ECMI Policy Brief no 31 | September 2021

Regulating crypto and cyberware in the EU[1]

Karel Lannoo*

Executive Summary

Crypto currency matters are seemingly in the news every day, but the EU's attempt to introduce a tailor-made regulatory regime is not. A draft regulation is currently before the European Parliament and Council of the European Union for adoption in the coming months, setting down a dedicated framework for crypto-assets, stablecoins and digital money, and the related trading platforms and virtual networks. Only authorised providers will be allowed to offer crypto currencies in the EU, and they will need to have an EU registered office. As a corollary, the EU also intends to regulate and supervise the digital resilience of financial institutions. If adopted, the EU's 'crypto regulation' will be the first act by an international institution to regulate this sphere. In this policy brief, we note:

- The lack of a common approach across countries for a global phenomenon such as crypto, and the profound differences with the US, which regulates crypto as a security under existing securities laws, whereas the EU is creating an entirely new regime, rendering implementation and user interpretation more difficult, and creating confusion across regulatory regimes;
- Diverse approaches enable regulatory arbitrage and a race to the bottom, where the providers are the winners, and the investors the victims;
- Much remains to be done to render the crypto world more transparent, in single data feeds, but also in the development of commonly agreed valuation and accounting methods, let alone the issue of taxation;
- The crypto hype emphasises the need for a more efficient network for international payments, outside the realm of the global reserve currencies;

Karel Lannoo is General Manager of ECMI and CEO of CEPS

[1] This policy brief builds upon discussions in an ECMI webinar on crypto currencies organised on 5 July 2021. Special thanks to Marie Brière, Niamh Moloney, Jesper Hansen and Florencio Lopez de Silanes for their input, and to Steven Blockmans, Robert Kopitsch, Almudena de la Mata, Monica Monaco, Nick Reinhardt and Apostolos Thomadakis for further comments on MiCA and DORA, and on this paper. All remaining errors are mine.

- The new proposals considerably increase the tasks for supervisors: in a complex set-up, national and European authorities will need to authorise and supervise virtual asset providers, and control ICT suppliers of the financial sector;
- Crypto is often associated with money laundering, mostly through third country providers. Strong international cooperation in the 'cryptosphere' is needed to detect criminal networks, but this is where the lack of a common global regulatory approach matters.

To European policymakers, we recommend:

- Clearer definitions of crypto assets in the draft EU's Markets in Crypto Assets (MiCA) regulation, and close alignment with existing rules;
- A simplification of the EU supervisory architecture for crypto assets, and a greater role for the European Supervisory Authorities in licensing and supervising crypto schemes;
- To advance the debate on transparency in the valuation of crypto assets;
- Enhanced international cooperation on crypto assets to tackle money laundering, fraud and the criminalisation of international payment networks;
- The need for more awareness raising and debate of the EU's efforts in this domain.

Introduction

The biggest opportunities and threats in finance these days come from the digital sphere. Fintech firms have made big inroads in financial intermediation, and several relatively new companies are valued higher than large banks. Blockchain and Artificial Intelligence (AI) have the potential to revolutionise the ways finance firms interact with their clients and structure their operations internally. The growing use of digital currencies in its different forms has created a large controversy among regulators and in central banking circles about the creation of a new asset outside the classic institutions. It has led the central bankers to announce the creation of a central bank digital currency (CBDC).

Innovation in the financial sector should be welcomed, but the policy response is not uniform, either at the global or European level. Innovation brings more competition and lowers costs for users, it creates new funding sources for enterprises and more integration of payment systems. But compared to ten years ago when the G20 managed a coordinated response to the challenges posed by the global financial crisis, this time is different. Bitcoins are an opportunity for small or rogue states to escape from the dominance of the big reserve currencies. Crypto-asset offerings carry huge financial and investor protection risks, and while some countries have adopted rules to facilitate token or Initial Currency Offerings (ICOs), and have important volumes of issuance, others are resisting. Approaches also differ for regulating fintechs and decentralised finance: some are registered as banks or trading platforms, others are under a much lighter scheme, or follow the regulatory sandbox approach.

An important element explaining the confusion is related to the definition of cryptofinance: Is it related to payments, to intangible assets or simply to tradable tokens or virtual gadgets? How are crypto 'transactions' regulated and protected? What are the implications for the operating systems of financial institutions? What is the impact on financial inclusion and literacy?

