attention is focused around cryptocurrencies and initial coins offerings (ICOs), assets can also take the form of securities (e.g. stocks and bonds), commodities and other non-financial assets. The potential of asset tokenisation is theoretically unlimited. Regarding types of crypto-assets, an interesting distinction proposed by the OECD could be made between **tokenised assets that correspond to assets off-the-chain** and **tokens that are built directly on-chain** and live exclusively on the distributed ledger. In practice, **Bitcoin and other cryptocurrencies** and payment tokens are examples of on-chain tokens.

Off-chain tokens refer to the tokens issued in asset tokenisation that exist on the chain and carry the rights of the assets they represent. They are thus acting as a store of value and the assets backing these tokens that exist off-the-chain need to be placed in custody. This points to an increasingly important role for **custodianship of assets** in tokenisation transactions, as the link between the off-chain (traditional financial market infrastructures) and on-chain environments is crucial for the credibility of this type of market. Recently, the issuance of off-chain tokens backed by fiat currencies (one form of stablecoins), has increased rapidly, with many new stablecoins being issued and growing market capitalisation. Other assets that are being tested in pilots or at concept stage include real estate assets, and commodities such as gold and art. Intangible assets, such as intellectual property, could also be tokenised, spurring new, innovative digital assets and markets.

Figure 2 – Crypto-asset market – simplified description



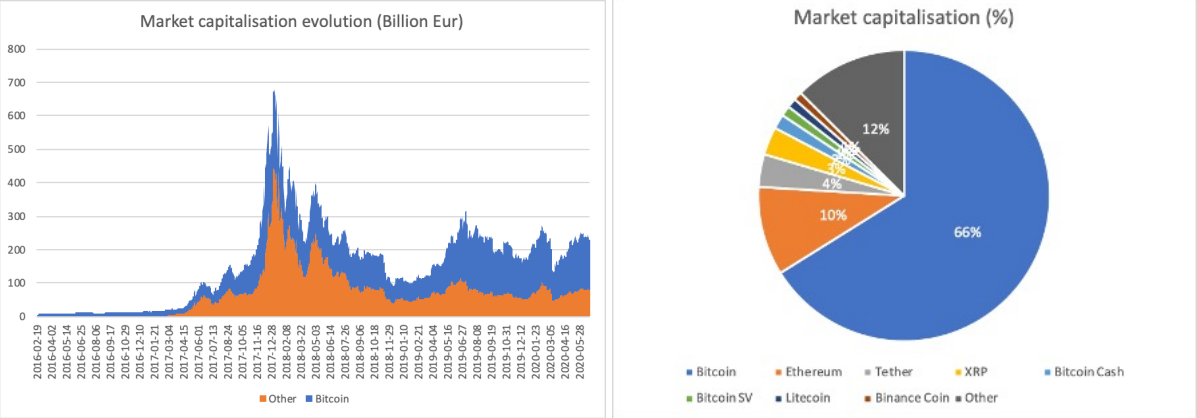
Source: O. Wyman, 2018.

Regarding the functioning and organisation of the crypto-assets market, the Bank for International Settlements (BIS) proposed a general framework for analysing different applications of DLT in the financial sector. This framework (see Figure 2) is organised in a systemic way around the various market components and actors. First, **investors in the crypto-assets market** take part and are involved in transactions. They could be individuals, institutions and businesses. Second, **financial intermediaries** such as brokers provide advice or facilitate the purchase of crypto-assets by investors against remuneration. Third, **system administrators**, such as crypto-assets developers, issuers (this includes those who issue tokens through an ICO) and auditors (allowed to view the ledger but not allowed to make changes). They design or issue crypto-assets, decide who can access the network, maintain and administer dispute resolution rules. As already explained, this role is not required in a permissionless DL. For instance, in the Bitcoin blockchain no entity plays this role, and the system itself creates new Bitcoins based on specific rules. Fourth, what are known as **minors/validator and transaction processors**, who are incentivised by remuneration to verify transactions and add them to the ledger. Fifth, **trading platforms, brokers and exchange** facilitate transactions between participants and ensure a liquid market. Sixth, **payment providers** enable customers to pay service or goods providers using a crypto-asset or transfer currency via a crypto-asset. Seventh, **wallet providers** offer custody services and secure storage of crypto-assets.

2.3. Size, importance and prospects for the crypto-asset market

The development of crypto-assets is linked to the rapid technological development of Fintech in traditional areas of financial services. In 2018, there were around 1 500 cryptocurrencies, today there are more than 5 500. Crypto-assets, especially those like Bitcoin and Ethereum that are not backed by a contractual claim, have experienced significant price volatility over the past year. In January 2018, they reached an estimated total market capitalisation of €700 billion, before falling sharply in subsequent months. Bitcoins represent by far the largest part of this market (see Figure 3).

Figure 3 – Size and evolution of the crypto-assets market

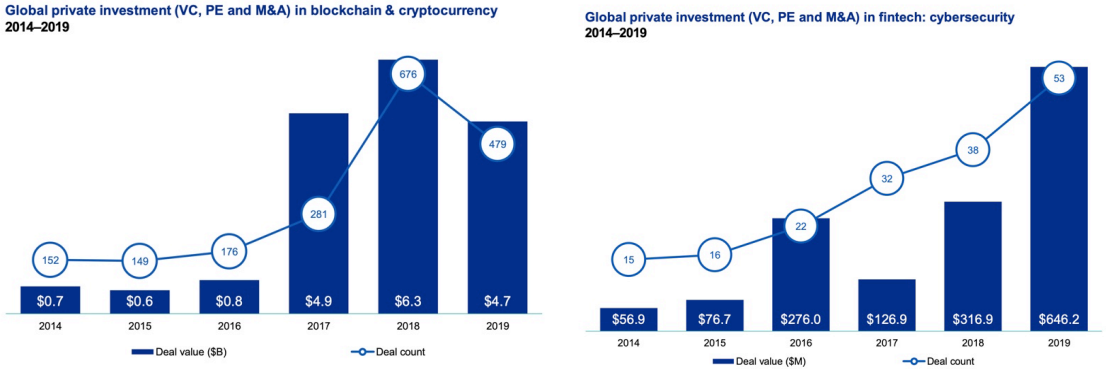


Source: Coinbase, 2020.

The market capitalisation of crypto-assets remains small relative to the global financial system, at around €230 billion as of 1 July 2020, about 0.9 % of the market capitalisation of the S&P Index 500 and 2.8 % of the global value of gold. The impact of the crypto-assets market is therefore still low and crypto-assets are so far not yet widely used for financial transactions. As businesses in this area are just starting to emerge and consolidation still has to take place, the impact at the global level also remains limited, but could rapidly accelerate in the coming years as financial markets are rapidly evolving. In particular, as explained by the World Bank, the emergence of cryptocurrencies and blockchain technologies is part of a broader wave of technologies that facilitate peer-to-peer (P2P) interactions, individualisation of products, and flexibilisation of production methods. For instance, stablecoins could represent a useful tool for cheaper cross-border money transfers and payments. Crypto-assets could also offer an alternative funding source for start-ups as, between January 2017 and January 2019, the capital raised through ICOs and private token sales already amounted to €24 billion globally. In addition, they could be more widely used in the financial services sector to improve efficiency and reduce costs. The growth of crypto-asset trading platforms; the introduction of new financial products (such as crypto-asset funds and trusts and exchange-traded products), and the growing interest from investors, raise questions about the future importance and the implications of crypto-assets for the financial sector, as the diffusion and the adoption of this new organisation of exchange is potentially transformational by nature – and it has just begun.

These prospects might explain the recent surge in the financial sector of investment and acquisitions in Fintech and in blockchain technologies (see Figure 4). As crypto-assets could, with the necessary legislation in place, create a store of value and means of payment without the cost and inefficiency associated with traditional financial institutions, they could give a comparative advantage to innovators. As competition increases in the financial sector, financial firms are strongly incentivised to invest in this area to remain competitive. That being said, and given the current absence of a common regulatory and legislative framework, the market for crypto-assets remains subject to considerable volatility, while cyber resilience and the questions surrounding personal data protection and resulting lower levels of trust, need to be addressed. This might explain the recent concomitant large increase in cyber security investment and acquisitions in the Fintech sector (see Figure 4). From the perspective of the financial sector as a whole, the emergence of DL and the development of crypto-assets have thus the capacity to significantly boost innovation, investment and the productivity of the sector. At the same time, these rapid transformational developments pose a series of challenges for the legislator which, while ensuring an adequate level of regulation, also needs to facilitate innovation and competitiveness. Given the intrinsic global nature of crypto-assets, international cooperation also needs to be enhanced, to avoid regulatory gaps that could be exploited for reprehensible cross-border activities.

Figure 4 – Private investment in cryptocurrencies and cyber security



Source: KPMG, 2019.

3. Analysis of the main current policy issues in the crypto-assets market

As innovation is making further progress and as established positions in the financial sector are challenged, new regulatory questions have emerged and have yet to be resolved. In particular, three areas central to the future development of crypto-assets and digital finance in Europe need specific attention at the current juncture. The first is the definition of a common framework for crypto-assets, the second is cyber resilience and the third concerns the establishment of a comprehensive data strategy.

3.1. Classification of crypto-assets

Crypto-assets have emerged as a direct result of recent digital technological developments, opening vast new possibilities for exchange, investment and financial transactions. In particular, DLT have been introduced in financial services to allow for a more efficient sharing and updating of information. The challenge in crypto-assets regulation is their inherent hybrid and transformative nature. The fast pace at which developments and innovation is happening in this market also complicates regulatory approaches and gives rise to regulatory gaps.[4] It is therefore particularly difficult for a comprehensive classification to emerge.

