

STUDY

Requested by the ECON Committee



# Remaining regulatory challenges in digital finance and crypto-assets after MiCA

---



Policy Department for Economic, Scientific and Quality of Life Policies  
Directorate-General for Internal Policies  
Authors: D.A. Zetzsche, R.P. Buckley, D.W. Arner, M.C. van Ek  
PE 740.083 – May 2023

EN



# Remaining regulatory challenges in digital finance and crypto-assets after MiCA

---

## **Abstract**

This study analyses the need to adopt further EU financial regulation on decentralized finance after the implementation of the Markets in Crypto Asset Regulation and the revision of the Transfer of Funds Regulation, with a special view on crypto lending, crypto staking, crypto custody, the use of non-formal information, NFTs and sustainability.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the Committee on Economic and Monetary Affairs (ECON).

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs (ECON).

## **AUTHORS**

Prof. Dr Dirk A. Zetsche, ADA Chair in Financial Law (inclusive finance), University of Luxembourg

Prof. Dr Ross P. Buckley, ARC Laureate Fellow and KPMG-KWM Professor of Disruptive Innovation, UNSW Sydney

Prof. Dr Douglas W. Arner, Kerry Holdings Professor in Law and RGC Senior Fellow in Digital Finance and Sustainable Development, University of Hong Kong

Maurits C. van Ek, LL.M., ADA Chair in Financial Law (inclusive finance), University of Luxembourg

*We acknowledge valuable comments and support by Areti Kolovou Nikolakopoulou, Stamatia Stylianopoulou, Carmen Preda, Louisa Künzel, Dr. Jannik P. Woxholth, Dr. Julia Sinnig and Dr. Marco Bodellini.*

## **ADMINISTRATOR RESPONSIBLE**

Radostina PARENTI

## **EDITORIAL ASSISTANT**

Marleen LEMMENS

## **LINGUISTIC VERSIONS**

Original: EN

## **ABOUT THE EDITOR**

Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:

Policy Department for Economic, Scientific and Quality of Life Policies

European Parliament

L-2929 - Luxembourg

Email: [Poldep-Economy-Science@ep.europa.eu](mailto:Poldep-Economy-Science@ep.europa.eu)

Manuscript completed: April 2023

Date of publication: May 2023

© European Union, 2023

This document is available on the internet at:

<http://www.europarl.europa.eu/supporting-analyses>

## **DISCLAIMER AND COPYRIGHT**

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

For citation purposes, the publication should be referenced as: Zetsche/Buckley/Arner/van Ek, *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*, publication for the Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

© Cover image used under licence from Adobe Stock

## CONTENTS

<b>LIST OF BOXES</b>	<b>6</b>
<b>LIST OF FIGURES</b>	<b>6</b>
<b>LIST OF TABLES</b>	<b>6</b>
<b>LIST OF ABBREVIATIONS</b>	<b>7</b>
<b>EXECUTIVE SUMMARY</b>	<b>13</b>
<b>1. INTRODUCTION</b>	<b>21</b>
<b>2. DECENTRALIZED FINANCE AND THE CRYPTO WINTER</b>	<b>22</b>
2.1. The term decentralized finance: “DeFi”	22
2.2. Traditional finance vs decentralized finance	23
2.2.1. Intermediaries and centralization in traditional finance	23
2.2.2. DeFi as counter model to traditional finance	23
2.3. Underlying technology	24
2.3.1. Exponential growth of data processing, storage and bandwidth capacity	24
2.3.2. Technical pillars of DeFi	24
2.3.3. The DeFi Stack	26
2.3.4. Centralization vs decentralization	27
2.4. The crypto industry	29
2.4.1. Use cases and industry characteristics	29
2.4.2. Interlinkages to traditional finance	29
2.4.3. Size of the industry	32
2.5. The Crypto Winter of 2022-23	33
2.5.1. Large-scale asset diversions starting in 2021	33
2.5.2. Terra/Luna collapse	35
2.5.3. Bankruptcies of SICs	36
2.5.4. In particular: FTX	38
2.5.5. All service models affected	40
<b>3. SUPERVISORY AND REGULATORY CHALLENGES OF CRYPTO</b>	<b>42</b>
3.1. Traditional risks of finance in crypto	42
3.1.1. Financial stability	42
3.1.2. Market efficiency and transparency	43
3.1.3. Client, depositor and investor protection	44
3.1.4. Market fairness and integrity	45
3.2. Partial decentralization: a crypto idiosyncrasy	46

3.2.1. Custody	46
3.2.2. Crypto stacking	47
3.2.3. Insolvency and resolution	48
3.2.4. Jurisdiction and applicable laws	49
3.2.5. Enforcement	50
3.2.6. Private law	51
3.2.7. Increasing tech-risk	52
3.3. In depth: crypto lending	52
3.3.1. Functions and structure of crypto lending	52
3.3.2. Facts and figures	56
3.3.3. Legal assessment	59
3.3.4. Regulatory challenges	61
3.4. In depth: crypto staking	64
3.4.1. Functions and services	64
3.4.2. Risk-benefit analysis	68
3.4.3. Regulatory challenges	69
3.5. In depth: sustainability impact	70
3.5.1. Crypto and sustainability	70
3.5.2. Centralized vs decentralized	72
3.6. In depth: use of non-formalized information (social media etc.)	74
3.6.1. Referral programmes and social network expansion	74
3.6.2. Social media	76
3.6.3. Outright circumvention of laws	77
3.6.4. Insider dealing and market manipulation	77
3.7. Non-financial regulatory challenges	78
<b>4. STATUS QUO PRIOR TO MICA AND THE REVISED TFR</b>	<b>79</b>
4.1. Ambiguity and legal uncertainty	79
4.1.1. Three categories of crypto-assets	79
4.1.2. Divergent application	80
4.1.3. Under-enforcement of existing EU financial law	81
4.2. Global stablecoins	81
4.3. AML/CTF concerns	82
<b>5. IMPACT OF MICA AND TFR</b>	<b>83</b>
5.1. Beneficial impact of MiCA	83
5.1.1. Gap-filling regarding the scope of EU financial law	83
5.1.2. Licensing, conduct of business, prudential regulation and supervision of crypto intermediaries	83

5.1.3. Disclosure and transparency	84
5.1.4. Segregation and custody	85
5.1.5. Fraud and market abuse	88
5.2. Remaining challenges under MiCA	89
5.2.1. Delineating scope	89
5.2.2. Periodic disclosures and accounting	90
5.2.3. Restructuring and resolution legislation	91
5.2.4. Cross-border harmonization and coordinated enforcement	92
5.3. Impact of Transfer of Funds Regulation (TFR)	92
5.3.1. In-scope transactions	92
5.3.2. Gap analysis	93
5.4. In depth: financial NFTs	96
5.4.1. Functions and structure of financial NFTs	96
5.4.2. Facts and figures	98
5.4.3. Work of international standard setters on NFTs	100
5.4.4. NFTs vs scope of MiCA	100
5.4.5. Remaining risks	103
<b>6. POLICY CONSIDERATIONS</b>	<b>105</b>
6.1. Work of global standard setters (IOSCO, BIS, IMF, FATF, FSB)	105
6.2. Capturing cross-border crypto	107
6.2.1. Solicitation cloaked as reverse solicitation	107
6.2.2. Broad default rule for scope and definitions	110
6.2.3. Cross-border cooperation among regulators	114
6.3. Addressing (partial) decentralization	115
6.3.1. Decentralized platforms and entity status for DAOs	115
6.3.2. Private law	118
6.3.3. Court jurisdiction, choice of law	118
6.4. NFTs	118
<b>7. CONCLUSIONS</b>	<b>120</b>
<b>REFERENCES</b>	<b>121</b>

## LIST OF BOXES

Box 1: DeFi and the patterns of technological evolution	24
Box 2: Distributed ledgers - modus operandi	26
Box 4: Enforcement in decentralized finance, part 2	51

## LIST OF FIGURES

Figure 1: Distributed ledger	25
Figure 2: DeFi Stack	27
Figure 3: Value Destruction in the Terra/Luna Collapse	36
Figure 4: Crypto bankruptcies by gross liabilities	37
Figure 5: Crypto Lending	53
Figure 6: Size of decentralized lending activity by way of DeFi protocols	56
Figure 7: Terms of Celsius crypto lending	60
Figure 8: International standard setters on crypto lending	62
Figure 9: US Securities and Exchange Commission on staking	69
Figure 10: International Standard Setters on Sustainability	72
Figure 11: International standard setters on use of non-formalized information	74
Figure 12: Statement by CFTC Commissioner (CFTC v Binance)	77
Figure 13: International standard setters on crypto custody	85
Figure 14: NFT trading volume (2022-23)	99
Figure 15: NFT trading volume per 24 Hours (01-03-2023)	99
Figure 16: International standard setters on NFTs	103
Figure 17: The “default rule”	110

## LIST OF TABLES

Table 1: Major Asset Diversions	34
Table 2: Major Decentralized Lending Protocols	57
Table 3: EU-Active centralized crypto lending intermediaries	59
Table 4: Staking on Blockchains with a market capitalization above USD 1 billion	64



## LIST OF ABBREVIATIONS

<b>3AC</b>	Three Arrows Capital
<b>ADA</b>	Cardano (Ada) (cryptocurrency)
<b>AI</b>	Artificial Intelligence
<b>AIF</b>	Alternative Investment Fund
<b>AIFMD</b>	Directive 2011/61/EU on Alternative Investment Fund Managers (Alternative Investment Fund Managers Directive)
<b>AML</b>	Anti-Money Laundering
<b>AMLD</b>	Anti-Money Laundering Directive
<b>AMLD5</b>	5th Anti-Money Laundering Directive
<b>APR</b>	Annual Percentage Rate
<b>ART</b>	Asset-Referenced Tokens
<b>BIS</b>	Bank for International Settlements
<b>BNB</b>	Binance Coin (cryptocurrency)
<b>BRRD</b>	Bank Recovery and Resolution Directive
<b>BTC</b>	Bitcoin (cryptocurrency)
<b>CASP</b>	Crypto-Asset Service Provider
<b>CBDC</b>	Central Bank Digital Currency
<b>CDS</b>	Credit Default Swap
<b>CeFi</b>	Centralized Finance
<b>CEX</b>	Centralized Exchange
<b>CFTC</b>	Commodity Futures Trading Commission
<b>CNBC</b>	Consumer News and Business Channel
<b>CRD</b>	Capital Requirements Directive

<b>CRR</b>	Capital Requirements Regulation
<b>CTF</b>	Counter-Terrorist Financing
<b>DAO</b>	Decentralized Autonomous Organisation
<b>DeFi</b>	Decentralized Finance
<b>DEX</b>	Decentralized Exchange
<b>DLT</b>	Distributed Ledger Technology
<b>EBA</b>	European Banking Authority
<b>ECB</b>	European Central Bank
<b>EEA</b>	European Economic Area
<b>eIDASR</b>	Regulation (EU) No 910/2014 on electronic identification and trust services in the internal market
<b>EMD</b>	Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (E-Money Directive)
<b>EMT</b>	Electronic Money Tokens
<b>EP</b>	European Parliament
<b>ERC</b>	Ethereum Request for Comment (token standard)
<b>ESA</b>	European Supervisory Authority
<b>ESG</b>	Environmental, Social, and Governance
<b>ESMA</b>	European Securities and Markets Authority
<b>ETF</b>	Exchange Traded Fund
<b>ETH</b>	Ether (cryptocurrency)
<b>EU</b>	European Union
<b>EUR</b>	Euro (fiat currency)
<b>FAQ</b>	Frequently Asked Question

<b>FATF</b>	Financial Action Task Force
<b>FDIC</b>	Federal Deposit Insurance Corporation
<b>FinFluencer</b>	Financial Influencer
<b>FinTech</b>	Financial Technology
<b>FSB</b>	Financial Stability Board
<b>FTT</b>	FTX Token (cryptocurrency)
<b>GameFi</b>	Game Finance
<b>GBTC</b>	Grayscale Bitcoin Trust
<b>GDPR</b>	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
<b>GFC</b>	Global Financial Crisis
<b>GHG</b>	Green-House Gas
<b>ICO</b>	Initial Coin Offering
<b>IMF</b>	International Monetary Fund
<b>IOSCO</b>	International Organization of Securities Commissions
<b>KYC</b>	Know Your Customer
<b>LoLR</b>	Lender of Last Resort
<b>LP</b>	Liquidity Provider / Pool
<b>LTV</b>	Loan-to-Value
<b>LUNA</b>	Luna (cryptocurrency)
<b>LUNC</b>	Luna Classic (cryptocurrency)
<b>MAR</b>	Regulation (EU) No 596/2014 on market abuse (Market Abuse Regulation)
<b>MATIC</b>	Matic (cryptocurrency)

<b>MiCA</b>	Markets in Crypto-Assets Regulation
<b>MiFID</b>	Directive 2014/65/EU on markets in financial instruments (Market in Financial Instruments Directive)
<b>MMF</b>	Money Market Fund
<b>MMoU</b>	Multilateral Memorandum of Understanding
<b>MoU</b>	Memorandum of Understanding
<b>NCA</b>	National Competent Authority
<b>NEXO</b>	Nexo (cryptocurrency)
<b>NFT</b>	Non-Fungible Token
<b>NYU</b>	New York University
<b>OECD</b>	Organization for Economic Co-operation and Development
<b>OP</b>	Operational Programme
<b>ORF</b>	Observer Research Foundation
<b>PoR</b>	Proof of Reserves
<b>PoS</b>	Proof-of-Stake
<b>PoW</b>	Proof-of-Work
<b>Prospectus Regulation</b>	Regulation (EU) 2017/1129 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market
<b>PSD2</b>	Directive (EU) 2015/2366 on payment services in the internal market (Revised Payment Services Directive)
<b>PWC</b>	PricewaterhouseCoopers
<b>RegTech</b>	Regulatory Technology
<b>RMB</b>	Renminbi (fiat currency)
<b>SBF</b>	Sam Bankman-Fried
<b>SEC</b>	Securities and Exchange Commission

---

<b>SEO</b>	Search Engine Optimization
<b>SFDR</b>	Regulation (EU) 2019/2088 on sustainability-related disclosures in the financial services sector (Sustainable Finance Disclosure Regulation)
<b>SICI</b>	Systemically Important Crypto Intermediary
<b>stETH</b>	Staked ETH
<b>SVB</b>	Silicon Valley Bank
<b>SVP</b>	Special Purpose Vehicle
<b>Taxonomy Regulation</b>	Regulation (EU) 2020/852 on the establishment of a framework to facilitate sustainable investment
<b>TFR</b>	Regulation (EU) 2015/847 on information accompanying transfers of funds (Transfer of Funds Regulation)
<b>Transparency Directive</b>	Directive 2004/109/EC on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market
<b>TradFi</b>	Traditional Finance
<b>TVL</b>	Total-Value-Locked
<b>US</b>	United States
<b>USD</b>	US Dollar (fiat currency)
<b>USDC</b>	USD Coin (cryptocurrency)
<b>USDT</b>	USD Token (cryptocurrency)
<b>UST</b>	TerraUSD (cryptocurrency)
<b>VA</b>	Virtual Asset
<b>VASP</b>	Virtual Asset Service Provider
<b>VC</b>	Venture Capital
<b>VPN</b>	Virtual Private Network

**VTL**            Value-to-Loan

**WSJ**            Wall-Street Journal

## EXECUTIVE SUMMARY

### Background

With its decisions of 20 April 2023, the European Parliament (EP) adopted the new Markets in Crypto-assets Regulation (MiCA)<sup>1</sup> and the revised Transfer of Funds Regulation (TFR)<sup>2</sup>. This study has been commissioned to support the work of the European Parliament's ECON Committee by identifying the potential challenges remaining after MiCA's adoption and the TFR's revision, and by discussing whether further legislation is necessary on decentralized digital finance and crypto-assets in light of the lessons learned from the Crypto Winter of 2022-2023.

The study is also relevant in view of the scheduled review of MiCA (18 months after its entry into force), in particular on areas which were not addressed in the Regulation, as well as in the broader context of ongoing legislative reviews of EU financial services legislation (i.e. MiFID review, proposed Listing Act, review of Market Abuse Regulation etc.).

### Aim

This study identifies policy options and discusses their upsides and downsides with regard to Decentralized Finance (DeFi), non-fungible tokens (NFTs) for financial use, crypto staking/lending, the use of non-formal communication means and sustainability related matters. In particular, it provides:

- a brief summary of relevant EU and global market developments and trends, and an analysis of the regulatory and supervisory challenges that justify regulatory intervention considering the state of knowledge in other jurisdictions and by international standard setters such as the Financial Stability Board (FSB), International Organization of Securities Commissions (IOSCO), International Monetary Fund (IMF) and Bank for International Settlements (BIS);
- an overview of risk mitigating tools at EU level to address the major risks in the status quo prior to MiCA's entry into application;
- a robustness check of the EU's upcoming MiCA framework and, assuming its adoption, the identification of remaining risks; and
- a list of policy proposals through which the remaining risks and deficiencies identified may be addressed at EU level.

### Key Findings

#### Different nuances of decentralization

A DeFi platform (hereafter "DeFi Stack") aims at delivering one or several types of financial services through a tailor-made platform to users identified by a given token type. Contrary to what the term "DeFi" suggests, the degree of decentralization varies wildly within the DeFi industry. Some platforms organize **peer-to-peer finance** (where one user lends to or borrows from another user). Other platforms **pool users' funds to bundle liquidity** before "the pool" transacts with other users, while in a third type, transactions are **booked on the balance sheet of an intermediary**. Some intermediaries have gained large market shares or provide critical valuation services to many DeFi Stacks; we refer to these as **systemically important crypto intermediaries (SICIs)**.

<sup>1</sup> EP position on the proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, [P9\\_TA\(2023\)0117](#).

<sup>2</sup> EP position on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), [P9\\_TA\(2023\)0118](#).

## Crypto Winter 2022-23

Several operational malfunctions and asset diversions of prominent (and in some cases, seemingly fully decentralized) platforms became known in the second half of 2021. Following the malfunction of the Terra-Luna stablecoin algorithms (with losses exceeding USD 50 billion) in May 2022, the crypto industry experienced large-scale downturns and severe volatility of crypto-asset prices, which then led to bankruptcies of several large and leading crypto projects and intermediaries (including Three Arrows Capital and FTX, as two leading examples). In the wake of these insolvencies, not only did the concentration of certain segments of DeFi markets become apparent, but also deficient risk management, conflicts of interest, lack of proper accounting and business continuity concepts, and unfit (and potentially un-proper) key staff of major crypto actors. This impression has been confirmed in March 2023 when the US Commodity Futures Trading Commission (CFTC) sued Binance, the largest crypto exchange, for (alleged) violations involving illegal client solicitation, wrongful disclosures, insider dealing and market manipulation.

### Rationale for regulatory intervention

Contrary to what DeFi proponents argue, **in terms of risk crypto** is, in many respects, **not different from traditional finance**, and thus the rationales for regulatory intervention are likewise similar. Risks present in crypto include: **agency risks** (e.g. incompetence, ignorance, passivity, asset appropriation, and outright fraud and theft); **conflicts of interests** stemming from the bundling of various intermediary functions (e.g. exchange, custody, proprietary trading, brokerage); **use of leverage**, often hidden in crypto lending and crypto stacking and analogous to the use of complex derivatives in traditional finance; **market abuse and market integrity** risks (i.e. Anti-Money Laundering/Counter-Terrorist Financing (AML/CTF) risks); and **concentration risks**, where a single entity is systemically important for one or several crypto or other ecosystems (i.e. a SICI). These risks require regulation under the principle “**same risks, same rules**”.

Moreover, **partial decentralization, even intensified decentralization as in the case of (apparently) “fully decentralized services”**, provides a number of additional challenges, requiring regulation under the complementary principle “**new risks, new rules**”. In fact, decentralization enhances challenges with regard to defining regulated activities, risk management and ensuring business continuity in insolvency and/or a general market crisis in crypto. In these instances, value locked-in into DeFi systems is often entirely lost, as tailor-made tokens lose their economic viability with a large number of users/token-holders, developers and nodes leaving the platform overnight, often after operational malfunctions. In such instances, there are no governance schemes ensuring the proper liquidation of operations, or ensuring that users’ rights are legally enforced vis-à-vis external attackers, developers and nodes, thus creating a ‘Wild West’ environment, in which fraudsters and thieves can get away with their proceeds from asset diversions and market abuse.

**Regulatory challenges of decentralization** include:

- (1) **lack of legal certainty in respect of basic concepts fundamental to private ordering** (e.g. property rights, asset separation in title, segregation, tracing, standing to sue),
- (2) **lack of legal certainty on basic concepts fundamental to public ordering** by way of EU financial regulation (e.g. scope of licensing in doubt),
- (3) **technical complexity** and lack of transparency on certain functional and governance details of crypto ecosystems (in particular in the context of custody and resolution), and



- (4) **barriers to cross-border enforcement and supervisory cooperation** caused by, on top of legal uncertainty, difficulties in ascertaining jurisdiction in crypto markets where regulators are uncertain whether they have jurisdiction within their own territory.

The study looks in detail into certain **bespoke regulatory challenges**:

- As to **crypto lending**, we find that the main challenge lies in the operational robustness of protocols and the application and enforcement of existing financial laws to crypto intermediaries active from outside the EU Single Market.
- As to **crypto staking** (which we define as the bundling of tokens, or entitlements of tokens, respectively, for a given financial or governance objective), again the operational robustness of processes raises concerns, as do matters around who can stake which tokens (or trigger the staking for the benefit of others) and related governance dimensions.
- As to **sustainability**, we argue that the use of energy by certain blockchains (particularly the old Bitcoin blockchain) is idiosyncratic to crypto and now dated. Modern blockchain technologies are much more energy efficient. Subjecting crypto to financial regulation may further increase energy efficiency.
- As to the **use of non-formalized information**, referral programmes and other incentives provide indirect forms of client solicitation, while centralized actors rely on exemptions for reverse solicitation in an unjustified manner, given the circumstances. MiCA will require very detailed implementing provisions to act meaningfully against Financial Influencers (FinFluencers) and the extensive use or abuse of social media and search engines to attract clients. Even if these are adopted at Level 2, with fully decentralized services being out of MiCA's scope, some need to regulate remains.

### Impact of MiCA and TFR

When examining the legal status prior to the adoption of MiCA and the revised TFR, we find that the legal uncertainty relating to basic definitions of EU financial law such as transferable security, financial instruments and e-money has led to an unharmonized application of existing EU financial regulation by national competent authorities (NCAs). This situation has facilitated regulatory arbitrage by the crypto industry in a European context. At the same time, third-country crypto intermediaries and “fully decentralized platforms” often navigate through the regulatory thicket and avoid regulation altogether. The uncertainty in respect of the applicability of basic EU financial regulation and the opaqueness of business models and EU clients renders supervisory enforcement by NCAs located in the EU difficult. Regulation is certainly no cure for *all* risks of the crypto industry. However, financial regulation allows NCAs to have an access point for further measures that address many of the risks relating to crypto, be it the traditional risks of finance, or the peculiar risks of crypto.

MiCA and TFR **address the main challenges relating to the centralized provision of crypto services**. In particular, MiCA introduces a bespoke licensing scheme for centralized crypto-asset service providers (CASPs) as well as providers of E-Money Tokens (EMTs) and Asset-Related Tokens (ARTs). These licensing schemes come with operational and conduct of business rules that address the main pain points of centralized crypto services. In particular, MiCA addresses risks of financial stability stemming from stablecoins, including so-called “global” stablecoins, by imposing reserve requirements and other operational requirements. Moreover, MiCA enhances disclosure for crypto-assets that are neither financial instruments, nor deposits, nor EMT and ART, by introducing a white paper registration scheme and related liability of entities involved in the distribution of these other crypto-assets. MiCA is placed in between all existing EU financial regulation, and is designed to fill gaps

stemming from the diverging application of key concepts of EU financial regulation, such as financial instruments, transferable securities, e-money, and deposits (including structured deposits). In theory, there should not be any space between MiCA and these general EU financial regulations. MiCA further provides for explicit legislation to address market abuse, as well as reverse solicitation. All in all, MiCA has added important cornerstones to EU financial regulation that allow for the robust enforcement of EU financial regulation.

### Remaining challenges

Following the worldwide trend to regulate *centralized* crypto services, the industry has increasingly centred on *more* (dubbed “fully”) *decentralized* provision of services, which are out of MiCA’s scope. Further, innovation has created new variants of crypto, most notably with the rise of NFTs. The many contributions to the Crypto Winter have transformed the social and legislative perspective on crypto, from a more permissive to a more restrictive approach. MiCA, on its foundational level, while far from lax, reflects the regulatory environment prior to these events. Since the crypto world today is different from the world for which MiCA was drafted, significant regulatory challenges remain and should be addressed either on the level of MiCA and TFR implementation or by legislation amending MiCA and TFR.

1) From a regulatory perspective, **addressing the legal uncertainty as to the applicability of EU law**, and of which specific EU law for each specific type of crypto-asset, is of utmost importance. In this regard, MiCA leaves the heavy lifting to the Level 2 implementing legislation and coordination by the European Supervisory Authorities (ESAs). Whether the implementing legislation can ensure a uniform answer of all NCAs on the many different aspects where the application of EU financial regulation diverges, is too early to say. The controversy will circulate, in practice, around two aspects:

- First, the **delineation** between the scope of MiCA and existing financial regulation, as in principle, MiCA applies where the overall financial services regulation does not apply. Due to complexity and divergent views across Member States, there is a **legal uncertainty inherent in EU concepts of financial regulation** (e.g. in the term “financial instrument” under MiFID). As MiCA builds on these concepts, its scope is in some respect uncertain. In turn, MiCA foresees at least seven different tools that aim at classification. We do not think that more can be done. However, applying and implementing these potentially complex classification criteria will be conditioned on the NCAs’ resources and capacity to inquire into the IT features, client base and solicitation practice of some 10,000 crypto-assets where each of these crypto-assets is somewhat unique, and in an environment often characterized by non-cooperation and opaque control structures. Even if the framework is developed, over time, only some NCAs will find themselves in the position to enforce the classification criteria (if any) consistently.
- Second, the **delineation** between “**partially decentralized**” services (in scope of MiCA) and “**fully decentralized** platforms ... without an intermediary”, which are exempted from MiCA. Many large crypto platforms claim to be “fully decentralized” although whether or not this is the case is subject to doubt. Implementing legislation could, with a view to consumer protection and financial stability, take a strict stance on “full decentralization” or follow industry demands that claim in all cases of ‘peer-to-peer’ or pooled finance that an intermediary is lacking and hence the service is “fully decentralized”.

**As to the first controversy**, regulators could facilitate effective solutions following the example of the United States (US) Securities and Exchange Commission (SEC) that has rendered, de facto, almost all

tokens subject to US securities regulation.<sup>3</sup> While we do not recommend use of the *Howey* test that is at the core of US securities regulation, the EU could, based on its current framework and the classification criteria developed with the various MiCA tools, adopt a **strict procedural default rule**: by way of EU financial regulation **all crypto-assets could be deemed, at first and prior to any involvement of supervisory authorities, “transferable securities” unless (and until) they are exempted and requalified by NCAs applying the classification criteria promulgated by the (Joint) ESAs under MiCA**. Once an NCA is involved, for instance upon application of an issuer or trading platform, this NCA may classify with binding effect the crypto-asset as a financial derivative, a deposit, as e-money, a payment service, an ART/EMT or “other crypto-asset” subject to Title II MiCA, any other type of financial services (for instance, an alternative investment fund (AIF) or insurance contract), or the NCA may entirely exempt the crypto-asset.<sup>4</sup> The default rule shifts the onus of gathering the technical facts and arguing the scope of regulation from NCAs and ESAs to the crypto industry. The application for exemption and requalification may be standardized based on the template to be provided by the ESAs under Article 97(1) MiCA. Such a default rule would **counter the industry tendency of seeking to arbitrage regulation through technological innovation**.

This should be supplemented with (1) a right of the ESAs to enquire into the EU client base vis-à-vis third-country firms, and (2) adequate thresholds across EU financial law that allow for financial innovation within reasonable limits. Currently, the thresholds under MiCA and in EU financial regulation are diverging, ranging from EUR 1 million to 5 million, while some regulations (including most notably MiFID and CRD) lack any threshold-based exemption. We recommend some cross-sectoral harmonization that establishes **one uniform threshold for all regulated activities of EUR 5 million** per country, **and a total of EUR 20 million for the EU**, to grant some (limited) space for innovation. However, to make use of this exemption, eligible firms must register with the respective NCA.