After a period of long hesitation – and then consultation – the European Commission in September 2020 proposed to regulate cryptocurrencies under the Markets in Crypto-Assets (MiCA) proposal (EC, 2020). This complex piece of regulation covers three different forms of crypto-assets that are based on distributed ledger technology (DLT): crypto assets, non-fungible and utility tokens, asset-referenced tokens, and e-money tokens. With regard to the related cybersecurity issues that the use of crypto-assets also introduces, another regulation, the Digital Operational Resilience Act (DORA) sets general rules for managing ICT risks in the financial sector, including oversight of third party providers, to strengthen business continuity. Both pieces of legislation create important new tasks for the European Supervisory Authorities (ESAs) and national authorities in supervising technology and technology providers in the financial sector.

This policy brief discusses the EU's digital finance proposals in the context of the broader regulatory and supervisory structure at EU level. MiCA and DORA have not received the attention they deserve. With MiCA, the EU is the first international jurisdiction to come up with a distinctive regulatory approach for crypto-assets, but it renders the framework rather complex, with an unclear supervisory set-up. As for DORA, the EU introduces a common regulatory approach in tackling digital dependence in the financial sector. The question remains whether European supervisors will have sufficient expertise to take on their new tasks. More broadly, these rules also interact with other horizontal rules, related to digital identity and privacy, e-commerce and digital markets and services, or specific rules on anti-money laundering (AML) and crowdfunding. First, we start with some broader conceptual and policy considerations raised by these technological developments, and then we go on to discuss the proposals and their implications in more detail, while also indicating where the central bank digital currency fits into these discussions. We conclude with some specific recommendations for EU policy making in this domain.

DLT and finance

Crypto-assets are any digital representation of value that utilises some kind of DLT or blockchain technology. DLT is a shared and synchronised digital database that is maintained by a consensus algorithm, the procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger, and stored on multiple nodes (i.e. computers that store a local version of the database). It is decentralised in distributed ledgers, or databases, shared across public or private computing networks, meaning that there are often many parties involved in the maintenance of these databases. Every piece of information is validated and stored as a new 'block' in the chain of historical records. The encrypted data reveals a user and transaction nexus that allows for transactions to be traced back to users (Reid and Harrigan, 2011). This decentralised structure brings efficiencies (Nascimento and Pólvora, 2019; BIS-SIX-SNB, 2020),[2] promotes competition (Lianos, 2019; Pike and Capobianco, 2020), but also entails inefficiencies (Casey *et al*., 2018; Atzori, 2021). There are public permissionless and private permissioned blockchains.[3] DLT includes different technologies, which are still evolving, hence any clear description or definition remains difficult to fully formulate.

Definitional problems are key, given that crypto-assets can cover many different realities. Is it a security, a commodity, a currency, a means of payment or simply a token? The definition provided in the EC's MiCA proposal – "*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology"* – is rather vague and broad. It certainly requires further clarification, as was highlighted in the European Central Bank's (ECB) opinion (ECB, 2021). But the question is: can a clear definition be made with a still evolving technology? And would a clear definition stifle innovation?

Blockchain has been around for some time, and although it has advanced, it is still nascent. The big breakthrough and broad adoption have been announced several times ("three to five years away from feasibility'' according to McKinsey, 2018) but is always delayed. Some have compared it to the emergence of the World Wide Web in the early 1990s (Iansiti and Lakhani, 2017), which also required fundamental governance issues to be resolved before it could really take off. Apart from that, there is the issue of blockchains' huge energy consumption, which in a world of increasing focus on decarbonisation is an important caveat.[4]

---

[2] An area, for example, in which such efficiencies might occur is post-trading. DLT offers the potential of merging/rendering obsolete back-office functions that are currently distributed to clear intermediaries along the value chain (e.g. trading, clearing, settlement).

[3] A permissionless blockchain is a type of blockchain network that allows anyone (i.e. open to the public) to become part of the network and contribute towards its upkeep. For example, cryptocurrencies like Bitcoin are powered by permissionless blockchain networks. The main characteristics of such a network are transparency, anonymity, and full decentralisation. On the other hand, in a permissioned blockchain one needs, as the name implies, permission to become part of the network. The owner of the network dictates who can or cannot join the network. As a result, such a network has a defined governance structure, a varying degree of decentralisation, but does not provide transparency.

[4] According to the Cambridge Bitcoin Electricity Consumption Index, Bitcoin's current yearly electricity consumption is at around 96 terawatt-hours (TWh) or at around 0.5% of global electricity consumption. In fact, the bitcoin economy has more CO_2 emissions than countries such as Belgium or Finland, and just a bit less than the Netherlands. However, there are differences between different types of blockchains depending on the approach followed to validate new blocks of information. Bitcoin is particularly demanding in energy due to the 'proof of work' approach, which requires huge computing power to validate new blocks. However, other methods might consume much less energy, such as the 'proof of stake', which only validate block transactions based on the amount of coins a miner holds (Gallersdörfer *et al*., 2020; Martin and Nauman, 2021).

