ECMI Policy Brief no 38 | July 2023

The EU's new crypto and cyber rules[1]

Karel Lannoo*

Executive Summary

Crypto currency matters are seemingly in the news every day, but the EU's new tailor-made regulatory regime is not. EU regulation is now in place 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 will also regulate and supervise the digital resilience of financial institutions. The EU's 'crypto regulation' is 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 updates the Lannoo, K. (2021), *Regulating crypto and cyber in the EU*, ECMI Policy Brief No 31, European Capital Markets Institute, and it is based upon the final texts of MiCA and DORA. It is also forthcoming in Adamski, D., Amtenbrink, F. and de Haan, J. (2023), *The Cambridge Handbook on European Monetary, Economic and Financial Integration*, Cambridge University Press.

- The new acts 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:

- 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 into financial intermediation, and several relatively new companies have a higher stock value 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 central bankers about the creation of a new asset outside the classic institutions. It has led several central banks 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, at the global or the European level. Innovation brings more competition and lowers costs for users; it creates new funding channels for enterprises, and more integration of payment systems. But unlike a decade ago with the response to the challenges posed by the Global Financial Crisis, views differ on how to deal with this development. 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 FinTech 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 supervised? What are the implications for financial institutions and central banks? What is the impact on financial inclusion and financial 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) . This complex piece of regulation covers three different forms of crypto-assets that are based on distributed ledger technology (DLT): non-fungible and utility tokens, asset-referenced tokens, and e-money tokens. In April 2023, the MiCA Regulation was adopted and entered into force in July 2023. The provision on stablecoins will become applicable from July 2024, with all others becoming applicable from January 2025.

Alongside MiCA, the Commission proposed the Digital Operational Resilience Act (DORA), aiming to set general rules for managing ICT and cybersecurity risks in the financial sector, including the oversight of third-party providers to strengthen business continuity. In November 2022, the DORA Regulation was adopted and came into force in January 2023. The regulation must now be transposed into national law no later than January 2025. Both pieces of legislation give important new tasks for the European Supervisory Authorities

(ESAs) and national authorities in supervising technology and its providers in the financial sector.

This policy brief discusses the EU's digital finance regulations in the context of the broader regulatory and supervisory structure at the 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 distinct 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 new rules 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 policymaking 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 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. This decentralised structure brings efficiencies (Nascimento and Pólvora, 2019; BIS-SIX-SNB, 2020)[1], promotes competition (Lianos, 2019; Pike and Capobianco, 2020), but also entails inefficiencies (Casey et al., 2018; Atzori, 2021). The 'tokenisation' of assets facilitates the processing of securities trades, as well as further automating and integrating the different steps post-trade. But it raises control and authorisation issues of these networks, which can consist of public permissionless and private permissioned blockchains[2]. DLT includes many different

[1] 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).

[2] 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

technologies, which are rapidly evolving, hence any clear description or definition remains difficult to 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 EU's MiCA Article 3.1(5) – '*a digital representation of a value or of a right that is able to be transferred and stored electronically, using distributed ledger or similar technology*' – is rather vague and broad. It certainly requires further clarification, as was highlighted by the European Central Bank (ECB). 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' – but have always been delayed. Some have compared it to the emergence of the World Wide Web in the early 1990s, 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 high energy prices and decarbonisation is a no-go[3].

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. Over the year 2021 and early 2022, the total value of outstanding crypto tokens fluctuated at around USD 2 trillion (roughly the same value as all US dollars in circulation, or double all euro banknotes in circulation) but it plunged to just below USD 1 trillion by mid-2022 and has fluctuated around that level since. This rapid emergence has impacted central banks' views on digital currencies. Until about the middle of 2018, central banks were cautiously 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 that central bank digital currencies could revolutionise the way money is provided and enhance the way monetary policy is concluded.

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. It eliminates intermediaries by allowing people, merchants, and businesses to conduct transactions through easily

---

it. Consequently, such a network has a defined governance structure and a varying degree of decentralisation but does not provide transparency.