**As to the second controversy**, as laid out above, we do not support the rationale that full decentralization results in lesser or no risks, but quite the opposite. **in addition to the risks of traditional finance, decentralization creates new risks that need to be addressed by bespoke regulation**. To what extent MiCA will address these new risks depends on the implementing guidelines as to which “partial decentralized” platforms are in scope. We hold that “full decentralization” is somewhat of a mirage because most (apparently) fully decentralized platforms exhibit features of concentration, by way of e.g. concentration of voting rights, golden tokens and control by developer teams. If MiCA’s scope is defined more broadly, the need for regulation of “fully decentralized” platforms after MiCA is lesser as few of these platforms are truly decentralized. If, however, the exemption for fully decentralized platforms remains in any form, some DeFi platforms will circumvent the scope of MiCA.

2) The above-mentioned legal uncertainty, together with uncertainty of whether NCAs have jurisdiction in terms of region, but also number of clients and volume invested, erects a barrier to enforcement in some cases. The NCAs would struggle to identify whether they have a case in their jurisdiction and lack the resources to find evidence to justify their jurisdiction. For instance, Title II MiCA requires evidence that an offer was made to 150 users and subscription volume exceeds EUR 1 million, which is a challenge in a business environment characterized by non-formal communication (e.g.

<sup>3</sup> A noteworthy exemption is the two major cryptocurrencies Bitcoin and Ether, instead subjected to regulation as commodities.

<sup>4</sup> In this process the various classification, monitoring and reporting requirements under MiCA of NCAs to the ESAs prevent NCAs’ shopping for crypto business.

referral programmes and indirect client solicitation via FinFluencers) and, in some cases, non-cooperation with regulators.

3) Another issue relates to **NFTs**, and the uncertainty existing as to what qualifies as NFTs, and “**financial NFTs**”, in particular. MiCA exempts crypto-assets that are “unique and non-fungible”. While the industry defines ‘uniqueness’ technically, by way of the embedded token standard, we find it necessary to apply a substantive definition in light of the rationales of EU financial law and to prevent regulatory arbitrage, as most financial NFTs are in fact tradeable and transferable. The recitals of MiCA provide for a so called “valuation test”: if several types of assets are so close to each other that the value of one token influences the valuation of the other, they are subject to MiCA, or EU financial regulation, respectively. MiCA implementing legislation must ensure that this test is rigorously applied to foreclose circumvention of EU financial law. To that extent ESAs guidelines could clarify that financial NFTs are, first and foremost, financial in nature and thus treated under MiFID or MiCA.

4) As to **crypto lending and crypto staking**, the robustness of the protocols and algorithms used is doubtful and abuses, such as asset diversions, are well known. Further, the governance dimension of crypto staking has been so far widely overlooked. While MiCA addresses the risk in the context of centralized platforms, staking is used extensively in what the crypto industry calls “fully decentralized” platforms. In fact, staking leads to concentration of control over certain processes, and thus renders the notion of “full DeFi” a myth.

5) Some decentralized platform protocols are **energy intensive**. If they remain out of scope of EU financial regulation, they will avoid reporting under the Sustainability-Finance Disclosure Regulation (SFDR) and EU Taxonomy Regulation altogether.

6) **Various MiCA rules will depend on Level 2 implementing legislation**. For instance, the extent to which Level 2 will require detailed business continuity concepts for CASPs, covering both technical malfunctions and bankruptcy of core intermediaries, cannot yet be assessed with certainty. Also, the example of market abuse rules on financial instruments under the Market Abuse Regulation (MAR) suggests that the wording of MiCA Level 1 on market abuse will not result in the desirable legal certainty to allow for NCAs’ active enforcement action. Extensive Level 2 legislation will be necessary to achieve a level playing field. This will take years to develop, and implementing a bespoke framework will take even longer. Including all crypto-assets in the scope of the MAR may be a more effective solution.

7) Further, we identify some issues regarding **ongoing and periodic disclosures** (MiCA is limited to initial disclosures), the lack of a **robust restructuring and resolution legislation** considering the impact of decentralization on third parties (so far CASPs need to hand in a business continuity concept, but this does not include third party creditors nor fully-decentralized platforms), and **cross border harmonization and coordination of NCAs** vis-à-vis platforms relying on the exemption for reverse solicitation.

8) Finally, all **private law matters** are beyond the scope of MiCA. Here, a significant amount of legal uncertainty prevails. Private law is extremely important as it defines the rights of clients (consumers or institutional) which controls what self-help by investors might result in a retransfer in case of fraud and theft. In the absence of an EU mandate to regulate private law, we recommend assigning a regulatory mandate to organize collective redress for holders of crypto-assets. Examples can be taken from the national regulations on Net Asset Value (NAV) calculation errors by managers of collective investment schemes.

As an intermediate conclusion, although MiCA is sound in principle and adequately addresses the main issues of centralized crypto services, **we are sceptical that MiCA will have positive short-term effects**

**given the difficulties of enforcing its rules in an opaque cross-border context where some 10,000 crypto protocols seek opportunities to find the lightest regulatory environment available.** We doubt that Level 2 legislation and ESA guidelines, sufficiently detailed to provide legal certainty, can be drafted any time soon to deal effectively with this challenge. A central issue is the ambiguity surrounding the definition of financial instruments versus MiCA's definition of crypto-assets. Even if these guidelines were drafted in a comprehensive manner, in the absence of intense cooperation and mutual support, and automation of supervision (for instance, through the Euro Wallet proposed in this study), some NCAs will lack the resources, expertise and enforcement means to launch meaningful supervisory cases against dozens of third-country protocols potentially operating in their jurisdiction.

**As to the revised FTR**, the industry challenges the feasibility of several of the tracing rules adopted by EU legislators, while legally the FTR's scope is limited and does not include "fully decentralized" services. Currently, techniques used by parties interested in hiding transactions include merging, repackaging and reuse of crypto-assets, the decentralization of wallets, and the transfer into non-cooperative jurisdictions. FTR may be made effective by **expanding the scope of EU financial regulation to include fully decentralized services**; singling out non-cooperative jurisdictions through a large network of cooperative supervisors; and providing a licensed Euro-wallet with embedded regulatory compliance features (e.g. allowing for transfers from wallets with a signature from cooperating jurisdictions only).

Implementing these techniques will require significant expertise and resources from the EU legislature and NCAs. Potentially, the new EU AML authority may provide both. From an EU financial regulatory perspective, and in view of consumers and financial stability, it is desirable that tracing data are forwarded to financial regulators (ESAs, NCAs and the ECB) and usable for collective (public or private) redress. AML authorities have not yet cooperated and exchanged data for the purposes of mere consumer protection and financial stability.

**Policy considerations.** We suggest that the following challenges should be addressed:

- Deal with reverse solicitation in a cross-sectoral harmonized manner in a Cross-border Solicitation of Financial Services Regulation by expanding the rules of the Cross-border Distribution of Funds Directive;
- Empower the ESAs to inquire into cases where third-country firms and platforms rely on reverse solicitation, into the number of EU users and their volume, and into the methods used for solicitation (if any), on behalf of NCAs, paired with robust sanctions in case of non-cooperation and an obligation to forward these data to the NCAs;
- Adding a broad default rule according to which crypto-assets are, by way of default, transferable securities unless exempted (and requalified) by NCAs; this proposal seeks to shift the onus of inquiring into technical details, control structures and client solicitation practice from NCAs to the crypto-industry, and assist NCAs in their struggle with financial innovation used for regulatory arbitrage;
- Assigning, from a regulatory perspective, an entity status to Decentralized Autonomous Organizations (DAOs), with a requirement to appoint a representative inside the EU as a precondition for serving EU users. This may also further sustainability-related disclosures given that DAOs would be able to qualify, under certain conditions, as reporting entities under the SFDR and Taxonomy Regulation;

- Adopting bespoke resolution and bankruptcy schemes for decentralized platforms (e.g. which could form part of the Bank Recovery and Resolution Directive (BRRD) or a new section of MiCA);
- Further harmonizing international private law (i.e. by endorsing the Unidroit approach or furthering a Hague Convention in relation to crypto-assets, or agreeing on property rights assigned to crypto-assets at an EU level) and ensuring legal certainty on court jurisdictions and choice of law by adding crypto-assets to the Rome II and Brussels Regulations (e.g. as part of Art 6 IV Rome II Regulation);
- Expanding existing supervisory networks to crypto-assets; for example, crypto-assets could be defined in the IOSCO frameworks as one case where the Multilateral Memorandum of Understanding (MMOU) applies;
- Adding a section on NFTs to MiCA that deals with the additional operational and financial risk of tokenization and DLT-based asset transfer by NFT-CASPs;
- Mandating the new EU AML authority to share with ESAs and NCAs data on client origins of entities reporting under TFR and AMLD, to further the effective enforcing of EU financial regulation; and
- Developing a “**Euro Wallet**” under the eIDAS Framework **with embedded compliance** as to AML/KYC, licensing, and client solicitation requirements, which allows only compliant (i.e. licensed and supervised actors that pursue AML/KYC checks) to transact with EU clients. Such a Euro Wallet may also provide opportunities to embed sustainability disclosures and provide the foundational infrastructure for the Digital Euro at a later point in time.

## 1. INTRODUCTION

With regard to Decentralized Finance (DeFi), this study discusses the lessons learned from the Crypto Winter of 2022-2023, which is characterized by the downturns and volatility in markets and collapse of many crypto projects and intermediaries, and as well as by insolvencies of “crypto-friendly” banks.

The study focuses particularly on crypto lending, crypto staking, crypto custody, the use of non-formal information, NFTs and sustainability. It also analyses the need to adopt further financial regulation in the context of the EU’s primary regulatory objectives: (1) the protection of consumers, clients and regulated financial institutions, (2) market efficiency, (3) market fairness and market integrity (including market abuse and money-laundering concerns), (4) financial stability, and (5) sustainable development (including environmental protection).

The study is structured as follows:

Part 2 provides a **primer on DeFi**, and a look at the crypto industry, its size and interlinkages to traditional finance. We show that **each combination of services on a DeFi platform (hereafter “DeFi Stack”) can be understood as a unique small financial system in itself**. Part 2 ends with an analysis of what is now called the **Crypto Winter of 2022-23**. We examine some large-scale operational malfunctions and asset diversions in the second half of 2021, the subsequent large-scale downturn and heavy volatility in crypto-asset prices, and the bankruptcies of several large and leading crypto intermediaries.

Part 3 summarizes the **supervisory and regulatory challenges** relating to crypto and DeFi. First, we show that crypto is in many respects **not different compared to traditional finance**. The related risks ask for regulation under the paradigm of “same risks, same rules”. Moreover, **partial decentralization**, even intensified decentralization as in the case of (seemingly) “fully decentralized services”, provides a number of **additional challenges**, asking for regulation under the paradigm “**new risks, new rules**”. Therefore, crypto is in many respects *not* special, and where it *is* special, that specialty does not warrant regulatory lenience. We go on in Part 3 to summarize the peculiarities of crypto that warrant bespoke regulation, such as legal certainty on basic concepts fundamental to private and public ordering, lack of standardization of technical concepts, paired with technical complexity and lack of transparency and barriers to cross-border enforcement and cross-border supervisory cooperation. At the end of Part 3, we address in detail the bespoke regulatory challenges related to **crypto lending, crypto staking, sustainability**, and the **use of non-formalized information**.

Part 4 provides an overview of the legal status and related legal challenges prior to the adoption of MiCA and the revision of the FTR.

Part 5 provides a legal impact assessment of MiCA and FTR, followed by a robustness check in light of the experiences throughout the Crypto Winter.

Part 6 discusses **policy options** in light of the deficiencies identified. We suggest certain remedies for general matters related to reverse solicitation, addressing the delineation of scope, and cross-border cooperation. As remedies to address (partial) decentralization, we suggest assigning entity status to DAOs, with a requirement to appoint a representative inside the EU as a precondition for serving EU users, adopting bespoke resolution and bankruptcy legislation, and further harmonizing international private law as well as the creation of a Euro Wallet with regulatory features embedded.

## 2. DECENTRALIZED FINANCE AND THE CRYPTO WINTER

### KEY FINDINGS

DeFi relies on technology, in particular distributed ledger technologies (DLT) including blockchain and smart contracts, which replaces human-based functions and services. DeFi seeks to replace the central role of concentrated intermediaries in traditional finance, and the too-big-to-fail risks that they embody, without reliance on the (apparent) weaknesses of regulation and supervision.

DeFi platforms are not necessarily decentralized *stricto sensu*; the degree of decentralization varies across the industry. In fact, the crypto industry has been characterized by the emergence of **Systemically Important Crypto intermediaries** (SICIs).

Since the second half of 2021, crypto has experienced large-scale operational malfunctions and asset diversions culminating in the collapse of the Luna/Terra stablecoin system, which resulted in a series of bankruptcies of SICIs ongoing since the second half of 2022. In the meanwhile, some spill over effects into the traditional financial system may be observed.

### 2.1. The term decentralized finance: “DeFi”

‘Decentralized Finance’ (DeFi) is neither a legal nor technical term. Common usage incorporates one or more elements of: (i) decentralization; (ii) DLT, with blockchain being an element of DLT; (iii) smart contracts; (iv) disintermediation; and (v) open banking.<sup>5</sup> While decentralized systems such as Bitcoin rely on DLT to underpin token-based ecosystems, DLT is not the only way to achieve decentralization. Further, many distributed ledgers operate today with a hierarchical, centralized governance model, limiting access to permissioned participants only. In turn, decentralized does not necessarily mean distributed.<sup>6</sup>

Disintermediation is not a prerequisite for decentralization; rather, disintermediation may be one (side) effect of decentralization, given that the establishment costs of centralized infrastructure will be difficult to recoup in a world where services can be provided on a distributed or decentralized basis. In fact, “where parts of the financial services value chain are decentralized, we expect re-concentration in a different (but possibly less regulated, less visible, and less transparent) part of the value chain.”<sup>7</sup> In fact, this has occurred. Many DeFi ecosystems rely on crypto intermediaries that are indispensable for that very ecosystem, called herein “Systemically Important Crypto intermediaries” (SICIs). (Cf. *infra*, at 2.5. discussing the Crypto Winter).

We understand DeFi to comprise, at its core, what its simple name suggests: the decentralized provision of some type of financial services through a mix of infrastructure, markets, technology, methods, and applications. Decentralized provision of financial services means, in turn, a provision by multiple participants, intermediaries, and end-users spread over multiple jurisdictions, with interactions facilitated, and often enabled in the first place, by technology.<sup>8</sup>

<sup>5</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, Decentralized Finance, *Journal of Financial Regulation*, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 173-175.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Ibid. at 173-175.



## 2.2. Traditional finance vs decentralized finance

To understand DeFi, a brief look at traditional finance provides context.<sup>9</sup>

### 2.2.1. Intermediaries and centralization in traditional finance

At the heart of traditional finance is a series of financial intermediaries, such as banks, market participants and securities exchanges that bring together supply (by savers, lenders and investors) and demand (by borrowers and investee firms) provided by a range of disparate financial market participants. In traditional finance, major intermediaries centralize functions and resources.<sup>10</sup>

This results in the ‘hub-and-spoke’ conceptualization of traditional finance: when clients have local access to services such as payments, ATMs, savings, investments, and insurance, these services are not provided at the point of access. Rather, financial services traditionally cluster in local, regional, and super-regional/global access points (“hubs”).<sup>11</sup>

Following this economic logic, local, regional, and global financial centres have evolved where sufficient concentration of transaction volumes and numbers in a given sector(s) or service(s) allow the development of expertise and resources. These financial centres fundamentally depend on trust and confidence in order to function. Failures of private ordering and self-regulation of traditional finance have come to the surface periodically, often in the context of financial crises, such as the 2008 Global Financial Crisis (‘GFC’). Due to global regulatory action and coordination, trust and confidence and the basic functioning of financial systems is now underpinned by law: rules, institutions, regulation, supervision, and courts.<sup>12</sup>

### 2.2.2. DeFi as counter model to traditional finance

DeFi seeks to address through technology what crypto proponents understand as the source of traditional finance’s instability: the centrality (if not dominance) of concentrated intermediaries and the ‘too-big-to-fail’ risks they embody – and the reliance on the weaknesses of states, governments and regulators.<sup>13</sup> DeFi envisages a utopia where technology replaces frail humans and their institutions: a world in which technology eliminates the risks inherent in the concentrated systems central to traditional finance.<sup>14</sup>

In traditional finance, services are booked on a single balance sheet, with the provider of that balance sheet usually headquartered in a hub.<sup>15</sup> This hub would usually be protected by high regulatory and supervisory standards, reflecting the large quantity of risks from pooling and balance sheet concentration at the hub.

DeFi challenges this hub logic. If scale were created by technology rather than by bundling business in a hub, hubs would make little sense as they come with downsides for clients. They need to adjust in terms of language and law, subscribe to high compliance standards reflecting the concentration of risks, accept information costs (e.g. for legal counsel), and face penalties for non-compliance with laws

<sup>9</sup> Ibid. at 175-178.

<sup>10</sup> Ibid.

<sup>11</sup> Ibid.

<sup>12</sup> Ibid.

<sup>13</sup> Ibid.

<sup>14</sup> We have questioned that vision in Enriques L., and Zetsche D. A., 2020, *Corporate Technologies and the Tech Nirvana Fallacy*, *Hastings Law Journal*, 72, pp.55-96, available at: <https://ssrn.com/abstract=3392321> or <http://dx.doi.org/10.2139/ssrn.3392321>.

<sup>15</sup> Zetsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, *Journal of Financial Regulation*, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 177-178.

implemented at the hub level but not (yet) at the local level. Further, hub structures create dependencies, which may be unattractive from a political standpoint – for instance, if RMB or EUR are settled in London or New York, English and US regulators acquire influence over the currency.<sup>16</sup>

DeFi helps avoid these costs and dependencies. Services could be tokenized and provided to the token holder regardless of the places of origin of provider and recipient.<sup>17</sup> For instance, Bitcoin holders are linked through common technology rather than a massive balance sheet in a highly regulated payment hub.<sup>18</sup>

## 2.3. Underlying technology

Underlying DeFi is a series of technologies.<sup>19</sup>

### 2.3.1. Exponential growth of data processing, storage and bandwidth capacity

DeFi emerges from three important patterns in technological evolution (see Box 1).

Box 1: DeFi and the patterns of technological evolution

**Moore’s law** refers to the assumption that the amount of data processing power grows exponentially. **Kryder’s law** posits the same for data storage capacity. The combination of ever-increasing processing power and data storage capacity leads to ever-lower costs for both. The **third pattern** making DeFi possible is the tremendous growth in communications bandwidth combined with decreasing costs – a phenomenon, which has been discussed since the late 1990s, if not earlier. The underlying assumption of bandwidth growth at decreasing costs is supported by increasing network efficiencies, which lead to more bandwidth per amount invested.

Source: Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*.<sup>20</sup>

These three evolutionary patterns enable hardware virtualization: software is hosted, updated, and run at decentralized servers rather than on each workstation. Only data that needs to be processed locally (under conditions of instant online connection and abundant bandwidth) tends to remain processed locally. Hardware virtualization allows for the creation and set-up of service-oriented architecture (‘software as a service’) which is at the heart of DeFi.<sup>21</sup>

### 2.3.2. Technical pillars of DeFi

DeFi rests on four technologies central to financial technology (FinTech) and regulatory technology (RegTech), best summarized with the acronym “ABCD” for AI, Big Data, Cloud, and DLT (including blockchain and smart contracts). We provide some context here on DLT, DeFi’s core technology.

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies, allowing a transaction to have multiple private or public “witnesses”.<sup>22</sup>

<sup>16</sup> Ibid.

<sup>17</sup> Ibid.

<sup>18</sup> Ibid.

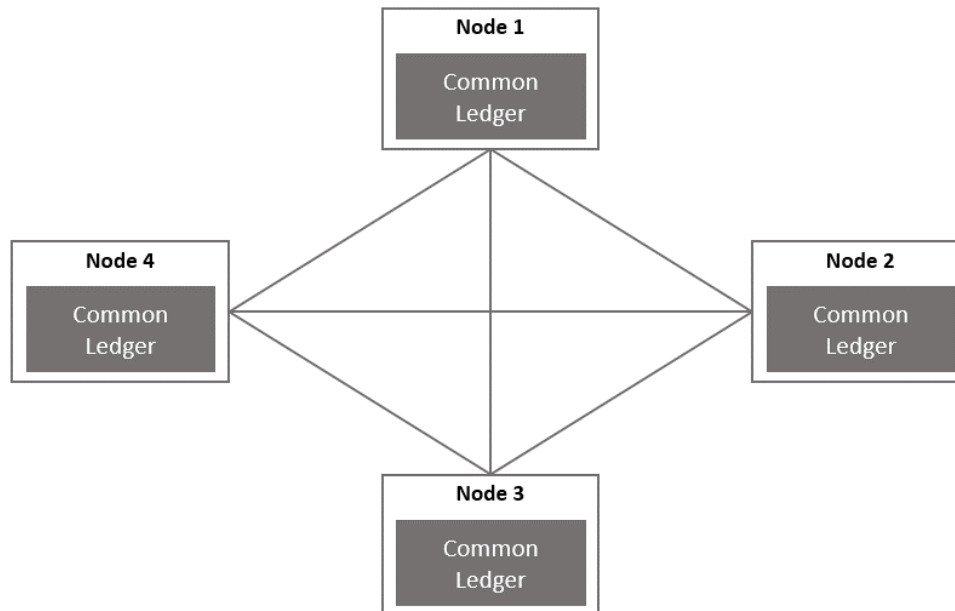
<sup>19</sup> This section of the report is based on Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at 179–182.

<sup>20</sup> Journal of Financial Regulation, 6(2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 179–182.

<sup>21</sup> Ibid. at 179 - 182

<sup>22</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 179.

Figure 1: Distributed ledger



Source: Zetzsche, D. A., Woxholth J., 2022, The DLT Sandbox under the EU Pilot Regulation.<sup>23</sup>

The sharing of data results in a database distributed across a network of servers, all of which function together as a ledger.<sup>24</sup> The servers involved in the data sharing come to agreements by way of a specified consensus mechanism, which reflects the investment in the network.<sup>25</sup> Distributed ledgers are characterized by an absence of, or minimal, central administration and no centralized data storage.<sup>26</sup> They are, hence, “distributed”, in that the authorization for the recording of a given piece of information results from the software-driven interaction of multiple participants. Coupled with cryptographic solutions, such features (decentralization and distribution across a network of computers) curtail the risk of data manipulation. This solves the problem of having to trust third parties, specifically data storage service providers, as this is the point where the data is stored and can most easily be manipulated.<sup>27</sup> (Cf. Box 2 for more details on the modus operandi of distributed ledgers).

<sup>23</sup> Capital Markets Law Journal 17:2, pp. 212-236, available at: <https://ssrn.com/abstract=3833766> or <http://dx.doi.org/10.2139/ssrn.3833766> at p. 212–236.

<sup>24</sup> Ibid.

<sup>25</sup> This may take place either by a given share ('Proof-of-Stake') or by work pursued for the network ('Proof-of-Work').

<sup>26</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, Decentralized Finance, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at 179.

<sup>27</sup> Ibid.

## Box 2: Distributed ledgers - modus operandi

The modus operandi of distributed ledgers is best understood by looking at their counterpart, the concentrated ledger. Let us assume that a centralized register administered by a single entity contains all relevant data, and further that, contrary to present practice, the centralized register is not secured and thus 'semi-distributed' through a myriad of back-ups stored on multiple servers. This arrangement entails a number of risks. First, if the hardware where the register is 'located' is destroyed, the information content and the authority to ascertain that it is correct is lost. Second, disloyal employees of the database administrator or an unfaithful administrator may manipulate the information content of the register. Third, a cyber-attack may result in manipulations and data losses.

Distributed ledgers address these problems by raising the barrier for manipulation. The underlying technology requires consensus of many data storage points ('nodes'). If there are a number of nodes (instead of one concentrated ledger), described as 'n', and 'e' describes the effort necessary to break into any single server, all other conditions being equal (safety per server etc.), the effort necessary to manipulate all the linked servers will be  $n \times e$  rather than  $1 \times e$ .

Distributed ledgers are usually paired with a blockchain protocol. Blockchain refers to the storage of data in data bundles (the "blocks") in a strict time-related series, with each block linked to the previous and subsequent blocks through a time stamp and a number of protocols providing evidence of a user's authority to amend the data stored.<sup>1</sup> The blockchain renders data corruption even harder because a successful cyberattack would have to simultaneously corrupt all subsequent data sets (i.e. the whole blockchain) and time stamps simultaneously.

Distributed ledgers have provided fertile ground for another innovation seeking to address the problem of trust in human interactions (especially relating to compliance with and enforcement of contracts): smart contracts. While neither "smart" nor "contract" in a legal sense, they are self-executing software protocols that reflect some of the terms of an agreement between two or several parties. The conditions of the agreement are directly written into lines of code. Smart contracts permit the irreversible execution of transactions between disparate, anonymous parties without an external enforcement mechanism (e.g. a court, arbitrator, or central clearing facility).

Source: Zetsche, D. A., Arner D. W., Buckley R. P., 2020, Decentralized Finance.<sup>28</sup>

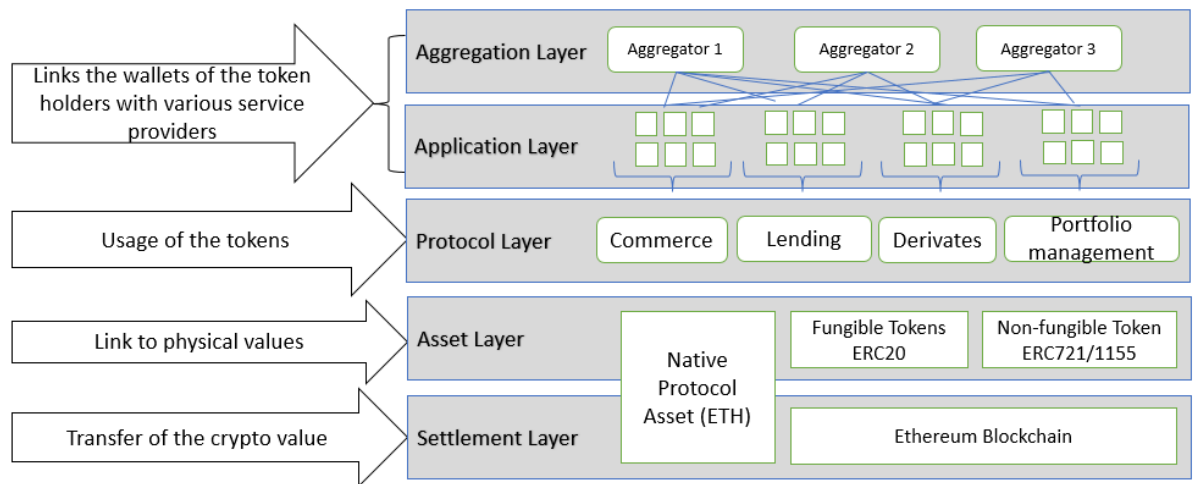
### 2.3.3. The DeFi Stack

The respective technologies tend to be bundled in a "DeFi Stack", referring to the technical interaction of several protocols and servers where each layer of protocols depends on a previous one. A DeFi Stack is equivalent to an entirely independent financial ecosystem relying on multiple layers of applications, ranging from clearing to settlement to applications where institutional clients hold assets,<sup>29</sup> as further shown in Figure 2.

<sup>28</sup> Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 179-180.

<sup>29</sup> Schär F., 2021, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, Economic Research Federal Reserve Bank of St. Louis Review, Second Quarter 2021, 103 (2), pp. 153-174, available at: <https://doi.org/10.20955/r.103.153-74> at 153.

Figure 2: DeFi Stack



Source: Based on the DeFi stack figure provided by Schär F., 2021, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets<sup>30</sup> (modified by the authors).

#### 2.3.4. Centralization vs decentralization

Some of the DeFi Stack's functions are decentralized, while others remain centralized. For instance, the stack may be governed in a decentralized manner through multiple token holders holding voting rights over technical or financial features of the protocol. The lending function may be provided by a pool of users' funds (functioning collectively like a credit institution, with interactions executed by smart contracts), while a single trading intermediary (i.e. functionally, an exchange) organizes the trading. Further, what is understood as the substance of decentralization varies. Financial services marketed as DeFi are often not DeFi *stricto sensu*.

DeFi *stricto sensu* is characterized by peer-to-peer transactions and a lack of any centralized intermediary where smart contracts execute all transactions between supply and demand automatically. All servers that support the operation of the protocols ("nodes"), or token holders as the case may be, have equal access to data and equal governance rights (or technical equivalents of governance rights). Such a setup is also referred to as a Decentralized Autonomous Organization (DAO). If a trading platform is governed by a DAO, the crypto jargon refers to Decentralized Exchanges (DEX). Examples of DEXs include *Uniswap*, *PancakeSwap*, *dYdX*, and *KyberSwap*.<sup>31</sup>

However, centralized intermediaries often deliver important functions to the DeFi ecosystem. For instance, *Binance*, *Coinbase*, *FTX*,<sup>32</sup> and others are operated by centralized entities and are thus dubbed Centralized Exchanges (CEXs). From the DeFi sector's perspective, they constitute a type of Centralized Finance (CeFi). While details change from stack to stack, these CEXs often allow for (a) the initial investment of fiat currency into tokens, (b) provision of crypto-asset prices crucial for valuation of margin and borrower's security, and (c) cross-chain bridge operations, which is the swap of one crypto-

<sup>30</sup> Economic Research Federal Reserve Bank of St. Louis Review, Second Quarter 2021, 103 (2), pp. 153-174, available at: <https://doi.org/10.20955/r.103.153-74> at 153.