Blockchain has clearly advanced as the basic technology for 'cryptocurrencies'. New types of cryptocurrencies have emerged, and its formal adoption in several jurisdictions has increased. The total value of outstanding crypto tokens is about 2 trillion today, which is roughly the same value as all US dollars, or the double of all euro banknotes in circulation (see coinmarketcap). This advance also impacts the central banks' digital currency proposals (CBDC), where plans are becoming more concrete. Until about two years ago, central banks were clearly against the very notion of digital currency, as it was seen as a threat to their core task. Today, central banks have accepted that important inefficiencies exist in cross-border and international payments, and some crypto-currency schemes have been launched as a response to these inefficiencies.

The same applies for decentralised finance (DeFi), where DLT is a response to the inefficiencies in financial infrastructures and back-offices, certainly for more complex products such as derivatives or collateralised debt positions. DeFi refers to financial services using smart contracts, which are automated enforceable agreements that operate entirely on blockchain networks, rather than through intermediaries like banks or lawyers. DeFi is seen to be more accessible, efficient, and transparent – a way to democratise the creation of markets and consumption. It is called the 'money-lego' concept, due to the simplicity of the building blocks.

Both public and private blockchains raise specific security issues related to scalability and network congestion, as well as the concentration of risk and interdependence. Moreover, the use of blockchain technology also raises governance concerns (who controls the protocol, where is it based), market abuse, inside information and money laundering. Although DORA attempts to address some of the cyber-operational matters, the question remains whether the European Commission goes far enough in both proposals.

Regulatory approaches to DLT

Definitional problems of DLT have prevented a more consistent regulatory approach. In addressing DLT, the EU and regulators around the world have followed different approaches. This problem however predates DLT, as payment systems – the most disruptive part of the financial sector – have been undergoing deep change for the last two decades, following the emergence of e-commerce. The EU's E-Money Directive was adopted in 2000[5] and the Payments Services Directive (PSD) in 2007.[6] Cross-border payments in the EU have been regulated since 2001[7] after long and protracted discussions with the banking sector on their costs. For as long a time, t high credit card sector interchange fees have been a stumbling block for the EU's competition policy authorities. Fees were capped at 0.2% of the value of a transaction for debit cards and 0.3% for credit cards in a 2015 regulation.[8] But this also remains contested, as some have argued that it maintains the credit card duopoly of Visa and Mastercard (Dolmans e.a., 2020).

Payment transmitters can thus operate under several regulatory regimes, at EU or global level. Regarding crypto-currency schemes, they have worked under regulatory sandboxes at the local level, or under no rules at all, provided they did not qualify as a financial instrument under the Markets in Financial Instruments Directive (MiFID). With the MiCA proposal, the European Commission wants to fill the void and set a common approach in the EU for DLT-based operators, ensuring consumer and

[5] Directive 2000/46/EC.
[6] Directive 2007/64/EC.
[7] Regulation (EC) 2560/2001.
[8] Regulation (EU) 2015/751.

investor protection, and market integrity. The question however emerges on why the EU has not tried to cover crypto-assets and crypto-currencies under existing rules, as is the approach taken in the US or in Hong Kong, rather than creating another new regime for a still emerging and fast-changing technology.[9] Moreover, the European Commission has brought three distinct forms of crypto-based services under one draft regulation.

One could advocate that the Commission's approach is correct, given that the main difficulty in regulating crypto-assets is that they bring new risks related to new 'functions', hence they require a specific regulation. For example, contracts that automate contingent transfers depending on the success of delivering the goods or services can pose new risks of collusion (Cong and He, 2019).[10] Another new functionality made possible through blockchain, is the 'fork' – an either accidental or intentional change in protocol – that can make the ledger less stable, reliable and useful (Biais *et al*., 2021).[11] Last but not least, a new functionality also arises from decentralisation which allows greater ease in benefitting from regulatory arbitrage (Nabilou, 2019; Amstad, 2019).

EU crypto regulation under MiCA

The draft regulation proposes a broad definition of crypto-assets and stablecoins, sets rules on their providers, including the trading platforms, and defines the role of the supervisors. Crypto-assets include three groups: 1) crypto assets and utility tokens, 2) asset-referenced tokens and 3) e-money tokens, with the lightest rules for the first group. Utility tokens are intended to provide digital access to a specific good or service. Asset-referenced tokens are stablecoins, referencing baskets of currencies or commodities. An e-money token is also a stablecoin, but its requirements are like those of traditional e-money. The rules will not apply to security tokens that are already subject to existing EU regulatory regimes, and to central bank digital currencies (CBDC).