[3] According to the Cambridge Bitcoin Electricity Index , Bitcoin's current yearly electricity consumption is at around 129 terawatt-hours (TWh) or at around 0.5 % of global electricity consumption. In fact, the bitcoin economy has more CO2 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 validates block transactions based on the amount of coins a miner holds (Gallersdörfer *et al*., 2020; Martin and Nauman, 2021).

accessible DLT technology. DeFi refers to financial services using smart contracts, which are automated enforceable agreements that operate entirely on blockchain networks, with tight security protocols and open connectivity, rather than through intermediaries like brokers or custodians. DeFi is seen to be more accessible, efficient, and transparent – a new way to disintermediate finance and 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 trigger specific security issues related to scalability and network congestion, as well as concentration of risk and interdependence. Moreover, the use of blockchain technology raises concerns about governance (who controls the protocol and where is it based?), about market abuse, inside information, and money laundering. DORA attempts to address some of the cyber-operational matters but the question remains whether the European Commission has taken consumer protection issues sufficiently into consideration, which is discussed below.

Regulatory Approaches to DLT

Definitional problems of DLT have prevented a consistent regulatory approach. In addressing DLT, the EU and regulators around the world have followed different approaches. This problem predates DLT, however, as payment systems – the most disruptive part in FinTech – have been undergoing deep change for the last two decades, following the emergence of e-commerce. This relates to the level-playing-field discussions and same risks-same rules debates, which are not easy to conclude. Payments traditionally formed a part of banking's functions but have expanded away from banks because of market developments.

Regulation has followed these developments, but not uncontested by the incumbents. The EU's first E-Money Directive was adopted in 2000 and the first Payments Services Directive (PSD) in 2007. Cross-border payments in the EU have been regulated since 2001 after long and protracted discussions with the banking sector on their costs. For a long time, high interchange fees for card-based payment transactions 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. But this remains contested, as some have argued that it maintains the credit card duopoly of Visa and Mastercard.

Payment transmitters can operate under several regulatory regimes, at the EU or global level. Regarding cryptocurrency schemes, they have worked under regulatory sandboxes at the local level, or were seen to be illegal, provided they did not qualify as a financial instrument under the Markets in Financial Instruments Directive (MiFID), the EU regulation concerning investment services providers. With MiCA, the European Commission wants to fill the void and set a common EU approach for DLT-based operators, ensuring consumer and investor protection, and market integrity. However, the question emerges why the EU has not tried to cover crypto-assets and cryptocurrencies under existing rules, as is the approach taken in the United States and Hong Kong, rather than creating another new

regime for a still emerging and fast-changing technology[4]. Moreover, the EU has brought three distinct forms of crypto-based services under one draft regulation, instead of having them under separate rules. In doing so, the EU is contributing to regulatory complexity, rather than reducing it.

It could be argued that the EU'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 specific regulation. For example, contracts that automate contingent transfers depending on the success of delivering goods or services can pose new risks of collusion. Through the decentralised consensus, sellers will have greater knowledge of aggregate business conditions on the blockchain, which could lead to tacit collusion among sellers.

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. In an ideal blockchain, there is a single sequence of blocks, with each of them offering an updated version of the ledger (taking the most recent transactions into account), 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. Finally, a new functionality also arises from decentralisation, which makes it easier to benefit from regulatory arbitrage (Amstad, 2019; Nabilou, 2019).

EU Crypto Regulation under MiCA

MiCA provides for a broad definition of crypto-assets and stablecoins, sets rules on their providers, including the trading platforms, and defines the role of supervisors. Crypto-assets include three groups: (1) utility tokens, (2) asset-referenced tokens, and (3) e-money tokens, with the lightest rules for the first group. Utility tokens provide digital access to a specific good or service, thus they are non-fungible tokens (NFT). Under DLT, NFTs are uniquely identifiable representations of information, art, music, etc., providing strong intellectual property protection. Asset-referenced tokens are the so-called 'stablecoins', coins that reference baskets of currencies or commodities. An e-money token is also a stablecoin, but they are like traditional e-money, meaning they should have a fixed value to a hard currency. The rules will not apply to security tokens that are already subject to an existing EU regulatory regime, or to central bank digital currencies, as discussed below.