An approach to considering these issues is to compare crypto-assets against the traditional definition of money, which identifies three functions to be fulfilled – means of payment, unit of account and store of value – to be qualified as such. A recent study for the European Parliament recalls how crypto-assets are not yet broadly accepted as a means of payment for goods and services. They are still not used to price such goods and services, and their current volatility might make it difficult for them to credibly retain value over time. This would seemingly make them fall outside the scope of most existing regulations. Another approach is to rely on a taxonomy of crypto-assets based on the functions they perform, to potentially include them under the umbrella of existing regulation. The European Commission for instance recently proposed three possible classification categories, namely payment/exchange, investment and utility. Further progress on a common and open taxonomy for crypto-assets is however necessary to arrive at a comprehensive framework.

3.2. Cyber-resilience

As DLT platforms rely upon the use of digital services and information and communication technologies (ICT) infrastructures, they can naturally be subject to cyber-attacks, fraudulent cyber activities and to technical failures. Moreover, in a traditional centralised system, institutions such as banks maintain records (ledgers) of transactions and positions. They also play the role of intermediary and are the guarantor of the validity of information linked to transactions and positions. However, DLT is organised differently, as it relies upon a database shared and synchronised across network of participants (nodes). Transaction records are thus visible to everyone and kept in a decentralised way by all participants, and P2P transactions can take place without intermediaries and are verified by so-called minors/validators for irregularities. As much as this innovation opens room for large potential economic benefits, it also entails some cyber risks, which have to be integrated. In particular, the design of a strategy for operational cyber resilience is under consideration to allow for the emergence of a beneficial regulatory framework. This concept of cyber resilience is at times used interchangeably with other cyber jargon, such as cyber security, cyber defence and cyber deterrence as again, the lines differentiating these concepts are not clear-cut, as they at times interact and overlap. For example, the International Monetary Fund (IMF)

[4] FSB, Crypto-assets: Work underway, regulatory approaches and potential gaps, May 2019.

definition of cyber-resilience includes aspects of cyber-deterrence, as in order to protect electronic data one ideally needs a robust IT system. Consequently, this brings cybersecurity into the picture, as the robustness of crypto-asset IT systems and technologies has to be guaranteed.

In this study, we therefore use the term cyber-resilience to refer to the ability to protect electronic data and systems from cyber-attacks, as well as to resume business operations quickly in case of a successful attack.[5] Following an EPRS glossary of cyber terms, cyber-defence is used in a broad way to encompass the range of strategies used to safeguard institutions, governments and individual citizens from IT-related risks and threats. Cybersecurity on the other hand relates to the technology, IT platforms and ICT security specific for digital assets. This last, cyber-deterrence, encompasses measures for dissuading potential perpetrators, through robust systems, sanctions mechanisms and cyber diplomacy. Beyond the sole focus on definition, as Fintech is growing, there is no doubt that cyber-resilience is going to become a crucial element. The occurrence of cyber incidents is indeed likely to increase if a constantly up-to-date regulatory reporting and resolving framework is not ensured. According to the European Parliament, the financial sector is already three times more at risk of being the target of cyber-attacks than any other sector, costing several billion euros to the EU economy each year. To allow for a secure and resilient digital environment that contributes to the development of crypto-assets, there is therefore a need for legislative improvements in this area.

3.3. Data sharing and related rights

One important issue with crypto-assets is that the blockchain technology allows use of DLT for generating and keeping records without the need for a central regulator to administer the system. As such, DLT platforms allow for direct data collection and distribution amongst participants. This raises some profound issues regarding rights of access and privacy. In addition, as crypto-assets are traded P2P globally, this also raises the question of the recording of these transactions and of the jurisdiction ultimately responsible for the accounting of the exchange and positions. International cooperation will be required to ensure that the countries in which providers are located collect information on the country of residency of the counterparts in transactions (from exchanges) and on positions in different types of crypto-assets (from wallet providers) while respecting data legislation regimes. Further progress in this area is therefore necessary to increase trust in crypto-assets and to guarantee an appropriate level of data protection and regulation that allows for EU innovators to grow and develop while also protecting investors and consumers rights.

Moreover, access to data is crucial for the development of digital finance in Europe, as most financial services now rely heavily on advanced digital technologies and large amounts of data. The use of big data analytics can help tailor the financial products to the consumer, as they provide behavioural insights and allow for the identification of patterns that might otherwise be overlooked. This in turn can also improve the provision of financial advice, which can be tailored to fit investor and consumer needs. Data analytics through AI and the development of algorithms, could optimise trade and investment through the recognition of patterns at both ends. As such, it could prove useful to further develop investment strategies based on the characteristics of the products and of the investors. In the same way, data collection can diminish risks related to lending, allowing for instance for a more precise computation of SMEs repayment capabilities. Digital platforms can also help investors and consumers in their individual planning, providing clear, precise and accessible information, as well as enabling broader comparisons among different financial products on the market. On the other hand, this raises questions regarding shared access to data, privacy, identification issues and, more widely, alignment with the requirements of the General Data Protection Regulation (GDPR).

[5] ECB, What is cyber resilience?, 2020.

4. Scope and policy context of this assessment

There are considerable barriers to the application of rules in the digital financial market, due to difficulties in determining territorial competence, and to the absence of practical means of monitoring activity, enforcing regulatory provisions and establishing accountability. Despite this complexity and the uncertainty surrounding the development of crypto-assets, the legislator has already started to look at the issue and some proposals are currently being debated. Moreover, a number of international organisations and regulatory authorities have issued guidance on the criteria to be followed for a beneficial regulation of digital finance and of crypto-assets. In this part, we therefore give a more precise description of the scope of the present EAVA regarding the definition of crypto-assets. We then describe the current general EU and international policy context in which this assessment is taking place.

4.1. Crypto-assets under consideration in this assessment

As we have seen, a wide range of crypto-assets exist, encompassing different features and functions, thereby presenting different challenges and risks. The lines are also blurred as there are a number of hybrid crypto-assets as well as overlaps in the defining features of these categories. In this paper, we consider crypto-assets as economic assets because the institutional units holding them can be identified and because they derive economic benefits to the holder in terms of holding gains/losses and other benefits. Moreover, they have monetary value and their price is determined by the market in which they trade. Regarding the scope of the term crypto-assets, we follow the definition of crypto-assets given by the European Commission.

Crypto-assets are therefore defined as a type of digital asset that

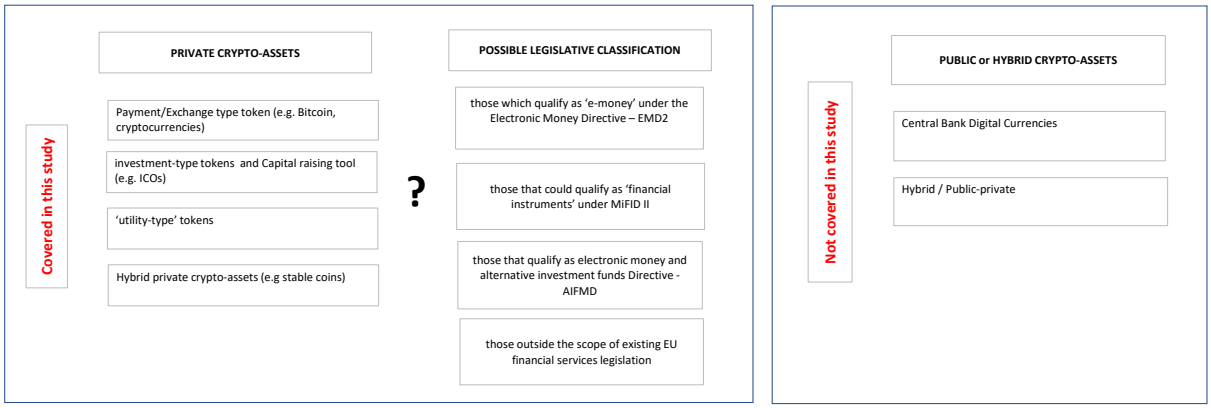
- depend primarily on cryptography and DLT

- and are private by nature.

Based upon this definition, we distinguish between three main categories of crypto-assets. First, there are payment/exchange-type tokens, as for example the 'virtual un-backed' currencies like Bitcoin. A second category is ICOs, which are increasingly used by start-ups and by investors to collect funding. Third, other investment-type tokens give right to ownership rights and/or entitlements similar to dividends, and for example can take the form of security tokens. Fourth, utility-type tokens grant access to a good or service, which is normally provided by the issuer of the crypto-asset itself. Lastly, there are hybrid private crypto-assets, such as some virtual backed cryptocurrencies like stablecoins.

According to the 2019 EBA report on crypto-assets, crypto-assets used as means of payment could qualify – in limited instances – as electronic money. Such a characterisation would put these cryptocurrencies under the scope of both the Electronic Money Directive (EMD2) and the Payment Services Directive (PSD2). Investment, utility tokens and ICOs pose a more complicated picture. Where crypto-assets qualify as financial instruments, they would fall under the scope of the Markets in Financial Instruments Directive (MiFID II/MiFIR) and the Prospectus Regulation. Some could fall under the Alternative Investment Fund Managers Directive (AIFMD), while hybrid crypto-assets such as most stablecoins would fall outside the scope of the existing EU financial services legislation.

Figure 5 – Categories and uses of crypto-assets



Source: EPRS.

4.2. Progress made in the current EU legislative context

At EU level, the European Commission published its Fintech action plan in 2018. Following up on the application of the action plan, European Supervisory Authorities (ESAs) assessed the suitability and the applicability of existing EU legislation to crypto-assets and they released joint advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector. They also released advice on the costs and benefits of developing a coherent cyber resilience testing framework. Following suite, the EBA issued guidelines on ICT and security risk management and on outsourcing and cyber resilience in the financial sector. Besides specifying the application of existing regulation to ensure the operational resilience of financial markets infrastructure against security risks, these recommendations set out supervisory expectations and management requirements around them. Moreover, in relation with the European System of Central Banks, the ECB developed TIBER-EU, a testing framework to assess the risk of cyber security threats in order to improve resilience of financial markets. The ECB also established a **crypto-assets task force** in 2018 and has published a series of recommendations on this issue.