Specific stipulations of MiCA include:

- Providers of crypto-assets and **utility tokens** shall draw up a 'crypto-asset white paper' for notification to the authorities before issuing this product. The white paper will contain disclosure, conduct and liability rules that are in principle prospectus requirements to address the inadequate disclosures, misrepresentations and fraud currently often observed in certain initial coin offerings. White paper issuers will benefit from a European passport for tokens. There is no formal *ex-ante* approval requirement (Art. 7(1) "*Competent authorities shall not require an ex-ante approval of a crypto-asset white paper, nor of any marketing* communications *relating to it before their publication*"), which is justified by not placing excessive burdens on supervisors (Recital 19).
- Issuers of **asset-referenced tokens** must be formally authorised. They shall respect a minimum capital of €350,000 and an ongoing capital requirement of 2% of the average amount of the reserve

[9] See the recent statements by Gary Gensler of the SEC on the US approach, asserting crypto assets should be regulated the same way as existing securities under the existing securities laws, whereas industry argues for a new approach. See also the first fraud case against a DeFi network on 6 August 2021. For the Hong Kong Securities and Futures Commission (SFC), ICO tokens are regulated as securities under Hong Kong's Securities and Futures rules and must be licensed and authorised by the SFC.

[10] Through the decentralised consensus, sellers will have greater knowledge of aggregate business conditions on the blockchain, which can lead to tacit collusion among sellers.

[11] In an ideal blockchain, there is a single sequence of blocks, with each of them offering an updated version of the ledger (taking into account the most recent transactions), on which all participants agree. However, if there are forks in the blockchain, it means that there are competing branches, with each of them trying to register a potentially different version of the ledger.

assets in the last six months in Tier 1 capital. Reserves must be kept in triple A securities and be prudently managed. The rules also contain a stabilisation mechanism of tokens, or the investment policy (Art. 32.4), including among other ''*the procedure by which the asset-referenced tokens are created and destroyed, and the consequence of such creation or destruction on the increase and decrease of the reserve assets*''. This also raises custody issues, which are detailed in Art. 33. Furthermore, issuers need to meet governance and conduct requirements, which service providers that intend to operate a dedicated crypto asset platform (Art. 68) need to respect.

- E-money tokens, can only be offered to the public by an issuer authorised as a credit institution or as an 'electronic money institution' within the meaning of the E-Money Directive (2009/110/EC). E-money tokens shall be issued at par value and on the receipt of funds, and upon request by the holder of e-money tokens, the issuers must redeem them at any moment and at par value.

The supervisory regime for MiCA is a mix: national authorities are in charge, but for significant issuers of asset referenced and e-money tokens, the European Banking Authority (EBA) is responsible, based on minimum criteria. EBA also chairs the supervisory colleges for these crypto assets (with national competent authorities (NCAs) and the European Securities and Markets Authority (ESMA)). EBA will have general investigative powers, can make on-site inspections, and request information from NCAs, also in third-countries. ESMA, on the other hand, has implementing powers for crypto-asset providers and needs to establish a register of all crypto-asset service providers. The complexity of this set-up has led the European Parliament in its initial reaction to ask for a clearer, better-defined role for the European Supervisory Authorities (ESAs).

The regime for third-country issuers is very rudimentary, considering that crypto-assets are global and most activity is outside the EU. NCAs shall conclude cooperation agreements with these countries. Whenever there is an issuance of a global stablecoin in the EU, EBA should be leading the supervisory college, with no voting rights for third countries. There is no reference to equivalence agreements with third-country regimes, only a request to examine the need for equivalence agreements three years after adoption of the measure. This is particularly problematic as MiFID II establishes a full framework for the operation of third-country firms (via Article 39 and following) while this is not the case at all for the MiCA Regulation.

Rules on the prohibition of market abuse, insider trading and market manipulation will apply (Title VI), but they are much lighter than the existing rules applicable to securities markets operators (regulation 596/2014). 'Issuers of crypto-assets and crypto-asset service providers are very often SMEs, it would be disproportionate to apply all the provisions of Regulation (EU) No 596/2014', Recital 64 of the draft states.