Specific stipulations of MiCA include:

- Providers of crypto-assets and utility or non-fungible tokens, or virtual gadgets, shall draw up a 'crypto-asset white paper' for notification to the authorities before

[4] See the speeches by Gary Gensler of the SEC on the US approach, asserting crypto-assets should be regulated the same way as existing securities under existing securities laws, whereas the industry argues for a new approach (e.g. the speech on Crypto Markets given at the Penn Law Capital Markets Association Annual Conference on 4 April 2022). 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.

issuing and commercialising 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 be allowed to benefit from a European passport. There is no formal *ex ante* approval requirement (Article 8(3): '*Competent authorities shall not require prior approval of crypto-asset white papers, nor of any marketing communications relating thereto before their respective publication*'), which is justified by the goal of not placing excessive burdens on supervisors (Recital 6).

- Issuers of asset-referenced tokens or stablecoins must be formally authorised. They shall respect a minimum capital of EUR 350 000 and an ongoing capital requirement of 2 % of the average amount of the reserve 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 value stabilisation mechanism, or the investment policy (Article 36.8d), including among others '*the procedure by which the asset-referenced tokens are issued and redeemed, and the procedure by which such issuance or redemption will result in the corresponding increase and decrease in the reserve of assets*'. This also raises issues of custody of these assets, which is detailed in Article 36. Furthermore, issuers need to meet governance and conduct rules –minimum operational requirements for the managers of a crypto platform (Article 76).

- 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 2009 E-Money Directive. 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. The EBA chairs the supervisory colleges for these crypto-assets (with national competent authorities (NCAs), the European Securities and Markets Authority (ESMA), and the ECB), with the frequency of meetings to be determined. 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, of which it needs to establish a register. The complexity of this set-up led the European Parliament in its reading to ask for a clearer, better-defined role for the ESAs.

The regime for third-country issuers is highly 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 shall be leading the supervisory college, with no voting rights for third countries. Third-country providers will thus need to fully conform to EU rules if they want to sell

cryptocurrencies in the EU. 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 under the MiCA Regulation.

Rules on the prohibition of market abuse, insider trading, and market manipulation will apply (Title VI of MiCA Regulation), but they are much lighter than the existing rules applicable to securities markets operators. According to Recital 95, 'Issuers of crypto-assets and crypto-asset service providers are very often SMEs, it would be disproportionate to apply all of the provisions of Regulation (EU) No 596/2014' (i.e. the Market Abuse Regulation). Hence a crypto trading platform that clears crypto-asset transactions can be created very easily without a high regulatory burden. The question remains whether this is justified.

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 securities markets law, in particular the prospectus rules and MiFID. In practice, MiCA will apply, unless it is within the scope of MiFID, which creates ample scope for arbitrage. The same lack of clarity exists for crypto trading platforms, where the question will emerge whether a MiFID licensed trading platform can trade crypto, or whether it should be authorised separately under MiCA. Because of this complexity, some have called MiCA 'a job-creation programme for lawyers'. 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. Compared to this, the approach of the US Securities and Exchange Commission (SEC) is more straightforward. It checks whether the basic objectives of the Securities Act of 1933 and the Securities Exchange Act of 1934 are respected, the protection of investors and the orderly functioning of markets, irrespective of new market functionalities[5].

The EU would have been better off to consider crypto under existing laws, rather than creating a new regulatory framework. This means applying prospectus rules for issuers and MiFID for crypto-assets service providers (considering these as financial instruments, not as a separate class of assets); and applying e-money, FinTech, or banking rules for digital money. NFTs do not require sperate rules but can be covered under existing consumer or intellectual property legislation. This would be much easier for consumers as well as regulators. Market and conduct of business rules should apply regardless of the 'packaging'.

Instead, it will take another 18 months, until the end of 2024, before the new rules will apply. After the publication of the new MiCA rules in the EU Official Journal on 9 June, some 18 different pieces of level 2 legislation or guidelines will have to be adopted by EBA and the European Commission. In the meantime, markets have moved on, and many citizens

[5] It needs to be added that there was a lot of criticism on the SEC because of its late reaction on crypto, which was clear following the collapse of the crypto trading platform FTX.

have been defrauded by crypto scams with only unclear redress procedures available to them[6].