Regarding data protection aspects of digital finance, the European Union has been a pioneer with the adoption of the GDPR, which entered into force in 2018. One of its main purposes is to ensure transparency in the collection, use and processing of individual data. The driving principle of the GDPR is that data legal ownership lies with the consumer, putting citizens in charge by requiring consent to be given to the processing of their data. Another GDPR guiding principle is that of purpose limitation, which is also enshrined in the PSD2 with reference to third-party payment providers.[6] Regarding digital identities more particularly, the 2016 Regulation on electronic identification and trust services for electronic transactions (eIDAS) gives citizens control over when and to what extend they share identity data when using cross-border digital services. The regulation also constrains the collection of such data beyond what is strictly needed for a transaction.

Building on all these insights, in line with European Commission President von der Leyen's new agenda and with the view of promoting digital finance in Europe, while adequately regulating its risks, the Commission continued to work towards a new digital finance strategy for the EU. The Commission is considering amending existing rules on resilience, particularly in the Network and Information Security Directive (NIS),[7] by developing digital operational resilience for financial services. This would aim at further mitigating the risks posed by crypto-assets such as potential fraud, cyber-attacks, market manipulation and data related issues. The Commission has also started

6 EBA, Report on innovative uses of consumer data by financial institutions, 2017.

7 The Network and Information Security Directive (NIS) provides general requirements for the security of network and information systems across sectors, including for some operators in the financial sector.

to investigate the emergence of crypto-assets and the effect that new technologies will have on how financial assets are issued, exchanged, shared and accessed in greater depth. The main purpose of this initiative is to assess:

- how far crypto-assets are covered by current EU legislation,
- whether new legislation is needed in this field,
- whether issuing guidelines would be sufficient.

In **December 2019**, the Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), published its recommendations on how to create an accommodative framework for technology-enabled provision of financial services. The group issued 30 recommendations related to the innovative use of technology in finance, maintaining a level playing field, access to data, the financial inclusion and ethical use of data. In the **same month,** the European Commission issued a roadmap towards a proposal for a directive/regulation establishing a European framework for markets in crypto-assets, with an accompanying inception impact assessment. At the same time, the Commission also published a roadmap towards a proposal for a regulation on digital operational resilience for the financial sectors, with an accompanying inception impact assessment.

A **public consultation ended in March 2020**. A complete proposal for the regulatory package on digital finance is planned for the third quarter of 2020. It will include an **updated 2020 action plan** aimed at setting out more precisely what the Commission intends to propose to promote digital finance while addressing and balancing risks and responsibilities. Taking the results from the public consultations on board, it will also detail the proposal for crypto-assets regulation and the proposal for operational resilience regulation.

4.3. Importance of cooperation at international level

As crypto-assets are by nature global, their efficient supervision requires effective cross-border cooperation, coordination and information sharing amongst the relevant authorities. As highlighted by the Financial Stability Board (FSB) in its 2019 report to the G20 Finance Ministers and Central Bank Governors, many complementary initiatives are underway at international level on regulatory and supervisory approaches to crypto-assets. Work at the Basel Committee on Banking Supervision (BCBS), Committee for Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), the Financial Action Task Force (FATF), the Organisation for Economic Co-operation and Development (OECD) and the Financial Stability Board (FSB) covers important aspects of crypto-assets risks. It notably focuses on investor protection, market integrity, anti-money laundering, bank exposures and financial stability monitoring.

Underlying all these regulatory efforts, the IMF has set out a list of principles that should underline the development of regulatory frameworks. Crucial importance is given to the need to be **commensurate to the risks without stifling innovation**.[8] Moreover, due to the rapidly evolving nature of the crypto-assets landscape, the IMF emphasised that a **flexible approach is key**. The decentralised nature of this sector seems to require a focus on market participants. Particular consideration should also be paid to the linkages between and integration of digital markets with the overall financial system and the real economy. In particular, regulators should pay attention to the role of intermediaries, as their conduct could have direct implications for the protection of investors and consumers and the stability of the payments system.

In 2019, the Financial Action Task Force (FATF) issued guidelines on understanding money laundering and terrorism financing risks associated with crypto-assets and the anti-money laundering/combating the financing of terrorism (AML/CTF) obligations for virtual asset service providers (VASPs). The FATF has underlined how the scope of most of its previous recommendations

[8] International Monetary Fund, Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note SDN/16/03, 2016.

concerning financial institutions could cover and is applicable to VASPs and to actors in the crypto-assets market, potentially subjecting them to the same obligations. More recently, the FSB released recommendations on regulatory, supervisory and oversight for 'global stablecoin' arrangements. This follows up on a series of reports on Fintech and on the crypto-assets market in 2019.[9]

Finally, with regard to cyber-resilience, the European Union has adopted two international standards and guidance: the CPMI-IOSCO principles for financial market infrastructure (PFMIs) and the CPMI-IOSCO guidance on cyber resilience for financial markets infrastructures. The PFMIs recognise operational risk, including cyber risk, as a specific key risk faced by FMIs and thus affirm the need for financial market infrastructures (FMIs) to have an overarching risk management framework.[10] The cyber-resilience guidance of 2016 builds on the principles for FMIs (PFMIs) and is more specifically tailored, as it outlines the primary risk-management categories and components that are needed in a comprehensive FMI cyber-resilience framework. The Systematic Important Payment System Regulation is the ECB regulatory framework for the implementation of the CPMI-IOSCO Principles for FMI. Among other things, structured investment products (SIPS) operators are required to have an effective cyber-resilience framework with appropriate governance measures in place to manage cyber risk.[11] The ECB increasingly recognises the need for international cooperation in this area and the additional operational risks that are generated by the increase vulnerability of financial systems to international cyber risks. In 2018, it adopted the cyber-resilience oversight expectation (CROE), based on the global guidance on cyber resilience for financial market infrastructures. The CROE outlines expectations on governance, identification and detection of cyber risks, protection, testing and putting procedures in place for response and recovery. The pursuit and the deepening of this international cooperation will be key to a development of crypto-assets that allows for innovation to thrive and for benefits to materialise while ensuring the necessary level of supervision of risks.

9 FSB, Crypto-assets: Report to the G20 on the work of the FSB and standard-setting bodies; BigTech in finance market developments and potential financial stability implications;

10 BIS-CPMI and IOSCO, Principles for financial market infrastructures, CPMI Papers No 101, 2012.

11 ECB, Revised assessment methodology for payment systems, 2018.

5. Identification of gaps in the existing EU regulatory and legal framework

At Member State level, authorities have generally already taken various types of action to address the issues associated with the development of crypto-assets. In some cases, differences in regulation between jurisdictions reflect local market developments and underlying legal and regulatory frameworks for the respective financial systems. Moreover, gaps may arise when some assets fall outside the perimeter of market regulators and payment system oversight. To some extent, this may reflect the hybrid nature of some crypto-assets. Gaps may also arise from the absence of standards or recommendations. Assessing the significance of these potential gaps will remain challenging, given the rapidly evolving nature of the crypto-assets ecosystem.

5.1. A framework for crypto-assets

As a result of the lack of taxonomy and of new and rapidly evolving technologies in the financial sector, there is **no legal certainty** in the treatment of crypto-assets in EU financial regulation, nor is it clear if and how the existing EU financial services regulatory framework applies to some crypto-assets. To respond to this challenge, and building upon the advice on crypto-assets provided by the ESAs, three regulatory situations and thus three possible levels of response can be differentiated.

First, for crypto-assets which fall within the scope of existing EU financial services legislation, and in particular, those that could qualify as financial instruments under MiFID II and those which qualify as e-money under EMD2, the objective is to make sure that the rules are fit for purpose and can be applied effectively. As highlighted in the Commission inception impact assessment, the challenge with crypto-assets is that the interpretation and the application of existing requirements in the current legislation may vary from one Member State jurisdiction to another. This can lead to fragmentation in the treatment of crypto-assets, to a reduction in transaction levels and to additional transaction costs for investors. The lack of common technological standards regarding DLT might also further complicate the applicability of legislation.

Second, for crypto-assets outside the scope of existing EU financial services legislation (e.g. some utility tokens and some payment tokens), the objective is to determine whether an EU regulatory approach is needed. The absence of common rules introduces a high level of risk for investors while significantly reducing the potential for development of new classes of assets in which EU consumers and businesses can invest. The potential asymmetry of information created by the lack of clarity and by the complexity of the technology might also increase the risk of fraud and therefore reduce confidence and investment. This, in turn, leads to low liquidity levels that further exacerbate price volatility and potential for market control by some actors. If no common framework is introduced, there is also the risk of multi-speed and diverging legislative action at Member State level, thus further complicating the regulatory environment.

Third, while some **stablecoins** could theoretically qualify as electronic money and fall under the Alternative Investment Funds Directive (AIFMD), it appears in reality that by design, the vast majority would fall outside existing EU legislation. The objective here is to determine whether an EU regulatory approach is needed. This is particularly relevant as some Member States are considering bespoke rules. This is likely to lead to substantial regulatory fragmentation, which may distort competition in the single market and give rise to regulatory arbitrage. As underlined in a recent G7 report on stablecoins, while the stablecoin market remains modest in size and does not currently pose a threat to financial stability, this type of stabilised crypto-asset would likely raise additional challenges in terms of financial stability, monetary policy transmission and monetary sovereignty if they reach a global scale. Due to their capacity to be an alternative to fiat currency and based on their take up in the market, it therefore appears urgent to anticipate and to prevent upcoming challenges in this area.