<sup>31</sup> 'Home | Uniswap Protocol' (Uniswap), available at: <https://uniswap.org/>, accessed 28 March 2023; 'PancakeSwap: Home' (PancakeSwap), available at: <https://pancakeswap.finance/>, accessed 28 March 2023; 'dYdX - Trade Perpetuals on the most powerful trading platform' (dYdX), available at: <https://dydx.exchange/>, accessed 28 March 2023; 'KyberSwap - Swap and earn tokens at the best rates' (KyberSwap), available at: <https://kyberswap.com/swap/ethereum>, accessed 28 March 2023.

<sup>32</sup> 'Binance - Cryptocurrency Exchange' (Binance), available at: <https://www.binance.com/en>, accessed 28 March 2023; 'Coinbase - Buy and Sell Bitcoin, Ethereum, and more with trust' (Coinbase), available at: <https://www.coinbase.com/>, accessed 28 March 2023.

asset with another (i.e. the equivalence of trading). CEXs provide most of the trading volume for tokens issued under the DeFi maxim and influence the valuation of crypto-assets, which may then be relied upon by DeFi protocols.

In this study, we use the term “crypto” for both CeFi and DeFi services that deal with crypto-assets. In fact, CeFi and DeFi are often interlinked. On the one hand, various malfunctions in “fully decentralized systems” occurring in the last half of 2021 through May 2022 have undermined trust in crypto, and impacted the stability of centralized crypto intermediaries. On the other hand, at the height of the Crypto Winter 2022-23, “fully decentralized systems” exclusively relied on some large crypto intermediaries (i.e. SICIs) for crucial operating data. When the SICIs stopped operations, many stacks experienced difficulties or stopped operations, and asset values on these “fully decentralized systems” were deteriorating. See *infra*, at 2.5. for further details.

Whether a service is **partially or fully decentralized will be hard to determine in practice**. These practical difficulties impair the effectiveness of EU financial regulation post-MiCA as they reduce the enforcement capacity of NCAs. Pursuant to its Recital 22, partially decentralized services are in scope of MiCA, while MiCA exempts (only) fully decentralized services in crypto-assets.<sup>33</sup> Even where crypto platforms pose as DeFi *stricto sensu*, it is far from certain whether they are, in fact, fully decentralized in MiCA’s sense. As shown *infra*, at 2.4. and throughout this study, some type of legal entity is often related to, in name, fully decentralized platforms. While avoiding transaction risks itself, this legal entity develops and maintains, directly or indirectly, the platform and markets its services. It functions as infrastructure provider and sales intermediary: is this intermediary function sufficient to apply MiCA?

Further, most lending platforms pool assets from various users prior to lending (cf. *infra*, at 3.3.1.). This could be understood as centralization of liquidity, similar to what a bank would do prior to lending: does pooling result in a partially centralized service, from a regulatory perspective? Finally, also in “fully decentralized” platforms, some concentration of influence usually occurs on the governance level as this enables developers to receive compensation for their efforts in stack development and maintenance.<sup>34</sup> Empirical evidence suggests that developers and founders retain control over their protocols after the initial token offering.<sup>35</sup> This puts the rationale for regulatory leniency for “fully decentralized services” in doubt.

At the same time, the numbers we show in this study indicate that (in name) “fully decentralized services” have collected immense financial capacity beyond the threshold of “too small to care”. Finally, while MiCA renders fully decentralized models out of scope, the regulatory text of MiFID diverges from MiCA. Currently, there is no exemption of fully decentralized crypto-asset services under MiFID. The sole factor that determines the scope of MiFID is whether a crypto-asset is classified as a financial instrument. If a fully decentralized protocol provides custody or organizes trading in crypto derivatives, qualifying as financial instruments, this decentralized protocol performs a regulated activity under MiFID and is subject to licensing as an investment firm. However, as it fits the definition of “fully decentralized”, and the MiCA rules for CASPs do not extend to services provided by “fully decentralized” protocols, the MiCA rules for CASPs will not apply.

---

<sup>33</sup> “This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, **including when part of such activities or services is performed in a decentralised manner**. Where crypto-asset services are provided **in a fully decentralised manner without any intermediary**, they should not fall within the scope of this Regulation.” (Emphasis by the authors).

<sup>34</sup> For details, see Anker-Sørensen, L., and Zetzsche D. A., 2021, *From Centralized to Decentralized Finance: The Issue of Fake-DeFi*, available at SSRN: <https://ssrn.com/abstract=3978815> or <http://dx.doi.org/10.2139/ssrn.3978815>.

<sup>35</sup> Goldberg, M., and Schär, F., *Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations*, Journal of Business Research 160 (2023), available at <https://www.sciencedirect.com/science/article/pii/S0148296323001224>.

For these inconsistencies and practical difficulties, we propose including fully decentralized platforms in the scope of EU financial regulation and harmonizing thresholds across EU financial legislative acts. This will bring the large “fully decentralized platforms” into scope, while higher and harmonized cross-sectoral thresholds for the application of licensing schemes ensure proportionality. Cf. 6.2.2.e).

## 2.4. The crypto industry

### 2.4.1. Use cases and industry characteristics

Prominent crypto-assets and services include:

- **Cryptocurrencies**, such as *Bitcoin (BTC)*, *Ether (ETH)*, *Tether (USDT)*, *Binance Coin (BNB)*, *Polygon (MATIC)* and *Cardano (ADA)*.<sup>36</sup>
- **Clearing and settlement systems**, such as *Lightning Network*, *Fireblocks*, *BitGo*, *Bakkt* and *Copper*.
- **Trading platforms**, in the form of:
  - CEXs, such as *Binance*, *Coinbase*, *Kraken*, *Huobi*, *Kucoin* and (the now bankrupt) *FTX*,<sup>37</sup> and
  - DEXs,<sup>38</sup> such as *Sushi Swap*, *Dodo*, *Uniswap*, *PancakeSwaap*, *Curve DAO*, *dYdX*, and *KyberSwap*.<sup>39</sup>
- **Investment funds**, in the form of:
  - centralized crypto funds, such as (the now bankrupt) *Three Arrows Capital*, and
  - decentralized investment DAOs, such as *BitDAO*, *DAOventures* and *DAO VC*.
- **Crypto lenders**, in the form of:
  - centralized crypto lenders, such as *Nexo*, *Binance Lending*, and (the now bankrupt) *BlockFi*, *Celsius*, *Voyager Digital* and *Genesis*,<sup>40</sup> and
  - decentralized crypto lenders, such as *Aave*, *Compound Finance*, *JustLend* and *Venus*.<sup>41</sup>

### 2.4.2. Interlinkages to traditional finance

To our knowledge, the links between the DeFi world and traditional finance are somewhat limited, **yet recent events show that some interlinkage exists, with the leading example being the failure of Silvergate Bank in the US**. These interlinkages may engender systemic risk for traditional finance if: (1) crypto loses rapidly in value, as it did in the last 24 months, (2) if operational risk (e.g. malfunctions

<sup>36</sup> *Cryptocurrency Prices, Charts And Market Capitalizations*, 2023, CoinMarketCap, available at: <https://coinmarketcap.com/> accessed 25 February 2023.

<sup>37</sup> *'Top Cryptocurrency Exchanges Ranked By Volume'*, 2023, CoinMarketCap, available at: <https://coinmarketcap.com/rankings/exchanges/>, accessed 25 February 2023.

<sup>38</sup> If we refer to a service as decentralized, we do not claim that these services are decentralized in all aspects.

<sup>39</sup> *'Top Cryptocurrency Exchanges Ranked By Volume'*, 2023, CoinMarketCap, available at: <https://coinmarketcap.com/rankings/exchanges/>, accessed 25 February 2023.

<sup>40</sup> *The Right Place For Your Digital Assets • Nexo* (Nexo), available at: <https://nexo.com/>, accessed 28 March 2023; *Crypto Loans | Borrow and Lend Cryptos Instantly* (Binance Loan), available at: <https://www.binance.com/en/loan>, accessed 28 March 2023; *BlockFi: Do More With Your Crypto - Buy, Sell, Trade & Earn* (BlockFi), available at: <https://blockfi.com/>, accessed 28 March 2023; *Genesis - Institutional Access. Global Scale* (Genesis), available at: <https://genesisstrading.com/>, accessed 28 March 2023.

<sup>41</sup> *DefiLlama*, 2023, *DefiLlama*, available at: <https://defillama.com/protocols/Lending>, accessed 25 February 2023.

and asset exploitation) materializes and results in liabilities of traditional financial intermediaries, or (3) if responding to pressure in crypto markets, crypto related firms and investors remove their financial assets from traditional institutions with a high concentration of crypto exposed clients.

#### a. Crypto backed lending

Crypto lending was one of the first, and remains one of the most popular, DeFi applications.<sup>42</sup> Originally, loans were collateralized with crypto-assets and the borrowed amount was equally extended in cryptocurrencies. Today, platforms like Nexo<sup>43</sup> allow users to deposit cryptocurrencies as collateral and obtain a loan denominated in fiat- or cryptocurrencies.<sup>44</sup> Milo,<sup>45</sup> Figure,<sup>46</sup> and USDC Homes<sup>47</sup> provide mortgage lending services to finance real estate. Users can deposit cryptocurrencies, such as Bitcoin or USDC (a popular stablecoin), as collateral and obtain a mortgage for US residential and commercial real estate.

DeFi ecosystems also attempt to attract traditional institutional investors. Aave Arc was the first large DeFi protocol offering a tailor-made institutional product that fully complies with AML regulations. It is unclear, however, how many institutional investors use this service.<sup>48</sup>

#### b. Payments

Crypto custodians, such as lending platform Nexo<sup>49</sup> and various CEXs (e.g. Binance,<sup>50</sup> Coinbase<sup>51</sup>), collaborate with Visa and MasterCard to offer credit cards that allow users to spend cryptocurrencies directly from their accounts at retailers or to withdraw cash at ATMs. The set-up is akin to how US financial institutions used money market funds as cash-equivalent prior to the “breaking of the buck” crisis in these funds that prompted a “bank run” on money market funds.<sup>52</sup>

#### c. Investments and retirement plans

Investors can gain exposure to crypto-assets via collective investment schemes. A number of Exchange Traded Funds (ETFs) open to retail investors offer direct exposure to cryptocurrencies, mainly Bitcoin, and cryptocurrency-derivatives.<sup>53</sup> Fidelity Investments<sup>54</sup> and ForUsAll<sup>55</sup> also allow their US customers to add cryptocurrencies to retirement plans. Further, theme-based collective investment schemes invest in companies (primarily) active in crypto.<sup>56</sup>

<sup>42</sup> Ibid.

<sup>43</sup> *The Right Place For Your Digital Assets • Nexo* (Nexo), available at: <https://nexo.com/>, accessed 28 March 2023.

<sup>44</sup> *Borrow Against Bitcoin & Other Leading Cryptos from 0% APRm*, 2023, Nexo, available at: <https://nexo.io/borrow/>, accessed 25 February 2023.

<sup>45</sup> *'Mortgages for Global and Crypto' Consumers* (Milo), available at: <https://www.milo.io/>, accessed 25 February 2023.

<sup>46</sup> *'Crypto Mortgage Loan'* (Figure), available at: <https://www.figure.com/mortgage/crypto-mortgage/>, accessed 25 February 2023.

<sup>47</sup> *Crypto Mortgage Loan* (USDC.Homes), available at: <https://usdc.homes/>, accessed 25 February 2023.

<sup>48</sup> Evans D., *Permissioned DeFi Goes Live with Aave Arc + Fireblocks* (Fireblocks), available at: <https://www.fireblocks.com/blog/permissioned-defi-goes-live-with-aave-arc-fireblocks/>.

<sup>49</sup> *'Nexo Card – Your Crypto Card with 2% Cashback'* (Nexo), available at: <https://nexo.io/nexo-card/>, accessed 25 February 2023.

<sup>50</sup> *'An Overview of the Binance Card'* (Binance Support), available at: <https://www.binance.com/en/support/faq/an-overview-of-the-binance-card-7258c9d01cd04e58b4269ae5a86acb6d>, accessed 25 February 2023.

<sup>51</sup> *'Coinbase Card'* (Coinbase), available at: <https://coinbase.com/card/>, accessed 25 February 2023.

<sup>52</sup> Birdthistle, W. A., 2010, *Breaking Bucks in Money Market Funds*, Wisconsin Law Review, 5, pp. 1155-1201, available at: <https://ssrn.com/abstract=1728929>, <https://ssrn.com/abstract=1728929>.

<sup>53</sup> *'BITO:Bitcoin Strategy ETF'* (ProShares), available at: <https://www.proshares.com/our-etfs/strategic/bit/>, accessed 25 February 2023.

<sup>54</sup> *'Fidelity Workplace Digital Assets Account'* (Fidelity), available at: <https://www.fidelityworkplace.com/s/>, accessed 25 February 2023.

<sup>55</sup> *'Cryptocurrency 401(K) Plans: Diversify Your Retirement Savings'* (ForUsAll), available at: <https://www.forusall.com/crypto-401k/>, accessed 25 February 2023.

<sup>56</sup> *'DAPP: VanEck Crypto and Blockchain Innovators UCITS ETF'*, (VanEck), available at: <https://www.vaneck.com/lu/en/dapp/>, accessed 25 February 2023.



#### d. Tokenization of assets

In principle, any asset may be tokenized. In addition to financial products (e.g. bonds and fiat currency), tokenization may extend to pieces of land, cars, horses or copyrights. Also, NFTs are the digital representation of a given asset, such as a picture or music piece, but the number of digital copies is limited so that the NFT derives value from scarcity.

A number of companies now offer tokenization services.<sup>57</sup> For instance, Fireblocks offers tokenization to institutional clients,<sup>58</sup> while Propy<sup>59</sup> provides a brokerage service for real estate that is minted as NFT, in addition to cryptocurrency escrow and exchange services for the purpose of buying real estate. Traditional finance is active in asset tokenization, representing an alternative to traditional securitization that appeals to new client groups.<sup>60</sup>

#### e. “Crypto-friendly” banks

A number of credit institutions have presented themselves as “crypto-friendly” to attract customers from the crypto industry. This friendliness may show in the function as a bank of reserves for stablecoins, crypto-oriented services (such as a 24/7 exchange service from fiat- to cryptocurrencies),<sup>61</sup> bespoke valuation of crypto-assets, or the issuance of specialized tokens in lieu of traditional financial services. The friendliness could result in a concentration of clients exposed to crypto, which may prove burdensome for traditional finance once crypto-asset prices decline. For instance, Silvergate was once the most significant “crypto-friendly” bank, but closed on 9 March 2023 after it was forced to sell debt securities usually held until maturity pre-maturely at a loss, to satisfy depositors’ demands prompted by the Crypto Winter and the collapse of FTX in particular (cf. *infra*, at 2.5.).<sup>62</sup>

Contagion risk these days is more pronounced after the forced dissolution of Silicon Valley Bank (SVB), the 16<sup>th</sup> largest US bank. SVB specialized in start-up and tech financing. While it did not have direct exposure to crypto, many crypto entrepreneurs and their firms used the bank to store their traditional assets. In particular, the crypto firm Circle deposited some funds used as reserve for its USD 40 billion stablecoin USDC, the second largest USD-oriented stablecoin after USDT, on SVB’s accounts.<sup>63</sup> Given the clubby nature of the DeFi industry, it is reasonable to assume that other ecosystems used SVB in a similar way, and that the large withdrawals SVB experienced in its last months, forcing SVB to prematurely sell assets, stem to some extent from crypto ecosystems liquidating reserves upon withdrawal requests from crypto-asset holders.

Be this as it may, when SVB was forced to liquidate on 10 March 2023, Circle could not retrieve USD 3.3 billion, and the stablecoin USDC broke for a period its 1:1 dollar parity (in jargon, it was “de-pegged”,

<sup>57</sup> ‘Tokenization: Opening Illiquid Assets to Investors’, (BNY Mellon), available at: <https://www.bnymellon.com/us/en/insights/all-insights/tokenization-opening-illiquid-assets-to-investors.html>, accessed 25 February 2023.

<sup>58</sup> ‘Tokenization Engine’ (Fireblocks), available at: <https://www.fireblocks.com/tokenization/>, accessed 29 March 2023.

<sup>59</sup> ‘The First Real Estate NFT Launched by Propy’ (Propy), available at: <https://propy.com/browse/propy-nft/>, accessed 29 March 2023.

<sup>60</sup> ‘Tokenization: Opening Illiquid Assets to Investors’, 2019, BNY Mellon, available at: <https://www.bnymellon.com/us/en/insights/all-insights/tokenization-opening-illiquid-assets-to-investors.html>, accessed 25 February 2023.

<sup>61</sup> ‘Silvergate Bank | Leading Bank for Business & Crypto’ (Silvergate Bank), available at: <https://www.silvergate.com/>, accessed 28 March 2023 ; Nikhilesh De, Ian Allison ‘Silvergate Closes SEN Platform Institutions Used to Move Money to Crypto Exchanges’ (Coindesk, 4 March 2023), available at: <https://www.coindesk.com/policy/2023/03/03/silvergate-suspends-sen-exchange-network/>, accessed 28 March 2023.

<sup>62</sup> Lang H. and Chakroborti A. ‘Crypto focused bank Silvergate plans to wind down following blow from FTX’ (Reuters), available at: <https://www.reuters.com/technology/crypto-focused-bank-silvergate-plans-wind-down-operations-2023-03-08/>, accessed 14 March 2023.

<sup>63</sup> Lutz S. and Beganski A. ‘Silicon Valley Bank Contagion: Crypto Companies Affected Include BlockFi, Circle, Avalanche, Ripple’ (Decrypt), available at: <https://decrypt.co/123199/silicon-valley-bank-crypto-companies-contagion>, accessed 14 March 2023.

trading afterwards at USD 0.87 to 0.94 per token<sup>64</sup>). DeFi proponents may argue that traditional finance impaired the DeFi firm's ability to deliver on its promises. Yet, had Circle been subject to proper regulation (e.g. relating to MMF business), regulatory requirements would have been designed to minimize risks involved, following the GFC experiences and post-crisis international regulatory efforts in respect of MMFs. If necessary liquidity provision and verbal support from regulators and authorities had also been available, potentially more regulatory requirements would have been designed around systemic concerns. The fact that no regulatory intervention is expected in crypto, combined with lack of transparency and reliable information or regulatory engagement, enhances the tendency in DeFi to leave the system when difficulties occur, propelling "crypto bank runs". In fact, with the collapse Terra's UST stablecoin in mind (cf. *infra* 2.5.2.),<sup>65</sup> the difficulties of USDC, a stablecoin with a market capitalization twice that of UST at its peak,<sup>66</sup> undermined overall confidence in crypto markets even more, resulting in a 20% decrease of overall crypto-asset prices.<sup>67</sup> Having said this, strict reserve rules for licensed stablecoin issuers as imposed by MiCA may ensure trust and prevent "crypto runs".

### 2.4.3. Size of the industry

To our knowledge, there are no uniformly accepted insights as to the size of the industry (which, from the perspective of systemic risk, is a reason for concern in itself<sup>68</sup>).

The volume of "fully decentralized" services is small compared to traditional finance. The industry value is estimated at USD 13.61 billion in 2022.<sup>69</sup> Venture capital invested exceeds \$3 billion p.a.<sup>70</sup> DeFi Llama, a platform that aggregates the Total Value Locked (TVL)<sup>71</sup> of DeFi protocols, estimates the TVL per February 2023 at USD 54.65 billion, **down from USD 206.05 billion at its peak** on 10 November 2021.<sup>72</sup> The 75% loss in TVL signals both the asset destruction and confidence loss experienced since 2021.

The size of the crypto industry is much larger, however, since the previous numbers tend to exclude centralized applications and services (e.g. CEXs, "centralized" crypto lenders and crypto hedge funds). To illustrate, Binance, the largest CEX by daily trading volume, reports to hold USD 78 billion in crypto-assets in February 2023.<sup>73</sup> PWC reports overall assets under management of crypto hedge funds in 2021

<sup>64</sup> Baker N. 'USDC Stablecoin Depeds, Crypto Market Goes Haywire After Silicon Valley Bank Collapses' (Coindesk), available at: <https://www.coindesk.com/markets/2023/03/11/usdc-stablecoin-and-crypto-market-go-haywire-after-silicon-valley-bank-collapses/>, accessed 14 March 2023.

<sup>65</sup> Dalmas Ngetich 'USDC Is In Trouble, But It Won't Go To Zero Like UST Did – Here's Why' (NewsBTC), available at: <https://www.newsbtc.com/stablecoin/usdc-is-in-trouble-but-it-wont-go-to-zero-like-ust-did-heres-why/>, accessed 30 March 2023.

<sup>66</sup> 'USD Coin (USDC) Market Cap is \$33,458,765,186' (CoinMarketCap), available at: <https://coinmarketcap.com/currencies/usd-coin/>, accessed 28 March 2023.

<sup>67</sup> Ge Huang, V., Miao, H., Ostroff, C. 'Circle's USDC Stablecoin Breaks Peg With \$3.3 Billion Stuck at Silicon Valley Bank' (The Wallstreet Journal, 11 March 2023), available at: <https://www.wsj.com/articles/crypto-investors-cash-out-2-billion-in-usd-coin-after-bank-collapse-1338a80f>, accessed 28 March 2023 ; 'Global Cryptocurrency Charts: Total Cryptocurrency Market Cap' (Coin Market Cap), available at: <https://coinmarketcap.com/charts/>, accessed 28 March 2023.

<sup>68</sup> This position is supported by the European Banking Authority as illustrated in its report on macroprudential risks related to crypto. See, 'Advice on the review of the macroprudential framework', 2022, European Banking Authority (EBA), at chapter 5.2, available at <https://www.eba.europa.eu/eba-proposes-simplify-and-improve-macroprudential-framework>.

<sup>69</sup> 'Decentralized Finance Market Size, Share & Trends Analysis Report', 2022, Grand View Research, available at: <https://www.grandviewresearch.com/industry-analysis/decentralized-finance-market-report>.

<sup>70</sup> PricewaterhouseCoopers, 3rd Annual Global Crypto Hedge Fund Report 2021, 2021, available at: [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf).

<sup>71</sup> TVL relates to the total value of all crypto-assets (expressed in USD) that are locked into a DeFi protocol. "Locked into" means that crypto-assets are locked for any duration by a smart contract operated by the protocol. This value is not meant to represent, for example, the number of outstanding loans, but rather the total amount of underlying supply that is secured by a specific application.

<sup>72</sup> 'DefiLlama' (DefiLlama), available at: <https://defillama.com/>, accessed 25 February 2023.

<sup>73</sup> 'Proof of Reserves by Cryptocurrency Exchanges – GeckoTerminal' (GeckoTerminal), available at: [https://www.geckoterminal.com/proof\\_of\\_reserves/exchanges/](https://www.geckoterminal.com/proof_of_reserves/exchanges/), accessed 25 February 2023.

as roughly USD 4 billion, up from roughly USD 2 billion in 2019.<sup>74</sup> We have estimated that the market valuation for initial coin offerings (ICOs) in the period of 2018-19, at the height of the ICO-bubble, was in the range of USD 100 billion.<sup>75</sup>

With the large-volume cryptocurrencies such as BTC and ETH included, the **capitalization of cryptocurrencies** is today at USD 1.10 trillion. At its peak (10 November 2021), the total capitalization was at USD 3 trillion.<sup>76</sup> The extreme drop of 60% is *one* of the drivers of the Crypto Winter discussed in the next section.

## 2.5. The Crypto Winter of 2022-23

The Crypto Winter of 2022-23 is first characterized by the collapse of DeFi stacks due to technical deficiencies or assets going missing from August 2021 onwards, and then from May 2022 onwards, by a set of bankruptcies of centralized crypto intermediaries.<sup>77</sup> All in all, these events undermined trust in the crypto industry, triggered asset valuation deterioration and prompted various regulators to move crypto-assets up their agenda.<sup>78</sup>

### 2.5.1. Large-scale asset diversions starting in 2021

The Crypto Winter 2022-23 was preceded by a series of events where **outsiders could exploit a system's deficiency and divert assets**.<sup>79</sup>

Table 1 lists some high-volume asset diversions in the crypto sector. Several large-scale asset diversions took place in the second half of 2021 and 2022, undermining trust in the institutional stability of crypto platform models and protocols in general.<sup>80</sup>

<sup>74</sup> PricewaterhouseCoopers, *3rd Annual Global Crypto Hedge Fund Report 2021*, 2021, available at: [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf).

<sup>75</sup> Zetsche, D. A., Buckley R. P., Arner D. W., Föhr, L., 2018, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, Harvard International Law Journal, 63 (2), available at SSRN: <https://ssrn.com/abstract=3072298> or <http://dx.doi.org/10.2139/ssrn.3072298>.

<sup>76</sup> 'Historical Snapshot' (CoinMarketCap), available at: <https://coinmarketcap.com/historical/20211107/>, accessed 29 March 2023.

<sup>77</sup> This section is drawing on Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>78</sup> See, International Monetary Fund (IMF), 2023, *Elements of Effective Policies for Crypto-assets*, available at: <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-assets-530092>; Aquilina M., Frost J., Scrimpf, A., 2023, *Addressing the risks in crypto: laying out the options*, Bank of International Settlement (BIS), available at: <https://www.bis.org/publ/bisbull66.htm>; Financial Stability Board (FSB), *The Financial Stability Risks of Decentralised Finance*, 2023, available at: <https://www.fsb.org/wp-content/uploads/P160223.pdf>.

<sup>79</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>80</sup> Ibid.

Table 1: Major asset diversions

DATE	PLATFORM	TYPE	D/C	ASSETS DIVERTED	METHOD
Jul '15	Mt. Gox	CEX	C	\$ 473,000,000	Inside job / mismanagement
Jan '18	Coincheck	CEX	C	\$ 534,000,000	Inadequate security
Feb '21	CreamFinance	Lender	D	\$ 38,000,000	Flash loan attack
Mar '21	PAID Network	Payment services	D	\$ 7,000,000	Infinite mint attack
Aug '21	CreamFinance	Lender	D	\$ 25,000,000	Flash loan attack
Aug '21	Poly Network	Bridge	D	\$ 611,000,000	Software bug
Oct '21	CreamFinance	Lender	D	\$ 130,000,000	Flash loan attack
Oct '21	Compound	Lender	D	\$ 150,000,000	Software bug
Nov '21	bZx Protocol	Lender	D	\$ 55,000,000	Stolen private keys
Dec '21	Bitmart	CEX	C	\$ 196,000,000	Stolen private keys
Dec '21	VulcanForged	GameFi	D	\$ 140,000,000	Stolen private keys
Dec '21	BadgerDAO	Bridge	D	\$ 120,000,000	Governance attack
Feb '22	Wormhole	Bridge	D	\$ 325,000,000	Bridge exploit
Feb '22	Qubit Finance (X-Bridge)	Bridge	D	\$ 40,000,000	Bridge exploit
Mar '22	Ronin Network	GameFi	D	\$ 625,000,000	Stolen private keys
Apr '22	Beanstalk	Stablecoin	D	\$ 182,000,000	Flash loan attack
Aug '22	Nomad Bridge	Bridge	D	\$ 190,000,000	Software bug
Sep '22	Wintermute	Market Maker	pD	\$ 162,000,000	Software bug
Oct '22	Binance	CEX	C	\$ 570,000,000	Bridge exploit
Nov '22	FTX	CEX	C	\$ 477,000,000	Inside job / mismanagement

Source: Research by ADA Chair in Financial Law (inclusive finance), University of Luxembourg.

In some of these instances, private keys were stolen through hacking the wallets of crypto custodians and exchanges while they were online (so-called “Hot Wallet Hacks”).<sup>81</sup> In others, the attackers hacked into the governance mechanism to adopt the means to control the protocols of the platform (so-called “Governance Hack”), allowing them to divert assets held by the platform.<sup>82</sup> Further, attackers conned users into disclosing their private key, or took the private key from the user’s wallet application, which were used to divert assets, or adopted thousands of tokens through ‘flash loans’ (i.e. loans that are granted and repaid back in milliseconds) to engage in arbitrage against the platform. Another common type of exploit has become the bridge exploit.<sup>83</sup>

It is revealing that **over a period of years several platforms experienced the same type of attack**, casting doubt on the industry’s ability to learn from incidents and enhance risk management. For

<sup>81</sup> Examples: Mt. Gox.