Overall, the problem with MiCA is that it brings together three distinct forms of crypto-assets under one regulation, but it does not clarify when the second group (i.e. asset-referenced tokens) falls within or outside the framework of existing EU financial law, in particular the prospectus rules and MiFID. In practice, MiCA will apply, unless it is not within the scope of MiFID. The same duality exists for crypto trading platforms, where the question will emerge over whether a MiFID licensed trading platform can trade crypto, or whether they should be authorised under MiCA. Because of this complexity, some have called MiCA 'a job-creation programme for lawyers' (Godschalk, 2021). In fact, it has been argued that even if it harmonises EU law for crypto instruments, it renders the overall application of financial law more difficult (Zetzsche *et al*., 2021). Compared to this, the approach of the US Securities and Exchange Commission (SEC) is more straightforward, as it applies the existing securities acts of 1933.

Where does the CBDC fit into the picture?

The announcement of the central bank digital currency (CBDC) has added to the confusion about cryptocurrency. All depends on who announces what. In the case of the large, well-established central banks, the CBDC will be nothing else than digital money but now directly issued by the central bank as legal tender, with the modalities still to be decided upon. For others, it could more or less resemble a stablecoin, or it could be an 'illegal' tender, depending upon the issuer and the modalities. But whether or not these CBDCs will be based upon DLT, remains to be seen.

After a lengthy consultation phase, the ECB's Governing Council decided on 14 July 2021 to launch the investigation phase of a digital euro project that will last two years. The project will also consider changes to the EU's legislative framework that might be needed, and for which the ECB is in close contact with the European Commission. The key issue is the modalities for the circulation of the digital euro, which will be closely watched by the European banking sector. If citizens can have a direct account at the central bank, it would be a further threat to the traditional retail banks for whom payments in all their forms are a core part of their business contributing to around one quarter of their revenues. Also, the Fed and the People's Bank of China (PBoC) are examining digital currencies. The PBoC already has pilot schemes of e-RMB running, involving private citizens, as a reaction against the blockchain-based currencies that are decentralised by definition.

The digital euro raises a host of core and critical bank regulatory matters. It could facilitate financial inclusion, although financial literacy will remain an issue. Access to and the cost of bank accounts for European citizens has been a matter of concern for consumer lobbies for a long time, as it determines overall societal participation. But direct accounts at the central bank could be a threat to financial stability, and undermine trust in the financial system in the case of stress or volatility. What will a 'bank run' look like with a CBDC? It would profoundly alter the liquidity transformation function of commercial banks. The ECB may be attracted by the perspective of a bigger role in the payment system, which it has been trying to do since the launch of the TARGET (Trans-European Automated Real-Time Gross Settlement Express Transfer) system in 1999, and also recently through its involvement in the European Payments Initiative (EPI). But this stands increasingly in contrast with its statute and beginning as a 'narrow' central bank.

A digital euro also raises data protection and privacy matters. Control on illicit activities and money laundering are advanced as a big advantage of the digital euro, because of the technology used - DLT - which allows transactions to be traced back to users through the digital identities (e-ID) and digital signature components. However, this also brings the 'Big Brother' state much closer to reality.[12] Moreover, it is by no means certain that the ECB, let alone the EU27, will manage to get all its members on one line on these matters. Some member states may wish the digital euro to be a substitute for cash, with less traceability than what the DLT would allow.

[12] See the blog post by Fabio Panetta, Member of the Executive Board of the ECB on "Preparing for the euro's Digital Finance".

Cyber resilience rules in DORA

Compared to MiCA, DORA is less controversial. Cybersecurity has been on the minds of many finance professionals and policymakers as a major concern and priority. DORA aims to meet the need for a more EU-wide standardised approach for cyber risks and disclosure by the financial sector. It clearly defines the applicable entities and requires them to have the necessary governance framework in place. It also gives a huge (but difficult) additional role to the ESAs to monitor digital resilience. A key novelty of DORA is that it brings third party providers into the financial supervisory domain, albeit only to an extent. The challenge here stems from digital finance and finding the right balance between financial regulation and supervision, in order to handle a more complex and diverse ecosystem where tech companies are increasingly important actors for the effective provision of financial services.

Building on the many work streams at European and international level, DORA's principle-based approach aims to streamline the provisions/requirements of the financial legislation and create a minimum baseline to boost the digital operational resilience of the financial sector. It completes the existing but generic Network of Information Systems Directive (NISD)[13], with much more detailed provisions and oversight. Furthermore, it covers almost the entire financial sector, including crypto-asset providers, and addresses five main areas that are relevant from a digital operational resilience perspective: 1) ICT risk management; 2) incident reporting; 3) testing; 4) third-party risk; and 5) information sharing. Importantly, proportionality is embedded in the rules and addressed by specific exemptions.[14] As for the supervision of DORA's application, this is down to the competent authorities responsible in the sectoral legislation.