5.2. Operational cyber-resilience

Crypto-assets, especially those that are decentralised and operate with limited or no formal governance structure, present **particular technological and operational risks**. As already highlighted, the particular application of DLT that underlies most crypto-assets is relatively nascent, and may be subject to technological errors and limitations. As these technological limitations and network governance issues arise, crypto-asset trading platforms can be, and in some cases have been, vulnerable to fraud, hacking, and other cyber incidents. A number of trading platforms with poor security have also collapsed after cyber incidents, causing real losses for investors. Some steps have been taken in setting up a European supervisory and reporting mechanism, but significant regulatory gaps remain at European levels.[12]

To begin with, the financial markets are much more integrated compared to the security strategies, which remain mainly in the hand of individual Member States. Moreover, most of the framework is based on non-binding guidance. As a result, heterogeneity between Member State legal systems and practices remains, as well as disparity in ICT security among operational resilience requirements across the EU financial services legislation. The issue is also significant when looking at market actors, in particular with regard to the **lack of coherent oversight over the activities of third-party providers to financial sector entities**. For instance, returns to scale in mining can lead to the creation of concentrated mining pools that have substantial control over a crypto-asset. In other cases, there may be concentrated governance structures around network nodes or software standards. Decentralisation and lack of or inadequate governance makes it difficult to resolve technological limitations or errors and may lead to uncertainty. The cross-border nature of the policy problem at hand magnifies the detrimental impact of this lack of harmonisation.

Cyber-attacks also have the potential to cause acute disruptions to financial systems and to render some risk management and business continuity arrangements ineffective. As pointed out by the IMF, attacks on payment systems could entail losses for consumers, cyber incidents could also cause the failure of the whole infrastructure – causing service interruptions and compromising the integrity of the system – or they could lead to a loss of confidence. The **absence of requirements or a multiplication of obligations** on the reporting of the same incident to different authorities makes it difficult to ensure resilience in a rapidly evolving environment. As the European Commission highlights, this results in an incomplete supervisory overview of security incidents, inconsistent reporting requirements and reduces capability to assess and monitor risks.

Finally, as with crypto-assets, the cyber threat landscape is highly dynamic and actors constantly change and evolve, requiring an agile and flexible supervision. The **incoherence of digital operational resilience testing frameworks at Member State level**, with differences in terms of scope, testing modalities and requirements or authorities involved, does not favour the emergence of such flexibility. Such mismatch even contributes to the fragmentation of the regulatory approach, to additional costs and leaves European financial markets more vulnerable to cyber threats. As the European Commission states in its inception impact assessment, the lack of a common approach in this area could even potentially lead to a segmentation of the single market and in turn undermine the EU single supervisory approach.

5.3. Data strategy

Fintech ability to leverage customer data through AI raises the question of how financial authorities should approach data rights, particularly in the wider context of data protection regulations. This relates to the question of how authorities should consider the potential to promote the sharing of data between the various actors that are involved in the provision of financial services. Doing so may

[12] Currently reporting requirements are set out in NIS, PSD2 and eIDAS.

help encourage competition and help ensure a level playing field amongst market participants. **Equitable access to data for Fintech entrepreneurs** should thus be ensured to allow for a healthy level of competition and innovation. Regulatory obligations for financial businesses to share relevant data with new entrants may however also pose new risks that need to be addressed. For the European Parliament, DLT introduces new challenges for operators and regulators regarding the use, sharing, storage and rights of access to data. The processing and the analysis of individual data through big data analytical techniques, weak authentication procedure, or the lack of transparent and clear terms and conditions, are all potential sources of concern, in particular as regards the respect of existing data legislation.

Regarding the effective **enforcement of the GDPR**, in practice, the GDPR is the EU data ownership framework that defines who retains control over the data, their use and their dissemination. Data storage should also be taken into account, particularly when it is stored through cloud computing services – which are often outsourced. Here, the risks once again mostly relate to cyber security and the possibility of breaches, which, as mentioned, calls for operational cyber resilience to be reinforced. In addition, there is a need for more specific guidance on the application of GDPR to the financial sector and with regards to the ethical use of data – particularly big data.

Regarding data usage, one concern entails matters of **oversight of big data analytics**. As the OECD points out, big data and AI applications could lead to consumer profiling, thereby enabling price discrimination and creating new impediments in accessing finance. Granular profiling could spur financial exclusion and inequalities in financial systems, as well as give rise to increasing price discrimination, particularly in insurance markets. Ethical use of data is to be ensured, and one option suggested by the IMF could be through data regulatory framework emphasising purpose specification as a guiding principle in their establishment.

Another concern is the lack of **harmonised process for digital identities**. The European Commission states that secure electronic identification (eIDs) would enable fast and cross-border identification that could benefit consumers, investors, businesses and authorities alike. They would contribute to enhancing a culture of trust among actors in the digital financial world, and more broadly within the European digital single market. Currently, 13 Member States have announced national e-identity schemes. Within digital finance, the adoption of eIDs has been linked to increased financial inclusion, lower costs and faster transactions, as well as reductions in fraudulent activities. The development of digital identities could also help mitigate the use of digital financial instruments for money laundering as well as improve FMIs and financial market actors' compliance with know your customer (KYC) requirements.

Finally, financial authorities could benefit from close engagement with other regulatory agencies, such as competition authorities and those involved with data protection, to ensure the establishment of **more transparent and enhanced reporting on digital finance**. This is particularly relevant as one shortcoming of data related regulation is the lack of sector-wide perspective. While FMIs – particularly banks – may be covered by most of the existing regulation, other actors in the market fall outside its scope, even though they provide the same services and are faced with the same risks. Moreover, the GDPR framework still presents a number of weaknesses, mostly stemming from uneven implementation across Member States. For example, there is considerable variation in national requirements concerning the disclosure of information, which for financial services, could have consequences on the ability to properly implement AML/CTF legal requirements.

6. Policy options to address the existing gaps

The previous sections outlined a number of regulatory gaps and challenges that the EU must overcome to benefit from new digital and technological advances and to boost innovation, investment and competition in EU financial markets. In this section, based upon an existing analysis of the most relevant literature,[13] we describe the main policy options currently under consideration and that aim at addressing the existing gaps and mitigating risks while avoiding excessive administrative burden.

6.1. Policy options under consideration on a framework for markets in crypto-assets

As explained in the previous section, it is crucial that the application of existing regulations is clarified, and that they are amended accordingly to encompass the hybrid and varied nature of crypto-assets. Crucially, early action in this sense would prevent further fragmentation, thus fostering integration in EU financial markets, and strengthening their resilience while addressing emerging and potential risks inherent to crypto-assets.

For that purpose, for crypto-assets which fall within the scope of existing EU financial services legislation, we envisage the possibility of **targeted amendments to existing financial services legislation**, so that their applicability to crypto-assets is further and better described. This would take the form of further guidance from the European Commission and of targeted amendments to related sectoral legislation. These should cover the issuance of crypto-assets and ensure that specific risks stemming from the use of DLT applications are effectively addressed while covering the development of crypto-asset related infrastructure.

For crypto-assets that currently fall outside the regulatory perimeter, a series of **legislative measures is envisaged for crypto-asset issuers and service providers** (such as trading platforms and exchanges, wallet providers) to increase investor protection, to foster market integrity and to reduce fragmentation within the single market. First, this would build around increasing the level of requirements on issuers so as to ensure a comprehensive disclosure on the key information concerning the crypto-assets under consideration. Second, requirement for service providers would also have to be upgraded to improve governance and ensure a higher level of compliance with rules, surveillance and enforcement mechanisms. Third, investors and consumer protection legislative measures would be introduced to reduce asymmetry of information and to prevent market abuse. Fourth, to ensure the effective supervision of crypto-asset issuances and the services related to crypto-assets, we also envisage the option of introducing a licencing procedure for the service providers.

Regarding the specific case of stablecoins, following a risk-based approach, we envisage the development of **bespoke legislative measures on stablecoin issuers**. Such an option would address vulnerabilities to financial stability, while supporting innovation. It could build on the extensive work already under way on this issue at international level.

6.2. Policy options under consideration on cyber resilience

The overall objective here is to strengthen the digital operational resilience of the EU financial sector, including ICT security, by streamlining and upgrading existing rules and introducing

[13] See, for instance, in references: European Commission, December 2019; ESMA, January and April 2019; ESAs April 2019; EBA April 2019; FSB, May and June 2019; BIS, 2020; CEPS, 2018; OECD, 2020.

requirements where gaps exist, duly taking recommendations endorsed at international level into account, as well as existing EU frameworks on ICT and security risk management.

First, we envisage an **EU-wide classification of cyber incidents**, to ensure convergence among Member State legislation and to provide a coherent categorisation of cross-border attacks. As was the case with crypto-assets, the fast-changing nature of cyber threats calls for a flexible and frequently updated taxonomy. There could also be more **harmonisation in incident reporting**, which at the moment remains scattered and varies according to the legislation applicable to individual cases. A coherent reporting framework would also enhance the broader understanding of the cyber threat landscape and foster the development of reliable analyses of cyber trends, and thus the development of effective deterrence.

This would need to be supported through cross-border cooperation and EU-wide information sharing among Member States. In order to make such cooperation systemic, it is important that EU institutions set out rules about which information and data is to be shared, and the modalities of such exchanges. These would ideally be needed not only for Member States, but also for supervisory authorities, financial firms and consumers, through the creation of **centralised data hubs for incident reporting.** These policy options could be complemented by **direct oversight of critical ICT tools** and by regular **EU-wide stress testing of ICT tools** and preparedness exercises that would help identify weakness to be addressed within European financial markets. Finally, European efforts should be coordinated with broader international regulatory exercises, to further enhance the sharing of best practices and lessons learned.

6.3. Policy options under consideration on data strategy

In addition to the introduction of a framework for regulation of crypto-assets and of a higher level of cyber resilience, a comprehensive digital finance policy should address the risks linked to some remaining gaps in the current EU data strategy. In particular, as the provision of Fintech financial services is highly dependent on data, the following policy options are envisaged to arrive at a comprehensive data strategy that reconciles the possibility to diffuse and provide access to data for innovators while ensuring respect of the rules on data protection.

Further **guidance on the application of GDPR** in relation to the innovative use of technology in financial services could be provided. In particular, in the context of storing personal data on blockchains, it is unclear how compliance with requirements to delete personal data can be achieved. Similarly, the terms of data subjects' consent for the use of their personal data for the purpose of AI experimentation and analysis should be clarified. Finally, the fact that personal and non-personal data are often difficult to separate should be addressed.