<sup>82</sup> Example: Beanstalk. The attackers take out an uncollateralized loan which must be paid back before all transactions are recorded on the blockchain (dubbed ‘flash loan’) to borrow a controlling stake of governance tokens of the beanstalk protocol. The attackers continued by creating a proposal via the governance system of the protocol that stated to send all treasury funds of the protocol to the attackers’ address. The attackers used the borrowed tokens (a controlling majority) to approve the proposal, which depleted the treasure and sent all funds to the attackers. After, the initial flash loan was repaid. This process is executed by smart contracts and was finished in seconds. Cf. Faife, C., ‘Beanstalk founders dismissed concerns about governance attacks before losing \$182 million’, (The Verge, 22 April 2022), available at: <https://www.theverge.com/2022/4/22/23037325/beanstalk-dismissed-governance-attacks-lost-182-million>, accessed 25 February 2023.

<sup>83</sup> Due to their design, blockchains are inherently non-interoperable. To achieve fully decentralized interoperability of two or more blockchains, DeFi protocols are necessary to facilitate the transfer of funds from one blockchain to another. These protocols are known as bridges. In contrast to what the name suggests, the tokens are not in fact transferred (bridged) from one blockchain to the other. Rather, the tokens are locked on the original chain by way of a smart contract and are supplemented by a similar token of equal value on the other chain (to which the asset shall be ‘transferred’). These smart contracts have been known to contain bugs that present vulnerabilities. Nefarious actors have used these bugs to “trick” the smart contract into thinking that the tokens on the original chain are supplied, allowing the hackers to create millions worth of tokens on the receiving blockchain without locking in value on the original chain in return, essentially creating millions worth of cryptocurrency tokens out of thin air (code). This kind of exploit was used in attacks on Wormhole, Qubit Finance’s X-Bridge, Binance and others (cf. Table 1). Cf. ‘BRIDGES’ (Ethereum Foundation), available at: <https://ethereum.org/en/developers/docs/bridges/>, accessed 26 February 2023.

instance, CreamFinance was subject to three similar attacks within a timespan of less than one year and different platforms are subject to similar attacks, again, in close time proximity of one another.<sup>84</sup>

### 2.5.2. Terra/Luna collapse

The pinnacle of the Crypto Winter was the set of **operational malfunctions** in prominent DeFi systems, **undermining the belief that developers could manage the technical and financial complexity related to the very protocols they had written**.<sup>85</sup> The Terra UST/Luna collapse is particularly insightful. Prior to its crash, Terra's UST stablecoin was the fourth-largest stablecoin with USD 18 billion in market capitalisation.<sup>86</sup> Terra's UST coin was pegged to the underlying fiat currency via Terra's LUNA token. That link was designed to stabilise the supply and demand of UST through contracting (or expanding) the UST pool by using the LUNA pool as a counterweight. As Terra grew in size, the protocols could not handle the resulting volume of activity and failed. Terra's algorithmic stabilisation mechanism probably became overwhelmed because its Anchor protocol offered a hefty, and probably overly ambitious, 20% return for staking UST (since UST holders often sold *en masse* if they feared LUNA would fail).<sup>87</sup> Additionally, it is speculated that the Terra project came under a coordinated attack to break the link and so bring profit to those that held short positions in the coins linked to the platform (as had happened with the IronFinance algorithmic stablecoin project in 2021).<sup>88</sup>

Compared to pre-collapse valuations, the UST token lost approximately USD 18.5 billion in value, while the LUNA token lost even USD 30 billion (5 April 2022) during the month of May 2022, with a loss of value of USD 10 billion in one single day (8 to 9 May 2022).<sup>89</sup> With these total losses of almost USD 50 billion in just a couple of days, the Terra/Luna collapse likely became the **largest realized operational risk ever experienced in finance**.

<sup>84</sup> Cf. Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>85</sup> Ibid.

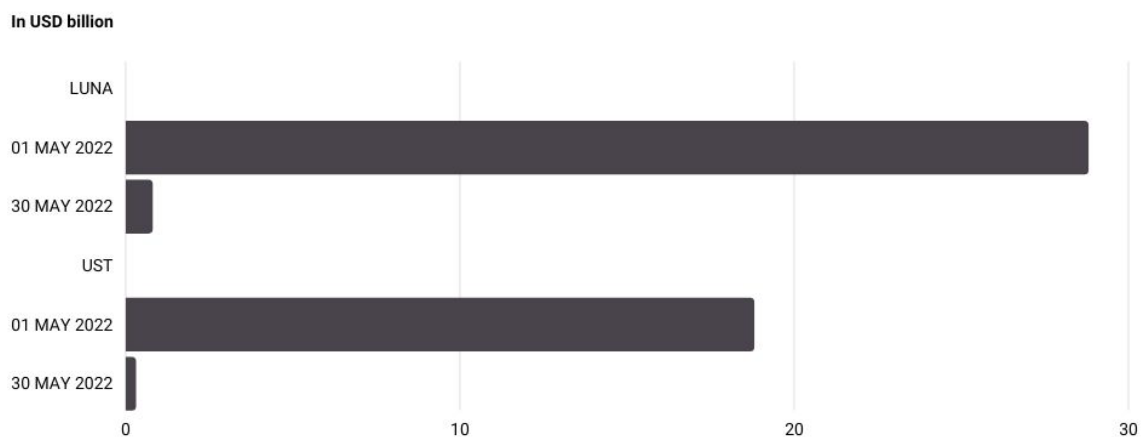
<sup>86</sup> 'Historical Data for TerraClassicUSD' (CoinMarketCap), available at: <https://coinmarketcap.com/currencies/terrausd/historical-data/>, accessed 29 March 2023.

<sup>87</sup> See e.g., Lopatto E., 2022, *How the Anchor protocol helped sink Terra*, The Verge, available at: <https://www.theverge.com/2022/5/20/23131647/terra-luna-do-kwon-stablecoin-anchor>, accessed 26 February 2023.

<sup>88</sup> See e.g., 'Locke T. 'Did a 'concerted attack' cause Terra's UST to crash below \$1? An exec behind the largest stablecoin and experts agree it's suspicious' (Fortune), available at: <https://fortune.com/2022/05/13/terra-ust-stablecoin-crash-suspicious-potential-attack-george-soros/>. See also Adams A., Ibert M., 'Runs on Algorithm Stablecoins: Evidence from Iron, Titan and Steel, Board of Governors of the Federal Reserve System' (FEDS Notes), available at: <https://www.federalreserve.gov/econres/notes/feds-notes/runs-on-algorithmic-stablecoins-evidence-from-iron-titan-and-steel-20220602.html>, accessed 26 February 2023.

<sup>89</sup> 'Historical Data for TerraClassicUSD' (CoinMarketCap), available at: <https://coinmarketcap.com/currencies/terrausd/historical-data/>, accessed 29 March 2023.

Figure 3: Value Destruction in the Terra/Luna Collapse



Source: Own figure based on 'Historical Data for TerraClassicUSD' (CoinMarketCap).<sup>90</sup>

Given that many other crypto ecosystems and intermediaries held UST and/or Luna as safe investments, such as part of their reserves, the USD 50 billion in losses spread through all of crypto. Generally speaking, decentralization meant that the large losses were born by a multitude of users such that each suffered a downturn of their respective token values (i.e. the losses were “decentralized” in a way). However, a substantial fraction of these losses materialized on the balance sheets of large crypto intermediaries and triggered the chain of bankruptcies discussed in the next section.

### 2.5.3. Bankruptcies of SICIs

The losses in Terra/Luna met an environment that was already destabilized by the set of operational malfunctions experienced since August 2021. The **Terra/Luna collapse in spring 2022 thus sparked a chain reaction resulting in a string of bankruptcies, culminating in the failure of FTX and Silvergate Bank and the closure of Signature Bank in New York.** To put these into context, while the second half of 2021 was characterized by events where *outsiders* could exploit a system’s deficiency and divert assets, both Terra/Luna and the bankruptcies that mark the peak of the Crypto Winter show the lack of **internal capacity** on the side of crypto intermediaries **to deal with the risks related to their business models.**<sup>91</sup> However, if crypto was truly or primarily decentralized, we would not expect such a chain reaction – the philosophy of crypto was to avoid the interlinkages known from traditional finance.<sup>92</sup>

Figure 4 lists the most prominent crypto bankruptcies since 2022 by gross liabilities.<sup>93</sup>

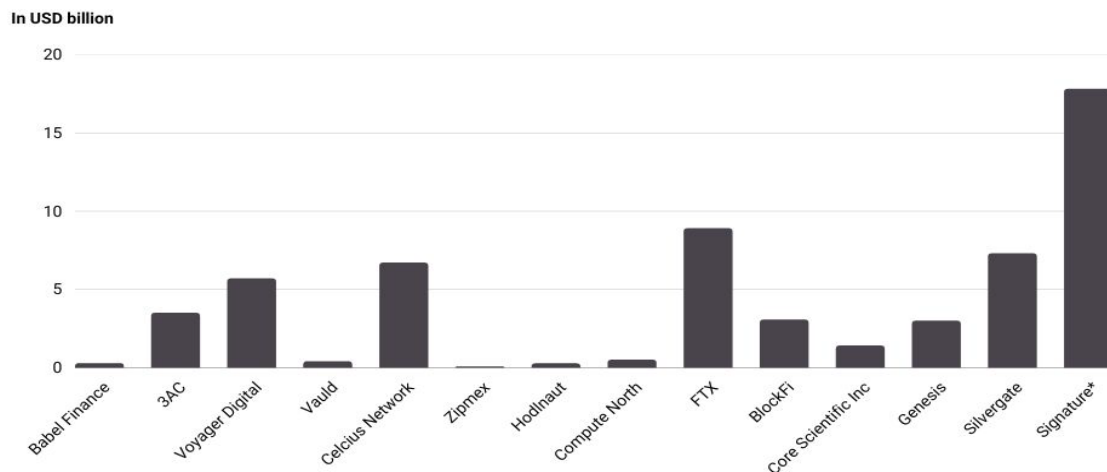
<sup>90</sup> Available at: <https://coinmarketcap.com/currencies/terrausd/historical-data/>, accessed 29 March 2023.

<sup>91</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>92</sup> Ibid.

<sup>93</sup> Note that we exclude SVB from this list as SVB was a traditional financial institution exposed to crypto clients’ withdrawal demands, rather than a crypto intermediary. In contrast, Silvergate and Signature do fit the definition of “crypto intermediary” since they offered several crypto related services, most significantly functioning as a clearing house for major CEXs.

Figure 4: Crypto bankruptcies by gross liabilities



Source: Research by ADA Chair in Financial Law (inclusive finance), University of Luxembourg.

Note: The figure only includes Signature Bank's exposure to crypto as stated in its yearly Federal Deposit Insurance Corporation (FDIC) filings.<sup>94</sup>

While crypto firms cite the negative price development in large crypto-assets as the main reason for their difficulties, we doubt that the price downturn in Bitcoin is the sole reason for the financial difficulties. Bitcoin miners such as Compute North and Core Scientific suffered from rising power costs and increased difficulty of mining bitcoin.<sup>95</sup> A closer look at the crypto intermediaries, however, suggests that a combination of **deficient accounting, lack of internal controls, deficient risk management** (especially lack of position limits and margin management) and **outright mismanagement** contributed to the state of bankruptcy.<sup>96</sup>

For instance, Babel Finance apparently lost USD 280 million when engaging in proprietary trading in Bitcoin using clients' assets: Babel had opened unhedged positions shortly before the BTC price went from USD 30,000 to 20,000.<sup>97</sup> Three Arrows Capital (3AC), a crypto hedge fund, used high levels of leverage to make a series of large directional trades in Grayscale Bitcoin Trust (GBTC), Luna Classic (LUNC) and Staked Ether (stETH).<sup>98</sup> Note that 3AC was trading funds primarily borrowed from over 20 other institutions, hence the losses on its positions spread throughout the DeFi sector. Yet, similarly to Babel Finance, unhedged position risk materialized and risk management was underdeveloped. The same pattern – large losses in proprietary trading covered with clients' funds – displayed also in FTX, at which we take a closer look *infra*, at 2.5.4.

<sup>94</sup> Signature Bank, 'FORM 10-K x ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2022'.

<sup>95</sup> The difficulty of mining Bitcoin increases the more "mining power" is active on the network.

<sup>96</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>97</sup> Oliver Knight 'Lender Babel Finance Lost \$280M Trading Customer Funds: Report' (Coindesk, 29 July 2022), available at: <https://www.coindesk.com/business/2022/07/29/babel-finance-lost-280m-trading-customer-funds-report/>.

<sup>98</sup> Wollinsky J. 'How Hedge Fund Three Arrows Capital Was Crypto's Long-Term Capital Management' (Forbes), available at: <https://www.forbes.com/sites/jacobwollinsky/2022/08/24/how-hedge-fund-three-arrows-capital-was-cryptos-long-term-capital-management/?sh=25138e94633e>, accessed 11 February 2023.

These cases of insolvency cast doubt on the fitness of DeFi key personnel and the crypto industry in general to manage financial institutions in market downturns, and on the operational robustness of crypto generally.<sup>99</sup>

#### 2.5.4. In particular: FTX

The bankruptcy of FTX Group may be understood as the “Lehman moment” of crypto.<sup>100</sup>

From one perspective, the FTX failure was a classic liquidity crisis that turned into a solvency crisis, similar to that of Lehmann Brothers in 2008. When a financial intermediary is unable to access sufficient liquidity to continue its business, this liquidity crisis will often turn into a solvency crisis triggering wider losses of confidence in the entire industry sector, and potentially a financial crisis. Despite its efforts to secure a solution in the form of emergency liquidity or otherwise maintaining trust and confidence of other market participants, FTX was unable to secure additional funds and was forced to file for insolvency. The result is a range of insolvency actions in major jurisdictions and regulatory, investor and customer actions spread around the world.<sup>101</sup>

From that liquidity perspective, the role of Binance as FTX’s largest competitor deserves a closer look. First, a web report disclosed and dissected “a private document” showing the assets of FTX’s trading arm Alameda,<sup>102</sup> criticizing (apparently) excessive exposures of FTX’s investment vehicle to Alameda and to FTX’s main crypto-asset, its own token FTT. Three days later, Binance publicly aired concerns of these exposures and announced via Twitter that Binance decided to liquidate any remaining exposure “due to recent revelations that have come to light”.<sup>103</sup> Binance’s CEO had publicly declared that Binance would reduce exposures in FTT over the following months to avoid pressure on the FTT token price.<sup>104</sup> However, that announcement was made a day after FTT tokens at a value of USD 560 million were transferred from a wallet to Binance Exchange. The transacting wallet stopped being active after the large FTT transactions.<sup>105</sup> This all occurred at a time when about USD 500 million was Binance’s exposure in FTT. If the wallet was operated through Binance, it was front running the liquidity crisis and preserving its own balance sheet from the hit that its own announcement imposed on other crypto investors, who could only sell *after* the announcement had undermined trust in FTX and caused a liquidity crisis in FTT and eventually FTX.<sup>106</sup> By accelerating the deterioration of FTT asset prices (with or without front-running), Binance is unlike regulated intermediaries who, in similar situations, act primarily in coordinated efforts to maintain the overall trust in financial markets. The follow-up behaviour further impresses that Binance expedited the failure of one of its most ambitious

<sup>99</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>100</sup> Ibid.

<sup>101</sup> Ibid.

<sup>102</sup> Allison I., 2022, Divisions in Sam Bankman-Fried’s Crypto Empire Blur on His Trading Titan Alameda’s Balance Sheet’, Coindesk, available at: <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>, accessed 5 March 2023).

<sup>103</sup> See @CZ\_Binance tweet 4:47 p.m. · 6 nov. 2022 (Twitter, 6 November 2022) [https://twitter.com/cz\\_binance/status/1589283421704290306](https://twitter.com/cz_binance/status/1589283421704290306), accessed 5 March 2023).

<sup>104</sup> Ibid.

<sup>105</sup> Transaction Hash: 0x449adc3af3a36d62994d08850a4b8b7ef9269da22b5a11555495bf2e276b6e07 (Etherscan, 5 November 2022), available at: <https://etherscan.io/tx/0x449adc3af3a36d62994d08850a4b8b7ef9269da22b5a11555495bf2e276b6e07>, accessed 5 March 2023).

<sup>106</sup> See Kharif O. ‘Binance To Sell \$529 Million of Bankman-Fried’s FTT Token’ (Bloomberg), available at: <https://www.bloomberg.com/news/articles/2022-11-06/binance-to-sell-529-million-of-ftt-token-amids-revelations#xj4y7vzkg>, accessed 5 March 2023); see Aliaj O., Fontanella-Khan J., Oliver J., Chipolinain S., and Palma S., ‘Binance Ditches Deal to Rescue Rival Crypto Exchange FTX’ (Financial Times), available at: <https://www.ft.com/content/ad440b22-00e2-44e9-b95d-449bb89fd504>, accessed 5 March 2023).



competitors: after posing as a potential “white knight” for several days, Binance opted out with another public statement that made any restructuring effort by third parties impossible.<sup>107</sup>

The answer to the wider question of why exactly FTX had financial problems really hinges on the structure of the FTX Group.<sup>108</sup> Based on publicly available information,<sup>109</sup> the FTX Group basically comprised of four main elements. First was the exchange, an entity licensed in the US which focused on US customers and was the second-largest US crypto exchange prior to the collapse of the group. Second was the global “exchange”, which was really an intermediary – a sort of trading venue, market maker and broker-dealer for cryptocurrency and crypto derivatives trading – supported by a number of regional intermediaries involved in ‘selling’, or intermediating, crypto products around the world. Third, there was a crypto hedge fund called Alameda investing in crypto-assets for its own account, and finally, a variety of venture capital investments.<sup>110</sup> The global exchange had moved its headquarters from Hong Kong to the Bahamas in September 2021 and was registered with the Securities Commission of the Bahamas in accordance with the Bahamas Digital Assets and Registered Exchanges Act 2020.<sup>111</sup> Although FTX as a group was commonly called an “exchange”, some group subsidiaries engaged in speculative buying and selling of crypto products whose issuance it itself controlled.<sup>112</sup>

It seems that the problems arose in the HQ trading arm Alameda.<sup>113</sup> When in financial difficulty, reports suggest customer funds were transferred from the crypto “exchange” to Alameda to cover its losses.<sup>114</sup>

<sup>107</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>108</sup> See e.g., Mollman S., ‘A lot of people have compared this to Lehman. I would compare it to Enron: Larry Summers has some choice words for Sam Bankman-Fried and FTX’ (Fortune), available at: <https://fortune.com/2022/11/11/larry-summers-ftx-crypto-collapse-more-like-enron-than-lehman/>. A Minsky moment, named after the Economist Hyman Minsky, is the moment in a liquidity crisis when the entity becomes insolvent – see e.g., Kregel J. A., 2010, Is this the Minsky Moment for Reform of Financial Regulation?, Levy Economics Institute Working Paper No. 586, available at: <https://ssrn.com/abstract=1559382> or <http://dx.doi.org/10.2139/ssrn.1559382>.

<sup>109</sup> See e.g., Bryce Elder ‘Untangling the knotty empire of Bankman-Fried and FTX’ (Financial Times, 10 November 2022), available at: <https://www.ft.com/content/c28e0570-d4c4-433c-b0a0-c99fba613822>, accessed 6 March 2023).

<sup>110</sup> See e.g., Hern A., and Milmo D. ‘What do we know so far about collapse of crypto exchange FTX?’ (The Guardian), available at: <https://www.theguardian.com/technology/2022/nov/18/how-did-crypto-firm-ftx-collapse> accessed 6 March 2023).

<sup>111</sup> Sam Bankman-Fried had claimed that the greater regulatory clarity in the Bahamas was the principal reason for the move – see Nagarajan S., ‘Sam Bankman-Fried says FTX has moved its HQ from Hong Kong to the Bahamas because of its crypto framework’ (Markets Insider), available at: <https://markets.businessinsider.com/news/currencies/sam-bankman-fried-ftx-crypto-hong-kong-bahamas-relocates-headquarters-2021-9>. As regards the Bahamas Digital Assets and Registered Exchanges Act 2020, see Aliya Allen and Allen A. G., and Mcweeney Jr S. G., 2021, 15 Faq’s on the Digital Assets and Registered Exchanges (‘DARE’) Act, 2020, GrahamThomson News & Insights, 3 (1), available at: <https://grahamthompson.com/wp-content/uploads/2021/01/GT-News-Insights-Vol-3-Issue-1-DARE.pdf>, accessed 12 February 2023.

<sup>112</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>113</sup> The determination of what precisely happened is being severely hampered by deficiencies of FTX’s internal controls, proper accounting systems, and systems for keeping track of customer accounts. As John Ray III, FTX’s court-appointed administrator in bankruptcy has stated, he has never in his entire career seen “such a complete failure of corporate controls”. See also Shubba K., Oliver J., and Indap S. ‘New FTX chief says crypto group’s lack of control worse than Enron’ (Financial Times), available at: <https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7>, accessed 1 March 2023.

<sup>114</sup> See Berwick A., and Wilson T. ‘Exclusive: Behind FTX’s fall, battling billionaires and a failed bid to save crypto’ (Reuters), available at: <https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/>. See, Angus Berwick and Tom Wilson, ‘Exclusive: Behind FTX’s fall, battling billionaires and a failed bid to save crypto’ (Reuters, 11 November 2022), available at: <https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/>. Ian Allison ‘Divisions in Sam Bankman-Fried’s Crypto Empire Blur on His Trading Titan Alameda’s Balance Sheet’ (CoinDesk, 2 November 2022) <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>, accessed 12 February 2023. cf. also the post that broke the scandal of FTX using customer funds to prop up the balance sheet of Alameda: Vicky Ge Huang, Alexander Osipovich and Patricia Kowsmann ‘FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall’ (The Wall Street Journal, November 11, 2022) <https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732?mod=e2tw>, accessed 12 February 2023. Further, see the congressional testimony of John Ray III about the use of customer funds at Alameda: Nikou Asgari ‘FTX allowed trading affiliate Alameda to borrow unlimited funds’ (Financial Times, 12 December 2023), available at: <https://www.ft.com/content/9f07539f-497d-495c-a1e3-3315b8c6f9c9>, accessed 12 February 2023.

If these allegations are true, that behaviour was utterly different from what one would expect from a *bona fide* exchange, or any regulated entity in traditional finance, as it involves large-scale expropriation and diversion of client assets and constitutes a type of fraud prompted by FTX's management.<sup>115</sup>

The lack of transparency has supported accusations of fraud, which the FTX founder Sam Bankman-Fried (SBF) has denied.<sup>116</sup> SBF was arrested in the Bahamas on 12 December 2022 and, owing to an extradition treaty with the US, was placed in the custody of the US authorities and charged in Federal Court in New York with eight counts of fraud and conspiracy.<sup>117</sup> SBF has now been released on a USD 250 million bail, and faces additional charges from the SEC for his role in participating in an (alleged) "scheme to conceal material information from FTX investors".<sup>118</sup> Interestingly, the SEC is in charge of regulating and supervising the trading of, and investment in, *securities* only. To establish jurisdiction in the FTX case, and to charge SBF for non-disclosure of material facts, the SEC classifies the crypto-products issued and traded by FTX as securities under the US securities regulation.<sup>119</sup> We see this approach as exemplifying how EU regulators should generally deal with crypto-assets. Cf. 6.2.2.

### 2.5.5. All service models affected

The incidents of the Crypto Winter confirm that institutional instability is widespread in the crypto industry, notwithstanding the business models beyond crypto "exchanges", including Bitcoin mining companies, stablecoin projects, crypto funds and crypto lenders, as well as crypto-friendly banks (e.g. Silvergate).

As to centralized exchanges, Vauld and Zipmex filed for credit protection on July 2022, Hodlnaut followed suit in August 2022,<sup>120</sup> and FTX and BlockFi filed for bankruptcy in November 2022.<sup>121</sup> The crashes of Babel Finance, Celcius Network, BlockFi and Genesis include crypto lending firms – note that business models are not clear-cut, for instance, both Holdnaut and FTX also ran crypto lending programmes. At the same time, Core Scientific and Compute North are Bitcoin mining firms, the Terra algorithmic crash concerned a stablecoin system, while 3AC acted as a crypto hedge fund (i.e. a proprietary trader on its own account, respective its investors).

<sup>115</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>116</sup> See e.g. Goswami R., and Sigalos M. 'In defensive interview, Sam Bankman-Fried claims he's broke and committed no fraud' (CNBC), available at: <https://www.cnbc.com/2022/11/30/former-ftx-ceo-sam-bankman-fried-says-i-didnt-ever-try-to-commit-fraud.html>, accessed 5 March 2023). See also Shumba C. 'US Justice Department Wants FTX Fraud Allegations to Be Investigated' (CoinDesk), available at: <https://www.coindesk.com/policy/2022/12/02/us-justice-department-wants-ftx-fraud-allegations-to-be-investigated/>, accessed 5 March 2023).

<sup>117</sup> See e.g., Yaffe-Bellany D., Rashbaum W. K., and Goldstein M. 'FTX's Sam Bankman-Fried Is Arrested in the Bahamas' (New York Times), available at: <https://www.nytimes.com/2022/12/12/business/ftx-sam-bankman-fried-bahamas.html?ref=upstrack.com>, accessed 11 February 2023.

<sup>118</sup> See e.g., Race M., and Miller M. 'FTX boss Sam Bankman-Fried arrives in US to face charges' (BBC News), available at: <https://www.bbc.com/news/business-64036615>, accessed 11 February 2023); Yaffe-Bellany D., Rashbaum W. K., and Goldstein M. 'Sam-Bankman-Fried Pleads Not Guilty to Fraud and Other Charges' (New York Times), available at: <https://www.nytimes.com/2023/01/03/technology/sam-bankman-fried-pleads-not-guilty.html>, accessed 29 March 2023.

<sup>119</sup> 'SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto-asset Trading Platform FTX, 2022, U.S. Securities And Exchange Commission-Press Release, available at: <https://www.sec.gov/news/press-release/2022-219>, accessed 29 March 2023.

<sup>120</sup> Oi R., 'Top 10 Biggest Crypto Failures of 2022 (Fintechnews.sg)', available at: <https://fintechnews.sg/67859/crypto/top-10-biggest-crypto-failures-of-2022/>, accessed 29 March 2023.

<sup>121</sup> 'BlockFi Agrees to Pay \$100 Million in Penalties and Pursue Registration of its Crypto Lending Product' 2022, U.S. Securities And Exchange Commission – Press Release, available at: <https://www.sec.gov/news/press-release/2022-26>, accessed 29 March 2023); Iacurci G., 'As BlockFi files for bankruptcy, what to know about crypto investor protections' (CNBC), available at: <https://www.cnbc.com/2022/11/28/what-to-know-about-crypto-investor-protections-as-blockfi-files-for-bankruptcy.html>, accessed 11 February 2023.

All these cases display the same pattern: significant interconnected centralized crypto intermediaries becoming unstable due to mismanagement, lack of internal controls, malfeasance, fraud, theft and a general lack of accountability and transparency.<sup>122</sup>

---

<sup>122</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

### 3. SUPERVISORY AND REGULATORY CHALLENGES OF CRYPTO

#### KEY FINDINGS

Contrary to the arguments of DeFi proponents, **in terms of risks crypto** is in many respects **not different compared to traditional finance**, and so the rationales for regulation are similar. Risks present in crypto – including **agency risks**, conflicts of interests stemming from the bundling of various intermediary functions, use of leverage often hidden in crypto lending and crypto stacking, and concentration risks where SICIs are present – justify regulation under the principle “**same risks, same rules**”.

DeFi is indeed special with regard to **partial, even intensified decentralization (as in the case of – apparently – “fully decentralized platforms”)**, yet this specialty does not warrant regulatory lenience. Decentralization poses severe challenges when defining regulated activities, ensuring compliance with solicitation rules vis-à-vis EU clients, curtailing operational risk, the application of proper risk management processes and ensuring business continuity in the vicinity of insolvency and a general market crisis in crypto. Further, crypto actors that create significant negative environmental externalities (in particular, energy intensive blockchain consensus mechanisms) evade the disclosure rules promulgated under the SFDR and Taxonomy Regulation under the premise of “full decentralization.”

The innovation, development and inclusion objectives have provided the strongest support for taking a permissive approach to the evolution of crypto from a regulatory standpoint.<sup>123</sup> While there are a range of increasingly sceptical views about the potential of the underlying technology, from our standpoint, it is important to highlight that it has been highly successful in supporting fundraising efforts to date, with capital formation being an important policy objective, especially in support of innovation and SMEs.<sup>124</sup> Additionally, an increasing range of successful applications are emerging in the context of traditional finance, particularly debt capital markets.<sup>125</sup>

However, the Crypto Winter has proven that in terms of risks crypto is in many ways not different from traditional finance, and these risks justify financial regulation (3.1.). In other respects, crypto *is* special, and these idiosyncrasies of crypto must be considered when regulating crypto (3.2.).