The key components of DORA can be summarised as follows:

- A clear taxonomy - what is cybersecurity and what is not? The draft defines 'digital operational resilience', 'ICT risk', 'cyber threat', 'cyber-attack', 'vulnerability', 'threat led penetration testing' ('a framework that mimics the tactics, techniques and procedures of real-life threat'), 'ICT concentration risk', etc.
- A clear ICT management framework. Every financial entity shall have a management body in charge of the implementation of all arrangements related to ICT risk, including the obligation to have a business continuity plan.
- Procedures for stress testing of cyber resilience, vulnerability disclosure and incident reporting, including cyber-attacks. These are based upon common templates, building upon the work already undertaken by the ECB (in TIBER-EU). Authorities should be informed of major incidents at the end of the business day, with a report one week after the initial notification.
- Procedures for ICT third-party service providers (ITPP) that are critical for financial entities, with a clear allocation of responsibilities, and reporting to authorities of contractual arrangements, with a definition of the necessary contractual provisions (Art. 27).
- The ESAs – based upon systemic stability criteria – will designate the ICT third-party service providers (ITPP) that are critical for financial entities. In addition, either EBA, ESMA or the European Insurance and Occupational Pensions Authority (EIOPA) will be appointed as Lead Overseer, with on-site inspections (Art 34), covered by fees charged to the ICT providers.

[13] Directive (EU) 2016/1148.

[14] For example, certain provisions do not apply to microenterprises, while some rules are only applicable to significant institutions (e.g. the threat led penetration testing and the reporting of incidents are only for major ICT related incidents).

- A central role for the ESAs Joint Committee, which together with the European Union Agency for Cybersecurity (ENISA) will aim to reinforce cross-border cooperation and improve the process of attribution and eventually criminalisation; and, an Oversight Forum as a specialised ICT subcommittee, to support the work of the Joint Committee.

When implemented, DORA should be a big step forward in improving digital resilience at EU level and creating a common approach for the disclosure of software vulnerability, although the definitions and risks will need to be clarified. Not every threat can be reported, it should be clearly identifiable incidents only. There is not an EU wide hub yet, but central incident reporting for major incidents will be explored (see recital 43 and Art. 19). Another element that is missing is the link with Anti-money laundering (AML), which digitisation is facilitating. The creation of a new AML agency, as the European Commission has proposed (EC, 2021), renders coordination with the Joint Committee more difficult, rather than keeping the task with EBA. A third critical element is data localisation. The draft forbids using critical ITPP based in (Art. 28.9) or subcontracting (Art. 31.1d) to a third country. As for the UK, as part of the Trade and Cooperation Agreement (TCA), it can, as a major financial centre, be part of the European data sphere, and decide whether to be a member of ENISA, thus allowing its be involvement to some degree in such a scheme. But this will need to be formally agreed upon, and will of course continue to have drawbacks due to the UK's status as a non-member state.

It should be recalled that CEPS was active on these matters early, with its reports on software vulnerability disclosure (Bouyon and Krause, 2018) and cybersecurity in the financial sector (Pupillo *et al.*, 2018). DORA goes a long way in bringing a harmonised approach to tackling cyber problems in the financial sector.

Table 1. Supervisory responsibilities under MiCA and DORA

		NCAs	ESAs
MiCA	Tokens	White Paper notification	
	Stablecoins	White Paper authorisation	Significant issuers supervised by EBA, and registered by ESMA
	E-money	Issuers	Significant issuers supervised by EBA
DORA		Incident reporting	ESAs as Lead Overseers
		ICT reporting of contractual engagements	ESAs Joint Committee for cross-border cooperation; ESAs as Lead Overseers

A DeFi regulatory sandbox

As part of the Digital finance package, the European Commission also proposed, somewhat surprisingly, the DLT infrastructures pilot regime, or EU-wide regulatory sandbox, for market infrastructures (or DeFi) based on DLT. It can be used by the DLT multilateral trading facility (MTF), by a DLT securities settlement system (SSS), by 'DLT market infrastructure', and by 'DLT transferable securities'. It has several exemptions from existing rules (such as the Central Securities Depositories Regulation, CSDR), but with ceilings as restrictions, and to be reviewed in five years. For DLT transferable securities, for example, the limit is €200 million, for a DLT market infrastructure, €2.5 bn. The pilot regime sets the operational requirements for these entities, the supervisory regime applicable, and the cooperation amongst authorities. This is the first time the Commission is using such a regime, to our knowledge.