Regarding data sharing, rules could be introduced to ensure equitable access to data. These rules should support user control and data-driven innovation by ensuring that sharing is easy, secure and effective, for example by mandating the use of **standardised sharing interfaces**. Potentially significant added value could be provided to users if their non-financial data were accessible to other firms, subject to their consent. In particular, this could enhance competition in the financial sector by levelling the playing field between different types of market participant via access to data.

Turning to the need for oversight of big data analytics and the potential negative social repercussions, the relevant EU authorities could develop **comprehensive guidance to assist financial institutions in the ethical use of** data in the context of the provision of financial services. In addition to transparent and fair use of data, this guidance should also address the issues of financial exclusion and the opacity of some models used by big data analytics. Regarding the setting up of eIDs, the **establishment of a harmonised process for digital identities** should be pursued. In view of the potential of these solutions to generate efficiencies in the digital identification process, relevant EU authorities should investigate the different models with a view to bringing forward a legislative strategy for the acceptance of common digital identity solutions in the EU.

Finally, regarding a more transparent framework and the provision of accessible data and information on Fintech, the regular **regulatory dialogue between institutions should be broadened**, with a view to keeping the practical application of relevant EU legislation concerning the processing of data (in particular GDPR and PSD2) under review, constantly taking account of technological developments within and beyond the financial sector. The objectives of this broadened dialogue should be to enhance knowledge-sharing about new technologies, share experiences, promote a common approach and provide rapid clarification on relevant EU legislation concerning the processing of data in a form that is publicly accessible.

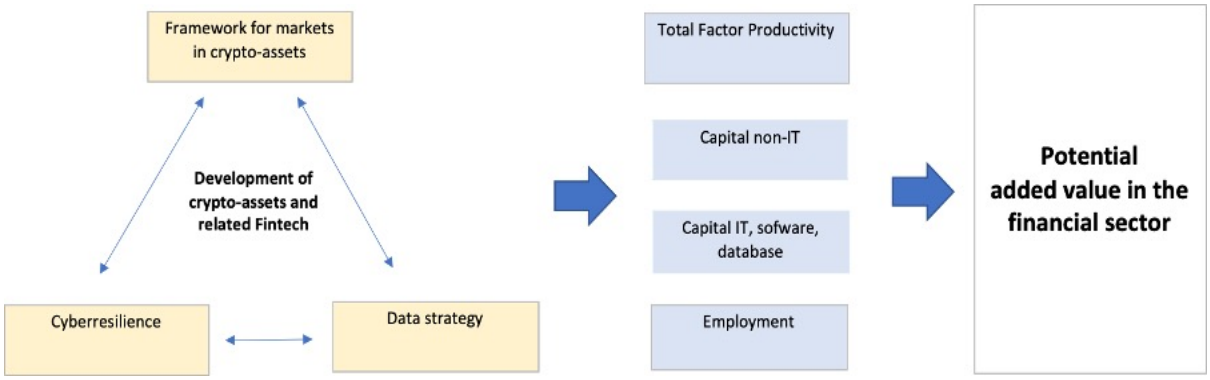
7. Comparative economic analysis of the EAV of policy options identified

In this part, we start by describing the conceptual framework and the scenarios underpinning the evaluation of the benefits in terms of added value in the financial sector of implementing the policy options previously described. We then detail the accounting model used and the main assumptions underpinning the simulations. We follow by presenting the results of the economic quantitative evaluation of the EAV in the area of digital finance. Finally, we broaden the scope by conducting a systemic qualitative EAV assessment of potential benefits and risk for the European economy as a whole, while also discussing the results.

7.1. Conceptual framework and scenarios

Recent analysis by the OECD has highlighted the potential risks and benefits associated with the development of crypto-assets. In particular, the OECD emphasises that technology driven innovation in the financial sector is favouring the emergence of new business models, applications, processes and products that have the potential to boost investment and productivity in the sector. This in turn would lead to more innovation and transformative development for the European economy. In particular, this could have a substantial impact on the organisation of financial markets, on the capital markets Union and on how financial services are provided both at EU and international level. Building on these insights, we assume in this study that the adoption of a comprehensive regulatory framework that allows for the development of crypto-assets while mitigating the associated risks could generate more digital finance activity, allocative, productive and dynamic efficiency gains and a reduction of negative externalities. In turn, this would support innovation, investment and productivity in the financial sector and thus boost added value creation while improving potential growth prospects (see Figure 6).

Figure 6 – The analytical model



Source: EPRS.

Regarding the strategy for the computation of this potential added value, we rely upon modelling built around two scenarios. Each scenario corresponds to a series of options for a framework for crypto-assets, cyber resilience and data privacy.

Baseline scenario

The baseline scenario serves as a reference to evaluate the potential economic impact of alternative policy options. It **assumes that no further significant legislative effort is undertaken at EU level**. Under this scenario, the European Commission would continue to monitor and maintain regular dialogue with the ESAs, the national competent authorities and Member States, as well as with crypto-asset service providers, to promote the sharing of best practice and continuous review of

national legislative developments. An increasing number of Member States could implement bespoke regimes for crypto-assets that do not qualify as financial instruments. The ICT and security risks under operational resilience rules for financial services would continue to be set by current disparate provisions in the EU financial services legislation and partly by the NIS Directive. Finally, remaining gaps in the EU data strategy would remain unaddressed or partially addressed at Member State level, thereby preventing a fully mutually beneficial development of innovation in this area. Cooperation at international level would be pursued.

Alternative scenario

This scenario forms the base for the evaluation of the EAVA in the financial sector. It **assumes that further legislative effort at EU level is undertaken** so that the policy options identified in the previous part are fully implemented. Under this scenario, the European Commission would introduce targeted amendments to existing financial services legislation to further detail their applicability to crypto-assets. For crypto-assets that currently fall outside the regulatory perimeter, the European Commission would propose a series of legislative measures for crypto-asset issuers and service providers and a bespoke legislative measure on stablecoin issuers. Under this scenario, a series of legislative proposals would strengthen the digital operational resilience of the EU financial sector entities, including their ICT security, by streamlining and upgrading existing rules and introducing requirements. Finally, the EU data strategy would be enhanced to allow for consistent, technology-neutral application of existing EU data legislation. Cooperation at international level would be pursued, deepened and reinforced.

7.2. Description of the accounting model and of the main assumptions

Regarding the economic methodology for the evaluation, we use a sectoral growth accounting model for the financial sector for the EU as a whole. This type of model is designed to evaluate the economic impact of policies and institutions on potential added value in the sector under consideration.[14] In terms of impact variable, we consider potential added value as this allows the structural impact of policies to be brought to light. This approach has also several advantages from the perspective of the EAVA analysis. It is based on a rather uncontroversial and commonly used description, based on a Cobb-Douglas representation of the production function. The simple disaggregation into two items (labour input and labour productivity) uses the basic accounting relation (multiplicative in level and additive in terms of growth rate). The more refined disaggregation relates potential added value to the quantity of production factors (labour, capital, technology) in the sector under consideration. Further decompositions of each production factor can be performed using simple accounting relations and the different contributions could be rearranged to fit analytical needs.

More specifically, the approach in this study involves disaggregating the potential added value[15] of the EU financial sector, in level, into the contribution of total factor productivity (a proxy for innovation), capital (which we disaggregate into non-IT capital and IT, software, database related capital), and employment. All data are taken from the 2019 version of the EU KLEMS database and relates to the former EU-28. Monetary variables are expressed in euro, in volume, taking 2010 as a reference. Employment is expressed in terms of number of persons employed in thousands. The model takes the following form:

[14] See OECD, The long view scenarios for the world economy to 2060, OECD economic policy paper 22, Organisation for Economic Co-operation and Development, June 2018.

[15] Potential added value is computed based upon yearly EU KLEMS data and using a common exponential smoothing method to obtain the underlying trend for each series of the accounting equation. Data for 2018 and 2019, which are not provided in the 2019 version of EU KLEMS, are extrapolated using the same method.

$$Y = a * K_{non\text{-}IT}^{\alpha} * K_{IT,\ software,\ database}^{B} * L^{(1 - \alpha - B)} \quad (1)$$

Where:

Y is potential added value for the EU-28 financial sector

a is total factor productivity

α is the share of non-IT capital in total value added

$K_{non\text{-}IT}$ is the stock of non-IT related capital

B is the share of IT, software and database capital in total value added

$K_{IT,\ software,\ database}$ is the stock of IT, software and database related capital

L is total employment

As the development of crypto-assets and Fintech has medium to long-term implications while the underlying technology is constantly and rapidly evolving, we limit our analysis to a reasonable time frame of 10 years (to 2030) for the evaluation. In that timeframe, the growth components will be directly influenced by governmental policies (mainly endogenous). Moreover, one of the advantages offered by this framework is to better interpret the progress made by, to the extent possible, offering insight for a more thorough and systemic understanding of the main channels of transmission of policy action. Finally, it allows for a structural analysis and quantification of the economic impact of measures at EU level.

As regards the limitation of the accounting approach, one should bear in mind that it is mainly descriptive in nature. Developments in each component might be difficult to interpret separately in practice, given the multiplicity of factors affecting them, the existence of trade-off between variables and the residual role of total factor productivity (TFP) as a catch-all variable. Statistical and measurement problems, issues related to the choice of a Cobb-Douglas specification of the production function, and the choice of labour share calibration can also sometimes be questioned as they affect the reliability of the growth accounting. In the present exercise, and following the approach used by EU KLEMS, we nevertheless always rely upon the most established assumptions and further robustness checks are conducted when necessary.