#### 3.1. Traditional risks of finance in crypto

##### 3.1.1. Financial stability

Financial regulation fundamentally seeks to prevent or reduce the impact of financial crises, and especially systemic financial crises. Financial stability regulation – both macroprudential and microprudential – is designed to achieve this objective.<sup>126</sup>

<sup>123</sup> Moy C., and Carlson J. ‘Cryptocurrencies can enable financial inclusion. Will you participate?’ (Weforum), available at: <https://www.weforum.org/agenda/2021/06/cryptocurrencies-financial-inclusion-help-shape-it/>.

<sup>124</sup> Essaghoolian N., 2019, *Initial Coin Offerings: Emerging Technology's Fundraising Innovation*, University of California Los Angeles Law Review 66 (1), p. 294.

<sup>125</sup> ‘Web3 and Blockchain’ (Bain & Company), available at: <https://www.bain.com/insights/management-tools-web3-and-blockchain>.

<sup>126</sup> Allen F., and Gu X., 2018, *The Interplay between Regulations and Financial Stability*, Journal of Financial Services Research 53 Journal of Financial Services Research 53, available at: <https://link.springer.com/article/10.1007/s10693-018-0296-7#citeas>, p. 233.

It is characteristic for financial technology to grow quickly due to the scale and scope economies inherent in IT (particularly data and software) and network effects.<sup>127</sup> In turn, any crypto model could bypass the stages of “too small to care” and “too large to ignore” rapidly, and enter the stage of “too big to fail”.<sup>128</sup>

While crypto is not displacing traditional finance, spill over effects within the crypto industry (e.g. from one SICI to another) and into traditional finance pose reasons for concern. In particular, Silvergate and Signature were two “crypto-friendly” regulated banks put into liquidation. SVB experienced a solvency crisis in early March 2023 and needed to be rescued by the US FDIC and Bank of the Federal Reserve. That crisis undermined trust in banking stocks worldwide with severe impact on, for example, Credit Suisse, previously Switzerland’s second-largest bank and a designated globally systemically important bank (G-SIB). SVB was known to be the bank of tech entrepreneurs, including many involved in crypto. Several large crypto platforms deposited their fiat currency reserves with SVB.<sup>129</sup> For instance, crypto giant Circle had, at the time of the bank’s solvency crisis, large deposits with SVB,<sup>130</sup> while SVB denied having had exposure to crypto.<sup>131</sup> Reports indicate that at the time of the insolvency, SVB held at a minimum USD 3.5 billion in deposits from crypto intermediaries. At the same time, it is confirmed that BlockFi (the bankrupt crypto lender with over USD 3 billion in crypto-assets under management)<sup>132</sup> and several other crypto firms were clients of SVB.<sup>133</sup> In addition to this direct exposure, it is likely that many tech-oriented SVB clients held crypto-assets or worked with crypto firms. Therefore, it is reasonable to assume that the deposit outflows prompted by the Crypto Winter were a significant contribution to SVB’s difficulties (indicating systemic risk in the interlinkages of traditional finance and crypto).

For preventative measures, regulators will need information on counterparties, exposures and interconnectivity both across crypto and traditional finance.<sup>134</sup>

### 3.1.2. Market efficiency and transparency

In addition to financial stability, financial regulation focuses on promoting market functioning, transparency and efficiency.<sup>135</sup> Market efficiency seeks a semi-strong form of informationally efficient markets – markets in which prices reflect all publicly available information.<sup>136</sup>

<sup>127</sup> Katz M. L., and Shapiro C., 1985, Network Externalities, Competition, and Compatibility, *American Economic Review*, 75(3) p. 424.

<sup>128</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>129</sup> Crypto firms and crypto related firms confirmed to have had deposits at SVB are: Ripple (undisclosed amount), BlockFi (USD 227 million), Circle (USD 3.3 billion), Pantera (undisclosed amount), Avalanche Foundation (USD 1.6 million), Yuga Labs (undisclosed amount), Proof (undisclosed amount), Nova Labs (undisclosed amount), Dapper Labs (undisclosed amount). Lutz S. and Beganski A. ‘*Silicon Valley Bank Contagion: Crypto Companies Affected Include BlockFi, Circle, Avalanche, Ripple.*’ (Decrypt), available at: <https://decrypt.co/123199/silicon-valley-bank-crypto-companies-contagion>, accessed 14 March 2023.

<sup>130</sup> Ibid.

<sup>131</sup> SVB Financial Group, Form 10-K for Fiscal Year ended December 31, 2022, EDGAR, Securities and Exchange Commission, 24 February 2023, p. 34, available at: <https://www.sec.gov/Archives/edgar/data/719739/000071973923000021/sivb-20221231.htm>, accessed 28 March 2023.

<sup>132</sup> See Figure 4.

<sup>133</sup> See note 129.

<sup>134</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>135</sup> Department of the Treasury, ‘Approaches to Financial Regulation’ (Australian Government, 1 November 1996), available at: <https://treasury.gov.au/sites/default/files/2019-03/p1996-fsi-dp-07-chapt04.pdf>.

<sup>136</sup> Fama E. F., 1970, Efficient Capital Markets: A Review of Theory and Empirical Work, *Journal of Finance*, 25(2), p. 383.

Market efficiency is a natural concern for crypto, for the following three reasons.<sup>137</sup>

First, information is available in a non-structured, unorganized manner and is made available through various private and unregulated channels; hence, investors – whether professional or retail – lack the necessary information to properly evaluate investment opportunities and related risks.

Second, due to erratic disclosure, unregulated and thus non-standardized information streams, and the opacity and complexity of intermediary structures, information and transaction costs are generally unclear while liquidity in most crypto-assets is limited. In turn, with some notable exceptions for some large volume crypto-assets like ETH, arbitrage is unable to push asset prices towards the “right price” based on publicly available information.

Third, for crypto non-financial information on IT architecture, systems design and stability is central to project evaluation. While white papers and project descriptions usually show some features of the IT design, few crypto customers fully understand *both* the technical side of crypto and their financial implications so as to understand and manage the risks. The informational advantages of the developers, and in the case of SICs, the crypto conglomerate developing and operating the system, are significant.

Disclosure is the principal traditional tool to further market efficiency,<sup>138</sup> and should apply in equal measure to crypto via standardization of crypto protocols and transparency on supply and demand of crypto-assets. In the case of crypto, disclosure could focus on standardization of information disclosure requirements and on assurance mechanisms about information quality, such as accounting and auditing standards, technical details of projects, supply and demand in markets and assets, and valuation methods and algorithms. As a beneficial side effect, micro-prudential regulation seeking to enhance the safety and soundness of the operations of crypto intermediaries (as required by MiCA) would reduce fraud and theft, further promote trust, and reduce the need for costly self-protective measures.<sup>139</sup>

### 3.1.3. Client, depositor and investor protection

The third central objective of financial regulation focuses on client, depositor and investor protection.<sup>140</sup> In particular, this focuses on less informed but sometimes overly enthusiastic market participants that lack the means or knowledge to protect themselves. It must also maximize rational behaviour while recognizing that rationality is often not the dominant characteristic of human behaviour. Consumer protection also forms a part of the client protection rationale. In this regard, the secret or hidden centralization and monopolization of market segments, contrary to DeFi principles, runs particularly counter to the expectations of crypto consumers.<sup>141</sup>

---

<sup>137</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>138</sup> Korsmo C. R. 2017, *The Audience for Corporate Disclosure*, *Iowa Law Review*, 102 (4) p. 1581, available at: <https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/ILR-102-4-Korsmo.pdf>.

<sup>139</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>140</sup> Goodhart C., et al., 1988, *The rationale for regulation in Financial Regulation: Why, How and Where Now?*, Routledge, 1998, 1.

<sup>141</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

Client protection takes a number of forms: disclosure to enable informed decisions (as discussed in the context of market functioning and efficiency), enforcement to address misconduct which is ever-present throughout financial history (considered in more detail in the context of market fairness and integrity), and prudential mechanisms to reduce the likelihood of losses from intermediary or infrastructure failures while allowing exit to support market discipline (and thus reinforcing financial stability regulation).<sup>142</sup>

In particular, similar to traditional finance, conflicts of interest that stem from the bundled intermediary functions need to be addressed. Unbundling and separation of functions and information barriers are of particular importance.<sup>143</sup>

### 3.1.4. Market fairness and integrity

Market fairness mainly focuses on criminal behaviour and financial misconduct, such as insider dealing and market manipulation, and thus relates to customer protection. The EU's Market Abuse Regulation (MAR) seeks to ensure market fairness in the field of financial instruments.

Market integrity focuses on the effective enforcement of sanctions, anti-money laundering and anti-terrorist financing rules. Bespoke regulations include the EU's Anti-Money Laundering Directives (AMLDs) and the Transfer of Funds Regulation (TFR).

The Crypto Winter provides examples that touch upon both dimensions of market fairness and integrity. The CFTC's lawsuit against Binance from March 2023<sup>144</sup> also contains allegations in this regard. Among others, Binance is accused of using several hundred anonymous accounts for manipulating token prices for tokens listed at Binance.

Moreover, some crypto intermediaries are still not following requirements from AML/CTF legislation by accepting new funds without Know Your Customer (KYC) checks.<sup>145</sup> Among others, the world's largest crypto exchange Binance is accused of failing to implement effective AML/CTF measures.<sup>146</sup>

There are two possible explanations for this. First, some of the intermediaries operate from jurisdictions where crypto intermediaries are beyond the scope of AML/CTF legislation, or AML/CTF legislation is not properly enforced. Second, in jurisdictions that enforce AML/CTF rules for crypto, some intermediaries characterise their services so as to circumvent existing rules. For instance, they argue they are - due to "full decentralization", the use of "non-custodial smart contracts" and peer-to-peer transactions - not intermediaries subject to this legislation.<sup>147</sup> Alternatively, they characterize crypto-assets as utility assets while only investment and payment crypto-assets are subject to regulation.<sup>148</sup>

<sup>142</sup> Ibid.

<sup>143</sup> Ibid.

<sup>144</sup> Commodity Futures Trading Commission (CFTC) v. Changpeng Zhao, Binance Holdings Limited, Binance Holdings (IE) Limited, Binance (Services) Holdings Limited, and Samuel Lim. *Case: 1:23-cv-01887*, available at: <https://www.cftc.gov/media/8351/%20enfbinancecomplaint032723/download>

<sup>145</sup> *The Chainalysis 2023 Crypto Crime Report*, 2023, Chainalysis, available at: <https://go.chainalysis.com/2023-crypto-crime-report.html>, Chapter 3: Money Laundering.

<sup>146</sup> 'CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange' (CFTC, 27 March 2023), available at: <https://www.cftc.gov/PressRoom/PressReleases/8680-23>, accessed 29 March 2023.

<sup>147</sup> See, e.g., 'Terms of Service, Staderlabs' (Staderlabs), available at: <https://www.staderlabs.com/terms-of-service/>, accessed 29 March 2023; 'Terms of Use 2022', (Aave), available at: <https://aave.com/term-of-use/>, accessed 29 March 2023.

<sup>148</sup> Zetsche, D. A., Buckley R. P., Arner D. W., Föhr, L., 2018, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, Harvard International Law Journal, 63(2), available at: <https://ssrn.com/abstract=3072298> or <http://dx.doi.org/10.2139/ssrn.3072298>.

We will discuss examples of market manipulation and insider dealing separately in the context of non-formalized information and disclosures (at 3.6.).

### 3.2. Partial decentralization: a crypto idiosyncrasy

Crypto differs, however, in some ways from traditional finance. The main aspect is the partial decentralization of functions within the financial ecosystem.<sup>149</sup> For instance, many DeFi systems are built upon the Bitcoin model where the holding of the token is decentralized.<sup>150</sup> In DeFi exchanges (a 'DEX'), the liquidity pool that allows for trading without middlemen is decentralized: the liquidity is generated by multiple users willing to hand over two types of tokens to the pool, in return for a share of the trading fees and for a reward offered by the exchange. Upon a trading event, the trading algorithm will then allocate these tokens to the trading parties.<sup>151</sup> The same partial decentralization may be seen in any other function of the DeFi stack, from valuation over crypto lending to crypto staking.<sup>152</sup>

This partial decentralization results in technical and financial complexity and often a cross-border situation, which renders regulation and enforcement a challenge.<sup>153</sup> Certainly not all functions are decentralized, but there may be cases where many entities (rather than one) must function together to ensure the proper functioning of the stack, and to ensure compliance, cybersecurity, asset recovery, and investor protection. In the example above, several entities must act together to confirm ownership or provide liquidity; without them, neither the holding nor trading of a crypto-asset may take place. In the same vein, several regulators must cooperate and coordinate their actions to enforce existing rules.<sup>154</sup>

Partial decentralization has consequences for the design of regulation.

#### 3.2.1. Custody

A particular concern of customer and investor protection is the technical structure of segregation and custody in the crypto industry. So far, "hot" custody is common practice: the wallet provider holds the private keys of their clients and thus establishes something akin to omnibus accounts that are permanently online and linked to the distributed ledger. Concurrently, crypto intermediaries often manage clients' private keys, that is, the data that confirms ownership of the client's assets are stored in the intermediary's systems. In this set-up, and depending on the technology used, *some* crypto intermediaries storing private keys for their clients represent a single point of failure - contrary to the

<sup>149</sup> This section draws in part on Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>150</sup> Schär F., 2020, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, SSRN, available at: <https://ssrn.com/abstract=3571335> or <http://dx.doi.org/10.2139/ssrn.3571335>.

<sup>151</sup> Ibid.

<sup>152</sup> Anoop V. S., and Goldston J., 2022, Decentralized finance to hybrid finance through blockchain: a case-study of acala and current, *Journal of Banking and Financial Technology* 6, available at: <https://link.springer.com/article/10.1007/s42786-022-00041-0> at p. 109. See also Antolin M., 'What Are Liquidity Pools?' (Coindesk), available at: <https://www.coindesk.com/learn/what-are-liquidity-pools/>.

<sup>153</sup> Carapella F., Dumas E., Gerszten J., Swem N., and Wall L., 2022, *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, Finance and Economics Discussion Series 2022-057, Washington: Board of Governors of the Federal Reserve Board, available at: <https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-potential-and-associated-risks.htm>.

<sup>154</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).



DeFi philosophy.<sup>155</sup> Cyberattacks, fraud or malfunctions can expose the private key (which together with the public one, allow transactions to be initiated) for some seconds at least, and prompt fraudulent transactions from the omnibus account to another controlled by the attacker or fraudster.<sup>156</sup>

Many other concerns have been reported in the context of custody. For instance, some crypto intermediaries have **reused client assets** held in custody without clients' consent. This has been facilitated by the unclear division of functions and authority within a crypto ecosystem, such that it is not always transparent who functions as the contractual party, the liquidity provider, margin agent, and so on. Note that any of these functions can also be provided by a group of nodes acting on the stack, rather than the SICI running the ecosystem.<sup>157</sup>

Further, the use of **omnibus accounts** results in the blending of an intermediary's own and third-party claims in crypto-assets.<sup>158</sup> The industry seems to make no use of the tracing feature implicit in blockchain and distributed ledgers' endless chain of transactions. This happens even as some crypto intermediaries demand ownership in crypto-assets deposited as collateral (cf. *infra*, at 3.3). The private law on competing claims stemming from reuse of assets is unsettled, which renders any true assessment of who holds an asset in bankruptcy and fraud cases very difficult.<sup>159</sup>

Some initial inquiries by the authors into **the terms and conditions of wallet providers** revealed, for instance, that:

- both providers of custodial and non-custodial wallets contractually exclude, in almost all cases, liability for lost assets;
- there is little information on what happens in cases of distress, malfunctions and insolvency;
- whether the provider keeps omnibus or segregated accounts is rarely disclosed clearly to users;
- whether the provider stores crypto-assets in so-called "hot" or "cold" storage is rarely disclosed in the terms and conditions (while it may be disclosed on the website); and
- there are no clauses entitling, or obliging, the provider to represent a token holder in litigation or measures resulting in damage mitigation.

All in all, these insights suggest that terms and conditions are currently drafted in a one-dimensional way and provide little certainty or protection for users. **Custody will warrant further regulatory attention in the future.** MiCA provides some basis for this. Cf. *infra*, at 5.1.4.

### 3.2.2. Crypto stacking

Some DeFi ecosystems are connected to other ecosystems, both technically and financially. For instance, crypto derivatives drawing on a basket of derivatives could connect multiple ecosystems financially, or one token type can integrate another token type in its algorithm, thus embedding the

<sup>155</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>156</sup> Zamani E., Ying He, and Phillips M., 2020, *On the Security Risks of the Blockchain*, Journal of Computer Information Systems, 60 (6) at p. 495.

<sup>157</sup> Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>158</sup> Ibid.

<sup>159</sup> Woxholt J., Zetsche D., Buckley, R. P., Arner, D. W., *Competing Claims to Cryptoassets*, 2022, SSRN, available at: <https://ssrn.com/abstract=4394952>.

other token technically.<sup>160</sup> We refer to this practice as “**crypto stacking**” as several apparently independent stacks are inherently intertwined and connected through protocols.<sup>161</sup> This should not be confused with “**crypto staking**” which refers to the bundling of tokens for operational reasons and which we discuss in-depth *infra*, at 3.4.

The Terra/Luna collapse discussed *supra*, at 2.5.2, provides a vivid example of the operational risks that these links can establish. While the link between UST and LUNA was designed to stabilise the supply and demand of UST through contracting (or expanding) the UST pool by using the LUNA pool as a counterweight, it failed to do so once trading volumes rose beyond technical limits (due to, potentially, some outside influences). As seen from this example, stacking creates operational and financial risks for token holders and crypto finance.

As to financial risks, this practice may create a type of leverage where, due to the multi-level processes, settlement is deferred. In this case, the concerns are similar to what we observed in complex derivatives, which are seen as a main driver of the 2008 Global Financial Crisis. There is no reason to suggest crypto derivatives are less risky for consumers and financial stability than financial derivatives. Absent regulation and disclosure of interconnections and exposures means that the opposite is likely to be true.<sup>162</sup> Besides derivative-style financial risk, the new dimension is the technical interlinkage which may trigger, and has triggered, operational malfunctions and system shutdowns.<sup>163</sup>

### 3.2.3. Insolvency and resolution

Partial decentralization poses particular difficulties in arranging business continuity in insolvency.

If a tech operation providing material financial infrastructure experiences difficulties, it is much more difficult to organize meaningful support for a decentralized network than for a concentrated system. Technical or financial support for one entity will mean that the entity providing the infrastructure has the technical or financial means to address the operational difficulties until a long-term solution can be worked out. Such technical or financial support can be through emergency liquidity assistance, ‘lender of last resort’ facilities, deposit guarantee schemes, or, indirectly, bankruptcy protection by way of special resolution schemes.<sup>164</sup>

This is particularly important in crises where systems and rescue schemes are stressed. Imagine that a network function depends on a myriad of small entities cooperating across the globe and all relying on crucial spare parts – it is easier to channel spare parts to a handful of firms than to dispersed network partners.<sup>165</sup>

The situation is particularly dire in case of insolvency of a SICI on whose operations a platform depends: token holders, nodes and developers derive their incentives to support the platform from benefits generated within the platform’s operations. With insolvency, financial incentives to maintain the

<sup>160</sup> See generally Hacıoglu U., 2019, *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age*, Springer Cham, available at: <https://link.springer.com/book/10.1007/978-3-030-25275-5>.

<sup>161</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, ‘*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*’, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)

<sup>162</sup> Ibid.

<sup>163</sup> For a more complete explanation, see Surujnath R., 2017, *Off The Chain! A Guide to Blockchain Derivatives Markets and the Implications on Systemic Risk*, Fordham Journal of Corporate and Financial Law, 22 (2), pp. 256–304, available at: <https://ir.lawnet.fordham.edu/jcfl/vol22/iss2/3>.

<sup>164</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at p. 191.

<sup>165</sup> Ibid.

systems vanish when several entities need to act together to maintain a system's operation.<sup>166</sup> For instance, where code maintenance requires the upload of an update on many nodes running a software, an update is impossible when nodes stop operating as insolvency looms. Similarly, users will provide less liquidity, and developers will invest less in cyber defence when it becomes likely that their investments will be lost. How to incentivize and integrate these many actors in insolvency, resolution and restructuring proceedings will require new regulatory approaches.<sup>167</sup>

### 3.2.4. Jurisdiction and applicable laws

In a DeFi world of whatever form – anywhere along the spectrum from fully centralized to fully decentralized – determining the jurisdiction of courts and applicable law becomes increasingly difficult.<sup>168</sup> For example, imagine an unincorporated distributed ledger system, such as the governance systems used for the Bitcoin or Ethereum Blockchain. The EU's civil procedural law (laid down in the Brussels regulation) and private international law (laid down in the Rome regulations) look at the substantive claim to determine a court's jurisdiction and the applicable law. The substantive claim regarding distributed ledgers may be based on entirely different legal concepts in different jurisdictions and may vary depending on the service provided and the cause of the claim, including but not limited to contracts, torts, joint venture and partnership law, antitrust law, specific legislation on collective investment schemes, and in some jurisdictions blockchain-specific legislation.<sup>169</sup> While in theory EU private international law is autonomous, that is independent from the national classification, prior to applying the EU private international law judges, similar to financial regulators, need first to classify the services to know which source of autonomous law they apply. Decentralization may blur the picture. In turn, decentralization results in uncertainty as to which courts and laws apply – if any.<sup>170</sup>

The same concern – determining jurisdiction – also extends to matters of financial regulation. While we think of finance as global, as is logical given the hub structure outlined at section 2.1., the reality is a world of individual legal jurisdictions and regulators, coordinated through a range of soft-law systems.<sup>171</sup> EU financial law approaches tend to look at the entity that provides the service, the client to whom the product is sold or services provided, or the market in which it is traded.

Each of these is problematic in the age of DeFi. In a network economy, multiple entities provide parts of a service and clients are similarly spread around the globe, and markets and individual providers lose

<sup>166</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>167</sup> See, e.g., Sarra S., Gullifer QC (Hon) L., 2019, *Crypto claimants and bitcoin bankruptcy: Challenges for recognition and realization*, *International Insolvency Review*, 28 (2) pp. 233–272, available at: <https://doi.org/10.1002/iir.1346>. See also, Mangano, 2019, *The insolvency of cryptocurrency exchanges: Lessons from the BitGrail case - reification of coins, pari passu ranking, and nominalism*, *Banking & Finance Law Review*, 35(1), pp. 197-204, available at: <https://pure.unipa.it/en/publications/the-insolvency-of-cryptocurrency-exchanges-lessons-from-the-bitgr>; Sears J., and Ng J., 2022, *Bit by Bit - the Future Direction of English Insolvency Law and Cryptocurrency, Corporate Rescue and Insolvency*, 15 (2), pp. 53–55, available at: <https://www.dentons.com/en/insights/articles/2022/april/19/bit-by-bit-the-future-direction-of-english-insolvency-law-and-cryptocurrency>.

<sup>168</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, *Journal of Financial Regulation*, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at 184 - 185.

<sup>169</sup> See the various approaches seeking to classify crypto services in Lehmann, M., and Krysa, F., Prévost, E., Schinerl, F., Vogelauer, R., *Staking Your Crypto: What are the Stakes?* 27 January 2023, available at: <https://ssrn.com/abstract=4339687> or <http://dx.doi.org/10.2139/ssrn.4339687>.

<sup>170</sup> Ibid. See also Lehmann, M., *Who owns Bitcoin?*, 21 *Minn. J.L. Sci. & Tech.* 93 (2019).

<sup>171</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, *Journal of Financial Regulation*, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at 184 - 185.

importance as supervisory access and control points. Further, technology allowing decentralization may render entity-based approaches generally less effective.<sup>172</sup>

The often-discussed alternative – a focus on functions – is less than convincing where the services are performed by a set of algorithms operated by a myriad of nodes. For instance, the Bitcoin blockchain is operated by some 100,000 nodes, and the Ethereum blockchain by more than 10,000 nodes!<sup>173</sup> In these cases, a legal focus on functions would require the supervision of a myriad of small contributors to the services, many of which lack the size and financial resources to pay supervision fees and many of which contribute only gradually and partially to the overall service. DeFi may force us to look beyond the entities involved and concentrate supervisory efforts on the technology connecting all relevant entities rather than simply the entities formally connected to the project.<sup>174</sup>

Even so, it remains a challenge to determine which regulator and supervisory authority is in charge. A full DeFi system is, most likely, going to be located everywhere and nowhere – which would make it very difficult to ascertain jurisdiction, assign responsibility and liability rules, and penalize misconduct.<sup>175</sup> Even if we rely on indirect regulation and supervision, the regulated entities will have little means to comply with the regulators' demands. If it is a truly independent system, they might not be able to influence its operation. Supervisory requirements in relation to, for example, organization, governance, legal structure, and management are impossible if there is no staff. Where, for instance, are the headquarters of the Bitcoin blockchain? The important point is there is no 'traditional' firm, entity, or headquarters to which financial regulation will apply. Without this, regulatory agencies are likely to struggle to exert control, which diminishes the important risk-reducing effect of law and regulation.<sup>176</sup>

### 3.2.5. Enforcement

Enforcement is also problematic in the context of DeFi. For instance, financial regulation on outsourcing and delegation generally seeks to ensure that one entity is in charge and liable for compliance with all laws and regulations applicable to that entity even where that entity relies on external service providers.<sup>177</sup> Regulation typically requires entities to manage legal, concentration, and reputation risks relating to outsourcing. In short, these rules create a hierarchy of liability and accountability, based on contractual rather than technical or financial relationships, where the supervised entity needs to ensure compliance from all service providers connected to it.<sup>178</sup> In the world of DeFi, how could a supervised entity enforce its oversight requirements vis-à-vis multiple, dispersed network participants that are spread around the world and subject to entirely different rules, ethics, and reputational concerns?<sup>179</sup> See Box 3 for more details on enforcement in decentralized context.

See Box 3 for further detail on enforcement in a decentralized context.

<sup>172</sup> Ibid.

<sup>173</sup> See 'Bitcoin Nodes' (Bitnodes), available at: <https://bitnodes.io/> accessed 25 March 2023) and 'ETH2' Nodewatch), available at: <https://nodewatch.io/> accessed 25 March 2023.

<sup>174</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at p. 184-187.

<sup>175</sup> Ibid.

<sup>176</sup> Ibid.

<sup>177</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, Available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at p. 187-189.

<sup>178</sup> Ibid.

<sup>179</sup> Ibid.

## Box 3: Enforcement in decentralized finance

The core concern is not that the network participants reside in different countries, but that they are anonymous, dispersed and decentralized. Non-compliance with rules in a network setting is best understood as a risk of defection. The service-integrating entity internalizes all risks from services further down in the financial services value chain. As the entity most likely to be sanctioned and held liable, it has a general interest to avoid sanctions and liability. The interests of the providers of the services that are integrated are not necessarily the same. To the extent that the provider is too financially insignificant to be sanctioned and held liable, they fear neither sanctions nor liability.

In a DeFi setting, many different providers contribute to the end product, and in the absence of collusion among the network participants, issues of causation may erect insurmountable hurdles to liability and sanctions since the burden is on the claimant or sanctioning entity to show that the specific non-compliance of a minor contributor caused the problems. Consequently, where compliance is costly, the many small contributors each have a strong incentive to defect – to deviate from the integrator’s general interest in complying with law, regulations, and contractual provisions. The risk of defection increases with the number of parties involved and decreases with the benefits generated by compliance for each party. In the cross-border world of DeFi, this incentive structure creates additional difficulties. The costs of complying only with one’s own rules are lower than complying with those rules plus the rules of one or more foreign jurisdictions, due to information costs and the necessity of duplicative processes internally and externally.

The problem of DeFi is that we are not talking about two entities (X;Y), but potentially dozens if not hundreds (with N referring to these multiple entities). In turn, X must compensate the many entities (N) for compliance with foreign laws in order to make their compliance profitable, while we see no reason why X’s benefits would increase from doing so. In turn, either X stops cooperating with others (in which case there is no decentralized finance) or X’s profitability decreases (rendering X more likely to be non-compliant to save costs) or the many entities (N) receive less for their compliance with foreign laws, so their likelihood of defection increases. In both DeFi scenarios, we will see less compliance by either X or the many entities (N), that is, existing rules will be enforced less stringently than in a world of a centralized financial services value chain.

Source: Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*<sup>180</sup>.

### 3.2.6. Private law

Due to the Crypto Winter, with several crypto intermediaries filing for insolvency and being subjected to schemes of arrangements, who owns crypto-assets or who has a claim on what, respectively, becomes important. While DLT has been frequently presented as a digital solution to competing claims for the same asset, neither technology nor law solves the competing claims issue with certainty. In fact, private law of EU Member States and beyond are utterly fragmented.<sup>181</sup> This mutes private enforcement of claims in crypto-assets and renders cross-border insolvencies costly and risky.

To remedy the situation, we suggest the law must: (1) recognize property rights in crypto-assets, (2) provide for negotiability based on the assertion of control over private keys (i.e. the holder of a

<sup>180</sup> Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> at p. 187-189.