Where Does the CBDC Fit into the Picture?

Central bank digital currency has added to the confusion about cryptocurrency. In the case of the large, well-established central banks, a CBDC will be nothing else than digital money but now directly issued by the central bank as legal tender, with the practical modalities still to be decided upon. In some developing countries, on the contrary, a CBDC resembles a stablecoin, where the composing parts and reserves will need to be controlled. It could be an 'illegal' tender if the rules or governance cannot guarantee the tender's stability. But whether these CBDCs will be based upon DLT remains to be seen. In principle, they are at opposite ends of the spectrum, as a DLT-based system is decentralised by definition, whereas a CBDC is not.

After a lengthy consultation phase, the ECB's Governing Council decided on 14 July 2021 to launch an investigation phase of a digital euro project that will last two years. The project also considers changes to the EU's legislative framework that might be needed. 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 store their digital currency with the central bank, it will be a further threat to the traditional retail banks for which payments in all their forms are a core part of their business, contributing to around one-quarter of their revenues.

The Federal Reserve and the People's Bank of China (PBoC) are also examining digital currencies. In the US, a 9 March 2022 Executive Order issued by President Biden supports the potential of CBDC and asked for a report on the possible design options, while insisting upon the benefits for the efficiency of payments systems and consumer protection. In China, the PBoC already has e-CNY pilot schemes involving private citizens running as a reaction against the blockchain-based currencies that are decentralised by definition.

The digital euro impacts core and critical bank regulatory matters. It could facilitate financial inclusion, although financial literacy will remain an issue, as the onus will be on central banks to explain the functioning of CBDCs. Access to and the cost of bank accounts for European citizens has long been a matter of concern for consumer lobbies, as it determines overall societal participation in the financial system. But direct 'accounts' at the central bank could threaten the stability of the financial system, as only central bank accounts may be seen to be safe. A 'bank run' in a system with a CBDC may thus provoke even more volatility and could lead to the total gridlock of the financial system. It would profoundly alter the liquidity transformation function of commercial banks, as banks would no longer be the main storage point for money, which could lead to liquidity shortages in times of stress. Creating a CBDC could mean the end of commercial banking as we know it, as the central

[6] In its work programme for 2023, EBA commits to work together with the other ESAs to develop and deepen the digital risk management dimension of the Single Rulebook, and contribute to a consistent framework for the regulation and supervision of crypto-asset activities.

bank would become the focal point of retail accounts, causing commercial banks' key loan function to essentially disappear. This would profoundly change the role of markets in a financial system.

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 in contrast with its statute and origin as a 'narrow' central bank, focusing on monetary policy and price stability. Payments systems raise a host of microeconomic and allocative efficiency issues – how to get cash, in which form, and where – beyond merely the payment assets, which are not core to the ECB's mandate, and which globally active providers can do better. The ECB is a supervisor of payment systems, not an operator, which is the task of private agents. Central banks should only monitor these markets based on their financial stability mandate.

Data protection and privacy matters will also be affected by a CBDC. Control on illicit activities and money laundering are raised as a big advantage of the digital euro, because of the technology used (i.e., DLT), which allows transactions to be traced back to users through the digital identities (e-ID) and digital signature components. However, this brings the 'Big Brother' state much closer to reality. Moreover, it is by no means certain that the ECB, let alone the EU-27, will manage to get all its members aligned on these matters. Some Member States may wish the digital euro to be a substitute for cash, with less traceability than DLT allows. The discussions on the Commission's latest AML package demonstrate that more restrictions on cash payments remains very sensitive, not the least in Germany.

Cyber Resilience Rules in DORA

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 of cyber-attacks. 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 ICT providers into the financial supervisory domain. The challenge here is to find the right balance in financial supervision in an ecosystem where tech companies are increasingly important actors for the effective provision of financial services, and to maintain a clear separation between both.