Moreover, as already underlined in the previous section, the legislative package envisaged in this evaluation could significantly affect all the components in our accounting model. Total factor productivity could be directly enhanced by the development of a culture of permanent innovation and the development of new Fintech technologies, by a more effective EU policy towards the integration of digital innovations, by the stimulation of research and innovation, and by more competition in the financial sector. Factors of a structural nature, such as the distance to the production frontier, also play a part in increasing TFP, while other policies have a more indirect impact. Non-IT-related capital, i.e. mostly non-residential and residential investment, is generally particularly sensitive to the quality of the economic and of the capital market framework. Policies with a direct effect on such capital might thus include measures which aim at supporting more investment, at facilitating access to capital for SMEs, at increasing the efficiency of the financial sector, at completing the single market and the capital markets Union, and at supporting entrepreneurship in the financial sector. The stock of IT, software and database related capital will also be impacted by development in the financial sector. It will also be particularly impacted by accelerating innovation, and by the move towards a higher share of Fintech and the development of big data. Finally, employment is structurally influenced by the overall economic level of potential added value and by more efficiency in the financial sector.

Given the relatively recent development of crypto-assets, detailed data and precise quantitative economic evolution on these impacts are not available in a suitable way for use in our model as is the case for other more traditional policy areas. While broad trends emerge and while the qualitative framework is well researched, a projection of the impact of future development of crypto-assets and of Fintech is also largely affected by uncertainty, while at the same time potentially of large

magnitude. To circumvent these issues and to derive a magnitude for the size of the shock on each component in the financial sector, and for the purposes of this exercise, we have therefore assumed a differentiation in the alternative scenario between two sub-alternatives, to arrive at a bounded order of magnitude of the potential added value.

The first sub-alternative assumes a rapid transformative impact following the adoption of the legislation, as described in the alternative scenario **(high impact alternative scenario, HIAS**). Under this sub-alternative, innovation is flourishing, meaning that the projected average growth rate for TFP used in the projection takes the highest level for the corresponding period of time observed in the past. More precisely, we used a projected average annual growth rate that corresponds to the highest five year annual average level observed in the past. Similarly, investment is boosted, in particular that related to IT, software and database. The same estimation procedure is applied to compute the projection for the stock of non-IT related capital and to the stock of IT, software and database related capital. As a result, employment is also expected to recover in line with the increased level of investment and activity.

The second sub-alternative assumes a more subdued impact, as new regulatory challenges might appear, or as transformation is not as deep as initially envisaged **(medium impact alternative scenario, MIAS**). This scenario corresponds to a more prudent assessment of the impact of the envisaged legislative action. Innovation and efficiency gains are reduced, which affects TFP growth. Compared to the HIAS, the projected average annual growth rate takes a value which corresponds to the average level between the baseline and the HIAS. The same assessment applies for the projections of the stock of non-IT related capital, the stock of IT software and database related capital and employment.

The corresponding average annual growth rates used in the simulations are given in Figure 7. The procedure is applied separately for each accounting component. With this methodology we thus obtain a relatively prudent but optimistic assessment. Once the magnitude for the size of the shocks is computed for each component, we introduce them into the simulation framework, using the same procedure for the computation of potential added value than for the baseline scenario. The added value for each scenario and alternative is simply recomputed using equation (1) above.

Table 1 – Average annual growth rates to be used in the simulations

	Baseline scenario	HIAS	MIAS
Innovation (TFP)	1.06 %	1.59 %	0.78 %
Capital non-IT related	0.93 %	1.73 %	1.33 %
Capital IT, software, database related	3.45 %	5.41 %	4.43 %
Employment (L)	0.21 %	0.78 %	0.49 %

Source: EPRS.

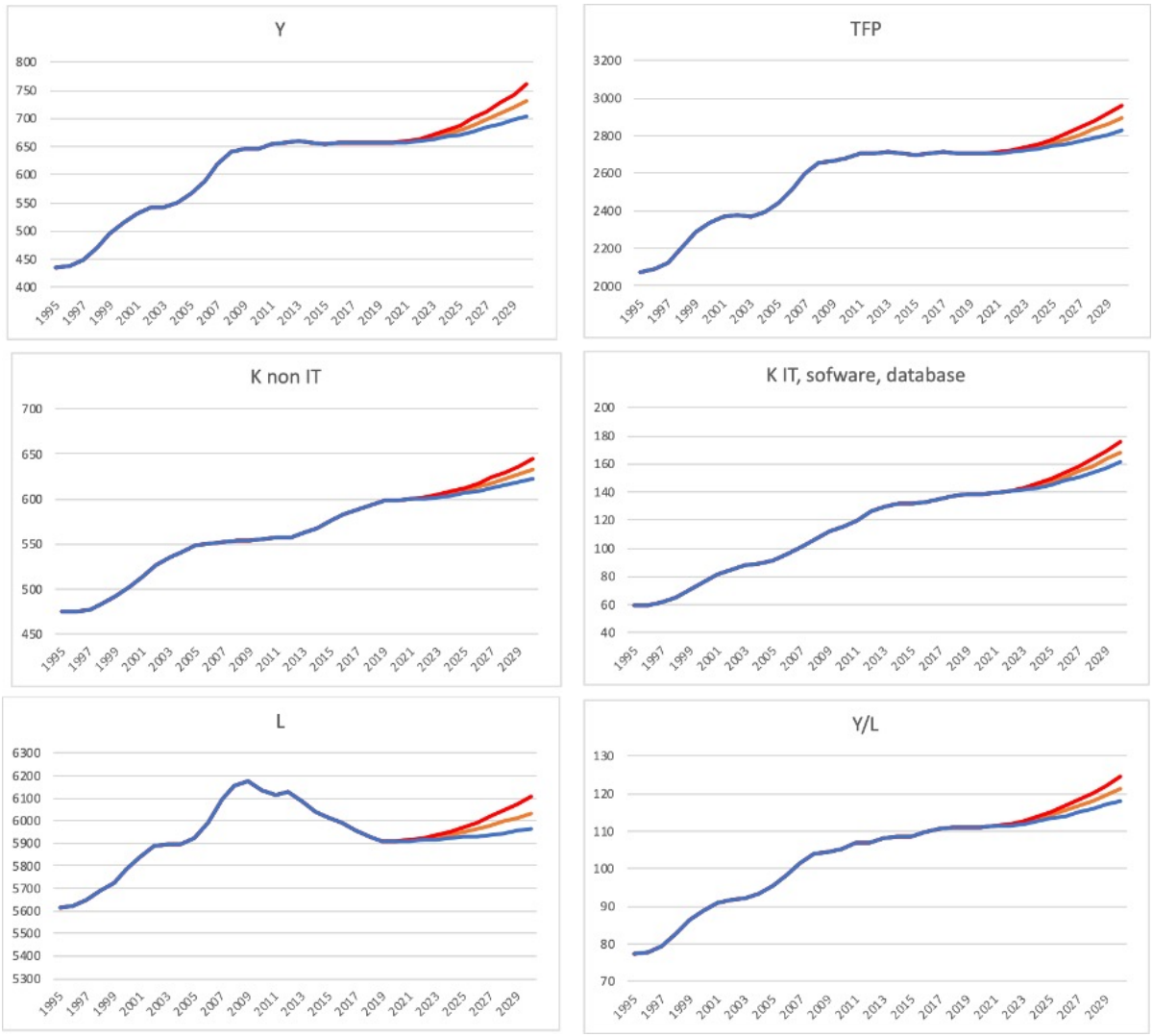
7.3. Economic assessment of the EAV for the European financial sector

As described above, the initial **baseline scenario** serves as a reference to evaluate the potential economic impact of alternative policy options. The scenario assumes no major change to initial institutional and policy-setting over the projection period. It is based on the prolongation of existing trends for each component of the accounting model up to 2030. The results are presented in

Figure 8. In line with our accounting framework, the level of potential added value, from 2019 to 2030, is set out in four components, namely total factor productivity, stock of non-IT related capital, stock of IT, software and database related capital, and total employment. We include productivity per person employed as an additional interesting analytical indicator. Results for 1990 to 2019 are also presented, to serve as reference points when interpreting the projections. Looking at the simulation from 2019 to 2030, our results indicate a moderate return to economic growth in the European financial sector, in line with long-term trends used to calculate the projection. The period of stagnation from 2008 is thus expected to end gradually, with potential added value in the sector reaching around €705 billion at the end of the simulation period for the EU as a whole. This moderate recovery is explained by similar returns to long-term growth potential in all components, again in line with expectations.

This outlook is of course subject to a very high level of uncertainty as the economic impact of the Covid-19 epidemic will undoubtedly have profound structural implications for the European economy. The baseline projections are therefore likely to be affected. To counterbalance this potential negative outlook, the EU needs to revive growth in the TFP, capital and employment components. The baseline projections assume some improvements in that respect. Regarding TFP, the projections gives an increase of almost 5 % for 2030 compared to 2019, while for the period 2008 to 2019, TFP increased by less than 2 %. Capital stock also increase substantially by around 4 % for non-IT related capital and 16 % for IT, software and database related capital. However, this will not be sufficient for employment levels to recover fully from the losses that followed the 2008 crisis, where the number of persons working in the financial sector reached close to 6.2 million. Currently this number stands at 5.9 million and is only projected to reach almost 6 million at the end of the simulation period. As a result, in the baseline scenario, productivity per person employed is growing, although it remains at a slower pace than during the previous periods of fast growth in the financial sector.

Figure 7 – Results of the simulations for the EU financial sector



Baseline scenario: blue line; HIAS: red line; MIAS: orange line

Source: EPRS.

Our **alternative scenario** serves to evaluate the economic benefits that could result from adopting a comprehensive legislative package that would allow for crypto-assets to develop while guaranteeing that risks are mitigated. The measures that would form part of such a scenario are those described as policy options in the previous section. We assume a complete front-loaded implementation at the beginning of the simulation period. The EAVA corresponds to the additional potential added value in the European financial sector, linked to the implementation of this legislative package compared to the baseline scenario. As explained, we differentiate between two alternatives in this scenario. The high impact alternative scenario (HIAS) assumes a rapid transformative impact following the adoption of the legislation. The medium impact alternative scenario (MIAS) assumes more prudent evolutions. The final results are presented in Figure 8 above and Figure 9 below.