<sup>181</sup> Lehmann, M., Who owns Bitcoin?, 21 Minn. J.L. Sci. & Tech. 93 (2019).

rightfully acquired private key is deemed the owner), and (3) facilitate the enforcement of titles in crypto-assets by the interplay of private and financial law.<sup>182</sup>

In this field, the harmonization projects under the guidance of Unidroit<sup>183</sup> with additional work provided by the European Law Institute<sup>184</sup> deserve support from EU regulators.

### 3.2.7. Increasing tech-risk

The very centrality of technology as the foundation of DeFi brings entirely new risks: DeFi in whatever form increases technological security risks due to tech dependency and connectivity. This is the case regardless of whether one considers 'strong form' DeFi or 'weak' DeFi, or even DeFi built on centralization (e.g. CEX, crypto lenders, etc.).<sup>185</sup> The risks from the rapid growth of financial technology continue to rise while international FinTech governance lags behind.<sup>186</sup>

Another risk stems from the increasing mix of national security and financial stability factors in financial regulation, leading to potentially sub-optimal regulation.<sup>187</sup>

Finally, the ongoing concentration in crucial financial market infrastructure and the underlying tech industry furthers a tech-monoculture, which facilitates cyberattacks: a weakness detected and used for a cyberattack on one network may be used to force entry into another network. If one adds the interdependence due to decentralization of finance, the outcome becomes potentially very dangerous for customers, and the financial system at large.<sup>188</sup>

Ultimately, any extensive DeFi system provides a huge potential vulnerability. The large losses occurring in the Crypto Winter confirm this assessment.

## 3.3. In depth: crypto lending

### 3.3.1. Functions and structure of crypto lending

Lending platforms provide loans from one user (the lending party) to another user (the borrowing party), hence they may be understood as an example of a peer-to-peer finance analogue to crowdfunding.

Two different set-ups exist. **Centralized service providers** organize the lending, similar to an arranging bank, and charge commission on each transaction to make a profit. Alternatively, the lending is organized by **DeFi protocols running smart contracts whose functioning is administered by a DAO**. As part of the DAO setup, holders of governance tokens tend to have a vote on certain matters (e.g., base interest rates or margin requirements), while the developers embed other decisions within the software code ('protocol') that manages the lending.

<sup>182</sup> Woxholt J., Zetzsche D., Buckley R. P., and Arner, D. W., *Competing Claims to Cryptoassets*, 2022, SSRN, available at: <https://ssrn.com/abstract=4394952>.

<sup>183</sup> See *Digital Assets & Private Law – UNIDROIT*, 2023, UNIDROIT, available at: <https://www.unidroit.org/category/law-technology/digital-assets-private-law/>.

<sup>184</sup> See *ELI Principle on the Use of Digital Assets as Security*, 2022, Report of the European Law Institute, available at: [https://www.europeanlawinstitute.eu/fileadmin/user\\_upload/p\\_eli/Publications/ELI\\_Principles\\_on\\_the\\_Use\\_of\\_Digital\\_Assets\\_as\\_Security.pdf](https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf).

<sup>185</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> <https://doi.org/10.1093/jfr/fjaa010> at p. 190-191.

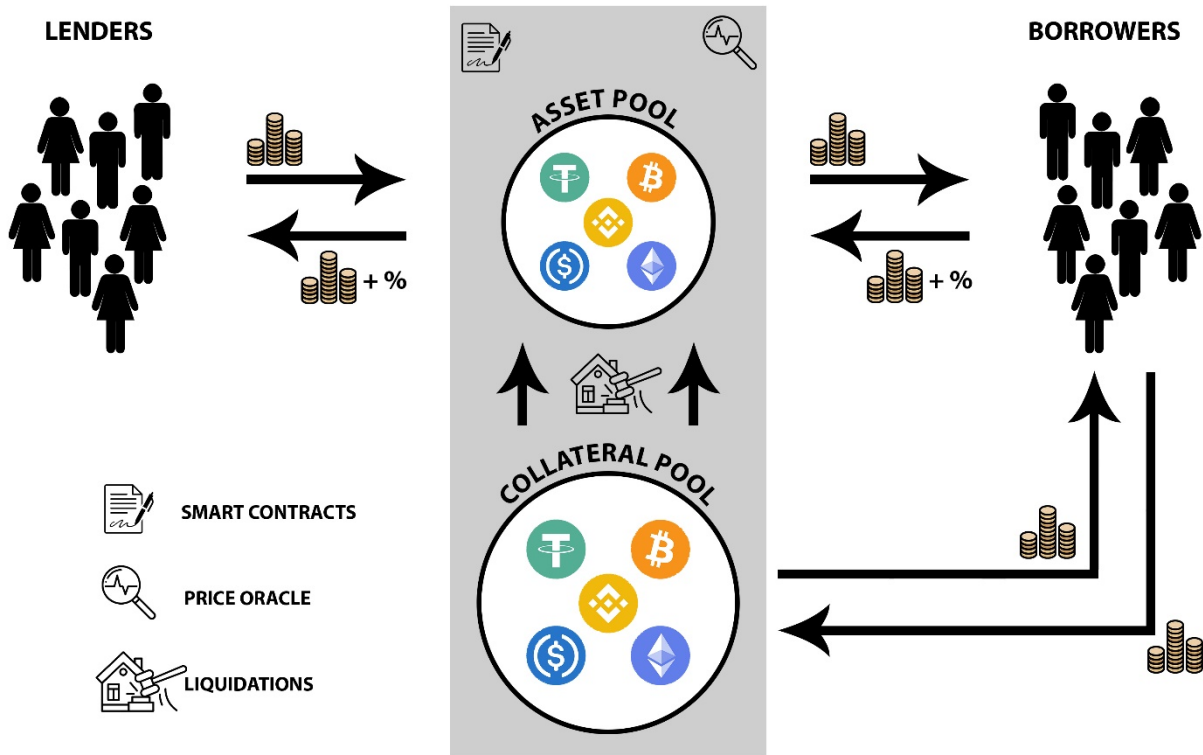
<sup>186</sup> Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. K., 2020, *Technisk*. Singapore Journal of Legal Studies, 35-62, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3478640](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640).

<sup>187</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010> <https://doi.org/10.1093/jfr/fjaa010> at p. 190-191.

<sup>188</sup> Ibid.

For participation in any lending form, users must deposit their crypto-assets on-chain and within reach of the protocol; for that purpose users link their wallet to the protocol and thus render it subject to the conditions of the lending algorithm.

Figure 5: Crypto Lending



Source: ADA Chair in Financial Law (inclusive finance), University of Luxembourg.

Crypto lending protocols offer three different lending services:

- **Peer-to-peer lending (“P2P lending”)**: automatically matches borrowers and lenders one on one.
- **Direct lending**: the platform, or the central lending intermediary, respectively, uses its own funds to lend to the borrower. These funds may initially come from users that had transferred their crypto-assets to that platform/intermediary by way of participating in an Earn Programme (cf. below).
- **Pool lending** (the most common variant amongst decentralized platforms):<sup>189</sup> users commit crypto-assets to a pool from which other users can borrow. In a fully decentralized setting, the pool is locked into (a series of) smart contracts. Users deposit or withdraw funds from the pool by interacting with the smart contracts. In return for locking in crypto-assets, the lenders receive tokens certifying their deposits. The tokens represent their claim (i.e., share of the pool). The tokens also reward the holder by distributing yield.<sup>190</sup>

<sup>189</sup> Pool lending is offered by Aave, JustLend, Compound Finance, Venus and Euler) which, collectively, support 82% of the total value locked of DeFi lending services. See ‘Protocol categories’ (DefiLlama, 2022), available at: <https://defillama.com/categories>, accessed 29 March 2023.

<sup>190</sup> The Aave protocol contains a set of smart contracts for each lending pool, which hold the tokens deposited by lenders. See, ‘Contracts Overview – Developer Documentation’ (Aave, 2022), available at: <https://docs.aave.com/developers/getting-started/contracts-overview>,

While the legal qualification of various users adding their own crypto-assets to the pool is somewhat unclear,<sup>191</sup> we hold that the best characterization is that lenders hold co-ownership in the pool's assets. Yet, none of them alone controls the pool. The collective of users also cannot control who receives the pool's assets, as all decisions are pre-programmed in the protocols, which are drafted by developers/administrators of the lending protocol.<sup>192</sup> Users submit to these conditions by connecting their wallet to the lending platform and signing (with their private key) the transaction sending digital assets to the pool (smart contract) and so participate in the lending program.

After signing the initial transaction to the platform, users may find themselves on one of two sides of the transaction.

In so-called **Earn Programmes**<sup>193</sup> users can register for participation in the program, transfer their cryptocurrencies to the platform and earn a reward in return ("earn interest"). Users function, from an economic perspective, as lenders of crypto-assets. However, the recipient of the assets may vary, depending on the set-up of the protocol. In the case of direct lending, the recipient is the protocol (provider). Earn Programmes are then the protocol's or centralized intermediary's method to generate its 'own' set of crypto-assets for a fee paid to the user. In P2P lending arrangements, the recipient peer is the counterparty – and that entity may change from transaction to transaction. In pool lending arrangements, the nature of the counterparty depends on whether the pool itself has legal entity status.

Regardless of the lending type, crypto firms often pose as counterparty (i.e. borrower). Crypto firms find it difficult to refinance themselves through traditional finance (i.e. bank credit, issuing of public debt) for lack of traditional securities. To get access to finance, these firms offer, on average, high interest rates to crypto lenders at rates that the crypto lenders would not get on traditional bank accounts. The reward ("earn interest") can be as high as a 24% Annual Percentage Rate (APR), and vary by the *token type* that users deposited to the platform (as the protocol seeks to exploit arbitrage opportunities, based on links to other protocols) and *duration* for which the users are willing to lock-in their tokens.<sup>194</sup> These high yields may find appeal among users and incentivize them to deposit (even more) crypto-assets onto their accounts. Yet, there is no free lunch on the market, so the interest rates reflect to some extent the higher risk of lending to these firms that cannot refinance themselves in traditional markets.<sup>195</sup>

Users may also function as **borrowers**. In this case, they borrow either fiat currency or other crypto-assets against the crypto-assets on their account, while the crypto-assets stay on their account as collateral. The funds are provided by the protocol or by other users whose assets are pooled (i.e., they

---

accessed 29 March 2023. The same applies for Venus, a similar decentralized lending protocol (cf. '*Venus: The Money Market & Synthetic Stablecoin Protocol*' (Venus, 2020), available at: [https://venus.io/White paper.pdf](https://venus.io/White%20paper.pdf) at p.6, accessed 29 March 2023 and Compound Finance (cf. Bavosa A. '*Supplying Assets to the Compound Protocol – Quick Start Guide*' (Compound Finance), available at: <https://medium.com/compound-finance/supplying-assets-to-the-compound-protocol-ec2cf5df5aa>, accessed 29 March 2023.

<sup>191</sup> Lehmann, M., and Krysa, F., Prévost, E., Schinerl, F., Vogelauer, R., Staking Your Crypto: What are the Stakes? 27 January 2023, available at: <https://ssrn.com/abstract=4339687> or <http://dx.doi.org/10.2139/ssrn.4339687>.

<sup>192</sup> Our statement is subject to the qualification that the users may in fact exercise control when they (1) collectively hold a majority of governance tokens and they are undertaking ground-breaking changes to the code, (2) organize themselves to exercise these votes in a coordinated manner, and (3) implement a new protocol by way of a vote.

<sup>193</sup> See '*Earn Interest on Your Crypto*' (Nexo, 2023), available at: <https://nexo.com/earn-crypto>, accessed 29 March 2023.

<sup>194</sup> Each platform offers different interest rates depending on which crypto-assets are in demand. See Hristov G., Ullman S., and Nusca A. '*Best Crypto Lending Rates 2023*' (Milkroad), available at: <https://milkroad.com/lend>, accessed 29 March 2023.

<sup>195</sup> The bankrupt lender Celsius serves as a clear example of the risks that users were (unknowingly) exposed to. As many as 1.7 million clients have now become unsecured creditors and may only see a portion of their original funds returned. See Lang H., Howcroft E., Wilson T., '*Analysis: Clients of crypto lender Celsius face long wait over fate of their funds*' (Reuters, 2022), available at: <https://www.reuters.com/technology/clients-crypto-lender-celsius-face-long-wait-over-fate-their-funds-2022-07-15/>, accessed 25 March 2023.



function collectively as lenders within the system). Borrowers, in turn, use the borrowed assets to create leverage. Their initial assets are locked in by the smart contracts that run the protocol as collateral. In case of a default, the smart contract will liquidate the collateral. The protocols remedy the risk of repayment by algorithmic margin management systems that sell the crypto-assets earmarked as security automatically when certain thresholds in terms of Value-to-Loan (VTL)<sup>196</sup> ratio are bypassed. The threshold differs depending on the borrowed and collateralized assets and is determined by the protocols based on the perceived risks of the involved crypto-assets.<sup>197</sup>

Note that lending platforms do **not rely on credit scores analysing the borrowers' personal data (in income etc.) to determine interest rates.**<sup>198</sup> The requirement of (over-)collateralization mitigates the risks of the lender, while liquidation events generally avoid personal indebtedness of users to the platform.<sup>199</sup> This allows the platform to offer the loan without knowing who the borrowers are (on related AML/KYC concerns see *infra*, at 4.3.). However, it also creates externalities that large traders ('whales') have exploited. The resulting losses may destabilize the platform.<sup>200</sup> In turn, platforms operate with substitutes for personal credit scores. Some of these substitutes come with strong incentives to remain inside the network, like "locking-in" clients' assets by rewarding network participation regardless of the financial or operational risk incurred. For instance, Nexo, the one large remaining centralized crypto lender (cf. next section), offers a different interest rate based on the user's **loyalty level**. The loyalty level is determined by the percentage of Nexo-issued crypto-assets (NEXO) held in an account relative to the total value of the account's holdings.<sup>201</sup>

**Multiple rounds of borrowing enable the build-up of leverage:** borrowers that use the *borrowed* funds to acquire new crypto-assets have, after the transaction, a new set of crypto-assets in their account against which they may borrow additional funds for the acquisition of a new set of crypto-assets, and so on. In each stage, the crypto-assets acquired with debt will be locked in, but enable further borrowing and thus enhanced leverage, similar to the way hedge funds operate and build up leverage. Depending on how the protocol values the crypto-asset and what minimum risk cushion it applies, the users may achieve high leverage ratios, with the risk of indebtedness when the crypto-assets' values crash and the debt is owed to the system.

The leverage ratio depends on how the crypto-assets in the deposit are valued by the protocol, and how the new funds are used. For that purpose, the algorithms use so-called **price oracles** that aggregate data from various exchanges to establish the price of the cryptocurrencies.<sup>202</sup> These price

<sup>196</sup> VTL is the relative value of the deposited collateral in relation to the loan that was provided. Protocols often also use the term "Loan-to-Value" (LTV) ratio.

<sup>197</sup> 'Risk Parameters – Aave Documentation' (Aave), available at: <https://docs.aave.com/risk/v/master/asset-risk/risk-parameters>, accessed 29 March 2023.

<sup>198</sup> 'Borrow Interest Rate – Aave Documentation' (Aave), available at: <https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate>, accessed 29 March 2023.

<sup>199</sup> With these processes, crypto lending is – again – more akin to securities lending than cash lending. See 'Why Nexo: Bank Loans vs. Selling Crypto vs. Crypto backed Credit' (Nexo), available at: <https://nexo.com/blog/why-nexo-bank-loans-vs-selling-crypto-vs-crypto-backed-credit>, accessed 29 March 2023 (stating that the users will not be left with personal indebtedness after the liquidation). However, some indebtedness may remain in the more complex case of crypto mortgages, as provided by firms like Milo, Figure and Teller. Teller, with reference to USDC.homes, does mention as a risk of borrowing on-chain: "For USDC.Homes, that may include foreclosure and legal process, or in the case of BNPL NFTs, liquidation of digital assets. Above all, we encourage users to plan their finances responsibly." See 'FAQ – Teller Documentation' (Teller), available at: <https://docs.teller.org/teller-v2/resources/faq>, accessed 29 March 2023.

<sup>200</sup> See Liu B. *Feature or Flaw? Aave Left With \$1.7M in Bad Debt*, (Blockworks, 2022), available at: <https://blockworks.co/news/aave-curve-bad-debt>, accessed 29 March 2023.

<sup>201</sup> 'Nexo Loyalty Program – Explained' (Nexo), available at: <https://support.nexo.com/s/article/nexo-loyalty-program-explained>, accessed 29 March 2023. Note that using loyalty as a measure is not common practice across all DeFi platforms.

<sup>202</sup> Lenders often use third-party oracles to determine prices (cf. 'Price Discovery – Aave Documentation' (Aave) <https://docs.aave.com/risk/asset-risk/price-discovery> accessed 29 March 2023) such as Chainlink (cf. 'Chainlink Data Feeds' (Chainlink) <https://data.chain.link/> accessed 29 March 2023). Nexo has created its own price oracle that can instigate automated re-collateralization

oracles are used by centralized and decentralized lending protocols alike, thus establishing a link between decentralized and centralized crypto lending.

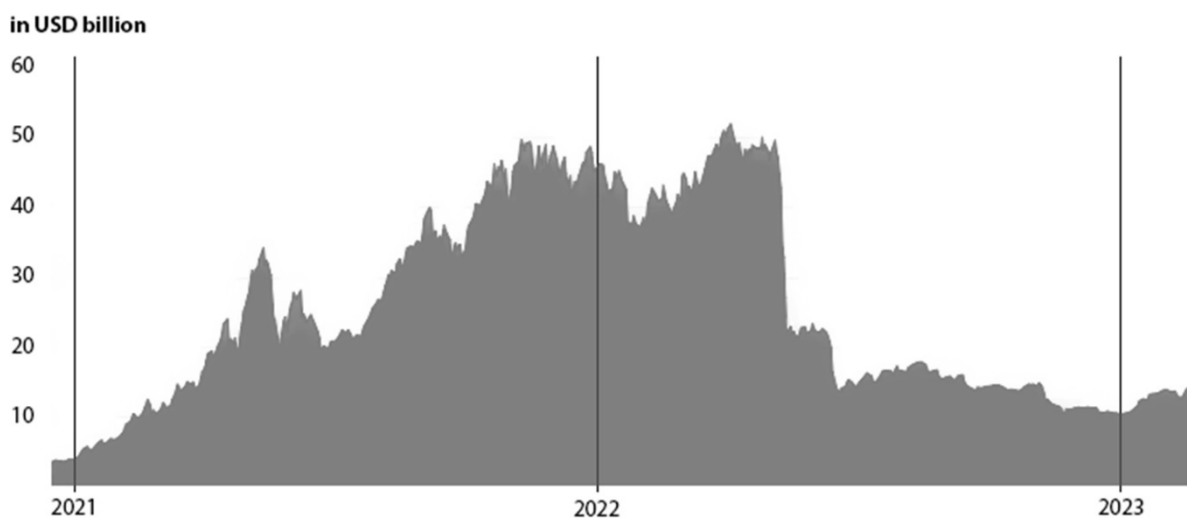
### 3.3.2. Facts and figures

As previously stated, the market differs between decentralized crypto lending protocols operated by DAOs and lending platforms operated by centralized intermediaries. The exact size of the crypto-lending market within the EU is unknown but reports by the European Banking Authority (EBA) indicate the market is limited but expanding within the EU.<sup>203</sup>

#### a. Decentralized protocols

According to the platform DeFi Llama, the cumulative value of loans across all **decentralized crypto lending protocols** reached its peak in the first quarter of 2022, with a total amount close to USD 50 billion globally. Due to the impact of the Crypto Winter, since the Fall of 2022, the cumulative value of loans fluctuated around the USD 10 billion mark.<sup>204</sup>

Figure 6: Size of decentralized lending activity by way of DeFi protocols



Source: 'DefiLlama' (DefiLlama)<sup>205</sup>.

It is estimated that **several hundred decentralized platforms** are operated by DAOs.<sup>206</sup> Table 2 shows the largest ones by TVL (i.e. the sum of all assets from users locked into the smart contracts of the protocols).

of loans (see. 'Automatic collateral transfer' (Nexo) <https://support.nexo.com/s/article/automatic-collateral-transfer> accessed 29 March 2023).

<sup>203</sup> Final Report on response to the non-bank lending request from the CfA on digital finance, 2022, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-provides-its-advice-eu-commission-non-bank-lending>, at para. 37.

<sup>204</sup> 'DefiLlama' (DefiLlama), available at: <https://defillama.com/categories/>, accessed 27 February 2023.

<sup>205</sup> Available at: <https://defillama.com/categories/>, accessed 27 February 2023.

<sup>206</sup> 'DefiLlama' (DefiLlama), available at: <https://defillama.com/categories/>, accessed 27 February 2023.

Table 2: Major Decentralized Lending Protocols

PROTOCOL	TVL (BILLION)	DAO	LEGAL ENTITY	COUNTRY
Aave	\$ 4.77	Yes	Avara UI Labs Ltd.	Cayman Islands
JustLend	\$ 3.49	Yes	n.a.	
Compound Finance	\$ 1.94	Yes	Compound Labs	United States
Venus Protocol	\$ 0.82	Yes	n.a.	
Euler	\$ 0.29	Yes	The Euler Foundation	Cayman Islands
Morpho	\$ 0.28	Yes	Morpho Association	France
Frax Lend	\$ 0.17	Yes	Frax Finance	Cayman Islands
Benqi Lending	\$ 0.12	No	BENQI Finance	United States
Radiant	\$ 0.11	Yes	n.a.	
Algofi	\$ 0.11	Yes	Algofi	United States

Source: Research by ADA Chair in Financial Law (inclusive finance), University of Luxembourg, based on data from 'DefiLlama Lending' (DefiLlama).<sup>207</sup>

Note: The table shows the top 10 decentralized lending protocols by total value locked.

The table shows six out of nine platforms driven by DAOs are linked to a legal entity. According to the self-issued terms and conditions, the legal entities do not perform an intermediary role. The platforms are described as non-custodial smart contracts, governed by DAOs. The legal entities describe their role as "information providers". We strongly disagree with this statement mainly based on the fact that these entities, directly or indirectly, control the smart contracts at the core of the lending protocols or can exercise strong control over the DAO governance.<sup>208</sup> Benqi Lending has announced plans to form a governance DAO shortly.<sup>209</sup> However, contrary to this impression most DeFi protocols are *not* carried by any legal entity, as they operate much smaller platforms where the set-up and administration of a legal entity is likely not economical.<sup>210</sup>

As all decentralized protocols operate on the internet and everyone can participate by linking their wallet to them **each of these services are always available to EU citizens**. Currently, data on these platforms is only available by category, blockchain and other perimeters, and not geographical location of users. Users can make use of DeFi protocols anonymously. To our knowledge, it is not possible to

<sup>207</sup> Available at: <https://defillama.com/categories/>, accessed 27 February 2023.

<sup>208</sup> For example, In 2020 Aave (founded in 2017) transitioned from a centrally controlled platform to a DAO with a decentralized governance model (cf. A Behrens A. 'Aave Officially Hands Over Governance Keys to DeFi Community' (Decrypt, 2022), available at: <https://decrypt.co/46544/aave-officially-hands-over-governance-keys-to-defi-community/>, accessed 29 March 2023. However, in reality, the decentralization is somewhat of a mirage. Firstly, during its ICO in 2017 Aave (then ETHlend) already claimed to be a "fully decentralized peer to peer lending protocol that runs on Smart Contracts". Considering Aave's own words from 2020, this claim would be false and thus the Aave was dishonest about its decentralization ('ETHlend ICO' (ICODrops), available at: <https://icodrops.com/ethlend/>, accessed 29 March 2023. Secondly, in the same article from 2020 it can be read that the original development team will remain (one of the) core developers of the platform. Even though the DAO votes on who develops which features and so exercises control over the platform, in practice and as stated, the platform is reliant on the efforts of the core team still (cf. Adejumo O. 'Aave developers to get \$16.8 in retroactive funding' (Cryptoslate, 2022), available at: <https://cryptoslate.com/aave-developers-to-get-16-8m-in-retroactive-funding/>, accessed 29 March 2023. Thirdly, the original governance token distribution allocated 23% of the tokens to the founders of the protocol (see. Mihajlović M. 'AAVE Tokenomics Explained' (Shrimpy), available at: <https://academy.shrimpy.io/post/aave-tokenomics-explained>, accessed 29 March 2023. The amount of governance tokens that the founders still hold is unknown.

<sup>209</sup> 'Governance' (Benqi), available at: <https://docs.benqi.fi/benqinomics/governance> accessed 29 March 2023.

<sup>210</sup> Examples are, Iron Bank with USD 28 million TVL (see. 'Iron Bank' (Iron Bank), available at: <https://app.ib.xyz/lending>, accessed 29 March 2023), Geist Finance with USD 41 million TVL (see. 'Geist' (Geist), available at: <https://geist.finance/markets>, accessed 29 March 2023 and others (see. 'Lending TVL Rankings – DefiLlama' (DefiLlama), available at: <https://defillama.com/protocols/Lending>, accessed 29 March 2023.

assess the size of the EU decentralized lending market or the number of EU citizens that use decentralized protocols.

#### b. Centralized crypto lending intermediaries

A significant number of **crypto lending platforms operated by centralized intermediaries** shut down in the period of 2022–23. Most notably, Celsius, which managed crypto-assets at a value of USD 12 billion at its peak,<sup>211</sup> experienced substantial losses on investments they acquired with crypto-assets borrowed from users via the Earn Programme,<sup>212</sup> and filed for creditor protection. Gemini Earn froze user withdrawals after its partner, Genesis, a USD 3.4 billion crypto lending company, filed for bankruptcy.<sup>213</sup> BlockFi filed for bankruptcy citing contamination of the bankruptcy of FTX.<sup>214</sup>

After the bankruptcy of these prominent crypto lending arrangers, one of the few remaining centralized crypto lending platforms is Nexo.<sup>215</sup> Nexo claims to have solid risk management principles, professional audits and enough reserves to always pay back customers 1-on-1.<sup>216</sup> Interestingly, Nexo has seen some close calls with regard to customer funds.<sup>217</sup> Further, Nexo uses Armino LLP as its auditor, the same company that had audited FTX.<sup>218</sup> Similar to Alameda's exposure to FTT (FTX's self-issued token) but in lesser amounts, 10 per cent of Nexo's reserves comprise of Nexo's self-issued tokens (NEXO) which may become illiquid when Nexo's financial status deteriorates. Notwithstanding the former, Nexo has never defaulted on any customer withdrawals and holds several licenses within the US, Canada and the EU.<sup>219</sup>

Besides Nexo, it is estimated that several dozen centralized crypto lenders remain. At least six of them – Binance Lending, Crypto.com Credit, CoinLoan, CEX.io, YouHodler and Nebeus – are known to be active in Europe<sup>220</sup> or use languages that indicate they serve EU clients. Others may be active as well but the extent is not easy to determine due to the lack of a central register or harmonized licensing process; further several lenders are observed to be established outside of the EU.<sup>221</sup>

<sup>211</sup> '1.7 million people call Celsius the home for crypto' (Celsius), available at: <https://celsius.network> accessed 29 March 2023.

<sup>212</sup> Knight, O., 'How crypto lender Celsius overheated' (CoinDesk, 16 June 2022), available at: <https://www.coindesk.com/business/2022/06/16/how-crypto-lender-celsius-overheated/> accessed 29 March 2023.

<sup>213</sup> 'Crypto lending unit of Genesis files for U.S. bankruptcy' (Reuters, 20 January 2023), available at: <https://www.reuters.com/technology/crypto-lending-unit-genesis-files-us-bankruptcy-2023-01-20/>, accessed 29 March 2023. 'Lending Rates 2023' (Milkroad), available at: <https://milkroad.com/lend>.

<sup>214</sup> 'Crypto lender BlockFi files for bankruptcy' (Reuters, 29 November 2022), available at: <https://www.reuters.com/video/watch/crypto-lender-blockfi-files-for-bankrupt-idRCV00BM8M>, accessed 29 March 2023.

<sup>215</sup> 'The right place for your digital assets' (Nexo), available at: <https://nexo.com>, accessed 29 March 2023.

<sup>216</sup> 'Nexo's guiding principles for always keeping your assets safe' (Nexo), available at: <https://nexo.com/blog/nexo-guiding-principles-for-always-keeping-your-assets-safe>, accessed 29 March 2023; 'Nexo's Guiding Principles for Always Keeping Your Assets Safe', (Nexo), available at: <https://nexo.com/blog/nexo-guiding-principles-for-always-keeping-your-assets-safe>.

<sup>217</sup> Sun, Z., 'Nexo dodges \$219 M bullet just days before FTX's solvency crisis' (CoinTelegraph, 9 November 2022), available at: <https://cointelegraph.com/news/nexo-dodges-219m-bullet-just-days-before-ftx-s-solvency-crisis>, accessed 29 March 2023.