DORA's principle-based approach aims to streamline the provisions of financial legislation to create a minimum baseline for the digital operational resilience of the financial sector, and hence financial stability. It completes the existing but generic Network of Information Systems Directive (NISD)[7], with much more detailed provisions and oversight. Furthermore,

[7] The Directive sets overall standards for cybersecurity in society and the economy, with a central role for the European Union Agency for Cybersecurity (ENISA).

it aims to cover almost the entire financial sector, including crypto-asset providers, and address 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, the proportionality of application is embedded in the rules and addressed by specific exemptions[8]. As for supervising DORA's application, this is up to the competent responsible authorities as defined in the respective EU legislation, which may be the ECB, specialised or generic financial supervisory authorities.

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., all elements that had not previously been clearly defined for the financial sector, and which will allow for a better framing of the risk.

- 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. Firms are required to set risk tolerance for ICT disruptions, they must identify their 'Critical or Important Functions' (CIFs) and map their assets and dependencies.

- Procedures for stress testing of cyber resilience, vulnerability disclosure, and incident reporting, including cyber-attacks. These are based on common templates, building upon the work already undertaken by the ECB (in its so-called Threat Intelligence-based Ethical Red Teaming (TIBER-EU) framework). Firms will need to assess the quantitative impact of incidents and analyse their root cause. Reporting deadlines to NCAs will be specified in technical standards.

- Procedures for ICT third-party service providers (ITPP) that are critical for financial entities, with a clear division of responsibilities, and reporting to authorities of contractual arrangements, with a definition of the required provisions (Article 28).

- The ESAs – based upon systemic stability criteria – will designate the ITPP that are critical for financial entities. EBA, ESMA, or the European Insurance and Occupational Pensions Authority (EIOPA) will be appointed as their Lead Overseers, with on-site inspections (Article 36), covered by fees charged to the ICT providers.

- 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

[8] 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).

of cybersecurity risks. A Joint Oversight Forum as a specialised ICT subcommittee will 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 in delegated acts. Only clearly identifiable incidents should be reported. DORA refrains from proposing an EU-wide cyber hub, but central incident reporting for major incidents will be explored (see Recital 53 and Article 19). Another element that is missing is the link with the fight against money laundering, which digitalisation is facilitating. A new AML agency, as the European Commission has proposed, will require close cooperation with the Joint Committee to facilitate action in this domain.

A third critical element for DORA is data localisation. The Act prohibits using critical ITPP only based in (Article31.12) or subcontracting (Recital 67) to a third country. With regards to the United Kingdom, 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 involvement to some degree in such a scheme. But this will need to be formally agreed and will have drawbacks due to the United Kingdom's status as a non-Member State.

DORA goes a long way towards developing a truly harmonised approach to tackling cyber problems in the financial sector. It was formally adopted in October 2022, but it will take another two years before the provisions will apply in full, as 12 different Level 2 mandates will need to be substantiated in both technical standards and delegated acts in the 18 months following adoption. Table 1 gives an overview of the new digital supervisory responsibilities under both acts.

Table 1. Supervisory responsibilities under MiCA and DORA

	Crypto-assets	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	Cyber-attacks	Incident reporting	ESAs as Lead Overseers for critical third-party ICT providers
	Third-party service providers (TPP)	Reporting of ICT 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 introduced the DLT infrastructures pilot regime regulation, or an EU-wide regulatory sandbox, for market infrastructures (or DeFi) based on DLT. It can be used by a DLT multilateral trading facility, a DLT securities settlement system, a DLT market infrastructure for DLT transferable securities, market facilities as defined in EU law. It has several exemptions from the existing rules (such as the Central Securities Depositories Regulation), but with thresholds over which the structures cannot be used, and to be reviewed in five years. For example, the limit for DLT transferable securities is EUR 200 million, while for a DLT market infrastructure EUR 2.5 billion. The pilot regime sets the operational requirements for these entities, the supervisory regime applicable, and the cooperation amongst authorities in the EU. This is the first time the Commission is using such a regime, to our knowledge, but it has been used in Member States for some time, with varying degrees of success. It facilitated innovation in some, such as the United Kingdom, but much less in other states, such as France.