Table 2 – Comparison with baseline scenario – end of the simulation period

	Baseline	HIAS	**Difference**	MIAS	**Difference**
Potential added value (Y) – difference in billion euro	705	760	**55**	732	**27**
Innovation (TFP) – difference in %	2 828	2 960	**5 %**	2 890	**2 %**
Capital non-IT related – difference in %	623	644	**3 %**	633	**2 %**
Capital IT, software, database related – difference in %	161	176	**9 %**	168	**4 %**
Employment (L) – difference in %	5 962	6 106	**2 %**	6 033	**1 %**
Productivity (Y/L) – difference in %	118	125	**5 %**	121	**3 %**

Source: EPRS.

Looking at the simulation from 2019 to 2030, our results confirm, as expected, a more dynamic return to economic growth in the European financial sector under the HIAS scenario. Potential added value in the sector would reach around €760 billion at the end of the simulation period for the EU as a whole. This represents an **increase of €55 billion** compared with the baseline scenario. The MIAS scenario indicates a potential added value of €732 billion, thus giving a **lower bound estimate** for the increase in added value of **€27 billion.** Regarding the components, thanks to growing innovation in the financial sector, TFP would be 5 % higher in the HIAS scenario than in the baseline scenario. Levels of capital would also be boosted and increased by respectively 3 % for non-IT related capital and by 9 % for IT, software and database related capital compared to the baseline scenario. As a result, employment would also recover, reaching 6.1 million at the end of the simulation horizon, but still short of the 6.2 million of employees in the EU financial sector at the peak of 2008. As efficiency in the financial sector improves, productivity per person employed would reach more healthy average annual rates of growth at around 1 % for the period 2010-2030, against 0.5 % in the baseline scenario. At the end of the simulation period, productivity per person employed would be 5 % higher in the HIAS scenario compared to the baseline scenario. The results for the MIAS scenario give further clues and references for comparison with lower bound estimates for each component.

7.4. Complementary qualitative EAV assessment of the impact on benefits and risks of policy option scenarios

Beyond supply side considerations and potential economic added value in the financial sector, the wider repercussions of the development of crypto-assets should also be considered. Significant spillovers could be affecting other sectors of the economy, while some institutions might also be impacted. More widely, the impact could be different for various components of society. In this part, taking a more systemic approach, we therefore look at these issues by complementing the quantification of the previous section with a broader qualitative EAV assessment. In particular, still considering the scenario previously described, we evaluate the impact – in terms of potential direct benefits and of risk reduction – which the adoption of a legislative initiative on a framework for crypto-assets, on cyber resilience and on a data strategy would bring.

First, from a **business** perspective, an EU legislative initiative on digital finance could improve safety, efficiency and integrity. This could foster the spread of crypto-assets as payment systems, which in turn could significantly lower transaction costs for businesses while increasing transaction speed. The technology indeed offers the possibility of reducing friction in transactions or in clearing and settlement processes. Businesses could also benefit from more individualised services and from

broader sources of investment. A beneficial legislative environment would also increase legal certainty and security, thus enabling long-term planning while decreasing the risk of unlawful behaviour and risks of high leverage on the market. It could also reduce uncertainty for market participants. With a higher level of cyber resilience, businesses would also face lower risks of financial losses due to cyber-attacks, which would increase confidence and reduce the risk of reputational damage.

Regarding **investors**, currently one drawback with crypto-assets is the high risk of volatility, which makes them rather unfit to store value. In particular, unbacked crypto-assets lack fundamental value. The implementation and the clarification of a legislative framework for crypto-assets would substantially alleviate these risks and bring more clarity and certainty to the market, thus benefiting investors. One issue also currently reducing the appeal of crypto-assets is the high level of cyber risks and a relative lack of investor protection. In this sense, questions of cyber security also arise, as crypto-assets could be subject to breaches, cyber-attacks and fraud. Increasing cyber resilience while implementing a coherent data strategy would contribute to mitigating these risks. Overall, more transparency and legal certainty would be ensured, thereby also fostering investor confidence in digital financial services and broadening investment perspectives.

Consumers could potentially benefit from the efficiency gains offered by the development of crypto-assets and digital finance, as this could lead to lower financial services costs, due to the abolishment of some financial intermediary functions. Thanks to tokenisation, consumers could also obtain more direct access to a broader range of financial products and services. These products and services could also be better tailored to their needs, thanks to decrease in principal-agent risks and a more effective use of data, assuming that a comprehensive data strategy is in place and that consumers' rights are respected. With a higher level of cyber resilience, consumers would face lower cyber risks, as they would be better protected. One last important consideration is that with a comprehensive legislative framework and data strategy in place, this risk of exclusion of some vulnerable consumers from access to financial services could be addressed. More generally, this would also significantly reduce the risks linked to the use of personal consumer data in digital finances.

From a **governmental and public finance** point of view, without a proper legislative framework in place, the anonymity of crypto-assets makes them prone to a risk of being used for illicit activities, money laundering, capital control and tax evasion. Currently, a large portion of cryptocurrency exchanges have weak anti-money laundering/combating the financing of terrorism (AML/CFT) and KYC practices. Ensuring clarity in that respect would reduce these risks and it could provide new avenues for direct government revenues through better taxation and indirectly through the development of a more efficient economy and of new services.

Finally, from a **macroeconomic perspective**, the digitalisation of assets could also **benefit the overall economy**. The overall broadening of the crypto-assets market, which as mentioned above would go hand in hand with digital financial innovation, could increase high skill employment, innovation and investment. Innovation in turn would foster the development of new products and services, creating new investment opportunities for businesses and start-ups to flourish. Crypto-assets such as investment tokens could widen access to financial capital for SMEs and start-ups in all areas of the economy. Potential gains through enhanced efficiency could be expected thanks to the absence of intermediaries, increased transparency through data integrity, immutability and security. Regarding the macroeconomic risks of financial instability, the use of crypto-assets is currently not widespread enough to represent an imminent threat. Nevertheless, if no action is taken at EU level, they hold the potential to become highly disruptive. This might result in the formation of speculative bubbles and give rise to negative spillover effects. This would naturally only happen if a legislative framework is not put in place. It is also important that the approach remain flexible, so that it can be adapted to the fast-changing nature of the technologies involved in digital finance. This, in turn, would ensure the integrity of the single market, lowering the risk of anti-competitive

behaviour while substantially reducing technological and operational risks and ensuring a higher level of protection for all market actors alike: financial institutions, consumers, businesses and investors.

Table 3 – EAVA of an EU legislative initiative on digital finance – Qualitative assessment (alternative scenario compared with baseline)

	Potential impact on benefits	Potential impact on risks
Businesses	Higher efficiency	Decreased risk of instability
	Broader market access	Less risk of anti-competitive behaviour
	Higher level of data protection	Lower risk of regulatory arbitration by Member States
	Higher level of cyber security and operational resilience	Less risk of unlawful behaviour (enabling long-term business planning)
	Lower transaction costs	
	Increase legal certainty and business confidence	Lower risks of financial losses due to cyber-attacks
	More individualised services	Reduced risk of reputational damage
	Broader sources of investment	
Investors	Increased confidence	Decreased volatility risks
	More transparency and legal certainty	Lower cyber risks, lower risks of fraud
	Increased security	
	New investment opportunities	
	Higher level of investor protection	
Consumers	Increase security	Lower risk of monetary losses
	Faster and cheaper payments	Lower risks of fraud
	More transparency and legal certainty	Lower principal-agent risk
	Lower costs of financial product and services	Lower risk of exclusion of vulnerable consumers
	Access to more financial products and services	Reduced risk linked to the use of personal consumer data in digital finances
	Secure data and identity	
	Higher level of consumer protection	
Government	Higher level of tax compliance	Reduced risk of capital control and tax evasion
		Lower risk of illicit activities and money laundering
Macro-economic level	Increase investment, new funding sources for SMEs and start-ups	Lower AML/CFT risks
	Foster large investment in IT, AI and in the technology sector	Lower risk of financial instability
	Development of innovation and technologies to be applied to other sectors	Lower the risk of anti-competitive behaviour
	Increase employment in high added value activities	Lower technological and operational risks
	Integrity of the single market and development of the capital markets Union	

Source: EPRS.

8. Conclusion

The conditions for significant structural change in the financial sector are currently developing. Enhanced technologies such as DLT, cloud computing and big data are increasingly widely adopted, while investor and customer preferences are changing rapidly and competition intensifies. The new Fintech firms have been faster than traditional institutions to take advantage of these advances in digital technology, developing products and services that are more user-friendly, cost less to deliver and are optimised for digital channels. Fintech could also expand well beyond the existing perimeter with the introduction and diffusion of crypto-assets. This would deliver fundamental changes to the infrastructure and processes at the core of the financial services industry. In such an environment, effective EU regulation of digital finance should aim at promoting innovation while ensuring long-term economic stability and mitigating the potential risks and negative externalities.

The recent growth of crypto-assets has raised questions about the appropriate regulatory perimeter and the ability of the existing regulatory architecture to adapt to changing conditions. In particular, an important issue when it comes to crypto-assets is being able to clearly determine what they are and which rules apply to them. Some crypto-assets fall under existing EU legislation, but most of them do not. This can leave investors and consumers exposed to substantial risks. Giving the complexity and the rapidly evolving nature of crypto-assets, there is a need to continually assess existing legislation to check whether it can be effectively applied to this type of asset or if amendments or guidance are needed. So far, no comprehensive and commonly accepted taxonomy of crypto-assets has been established. As a result, there is still a large number of definitions as to what exactly the term crypto-assets encompasses. The various classifications of crypto-assets are also sometimes difficult to navigate, which contributes to a high level of fragmentation and complexity between Member States and at international level.