<sup>218</sup> Foley, S., 'FTX US auditor Armanino defends work for failed crypto exchange' (Financial Times, 23 December 2022), available at: <https://www.ft.com/content/42087255-92ad-45b7-b5ad-3b8457e0c1f8>, accessed 29 March 2023.

<sup>219</sup> 'Licences & registrations' (Nexo), available at: <https://nexo.com/licenses-and-registrations>, accessed 29 March 2023.

<sup>220</sup> Binance, 'Welcome to Binance', available at: <https://www.binance.com/en/about>, accessed 29 March 2023; Crypto.com 'Crypto.com Announces Paris as European Regional Headquarters' (Crypto.com, 12 October 2022), available at: <https://crypto.com/company-news/crypto-com-announces-paris-as-european-regional-headquarters>, accessed 29 March 2023; CoinLoan 'New European Crypto License' (CoinLoan, 10 September 2020), available at: <https://coinloan.io/blog/coinloan-got-a-new-european-crypto-license/>, accessed 29 March 2023; Lielacher, A., 'CEX.IO is a well-regulated exchange with a lot to offer' (Investopedia, 28 February 2023), available at: <https://www.investopedia.com/cex-io-review-5215239>, accessed 29 March 2023; Volkov, I., 'About YouHodler', available at: <https://www.youhodler.com/company>, accessed 29 March 2023; Nebeus 'The Story of Nebeus' available at: <https://nebeus.com/about-us>, accessed 29 March 2023.

<sup>221</sup> 'Final Report on response to the non-bank lending request from the CfA on digital finance, 2022, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-provides-its-advice-eu-commission-non-bank-lending>, at para. 37.

Table 3: EU-Active centralized crypto lending intermediaries

LENDER	LICENSE/REGISTRATION	LICENSER/REGISTRAR	COUNTRY
Binance Lending	Digital Asset Service Provider	Autorité des Marchés Financiers (AMF)	France
	Digital Asset Service Provider	Organismo Agenti e Mediatori (OAM)	Italy
	Virtual Asset Service Provider	Registry of Legal Entities of the Republic of Lithuania and local Financial Intelligence Unit (FIU)	Lithuania
	Virtual Asset Service Provider	Bank of Spain	Spain
	Crypto Asset Service Provider, Class 3	Cyprus Securities and Exchange Commission (CySEC)	Cyprus
	Virtual Asset Service Provider	Polish Tax Administration Chamber of Poland	Poland
	Financial Institution	Swedish Financial Supervisory Authority	Sweden
NEXO	Virtual Currency Operator	Organismo Agenti e Mediatori (OAM)	Italy
	Execution of Virtual Currency Exchange Operator and Deposit of Virtual Currency Wallets Operator	Financial Crime Investigation Service	Lithuania
	Registration of Activities in the Field of Virtual Currencies	Ministry of Finance	Poland
Crypto.com Credit	Virtual Financial Assets Service Provider, Class 3	Malta Financial Services Authority	Malta
Nebeus	Virtual Asset Service Provider	Bank of Spain	Spain
Youhodler.com	Digital Asset Service Provider	Organismo Agenti e Mediatori (OAM)	Italy
CEX.io	Distributed Ledger Technology (DLT) license	Financial Services Commission (GFSC)	Gibraltar
	Moneylending license	Financial Services Commission (GFSC)	Gibraltar
CoinLoan	Financial services, Providing a virtual currency service	Rahapesu Andmebüroo	Estonia
	Financial services, Operating as a financial institution	Rahapesu Andmebüroo	Estonia

Source: Research by ADA Chair in Financial Law (inclusive finance), University of Luxembourg.

### 3.3.3. Legal assessment

According to the terms of some crypto lenders (e.g., bankrupt Celsius), when participating in their Earn Programme, ownership of the deposited tokens is transferred to the crypto lender. In return, users receive a legal claim against the crypto lender for the amount of the deposited funds plus any earned interest. Note that no depositor protection and no insurance scheme for operational risks secures the body of the claim against the crypto lender.

In more modern variants of the protocols, however, users had the choice to retain the title by foregoing participation in the Earn Programme and choosing participation in the Custody Programme.

Figure 7: Terms of Celsius crypto lending

## Key Business Segments – Retail



### **Earn Program: Retail customers transferred coins to Celsius and earned rewards**

- Under the Terms of Use (“TOUs”), title to coins is transferred to Celsius, and Celsius is entitled to use, sell, pledge, and rehypothecate those coins.
- Since April 15, 2022, the Earn product has been limited to U.S. accredited investors and foreign customers.

### **Borrow Program: Celsius lent USD or coins to borrowers who post coins as collateral**

- Borrowers were able to choose from different loan products based upon LTV ratios of posted collateral, with applicable interest rates being higher for higher LTV loans.
- Title to coins is transferred to Celsius and Celsius is entitled to use, sell, pledge, and rehypothecate those coins.

### **Custody Program: Custodial services for customer, incl. U.S. non-accredited investors**

- Began in April 2022
- Title remains with customer and Celsius cannot use coins without instructions from the customer.

Source: Newar, B., ‘Celsius lawyers claim users gave up legal rights to their crypto’ (CoinTelegraph, 19 July 2022).<sup>222</sup>

Crypto intermediary Nexo claims that the title of the assets does not change when they are deposited.<sup>223</sup>

If title transfer takes place, as stated above, **crypto lending is more akin to securities lending** than cash-based credit. In fact, if the crypto-asset is classified as “transferable security”, it is outright securities lending and EU financial laws will apply. This has a number of consequences. For instance, the handling of these transactions will require the license of an investment firm. That investment firm will have to segregate the assets held in custody, ensure proper collateral, calculate operational risks and capitalize the exposures under capital requirements for investment firms. On top, trading of the crypto-asset may require a MiFID-regulated trading platform, and the MAR will apply, rendering price manipulations more difficult.

The notion to apply EU law on securities lending to crypto lending is not entirely novel. In fact, while the term ‘security’ under US law is based on a broader concept than the EU’s financial instrument, dubbed the *Howey* test,<sup>224</sup> some lessons can be learned from the classification of (now bankrupt) crypto

<sup>222</sup> Available at: <https://cointelegraph.com/news/celsius-lawyers-claim-users-gave-up-legal-rights-to-their-crypto>, accessed 29 March 2023.

<sup>223</sup> To prepare this study, we entered into a mock exercise where we asked the one remaining prominent crypto lender Nexo explicitly about the title of assets. The representative confirmed that the title remains with the users.

<sup>224</sup> The *Howey* framework defines an investment contract as “an investment of money in a common enterprise with profits to come solely from the efforts of others.” The *Howey* test is named after the leading case, cf. U.S. Supreme Court (1946), *SEC v Howey Co.* 328 U.S. 293, 307, available at: <https://supreme.justia.com/cases/federal/us/328/293/>, accessed 29 March 2023. For a comparison with EU law, cf. Hacker, P., Thomale, C., Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, (2018) 15:4 European Company and Financial Law Review 645-696, available at: <https://doi.org/10.1515/ecfr-2018-0021>.

lender BlockFi's Earn Programme in a settlement with the US SEC<sup>225</sup>. Gemini Earn and Genesis were also charged by the SEC for offering unregistered securities via their Earn Programme.<sup>226</sup>

The US SEC classified the respective Earn Programme as securities since:

- investors received a *variable* interest rate *determined by the crypto intermediary* on a periodic basis;
- in exchange for crypto-assets loaned by the investors; and
- while investors could demand that the crypto intermediary return their loaned assets at any time.

In the words of the SEC:

'Investors in the BIAs [BlockFi Interest Accounts] had a reasonable expectation of obtaining a future profit from BlockFi's efforts in managing the BIAs based on BlockFi's statements about how it would generate the yield to pay BIA investors interest. Investors also had a reasonable expectation that BlockFi would use the invested crypto-assets in BlockFi's lending and principal investing activity, and that investors would share profits in the form of interest payments resulting from BlockFi's efforts.'<sup>227</sup>

These characteristics mimic what investors that transfer securities for the purposes of securities lending to an investment firm would receive. Under EU law, the contract with the investment firm underlying the securities lending arrangement could be classified as financial instrument. Similar economic characteristics are offered by Money Market Funds (MMFs); EU financial law equally treats MMF units as financial instrument.

### 3.3.4. Regulatory challenges

While inherent to the title transfer users consent to when entering the Earn Programme, users are often **unaware of the fact that the committed cryptocurrencies are "re-used" and even transferred to third parties by the borrower**. For instance, BlockFi has used the committed cryptocurrencies for own investments, i.e. they acquired other crypto-assets and paid for them by transferring the crypto-assets they received from their users. The reuse of crypto-assets was a central aspect in the bankruptcy of crypto lender Celsius that managed at its peak crypto-assets at a value of USD 12 billion.<sup>228</sup> Celsius experienced substantial losses on investments they acquired with crypto-assets borrowed from users via the Earn Programme.<sup>229</sup>

<sup>225</sup> US Securities and Exchange Commission, 'BlockFi Agrees to Pay \$100 Million in Penalties and Pursue Registration of its Crypto Lending Product' (Press release, 14 February 2022), available at: <https://www.sec.gov/news/press-release/2022-26>, accessed 29 March 2023.

<sup>226</sup> US Securities and Exchange Commission 'SEC Charges Genesis and Gemini for the Unregistered Offer and Sale of Crypto Asset Securities through the Gemini Earn Lending Program' (Press release, 12 January 2023), available at: <https://www.sec.gov/news/press-release/2023-7>, accessed 29 March 2023.

<sup>227</sup> Securities and Exchange Commission 2022 'BlockFi Lending LLC, 3-20758', available at: <https://www.sec.gov/litigation/admin/2022/33-11029.pdf>, accessed 29 March 2023.

<sup>228</sup> '1.7 million people call Celsius the home for crypto' (Celsius), available at: <https://celsius.network>, accessed 29 March 2023..

<sup>229</sup> Knight 'O. 'How crypto lender Celsius overheated' (CoinDesk, 16 June 2022), available at: <https://www.coindesk.com/business/2022/06/16/how-crypto-lender-celsius-overheated/>, accessed 29 March 2023.

Figure 8: International standard setters on crypto lending



Source: Author’s own elaboration.

Another issue is **enforcement of existing financial regulation**. It is all but certain that crypto intermediaries comply with all existing financial rules, including AML/CTF and lending requirements.<sup>230</sup> A main concern in the context of enforcement is **jurisdiction**. Upon enquiry within the industry, crypto intermediaries refer to “reverse solicitation”, i.e. they allege they do not need a license when they are contacted by clients upon the clients’ own initiative. Given that the lending intermediaries’ services are available online, any initial contact of clients is classified as reverse solicitation. At the same time, various indicators suggest that the services are oriented towards EU clients. For instance, the system accepts the registration for its newsletters with mail addresses from EU countries, accepts referrals by existing users of EU clients, and accepts EU users in their affiliate programmes. We discuss the related issues more in detail *infra*, at 3.6.

<sup>230</sup> To prepare this study, we entered into a mock exercise where we asked the one remaining prominent crypto lender Nexo explicitly about licenses in Luxembourg and the Netherlands. The website of that lender appoints England and Wales as governing jurisdictions (see, ‘Terms & Conditions – Instant Crypto Credit Lines’ (Nexo), available at: <https://nexo.io/credit-terms>, accessed 29 March 2023). Nexo holds dozens of licenses across jurisdictions, but among EU countries only as “Organismo Agente e Mediatori (OAM) | Virtual Currency Operator” (Italy), as “Virtual Currency Exchange Operator and Depository Virtual Currency Wallet Operator” (Lithuania) and a registration of “Activities in the Field of Virtual Currencies” (Poland). None of these licenses comes, to our knowledge, with passporting rights to the Netherlands and Luxembourg. Upon requests, Nexo’s client services claimed that a) they operate in Luxembourg, and b) they hold licenses for each jurisdiction in which they operate (“We do offer our services in Luxembourg and we have legal entities operating in each supported jurisdiction.”). Furthermore, the AMLD5 applies to Nexo since it offers custodial wallet services as well as on- and off-ramp services. Nexo offers these services to Dutch citizens, which requires Nexo to register with the Dutch Central Bank. However, no such registration is found when consulting the Dutch Central Bank’s register. While we do not claim that Nexo does not apply KYC processes regarding their clients, there is a strong indication that inside the EU’s single market Nexo chooses which laws it likes to apply – and which it does not.



Another challenge, from a user protection perspective, is the innovative capacity of the sector, which has developed a number of credit substitutes with sometimes uncertain financial and legal implications. The following list provides an overview, without claiming completeness:

- users can effectively vouch for the credit provided to other users by **'delegating' their lending capacity;**<sup>231</sup>
- some platforms offer **credit default swaps;**<sup>232</sup>
- some platforms offer **uncollateralized peer-to-peer lending**, by allowing lenders to create lending markets with bespoke know-your-customer and know-your-business checks<sup>233</sup> or, on a larger scale, provide uncollateralized lending to institutional clients;<sup>234</sup> and
- **flash loans** are bespoke uncollateralized loans executed entirely by smart contracts that are designed for making use of arbitrage opportunities and must be repaid within a very short time span of milliseconds and seconds (timespan of "one block").<sup>235</sup> If the conditions for repayment are not met, the transactions will be reversed. That is the reason why the entire loan cycle must be completed within one block or, in other words, before the transaction is recorded on the blockchain.<sup>236</sup> Flash loans have been used to launch governance attacks (cf. *supra*, at 2.5.a).

All in all, crypto lending poses **significant risks for consumers**. While this is both true for decentralized and centralized protocols, from a consumer perspective, the risks are even higher in decentralized platforms for lack of a centralized intermediary that can be held accountable for malfunctions and deficient disclosures. Losses created via the protocols then spread through the crypto system and undermine stability of crypto and related traditional finance.

At the same time, most of these decentralized protocols have evaded regulation so far, for the very reason that they claim to be "fully decentralized" and NCAs find it difficult to provide evidence to the contrary. While we have laid out the difficulties to deal with (apparently) "fully decentralized protocols" generally *supra* at 2.3.4., regulators may find it particularly difficult to apply EU prudential requirements to crypto lending. For instance, the EU capital adequacy and liquidity framework (CRR/CRD) does not apply to peer-to-peer lending, while the Crowdfunding Regulation, the EU's bespoke legislation for peer-to-peer finance, regulates only loans of 'money'<sup>237</sup> and thus does not apply to loans of crypto. At

<sup>231</sup> The Aave platform offers the ability to delegate borrowing power from one user to another. A user who has deposited funds into the pool can delegate their ability to borrow to another user of the protocol. The terms of the delegation are agreed upon between the delegator and the borrower, either off-chain (via any legal agreement) or on-chain via a smart contract (see, 'Credit Delegation – Developers' (Aave), available at: <https://docs.aave.com/developers/guides/credit-delegation> accessed 29 March 2023).

<sup>232</sup> Opium Team collaborated with Aave and created credit default swaps (CDS) based on the Aave credit delegation product (Belyakov A. 'First Credit Default Swap on Aave Credit Delegation Launched' (Medium.com), available at: <https://medium.com/opium-network/first-credit-default-swap-on-aave-credit-delegation-launched-5e3efc961317>). The CDSs are tradable on Opium's exchange. Opium's exchange terms and conditions claim not to be involved in the actual trading since this is executed by non-custodial smart contracts and positions themselves merely as "information provider". Equally, it lacks any reference to registration in accordance with securities laws or the licensed trade in derivatives ('Terms of Service' (Opium Finance), available at: <https://app.opium.finance/eth/terms-of-service>, accessed 29 March 2023).

<sup>233</sup> For instance, 'Borrow against any token in your wallet' (Teller), available at: <https://teller.org>, accessed 29 March 2023.

<sup>234</sup> For instance, 'Make the most of your USDC' (TrueFi), available at: <https://truefi.io>, accessed 29 March 2023.

<sup>235</sup> Flash loans were first introduced by Marble Max, see Wolff 'M., 2018, *Introducing Marble. A Smart Contract Bank*' (Marble.org via Medium, 16 July 2018), available at: <https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890>, accessed 29 March 2023.

<sup>236</sup> 'Flash Loans' (Aave), available at: <https://docs.aave.com/faq/flash-loans>, accessed 29 March 2023.

<sup>237</sup> Art. 2 (1) lit. b European Parliament and the Council 2020 'Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1503>, accessed 29 March 2023.

the same time, the ‘pool’, at least in the view of the protocol developers, is not seen as an entity for regulatory purposes in itself; hence, crypto lenders are often out of scope of any EU financial regulation. We propose to change that (cf. *infra*, at 6.3.1.).

### 3.4. In depth: crypto staking

#### 3.4.1. Functions and services

##### a. Definition and industry size

The staking of crypto-assets is the process of locking up crypto-assets to support the operations of a blockchain network and receive rewards for doing so. Staking is a key mechanism used by Proof-of-Stake (PoS) blockchains, as opposed to Proof-of-Work (PoW) networks that use mining to validate transactions.<sup>238</sup> Staking as part of the PoS mechanism requires the original token of the designated blockchain to be staked with a so-called validator.

Staking services have attracted wide interest across the crypto industry, with several staking services exceeding, in terms of cumulative value, USD 1 billion (cf Table 4).

Table 4: Staking on Blockchains with a market capitalization above USD 1 billion

NETWORK	TOKEN	MKT CAP (USD)	STAKED (USD)	DELEGATORS	VALIDATORS
Ethereum	ETH	\$ 210,938,714,633	\$ 30,936,542,412	n/a	549949
Binance Chain	BNB	\$ 52,909,328,474	\$ 8,012,478,271	> 11000	29
Cardano	ADA	\$ 12,044,596,086	\$ 8,407,356,878	n/a	885
Solana	SOL	\$ 7,919,895,672	\$ 7,948,402,916	296403	10895
Polkadot	DOT	\$ 7,899,419,242	\$ 4,134,694,733	> 7399	924
Avalanche	AVAX	\$ 5,492,521,113	\$ 3,814,288,891	72996	1167
Algorand	ALGO	\$ 1,569,989,852	\$ 835,187,761	22,558	120
Fantom	FTM	\$ 1,300,577,546	\$ 641,898,230	n/a	64
Multiversx	EGLD	\$ 1,081,652,189	\$ 692,257,401	n/a	n/a

Source: Research by ADA Chair in Financial Law (inclusive finance), University of Luxembourg.

Note: Significant difference in the number of validators is mostly due to different variants of the PoS mechanism. Data gathered on 17 March 2023.

##### b. Use cases

While the terminology is somewhat inconsistent, we have identified several use cases for staking.

First and foremost, staking is used in the context of **validation of transactions**.<sup>239</sup> In a PoS network, validators confirm transactions and add them to the blockchain network, i.e. execute the creation of new blocks and decide which transactions are stored in blocks.<sup>240</sup> Validators earn income from the transaction fees paid for the transactions gathered in the block. Some blockchains offer an additional reward that is given by the protocol to incentivize validators.<sup>241</sup> The likelihood of a validator being selected to create the next block depends on the validator’s stake.<sup>242</sup> In theory, each of the validators is qualified. However, the likelihood to be chosen by the protocol as validator for the creation of new

<sup>238</sup> Irresberger F., Kose J., Mueller P., Saleh F., 2021, *The Public Blockchain Ecosystem: An Empirical Analysis*, NYU Stern School of Business, p. 5.

<sup>239</sup> Please note that the following text describes staking in a basic context. Several blockchains offer an adjusted version of the PoS mechanism.

<sup>240</sup> They do so by combining transactions into a block, validating them and propagating the block to the network.

<sup>241</sup> This practice is common with new blockchain protocols since the transaction fees are often too low to attract validators. See ‘*Stake Fantom, earn rewards*’ (Fantom), available at: <https://fantom.foundation/ftm-staking/>, accessed 29 March 2023.

<sup>242</sup> Irresberger F., Kose J., Mueller P., Saleh F., 2021, *The Public Blockchain Ecosystem: An Empirical Analysis*, NYU Stern School of Business, p. 5.

blocks depends on the number of tokens they have committed ('staked'). As an analogy, you may consider each staked token as a lottery ticket. This follows the assumption that the validators with the largest stakes have the greatest interest in the smooth operations of the blockchain and are thus the most trustworthy agents. It also incentivises the aggregation of the cryptocurrencies involved, resulting in a potentially higher market value.<sup>243</sup> The staked tokens are exposed to risks. If a validator acts dishonestly or shows harmful behaviour<sup>244</sup> the protocol can "slash" a portion of the staked tokens, resulting in a loss of tokens.

PoS mechanisms contain known security risks that can be exploited.<sup>245</sup> The intent of these so-called consensus attacks is mostly to: 1) disrupt the flow of the blockchain and create distrust and 2) double-spend cryptocurrencies.<sup>246</sup> In practice, these attacks require substantial amounts of staked cryptocurrencies.<sup>247</sup> However, in theory, it is possible to perform a consensus attack with only a small percentage of staked tokens.<sup>248</sup> If blockchains are sufficiently large, the attacks become less likely due to the increased costs of acquiring a substantial enough stake.<sup>249</sup>

To become a validator, it is required to commit an initial amount of tokens of the specific blockchain. The Ethereum blockchain requires a minimum of 32 ETH (USD 55,873).<sup>250</sup> Blockchain participants with insufficient capital or know-how can stake via pooled staking services or other staking programmes.<sup>251</sup>

Beyond the context of transaction validation, **the term crypto staking is often used in a broader sense.** Crypto staking could mean:

- in the context of crypto lending, the automated collection of tokens which are then used as margin for forward transactions (substantively similar to "securities lending"). We have discussed this use case in the context of crypto lending (cf. *supra*, at 3.3.);
- in the context of DeFi governance, the staking of (governance) tokens, which is often required to be able to exercise the voting right over a protocol;<sup>252</sup>
- in the context of DeFi reward schemes, DeFi protocols, such as DEXs and blockchain-based games (GameFi), offer staking services that allow users to stake tokens or NFTs to earn rewards

<sup>243</sup> Gonzalez N. E., 2022, Does Cryptocurrency Staking Fall under SEC Jurisdiction?, *Fordham Journal of Corporate and Financial Law* 27 (2), pp. 521-561 at p. 531.

<sup>244</sup> Examples of dishonest and harmful behaviour include severe connectivity disruptions, running modified software or incorrect execution of validation tasks. The exact parameters of when tokens get slashed differs depending on the blockchain.

<sup>245</sup> Security risks of consensus models are not unique to the PoS model. In fact, PoS is more resilient against certain risks than PoW. See 'Proof-of-stake' (Ethereum), available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> accessed 29 March 2023.

<sup>246</sup> Contrary to popular belief, a consensus attack cannot create new tokens or drain tokens from arbitrary accounts. See, 'Pfledderer T. 'Proof-Of-Stake Attack and defense' (Ethereum), available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/> accessed 29 March 2023.

<sup>247</sup> A consensus attack that aims to reorganize the flow of new blocks (reorg attack) on the Ethereum Blockchain is likely to succeed with a 30% stake. See Neuder M., Moroz D., Rao R., Parkes D., 2021, *Low-cost attacks on Ethereum 2.0 by sub-1/3 stakeholders*, School of Engineering and Applied Sciences, Harvard University, p. 5, available at: <https://arxiv.org/pdf/2102.02247.pdf>.

<sup>248</sup> In theory, a two per cent stake in the Ethereum Blockchain would be sufficient to execute a disruptive reorg attack that can disrupt the flow of new blocks and can force valid blocks to be invalidated. See, 'Pfledderer, T., 'Proof-Of-Stake Attack and defense' (Ethereum), available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/>, accessed 29 March 2023.

<sup>249</sup> Even acquiring two per cent of the total amount staked on the Ethereum Blockchain requires a substantial investment. Two per cent of the total amount of staked ETH is currently 351967.58 ETH, which at today's value equates to USD 611 million (17 March 2023).

<sup>250</sup> USD value taken on 28 March 2023. See, 'Solo stake your ETH' (Ethereum), available at: <https://ethereum.org/en/staking/solo/> accessed 29 March 2023. Please note that the initial amount varies per network.

<sup>251</sup> For instance, 'Binance DeFi Staking' (Binance), available at: <https://www.binance.com/en/defi-staking>, accessed 29 March 2023 and 'Earn up to 6.00% APY on your crypto' (Coinbase), available at: <https://www.coinbase.com/earn>, accessed 29 March 2023.

<sup>252</sup> 'Gauge Voting & Bribes' (Equalizer Exchange Docs), available at: <https://equalizer0x.gitbook.io/equalizer-exchange-docs/guides/gauge-voting-and-bribes>, accessed 17 March 2023.

(tokens or NFTs). The purpose of this type of staking is to incentivise users to purchase tokens or NFTs and is not related to a consensus protocol;<sup>253</sup> and

- in the context of DeFi liquidity, the staking of liquidity provider (LP) tokens.<sup>254</sup> The staked LP tokens accrue rewards from cryptocurrency swaps of LP tokens' underlying cryptocurrencies. LP tokens can also be staked in so-called vaults, also known as yield compounders, essentially lending the LP Token to a DeFi protocol that will strive to optimize the yield of the LP Token.<sup>255</sup>

### c. Crypto staking services

We have identified two archetypes of staking services:

- (1) **Pooled staking services** consist of validator nodes setting up so-called staking pools, to which other token holders can delegate tokens. The validator node stakes the delegated tokens on the delegator's behalf. The delegators earn a pro-rata portion of the rewards, minus a validator fee.<sup>256</sup>
- (2) **Staking Programmes** differ from pooled staking services because an intermediary exists between the delegator and the validator. From the perspective of the customer (delegator), the process is similar. However, in reality, the tokens are delegated to the intermediary who, in turn, delegates the tokens to one or various validators.

The existence of an intermediary can have significant effects on the classification of the programme, at least under US securities law. *SEC v Kraken Exchange* illustrates how the SEC determined that the Kraken Staking Programme was in fact an investment contract since it:<sup>257</sup>

- provided passive investment opportunities by allowing Kraken's customer to delegate their eligible tokens to Kraken Staking Programme and with that to the possession and control of Kraken. Kraken in turn performed various staking-related services (delegation, rewards distribution, and more) to earn the promised return;
- pooled customer assets with Kraken's own proprietary tokens in wallets controlled by Kraken and in turn staked the pool of tokens;
- determined the returns on customers' staked tokens and that the returns differed from those that would have been earned if the customer would have staked directly in the underlying protocol. Kraken also reserved the right to not pay any rewards. Equally so, any surplus of rewards as compared to the advertised reward rates was kept by Kraken;
- altered the reward payment frequency as compared to the frequency that would have existed if the customer staked directly in the underlying protocol;
- offered instant rewards and improved liquidity as compared to staking directly in the underlying protocol. De facto this meant that, even though a protocol would pay rewards only

<sup>253</sup> For instance, 'Fantom Mummy Club' (Mummy Finance), available at: <https://app.mummy.finance/#/nft>, accessed 29 March 2023. This DeFi protocol sold NFTs at the launch of the protocol that earn rewards when the NFTs are "staked".

<sup>254</sup> LP Tokens are minted by supplying two different cryptocurrencies as a pair to a DEX. As proof of deposit of funds, the provider is given a so-called LP Token that resembles his/her claim against the liquidity pool. See 'What Are Liquidity Pool (LP) Tokens?' (Binance Academy, 14 June 2022), available at: <https://academy.binance.com/en/articles/what-are-liquidity-pool-lp-tokens>, accessed 29 March 2023.

<sup>255</sup> See 'Vaults' (Beefy.com), available at: <https://docs.beefy.finance/products/vaults>, accessed 29 March 2023.

<sup>256</sup> See, 'Pooled staking' (Ethereum), available at: <https://docs.beefy.finance/products/vaults>, accessed 29 March 2023.

<sup>257</sup> U.S. District Court Northern District of California San Francisco Division 2023 'SEC v Payward Ventures, Inc. and Payward Trading, Ltd. (Kraken) 23-cv-588', available at: <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-25.pdf>.

after a certain period (bonding period), the Kraken customer was paid instantly, regardless of the rewards paid by the underlying protocol;

- did not stake all delegated tokens with the intent to preserve enough liquidity to pay customers instantly. Kraken did not disclose the size of this reserve, nor how it was stored;
- covered fees and transaction costs, and mitigated minimum staking thresholds, that customers otherwise would have incurred when they would stake directly in the underlying protocol. However, it is unclear if Kraken subtracted any of these costs from the rewards; and
- touted that the Programme was easy and safe to use and complied with global legal standards in various marketing efforts.

The SEC continues by establishing that Kraken promoted the Kraken Staking Programme as an investment opportunity and established that the Programme has earned millions of USD in rewards.