Conclusions

With its digital finance strategy, the European Commission is embracing innovation in finance, aligning it with the single market and further facilitating access to finance. Enhancing competition and market access in the retail and small business segments of EU financial markets is a priority for the EU, 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, and payments in particular. 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 were needed for crypto-assets and cryptocurrencies for still very rapidly evolving blockchain or distributed ledger technologies. For the EU Commission, most crypto-assets fall outside the scope of EU financial services legislation and are therefore not subject to the existing provisions on consumer and investor protection and market integrity, among others, although they give rise to 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 introduce rules on the matter. Other regulators around the globe are following different approaches, however, and prefer to stand on the side-lines or prohibit cryptocurrencies.

MiCA's proposed classification system for all the different tokens is very confusing for citizens and a huge new task for supervisors. The value of a token or a crypto-asset is difficult to know for a citizen: How are they valued and what accounting or tax rules apply? What are reliable sources of price information about crypto-assets? What is a stablecoin, what is e-money, and what is a CBDC? Keeping e-money out of the MiCA regulation could have made it easier to understand that crypto is about a highly speculative and volatile asset, not money.

For supervisors, the new tasks to monitor the different regimes, with different degrees of involvement, is also an enormous challenge. They will need to understand the motives of investors and judge the intentions of the crypto providers (BIS, 2021). They should assess whether consumer protection and financial stability will affected but will be unsure how to react in case of trouble, as they may not have all the necessary information to make the best decision on how to respond. In the latter case, a clearer division of labour between (and among) the ESAs and the national authorities is required. The same applies to DORA – monitoring the cyber resilience of financial services firms and their third-party ICT providers is a substantial new task, for the ESAs, as well as for the NCAs, let alone central banks. More centralisation of tasks would be better, given the competences needed.

Rather than amplifying and fragmenting the 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 investment 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 like money market funds? In the MiCA regulation, the reference to existing law is only made for e-money tokens, by limiting the issuance to those subject to the banking and e-money directives.

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, rather than those that already exist. And will investors notice the difference between EU and non-EU crypto-assets and offerings, or are the products potentially forbidden in the EU? 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.

References

AmCham (2023), *DORA: Potential overlaps with other legislation and implementation challenges*, Position Paper, https://www.amchameu.eu/system/files/position_papers/amchameu_dora_potential_overlaps_with_other_legislation_final.pdf.

Amstad, M. (2019), *Regulating FinTech: Objectives, principles, and practices*, ADBI Working Paper No 1016, Asian Development Bank Institute, October, https://www.adb.org/sites/default/files/publication/533791/adbi-wp1016.pdf.

Atzori, M. (2021), 'Blockchain technology and decentralised governance: Is the state still necessary?', *Journal of Governance and Regulation*, Vol. 6, Issues 1, pp. 45–62.

Bindseil, U., Papsdorf, P. and Schaaf, J. (2022), *The encrypted threat: Bitcoin's social cost and regulatory responses*, SUERF Policy Note, Issue No 262, January, https://www.suerf.org/docx/f_88b3febc5798a734026c82c1012408f5_38771_suerf.pdf.

BIS (2021), *Central bank digital currencies for cross-border payments*, Report to the G20, Bank for International Settlements, July, https://www.bis.org/publ/othp38.pdf.

BIS-SIX-SNB (2020), *Project Helvetia: Settling tokenised assets in central bank money*, Bank for International Settlements, SIX Group AG, and Swiss National Bank, December, https://www.snb.ch/en/mmr/reference/project_helvetia_phase_II_report/source/project_helvetia_phase_II_report.en.pdf.

Bouyon, S. and Krause, S. (2018), *Cybersecurity in finance: Getting the policy mix right*, Report of a CEPS-ECRI Task Force, Centre for European Policy Studies and European Credit Research Institute, 6 June, https://www.ceps.eu/ceps-publications/cybersecurity-finance-getting-policy-mix-right/.

Casey, M., Crane, J., Gensler, G., Johnson, S. and Narula, N. (2018), *The impact of blockchain technology on finance: A catalyst for change*, Geneva Reports on the World Economy 21, 7 December, https://cepr.org/system/files/publication-files/60142-geneva_21_the_impact_of_blockchain_technology_on_finance_a_catalyst_for_change.pdf.