Conclusions

With its digital finance strategy, the European Commission is embracing innovation in finance, aligning it with the single market and opening up access to the financial sector. Enhancing competition and market access in the retail and small business segments of EU financial markets remains a priority, and the ambition to facilitate payments and digital innovation in finance should be welcomed. Crypto and cyberware have made big inroads in finance, and will continue to shake up the supply and operation of financial services. Consumer and investor protection should be guaranteed, or they should at least be well informed, as many Europeans are involved as providers or customers.

The question remains, however, whether a specific regulatory response and new rules are needed for crypto-assets and 'cryptocurrencies' for still very rapidly evolving blockchain or distributed ledger technologies. For the Commission, most crypto-assets fall outside the scope of EU financial services legislation and therefore are not subject to the existing provisions on consumer and investor protection and market integrity, among others, although they give rise to these risks. And in regulating DLT-based providers, the Commission wants to place the EU at the forefront of change, as it is the first international jurisdiction to propose rules on the matter. Other regulators around the globe are following different approaches, however, or prefer to stand on the sidelines and watch.

Proposing new rules is a challenge for citizens and supervisors. The classification of the different tokens as proposed in MiCA is potentially very confusing for citizens, and a huge task to undertake for supervisors. What is the specific value of a token or a crypto-asset is difficult to know for a citizen. How are crypto-assets valued and what accounting or tax rules apply? What reliable sources of information exist about crypto-assets? Also for supervisors, the new tasks to monitor the different regimes, with different degrees of involvement, is an enormous challenge. They will need to understand the motives of investors and judge the intentions of the crypto providers.[15] They will need to judge whether financial stability will be affected, but will be unsure how to react in case of trouble. For the latter case, a clearer division of labour between (and among) the ESAs and the national authorities is required. The same applies to the DORA proposal: monitoring ICT companies is a substantial new task, as well for the ESAs, as for the NCAs.

Rather than amplifying and fragmenting regulatory schemes, it would have been preferable to bring crypto-assets as much as possible under the existing rules, with possible derogations. How will the different regulatory regimes apply with the new MiCA rules on the one hand, and the existing EU's prospectus rules for issuers, and the MiFID rules for service providers and trading platforms on the other. Is it appropriate to have a much lighter regime for crypto-asset trading platforms, or for market abuse and insider trading in crypto assets? Are stablecoins not alike to money market funds? In the MiCA draft, the reference is only made for e-money tokens, by limiting the issuance to those subject to the banking and e-money directives. The only piece of existing EU financial law with clear references to crypto-assets and platforms is the 5th AML Directive (2018), which will be reinforced by the new AML package adopted in July 2021. However, the valuation trigger for these assets remains a problem (apart from effective control over transactions).

The danger with a distinct regulatory set-up is the possibility for arbitrage, with clearly much lighter rules for crypto-asset providers and their platforms, than for providers of traditional financial instruments, and their platforms. It gives the impression that these are different financial products to which lighter forms of investor protection can apply, not those that already exist. And will investors notice the difference between an EU and a non-EU crypto-asset and offering, or with in the EU potentially forbidden products? For Europe to stimulate innovation in digital finance, investors need the same level of protection. **The EU will definitely need to follow up – and quickly – with its international counterparts and ensure both international consistency and cooperation**.

[15] See for example BIS (2021).

References

Amstad, M. (2019), "Regulating Fintech: Objectives, Principles, and Practices", Working Paper, No. 1016, October, Asian Development Bank.

Atzori, M. (2021), "Blockchain Technology and Decentralised Governance: Is the State Still Necessary?", *Journal of Governance and Regulation*, 6(1): 45-62.

Biais, B., C. Bisière, M. Bouvard and C. Casamatta (2021), "The Blockchain Folk Theorem", *Review of Financial Studies*, 32(5): 1662-1715.

BIS (2021), Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments by Raphael Auer and David Tercero-Lucas, BIS Working Papers No. 951, https://www.bis.org/publ/work951.pdf.

BIS-SIX-SNB (2020), "Project Helvetia: Settling Tokenised Assets in Central Bank Money", December, Bank for International Settlements, SIX Group AG, and Swiss National Bank.

Bouyon, S. and S. Krause (2018), "Cybersecurity in Finance: Getting the Policy Mix Right", Report of a CEPS-ECRI Task Force, June, Centre for European Policy Studies and European Credit Research Institute.