To understand whether and which types of crypto-assets fit into existing regulatory classifications, and to assess if and how these need to be amended, it is crucial to agree on common criteria for the categorisation of each crypto-asset and to establish a European framework for markets in crypto-assets including stablecoins and cryptocurrencies. Such a framework should ensure legal certainty for innovators and investors, while addressing risks to market integrity, of market fragmentation and of financial instability. It should also be flexible and open, as it may need to be revisited based on future evolutions. Furthermore, the ongoing digital transformation in the financial sector has prompted an increasing focus on the issues of cyber-resilience and on the need to implement a comprehensive data strategy.

In this paper we have analysed these issues with a view to identifying the possible gaps in EU legislation and to evaluating the EAV of policy options to address these gaps. In particular, we recalled the current state of play in the EU digital finance market, subsequently outlining the current policy context. Secondly, we described the main weaknesses and the gaps in the existing EU legislative framework. Thirdly, we outlined a series of possible options to address these gaps, with a view to allowing digital finance to develop while addressing underlying risks. Fourthly, we estimated the EAV through a sectoral growth accounting model for the financial sector and using various scenarios. The scenario which forms the base for the evaluation of the EAV in the financial sector assumes that further legislative effort at EU level is undertaken so that the policy options identified in the previous part are fully implemented. Under this scenario, the European Commission would introduce targeted amendments to existing financial services legislation to add further detail for their applicability to crypto-assets. For crypto-assets that currently fall outside the regulatory perimeter, the European Commission would propose a series of legislative measures for crypto-asset issuers and service providers and a bespoke legislative measure on stablecoin issuers. Under this scenario, a series of legislative proposals would strengthen the digital operational resilience of EU financial sector entities, including their ICT security, by streamlining and upgrading existing rules and introducing requirements. Finally, the EU data strategy would be enhanced to allow for

consistent, technology-neutral application of existing EU data legislation. Cooperation at international level would be pursued, deepened and reinforced.

The results from our simulations confirm a more dynamic return to economic growth in the European financial sector under this scenario.[16] Potential added value in the sector would reach around €760 billion at the end of the simulation period for the EU as a whole. This represents an **increase of €55 billion** compared with the baseline scenario. A more prudent scenario indicates a potential added value of €732 billion, thus giving a **lower bound estimate** for the increase of added value of **€27 billion.** Regarding the components, thanks to growing innovation in the financial sector, TFP would be 5 % higher than in the baseline scenario. Levels of capital would also be boosted and increased by respectively 3 % for non-IT related capital and by 9 % for IT, software and database related capital compared to the baseline scenario. As a result, employment would also recover, reaching 6.1 million at the end of the simulation horizon. As efficiency in the financial sector improves, productivity per person employed would reach more healthy average annual rates of growth at around 1 % for 2010-2030 against 0.5 % in the baseline scenario. Finally, beyond quantitative results for the financial sector and with a view to broaden the EAVA, a more systemic qualitative EAVA is also performed. In particular, still considering the scenario previously described, we evaluate the impact in terms of the potential direct benefits and risk reduction that the adoption of a legislative initiative on a framework for crypto-assets, on cyber resilience and on a data strategy would bring. The results highlights the broader gains that could be expected from well-designed, comprehensive and well-balanced EU legislative action in these areas.

[16] This outlook is of course subject to a very high level of uncertainty as the economic impact of the Covid-19 epidemic will undoubtedly have profound structural implications for the European economy.

REFERENCES

Adrian T., Mancini-Griffoli T., The rise of digital money. Fintech Note 19/01, IMF, 2019; Adriano A., A short History of Crypto Euphoria, IMF, 2018.

BIS-BCBS, Cyber resilience: Range of practices, 2018.

BIS-CPMI and IOSCO, Guidance on cyber resilience for financial market infrastructures, 2016.

BIS, Investigating the impact of global stablecoins, G7 Working Group on Stablecoins Report, 2019.

BIS, Impending arrival – a sequel to the survey on central bank digital currency, BIS Papers, No 107, 2020.

BIS, How Fintech can promote financial inclusion - a new report on the opportunities and challenge, 2020.

BIS, Policy responses to fintech: a cross-country overview, January 2020.

Blandin A., et al., Global Crypto-asset Regulatory Landscape Study, University of Cambridge Centre for Alternative Finance, 2019.

Boucher P., How blockchain technology could change our lives, EPRS, European Parliament, 2017.

Bouveret A., Haksar V., What Are Cryptocurrencies? A potential new form of money offers benefits while posing risks, IMF Finance & Development, March 2018.

Centre for European Policy Studies (CEPS), Cyber security in Finance: Getting the policy mix right!, Report of the CEPS-ECRI Task Force, 2018.

Darvas Z., Domínguez-Jiménez M., Wolff G.B., From Climate Change to Cyber-attacks: Incipient Financial Stability Risks for the Euro Area, Bruegel Policy Contribution No 2, 2020.

Demertzis M., and Wolff G.B., Hybrid and cyber security threats and the European Union's financial system, Bruegel Policy Contribution N 10, 2019.

Digital Europe, Two years of GDPR: A report from the digital industry, June 2020.

EBA, Report with advice for the European Commission on crypto-assets, EBA Report, January 2019.

EBA, EBA Guidelines on ICT and security risk management, Final report, November 2019.

EBA, EBA Guidelines on outsourcing arrangements, Final report, 2019.

ECB, Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures, Occasional Paper Series, No 223, May 2019.

ECB, Understanding the crypto-asset phenomenon, its risks and measurement issues, ECB Economic Bulletin, 05/2019, May 2019.

ECB, Crypto-assets – trends and implications, June 2019.

ECB, Implications of digitalisation in retail payments for the Eurosystem's catalyst role, July 2019.

ECB, ECB Banking Supervision: Risk assessment for 2020, 2019.

ECB, Monetary policy: the challenges ahead, transcript of the Colloquium in honour of Benoît Coeuré of 17-18 December 2019.

ECB, What is cyber resilience?, 2020.

ESMA, Advice on Initial Coin Offerings and Crypto-Assets, January 2019.

ESMA, Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, April 2019.

ESMA, Joint Advice of the European Supervisory Authorities to the European Commission on the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sec, April 2019.

EU Blockchain Observatory, Blockchain and the Future of Digital Assets, Thematic Report, 2020.

European Commission, FinTech action plan: For a more competitive and innovative European financial sector, March 2018.

European Commission, ROFIEG (Expert Group on Regulatory Obstacles to Financial Innovation), 30 Recommendations on Regulation, Innovation and Finance, Final Report, December 2019.

European Commission, Consultation paper on an EU Framework for markets in crypto-assets, December 2019.

European Commission, roadmap towards a proposal for a directive/regulation establishing a European framework for markets in crypto-assets, December 2019.

European Commission, roadmap towards a proposal for a regulation on digital operational resilience for the financial sectors, December 2019.

FAFT, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019.

Ferrari V., The regulation of crypto-assets in the EU – investment and payment tokens under the radar, *Maastricht Journal of European and Comparative Law*, 1-18, 2020.

FSB, Financial Stability Implications from FinTech, June 2017.

FBB, Crypto-assets: Report to the G20 on the work of the FSB and standard-setting bodies, July 2018.

FSB, FinTech and market structure in financial services: Market developments and potential financial stability implications, February 2019.

FSB, Crypto-assets: Work underway, regulatory approaches and potential gaps, May 2019.

FSB, Decentralised financial technologies: Report on financial stability, regulatory and governance implications, June 2019.

Goodkind A.L., Jones B.A., and Berrend R.P., Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining, Energy Research & Social Science, 59, 2020.

IMF, The Bali Fintech Agenda, IMF Policy Paper, 2018.

IMF, Cyber security Risk Supervision, Departmental Paper Series, No 19/15, 2019.

IMF, Framing the Debate on Fintech: Current Trends and Continuing Policy Concerns, Remarks by Tobias Adrian, 2019.

Latici T., Cyber: How big is the threat?, EPRS, European Parliament, 2019.

OECD, Tax Challenges Arising from Digitalisation – Interim Report 2018, OECD/G20 Base Erosion and Profit Shifting Project, 2018.

OECD, Enhancing Access to and Sharing of Data, 2019.

OECD, Initial Coin Offerings for SMEs financing, 2019.

OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, OECD Blockchain Policy Series, 2020.

OECD, Digital Disruption in Banking and its Impact on Competition, 2020.

Philippon T, The FinTech Opportunity, NYU working paper, March 2018.

Policy Department for Economic, Scientific and Qualityof Life Policies, Crypto-assets: Key developments, regulatory concerns and responses, European Parliament, 2020.

Policy Department for Economic, Scientific and Quality of Life Policies, Cryptocurrencies and Blockchain -Legal Context and Implications for Financial Crime, Money laundering and tax Evasion, European Parliament, 2018.

Policy Department for Economic, Scientific and Quality of Life Policies, Virtual currencies and central banks monetary policy: challenges ahead, European Parliament, 2018.

Siddigi L., Why cyber risk should take centre stage in financial services, World Economic Forum, 2020.

Szczepański M, Is data the new oil? Competition issues in the digital economy, EPRS, European Parliament, 2020.

Vives X., Digital Disruption in Banking, Annual review of Financial Economics, 11:243-72, 2019.

White O., Madgavar A., Manyka J., and Mahajan D., Digital identification: A key to inclusive growth, McKinsley Report, 2019.

World Bank, Cryptocurrencies and blockchain: hype or transformational technologies? 2018.

Yaworsky K., Goswami P., and Shrivastava D., Unlocking the promise of (Big) Data to promote financial inclusion, *Accion Insights*, 2017.

The rapid growth of digital finance and crypto-assets has raised questions about the appropriate regulatory perimeter and the ability of the existing regulatory architecture to adapt to changing conditions. In this study, we evaluate the impact in terms of benefits and in terms of risk reduction that the adoption of an EU legislative initiative on a framework for crypto-assets, on cyber-resilience and on a data strategy would bring.

QA-02-20-663-EN-N

This is a publication of the European Added Value Unit
EPRS | European Parliamentary Research Service

PDF ISBN 978-92-846-7078-9 | doi:10.2861/525 | QA-02-20-663-EN-N