De la Mata, A. (2022), 'Blockchain, NFT y la indefinicion juridica', *La Lectura*, https://blockchainintelligence.es/wp-content/uploads/2022/02/Blockchain-NFT-y-la-indefinicion-juridica.pdf.

ECB (2021), *Digital euro experimentation scope and key learnings*, European Central Bank, 14 July, https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf.

Finck, M. (2019), *Blockchain and general data protection regulation: Can distributed ledgers be squared with European data protection law?*, EPRS Study, European Parliamentary

Research Service, www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Gallersdörfer, U., Klaaßen, L. and Stoll, C. (2020), 'Energy consumption of cryptocurrencies beyond bitcoin', *Joule*, Vol. 4, Issue 9, pp. 1843–1846.

Lannoo, K. (2021), *Cyber finance challenges require a common response*, CEPS Policy Insight No 2018/12, Centre for European Policy Studies, 25 October, https://www.ceps.eu/ceps-publications/cyber-finance-challenges-demand-unified-response/.

Lannoo, K. (2022), 'The EU's proposed crypto regulations are flawed', *Financial Times*, 16 May, https://www.ft.com/content/83ddff31-fb9a-4765-becf-82a52cc7291d.

Allen, J. and Lastra, R. (2019), *Towards a European governance framework for cryptoassets*, SUERF Policy Note, Issue No 110, November; https://www.suerf.org/policynotes/7839/towards-a-european-governance-framework-for-cryptoassets.

Lianos, I. (2019), 'Blockchain competition – gaining competitive advantage in the digital economy: Competition law implications', in Hacker, P., Lianos, I., Dimitropoulos, G. and Eich, S, (eds.), *Regulating Blockchain: Techno-Social and Legal Challenges*, Oxford University Press, Oxford, pp. 329.

Martin, K. and Nauman, B. (2021), 'Bitcoin's growing energy problem: 'It's a dirty durrency'', Financial Times, 20 May, 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*, Vol. 27, Issue 3, pp. 266–291.

Nascimento, S. and Pólvora, A. (2019), *Blockchain now and tomorrow: Assessing multidimensional impacts of distributed ledger technologies*, Joint Research Centre, European Commission, https://publications.jrc.ec.europa.eu/repository/handle/JRC117255.

Pike, C. and Capobianco, A. (2020), *Antitrust and the trust machine*, OECD Blockchain Policy Series, Organisation for Economic Co-operation and Development, 4 November, https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

Pupillo, L., Ferreira, A. and Varisco, G. (2018), *Software vulnerability disclosure in Europe: Technology, policies and legal challenges*, Report of a CEPS Task Force, Centre for European Policy Studies, 28 June, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.

Thomadakis, A. (2021), *How crisis-proof are financial market infrastructures?*, ECMI Event Report, European Capital Markets Institute, 25 January, https://www.ecmi.eu/sites/default/files/event_report_operational_resilience.docx.pdf.

Villeroy de Galhau, F. (2021), *Roads towards the future for CBDC and innovative payments*, SUERF Policy Note, Issue No 250, August, https://www.suerf.org/policynotes/29965/roads-for-the-future-central-bank-digital-currency-cbdc-and-innovative-payments.

Zandersone, L. (2021), *Updating the Crypto Assets Regulation and establishing a pilot regime for distributed ledger technology*, PE 612.617, European Parliamentary Research Service, March, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662617/EPRS_BRI(2021)662617_EN.pdf.

European Capital Markets Institute

ECMI conducts in-depth research aimed at informing the public 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, supervisors and academics. These exchanges result in commentaries, policy briefs, working papers, task forces as well as conferences, workshops and seminars. In addition, ECMI undertakes studies externally commissioned by the EU institutions and other organisations, and publishes contributions from high-profile guest authors.

Centre for European Policy Studies

CEPS is widely recognised as one of the most experienced and authoritative think tanks operating in the EU. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe and to maintaining the highest standards of academic excellence and unqualified independence. It also provides a forum for discussion among all stakeholders in the European policy process that is supported by a regular flow of publications offering policy analysis and recommendations.