Casey, M., J. Crane, G. Gensler, S. Johnson and N. Narula (2018), "*The Impact of Blockchain Technology on Finance: A Catalyst for Change*", Geneva Reports on the World Economy, No. 21.

Central bank digital currencies for cross-border payments (2021), BIS, Report to the G-20, July, https://www.bis.org/publ/othp38.pdf.

Cong, L. and Z. He (2019), "Blockchain Disruption and Smart Contracts', *Review of Financial Studies*, 32(5): 1754-1797.

Dolmans, Maurits, Paul Glbert, John Messent, Mario Siragusa, Romano Subiotto (2019), "Payment services in the EU: price regulation to protect a duopoly", Competition Law Journal, Vol. 18, No. 4.

European Commission (2020), "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937", COM(2020) 593 final, September 24.

European Commission (2021), "Proposal for a Regulation of the European Parliament and of the Council Establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and Amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010", COM(2021) 421 final, June 20.

ECB (2021), Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021AB0004.

ECB (2021a), Digital euro experimentation scope and key learnings, https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf.

EPRS (2021), Updating the Crypto Assets Regulation and establishing a pilot regime for distributed ledger technology, PE 612.617 – March 2021.

Gallersdörfer, U., L. Klaaßen and C. Stoll (2020), "Energy Consumption of Cryptocurrencies Beyond Bitcoin", J*oule*, 4(9): 1843-1846.

Godschalk, H. (2021), "Crypto-Assets, Fiat Currency and Aa: Some Notes on the MiCAR", March 16, https://paytechlaw.com/en/crypto-assets-fiat-currency-micar/.

Iansiti, M. and K. Lakhani (2017), "The Truth About Blockchain: It will Take Years to Transform Business, but the Journey Begins Now", Harvard Business School, January-February.

Lannoo, Karel (2021), "Cyberfinance challenges require a common response", CEPS Policy Insight, No 2018/12, October https://www.ceps.eu/ceps-publications/cyber-finance-challenges-demand-unified-response/.

Lastra, Rosa and Jason Grant Allen (2019), Towards a European Governance Framework for Cryptoassets, SUERF Policy Note, November.

Lianos, I. (2019), "Blockchain Competition – Gaining Competitive Advantage in the Digital Economy: Competition Law Implications",in Hacker, P., I. Lianos, G. Dimitropoulos and S. Eich (eds.), "*Regulating Blockchain: Techno-Social and Legal Challenges*", Oxford University Press.

Martin, K. and B. Nauman (2021), "Bitcoin's Growing Energy Problem: 'It's a Dirty Durrency'", May 20, Financial Times, https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac.

Nabilou, H. (2019), "How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency", *International Journal of Law and Information Technology*, 27(3): 266-291.

Reinhardt, Nickolas (2021), DORA, Position Paper, Amcham, February.

Michèle Finck (2019), "Blockchain and General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?", EPRS study (STOA), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Nascimento, S. and A. Pólvora (2019), "Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies", Joint Research Centre.

Pike, C. and A. Capobianco (2020), "Antitrust and the Trust Machine", OECD Blockchain Policy Series, Organisation for Economic Co-operation and Development, November 4.

Pupillo, L., A. Ferreira and G. Varisco (2018), "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges", Report of a CEPS Task Force, June, Centre for European Policy Studies.

Reid, F. and M. Harrigan (2011), "An Analysis of Anonymity in the Bitcoin System", IIEEE International Conference on Privacy, Security, Risk, and Trust, October 9-11, Boston.

Thomadakis, Apostolos (2021), "How crisis-proof are financial market infrastructures?", ECMI event report, https://www.ecmi.eu/sites/default/files/event_report_operational_resilience.docx.pdf.

Villeroy de Galhau, François (2021), "Roads towards the future for CBDC and innovative payments" https://www.suerf.org/policynotes/29965/roads-for-the-future-central-bank-digital-currency-cbdc-and-innovative-payments.

Zetzsche, D., F. Annunziata, D. Arner and R. Buckley (2021), "The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy", *Capital Markets Law Journal*, 16(2): 203-225.

European Capital Markets Institute

ECMI conducts in-depth research aimed at informing the debate and policymaking process on a broad range of issues related to capital markets. Through its various activities, ECMI facilitates interaction among market participants, policymakers and academics. These exchanges are fuelled by the various outputs ECMI produces, such as regular commentaries, policy briefs, working papers, statistics, task forces, conferences, workshops and seminars. In addition, ECMI undertakes studies commissioned by the EU institutions and other organisations and publishes contributions from high-profile external researchers.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes around the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.