The SEC subjected the above to the Howey framework<sup>258</sup> and concluded that the Kraken Staking Programme was offered and sold as a security, with the following reasoning:

- Participating in the Kraken Staking Programme involved a **payment of money**. Money, not having to take the form of fiat currencies, in the form of cryptocurrencies was transferred to Kraken to be able to partake in the staking Programme and by partaking investors' crypto-assets incurred risks (risk of slashing, liquidity risk and market risk).
- Investors and Kraken **participated in a common enterprise** since all delegated tokens are pooled with Kraken's own tokens and in turn staked.
- Investors could **reasonably expect profits from the efforts of Kraken**. Kraken marketed the Programme as an investment opportunity with high returns and performed various services to achieve these returns and because Kraken's own profits depended on the success of the program, investors could reasonably expect that Kraken would undertake significant and essential technical, managerial, and entrepreneurial efforts to achieve the returns.

The SEC's settlement with Kraken resulted in the discontinuation of the Kraken Staking Programme in the US and a USD 30 million fine.<sup>259</sup> The Kraken Staking Programme is still available in the EU.<sup>260</sup> At face value and considering their terms and conditions, the staking Programme is unchanged as compared to the findings of the SEC.<sup>261</sup>

In the Kraken case, the SEC classified staking *programmes* as investment contracts, but the situation is less certain with regard to staking *pools*.<sup>262</sup> Academics have argued that all staking arrangements,

<sup>258</sup> See references *supra*, note 224.

<sup>259</sup> U.S. Securities and Exchange Commission 'Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges' (SEC Press release, 9 February 2023), available at: <https://www.sec.gov/news/press-release/2023-25>, accessed 29 March 2023.

<sup>260</sup> Kraken's services are offered to residents of European Economic Area (EEA) via its Italian subsidiary Payward Europe Solutions Limited (Italian residents only) or its subsidiary Payward International Markets Limited located on the British Virgin Islands (all other residents of the EEA). However, its staking service is solely offered via its subsidiary Payward Commercial Limited, located on the BVI as well. With regard to the staking service, see 'Earn Staking Rewards | Crypto Staking' (Kraken), available at: <https://www.kraken.com/features/staking-coins>, accessed 29 March 2023. With regard to the terms and additional information about the subsidiaries, see 'Terms of Service' (Kraken), available at: <https://www.kraken.com/legal>, accessed 29 March 2023 at 1. Complete Terms of Service.

<sup>261</sup> 'Terms of service' (Kraken), available at: <https://www.kraken.com/legal>, accessed 29 March 2023 at Annex C.

<sup>262</sup> The enforcement actions and warnings of the SEC to date have been focused on staking programs. In the press release regarding the settlement SEC Chair Gary Gensler is quoted saying "Today's action should make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection."

including pooled staking services, classify as investment contracts,<sup>263</sup> with the notable exception for staking arrangements where profits and losses of validators and delegators are not correlated. In this case, the criteria of a common enterprise is not established.<sup>264</sup>

### 3.4.2. Risk-benefit analysis

Staking is considered a more environmentally friendly alternative to mining, as it does not require the same energy-intensive computation as PoW mining.<sup>265</sup> It also incentivizes users to hold onto their tokens rather than sell them, which can help to stabilize the price of the crypto-asset.

However, staking does come with some risks. Risks include financial and operational risks.<sup>266</sup>

As to financial risks, staking is exposed to liquidity and market risk. As to liquidity risk, when staking, funds are typically locked up for a specified period, which can vary from a few days to several months or more. During this period, the staked funds may not be available for trading or withdrawal, which can lead to temporary illiquidity of the staked token. As to market risk, the value of the cryptocurrency being staked can be volatile and subject to market fluctuations. Depending on the staking protocol, staked tokens can have a so-called “un-bonding” period before they can be withdrawn from a validator. This would prevent a user from being able to react to market conditions.

Staking may also involve significant operational risks. These include:

- **Validator risk:** A validator might act dishonestly which can result in the staked tokens being slashed partially or completely;
- **(Technical) operational risk:** Validators may suffer from technical issues such as software bugs, failed upgrades and server outages; and
- **Network-related operational risk:** If the network fails or experiences a major disruption, staked funds can be lost.

Staking has often been the focus of high returns, attracting users who perceived the risks to be low. However, lack of segregation and custody has instead often meant that rather than a safe high-return investment (which is impossible), users were taking on high levels of **risk via the arranger**, often a decentralized protocol or a crypto intermediary.<sup>267</sup>

There is another less-often discussed aspect of staking. From a more abstract perspective, crypto staking may lead to the **bundling of governance rights to influence the outcome of the voting mechanism** on protocol features and changes. For instance, users may “lend” their tokens or only the governance rights attached to them,<sup>268</sup> to other users, for a fee or altruistic motives.<sup>269</sup> In some of these cases, governance rights remain decentralized in form, but not in function. A person, or group of

<sup>263</sup> Nicholas E. Gonzalez, ‘Does Cryptocurrency Staking Fall under SEC Jurisdiction?’, *Fordham Journal of Corporate and Financial Law* 27, no. 2 (2022): 521-561 at 554.

<sup>264</sup> *Idem* at p. 558

<sup>265</sup> Irresberger F., Kose J., Mueller P., Saleh, F., 2021, *The Public Blockchain Ecosystem: An Empirical Analysis*, NYU Stern School of Business, p. 5.

<sup>266</sup> These risks are the general risks associated with staking. Specific risks stemming from staking via staking programs related to specific terms agreed upon with the intermediary can only be assessed on a case-by-case basis.

<sup>267</sup> See, e.g., Levitin A. J., 2022, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, *Texas Law Review* (forthcoming), 101, available at: <https://ssrn.com/abstract=4107019> or <http://dx.doi.org/10.2139/ssrn.4107019>.

<sup>268</sup> For instance, on the Fantom blockchain, token holders can delegate their token to a validator but still vote on governance proposals based on the amount of tokens that were delegated. If the votes are not exercised, the voting rights are allocated to the validator. ‘Governance’ (Fantom), available at: <https://docs.fantom.foundation/staking/governance>, accessed 29 March 2023.

<sup>269</sup> See, e.g., Chidinma Okoye M. Clark J., 2019, *Toward Cryptocurrency Lending* in Zohar A. et al., *Financial Cryptography and Data Security*, Springer, pp. 367–380. See also, Lau, H., Tse, S., 2021, *Decentralized Basic Income: Creating Wealth with On-Chain Staking and Fixed-Rate Protocols*, Cornell University, available at: <https://arxiv.org/pdf/2107.14312.pdf>.

persons, becomes a dominant stakeholder, contrary to the disclosed functioning of the ecosystem. The situation is not unlike what was debated at length<sup>270</sup> in the context of “vote buying” and “empty voting” in corporate and securities law, yet without the mitigating effects of disclosure rules, corporate law-based collective redress, and in some countries fiduciary duties of large shareholders and “group law” (*Konzernrecht*). All in all, in the governance context, staking could result in an “fully decentralized platform” being controlled by one or a few entities, either temporarily or even permanently, when the control-holders exercise influence over the staking protocol.

### 3.4.3. Regulatory challenges

Staking may **mislead consumers** that do not understand the risks involved in transferring one’s rights to another. We have discussed the issues of an implicit rights transfer in the context of crypto lending. Licensing, disclosure and limitation of lending to sophisticated investors may be the regulatory remedy.

Figure 9: US Securities and Exchange Commission on staking



Source: Author’s own elaboration.

Staking protocols may also be misused for governance and consensus attacks and be a source of **operational risks**. Shortly before a protocol change is voted upon, a staking algorithm may be used to bundle voting rights and adopt, by way of majority, a protocol that allows asset diversion to an attacker. Regulators could address this risk by slowing down the overall voting process, implementing validators and auditors for the voting process, and by setting a maximum limit for votes exercised by one person (‘voting cap’).

Where staking is used in the context of governance, it also stands at odds with the self-presentation of a platform as “**fully decentralized**”. In these cases, staking may facilitate one person or a small group of persons to exercise control over the platform and its processes. Financial regulation seeks to ensure that control over financial assets comes with responsibility for compliance and processes, and liability in the case of malfunctions and non-compliance. Staking thus may help to further regulatory arbitrage, by allowing decentralized platforms to maintain the façade of decentralization, while a small group of people control their operations.

This supports our argument to submit (apparently) decentralized platforms to EU financial regulation (cf. 6.3.). In addition to assigning entity status to DAOs, disclosure as to who has exercised voting rights, and whether staking algorithms were bundling votes, could be installed as a remedy.

<sup>270</sup> See for the US H. Hu & B.S. Black, *The New Vote Buying: Empty Voting and Hidden (Morphable) Ownership*, 79 *Southern California Law Review* 811-908 (2006); for Europe see D.A. Zetsche, *Continental AG vs. Schaeffler, Hidden Ownership and European Law - Matter of Law or Enforcement?*, 10 *European Business Organization Law Review* 115-147 (2009).

### 3.5. In depth: sustainability impact

The innovation, development and inclusion objectives have provided the strongest support for taking a permissive approach to the evolution of crypto from a regulatory standpoint.<sup>271</sup> While we present in this report good reasons for an increasingly sceptical view about the potential of decentralization or token technology, it has been highly successful in supporting fundraising efforts.<sup>272</sup> Further, an increasing range of successful applications of these technologies have emerged in the context of traditional finance.<sup>273</sup>

However, the arguments in favour of a permissive approach conflict, to some extent, with the sustainability objective that takes centre stage in the EU Sustainable Finance Action Plan (2018),<sup>274</sup> the revised Sustainable Finance Strategy (2021)<sup>275</sup> and the related legislation implementing these strategies, in particular the SFDR and the Taxonomy Regulation.<sup>276</sup> Out of the Environmental, Social and Governance triad that characterizes sustainable finance, the EU implementing legislation so far has **emphasized environmental concerns**, with reduction of greenhouse gas (GHG) emissions as the core agenda, putting social and governance issues in second rank.<sup>277</sup>

#### 3.5.1. Crypto and sustainability

There is, in fact, a **tension between the energy-intensive set-up of some types of DLT** and the emphasis on energy savings and GHG reductions of EU politics. Design features of some DLTs raise energy issues.<sup>278</sup> It is estimated that the Bitcoin Blockchain uses collectively as much energy as the Netherlands, a country with some 18 million people.<sup>279</sup>

While some crypto models waste energy and are inherently exclusive in nature, others are highly energy efficient and inclusive in that customers with low degrees of financial and technical literacy may participate. For instance, developers claim that the Ethereum Merge, a major software upgrade to the Ethereum blockchain in September 2022, reduced the Ethereum blockchain's energy usage by 99.95 per cent. At the same time, another upgrade dubbed "the Surge" will reduce costs and enhance speed and system stability.<sup>280</sup>

While these upgrades clearly show the potential of technological innovation, the absence of similar upgrades to the Bitcoin blockchain are deeply regrettable. One reason for the absence of such

<sup>271</sup> Moy C., and Carlson J., 'Cryptocurrencies can enable financial inclusion. Will you participate?' (Weforum), available at: <https://www.weforum.org/agenda/2021/06/cryptocurrencies-financial-inclusion-help-shape-it/>, accessed 29 March 2023.

<sup>272</sup> Essaghoolian, N., 2019, Initial Coin Offerings: Emerging Technology's Fundraising *Innovation*, *University of California Los Angeles Law Review* 66 (1), p. 294.

<sup>273</sup> 'Web3 and Blockchain' (Bain & Company), available at: <https://www.bain.com/insights/management-tools-web3-and-blockchain>, accessed 29 March 2023.

<sup>274</sup> European Commission, 2018, *Action Plan: Financing Sustainable Growth* COM/2018/097 final (8 March 2018), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0097>.

<sup>275</sup> European Commission, 2021, *Strategy for Financing the Transition to a Sustainable Economy*, COM/2021/180 final (6 July 2021), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0390>.

<sup>276</sup> Zetzsche, D. A., Anker-Sørensen, L., 2022, Regulating Sustainable Finance in the Dark, *European Business Organization Law Review*, 23, pp. 47–85, available at: <https://doi.org/10.1007/s40804-021-00237-9>.

<sup>277</sup> Zetzsche, D. A., Bodellini, M., Consiglio, R., 2022, The EU Sustainable Finance Framework in Light of International Standards, *Journal of International Economic Law*, 25 (4), pp. 659–679, available at: <https://doi.org/10.1093/jiel/jgac043>.

<sup>278</sup> Sedlmeir J., et al., 2020, The Energy Consumption of Blockchain Technology: Beyond Myth, *Business and Information Systems Engineering Journal*, 62 (6), p. 599.

<sup>279</sup> University of Cambridge, The Cambridge Centre for Alternative Finance, 'Cambridge Bitcoin Electricity Consumption Index: Comparisons', (Cambridge University, 2023), available at: <https://ccaf.io/cbeci/index/comparisons>, accessed 29 March 2023.

<sup>280</sup> 'Crypto winter end in sight as Ethereum looks to shake the chills-analysts' (Reuters), available at: <https://www.reuters.com/markets/currencies/crypto-winter-end-sight-ethereum-looks-shake-chills-analysts-2022-12-12/>, accessed 29 March 2023.



upgrades is Bitcoin's absence of a centralized governance mechanism, which could design and implement them.

From a regulatory point of view, EU **financial regulation addresses sustainability concerns by subjecting "financial market participants"** (Article 2 (1) SFDR) and **companies, credit institutions, insurance companies and other intermediaries obliged to report under Article 8 of the Taxonomy Regulation** to additional disclosures and, in the case of financial market participants, additional investment policy and risk management requirements. These duties aim to enhance sensitivity of their investors and clients regarding Environmental, Social, and Governance (ESG) matters so these investors and clients can consider both the sustainability risks and the impact on sustainability factors in their financial decisions.<sup>281</sup>

The disclosure and risk management concept fails entirely in an environment where there are, at least in the reading of DeFi proponents, no "financial market participants" or companies and intermediaries that could be subject to regulation. This is true for **centralized crypto intermediaries that deal in crypto-assets other than financial instruments only** (as these firms do not qualify as reporting entities under Article 2(1) SFDR nor Article 8 Taxonomy Regulation so far). It remains to be true for fully decentralized protocols that, in their own reading, do not function as, nor are operated by an intermediary. In turn, **only very few crypto intermediaries report on sustainability matters, and none, to our knowledge, meet the strict sustainability disclosure requirements imposed by the Taxonomy Regulation, or SFDR, respectively.**<sup>282</sup>

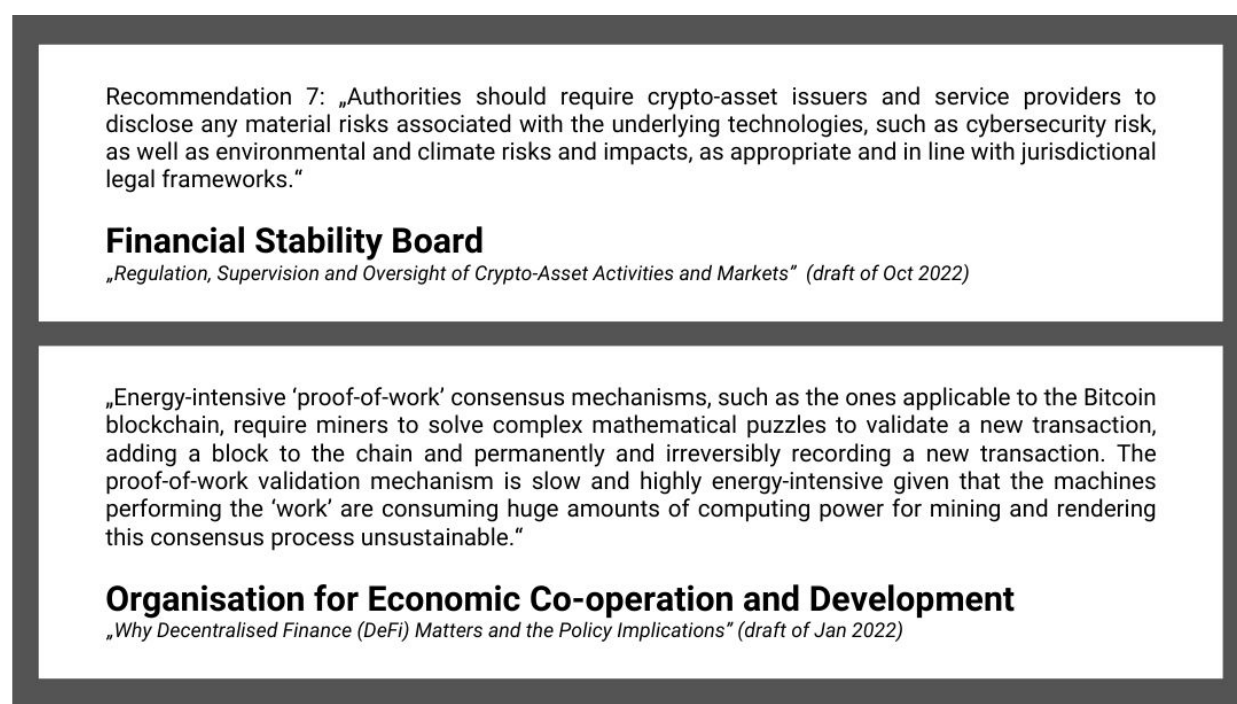
Surprisingly, while the use of energy of the old Bitcoin blockchain is well known few **regulators have addressed sustainability matters in the DeFi guidance or practice.**

---

<sup>281</sup> See European Commission, *Action Plan: Financing Sustainable Growth*, COM/2018/097 final, *supra* note 274, at note 274.

<sup>282</sup> Research by Util, a data-driven sustainability watchdog, shows that Coinbase scores (minus) -43% on Sustainable Development Goal 13: Climate action (See, *'Putting Coinbase to the test: Can crypto ever be sustainable?'* (Util), available at: <https://www.util.co/post/putting-coinbase-to-the-test-can-crypto-ever-be-sustainable>, accessed 29 March 2023. Binance mentions sustainability only in the context of the growth of the crypto industry in its 2022 end-of-the-year report (cf. *'End of the year report 2022'* (Binance), available at: <https://public.bnbstatic.com/static/content/End-of-Year-Report-2022.pdf>, accessed 29 March 2023. Binance has shared several blog posts related to sustainability (for instance, Encila 'J. *'Tron Uses Nearly 100% less energy than Bitcoin and Ethereum, study shows'* (Binance, 25 August 2022), available at: <https://www.binance.com/en/news/top/7184556>, accessed 29 March 2023. Kraken Exchange published a post mitigating most of the concerns about the environmental impact of Bitcoin (cf. *'Busting Crypto Myths: "Bitcoin is destroying the environment"'* (Kraken blog), available at: <https://blog.kraken.com/post/16645/crypto-myths-bitcoin-destroying-environment/>, accessed 29 March 2023.

Figure 10: International Standard Setters on Sustainability



Source: Author’s own elaboration.

These high-level recommendations from the FSB (cf. Figure 8) do not provide details on how these disclosures may take place. Further, they focus on issuers and CASPs, and leave decentralized systems aside, although these are the most energy-intensive applications.

We address this matter in the next section.

### 3.5.2. Centralized vs decentralized

#### a. Ensuring that centralized services are in scope

SICIs as centralized intermediaries could easily be subjected to disclosure rules under both the SFDR and the Taxonomy Regulation. The easiest way is to **classify, as a default rule, all crypto-assets as transferable securities** unless the token is reclassified applying MiCA-based classification criteria (and potentially exempted) by an NCA (cf. *infra*, at 6.2.2.). In turn, most crypto-assets would be deemed listed securities once traded at an exchange, and their issuers subject to disclosure requirements as public-interest entities subject to Article 2(1) lit. a Directive 2013/34/EU (and the forthcoming Corporate Sustainability Disclosure Directive, respectively), while CASPs would be, in most cases, investment firms under MiFID. Some of them qualify also as financial market participant under SFDR and, if sufficiently large, are subject to disclosure under Article 8 Taxonomy Regulation.

As an alternative measure, **CASPs could be added directly to the scope provisions of EU sustainable finance regulations**, by including them under the definition of ‘financial market participants’ (cf. Article 2 (1) SFDR). The current catalogue of that provision lists, however, only investment firms active in portfolio management; few CASPs engage that way. To capture activities that are, from a functional perspective, analogue to portfolio management, the EU legislature could add to the list of financial market participants in Article 2 (1) SFDR the following: (i) **CASPs that “pool crypto-assets with a view to using these assets for lending or investment purposes, regardless of whether the lending or investment activity is on the CASP’s own account”** as well as (ii) CASPs that **“facilitate peer-to-peer transactions in relation to crypto-assets”**.

While this would impose the same rules for functionally equivalent activities, we note that centralized intermediaries already have incentives to reduce energy consumption since they internalize the energy costs of their centralized services.

b. Ensuring that decentralized services are in scope

The enormous energy consumption **stems from the decentralized functions**. Implementing the principles of EU sustainable finance regulations poses a challenge where DeFi is fully decentralized given that in a full DeFi setting no one controls operations, and no one could be subjected to disclosure rules or sustainability-oriented risk management.

At the same time, we do not find it adequate to ban PoW altogether as ESMA former Vice-Chair proposed, according to the Financial Times.<sup>283</sup> Due to its intrusive nature, such a ban would hardly be respected outside of the EU because many EU clients use services offered from third-countries. Conversely, more recent PoW technologies have shown enormous energy savings.

Instead, we find it desirable to bring decentralized models into the scope of EU financial regulation and ensure that users of fully decentralized protocols have access to the same disclosures on sustainability risks and factors, similar to the clients of regulated financial institutions.

We envisage this objective may be achieved in two ways.

First, through **RegTech**, by embedding regulatory principles – including relating to sustainability – into system design. For instance, financial regulation could prescribe that DeFi protocols calculate the estimated use of energy of its nodes and other processes, update this data in short intervals based on data processing volume, and disclose it permanently on the system's website to inform users. To make this information useful, the disclosure may be paired with comparisons, either to non-DeFi use cases or other DeFi protocols.

Second, the **scope of existing EU financial regulation may be expanded** to ensure sustainability disclosure of decentralized crypto platforms to users and NCAs. Yet, fully decentralized platforms have evaded regulation so far, arguing they lack an entity that could provide the disclosure. As we have pointed out frequently, we do not believe this argument holds merit; most often, an entity or a group of persons drives the code development and marketing of its tokens. It is for these reasons that we suggest granting entity status for regulatory purposes to DAOs, for micro-prudential and also sustainable finance regulation (cf. *infra*, at 6.3.1.). These regulated entities should then be added to the scope of the SFDR and the Taxonomy Regulation, subject to reasonable size thresholds. However, the legal entity engaged in product development and distribution of services of the fully decentralized platform may register itself as an operator for the purposes of EU financial regulation and comply with sustainability disclosure obligations on behalf of the platform.

---

<sup>283</sup> Szalay E., 2022, *EU should ban energy-intensive mode of crypto mining, regulator says* (Financial Times, 19 January 2022), available at: <https://www.ft.com/content/8a29b412-348d-4f73-8af4-1f38e69f28cf>, accessed 29 March 2023.

### 3.6. In depth: use of non-formalized information (social media etc.)

Figure 11: International standard setters on use of non-formalized information



Source: Author’s own elaboration.

#### 3.6.1. Referral programmes and social network expansion

Crypto intermediaries often offer so-called ‘referral programmes’ where businesses and users can earn from referring new users. Our research has shown that these programmes accept users from the EU and that affiliates focus their marketing efforts on EU countries.<sup>284</sup> Also, other methods suggest that the

<sup>284</sup> Several websites, accessible to EU citizens, contain marketing of crypto intermediaries. Inspection of the URLs reveals that they contain tracking parameters that are required by affiliate programs to track referrals. Examples are Rodriguez, G., ‘6 Best Crypto Exchanges of March 2023’ (Money.com, 1 March 2023), available at: <https://money.com/best-crypto-exchanges/>, accessed 29 March 2023 and Lielacher, A., ‘Best Crypto Exchanges: Our top picks for the best cryptocurrency exchanges of 2023’ (Investopedia, 16 March 2023), available at: <https://www.investopedia.com/best-crypto-exchanges-5071855>, accessed 29 March 2023. Several other websites are distinctly focussed on EU countries. For instance, ‘Moesman N., and Munro A., ‘De 11 beste crypto exchanges in Nederland’ (Finder), available at:

providers like to understand themselves more as a social community than a financial service, resulting in community-building efforts, such as newsletter signups (available to mail-addresses from EU countries) and chat groups, such as Telegram groups (available to phone numbers from EU countries).<sup>285</sup>

The revenue share model of affiliate programmes<sup>286</sup> may result in de facto marketing outside of channels controlled by the crypto intermediary and in an informal way that is not consistent with prerequisites in place for advertising financial services under the respective union legislation for the cross-border distribution of financial services.<sup>287</sup> By relying on web blogs, social media and similar services, these platforms circumvent the distribution rules for financial services, as existing users prompt new users to contact the crypto intermediary via its website, so the intermediary can classify that initial contact as “reverse solicitation”.

Moreover, crypto-intermediaries may pay search engines for priority positions (paid positions above the so-called “organic search results”) upon searches for keywords of the industry, such as “crypto-assets”, “token”, “stablecoins” and others, even where searches are initiated from areas where the crypto-firm is not entitled to perform financial services. Even when the search engines do take appropriate steps to prevent the advertisement of illegal or otherwise unwanted products and services, including financial products,<sup>288</sup> crypto-intermediaries can exploit various search engine optimization (SEO) techniques to rank high in the organic search results.<sup>289</sup> Paid priority positions can be specifically chosen for specific countries, cities or even a neighbourhood. Organic optimization, other than choosing a specific language or targeting content based on popular searches in a specific country, is untargeted. The latter may thus result in unintentional targeting of EU citizens. Furthermore, the ranking of organic search results may also be considered somewhat of a “free-for-all” since the indexation of the results is done via algorithms and only in exceptional circumstances edited by the search engine operators.<sup>290</sup>

A way to preserve the effective enforcement of EU financial law is to attribute referrals by existing clients, contacts via newsletters or partner programs, regardless of their name, legally to the crypto intermediary. For instance, financial regulation could provide that if any existing client contacts new potential clients, that initial contact is treated as initial contact by the crypto intermediary if the intermediary encourages the client to do so. Similarly, relying on existing EU financial law, if products are offered through newsletters and partnership programs, or if the crypto-firm pays search engines

---

<https://www.finder.com/nl/cryptomunten/keurzen>, accessed 29 March 2023, targets Dutch citizens and promotes crypto intermediaries that are not registered with De Nederlandsche Bank (see, De Nederlandsche Bank ‘Register of crypto service providers’, available at: <https://www.dnb.nl/en/public-register/register-of-crypto-service-providers/?p=1&l=10&rc=V1dGVEFD>, accessed 29 March 2023).

<sup>285</sup> Cf. ‘Account: @BNBchaincommunity’ (Telegram), available at: <https://t.me/BNBchaincommunity>, accessed at 29 March 2023; ‘Account: @Avalanchavax’ (Telegram), available at: <https://t.me/avalancheavax>, accessed 29 March 2023; ‘Account @Lidofinance’ (Telegram), available at: <https://t.me/lidofinance>, accessed 29 March 2023.

<sup>286</sup> Affiliates (users that sign up for the program and promote the crypto intermediary’s services) are paid a share of the revenue that intermediaries earn from referred customers.

<sup>287</sup> The terms of service of Binance’s affiliate program solely include a passage deferring affiliates (members of the affiliate program) from the US. The EU or any other jurisdiction is not mentioned. See, ‘Binance Affiliate Program Standard Terms and Conditions | Binance Support’ (Binance), available at: <https://www.binance.com/en/support/faq/binance-affiliate-program-standard-terms-and-conditions-b5b4a734aaaf42d0b7a32d5b30930408>, accessed at 29 March 2023.

<sup>288</sup> Search engine operators have advertising policies that are aimed at preventing the advertisement of products and services that are illegal in the areas that the advertisements are focused on. Google, for example, dedicates specific attention to financial products. See, ‘About restricted financial products certification’ (Google), available at: <https://support.google.com/adspolicy/answer/7645254>, accessed on 14 April 2023.

<sup>289</sup> Goodwin, D., ‘What Is SEO – Search Engine Optimization?’ (Search Engine Land), available at: <https://searchengineland.com/guide/what-is-seo> accessed on 14 April 2023.

<sup>290</sup> An exceptional circumstance would be the so-called “right to be forgotten”. See, ‘Right to be Forgotten Overview’ (Google), available at: <https://support.google.com/legal/answer/10769224?hl=en>, accessed on 14 April 2023.

for high search positions in the EU, the mentioning of products and services is treated as marketing efforts from the crypto intermediary in the direction of EU clients. The logic behind such a rule is that the intermediary initiated the potential clients' "initial contact" through the referral, loyalty and newsletter programs. We consider this proposal more in detail *infra*, at section 6.

### 3.6.2. Social media

The crypto industry extensively uses social media channels ("**Crypto Twitter**").<sup>291</sup> All large crypto intermediaries have well-promoted social media channels with millions of followers.<sup>292</sup> Smaller DeFi protocols use Twitter to gather new customers by posting about rewards, high-yielding products and new listings on CEXs.<sup>293</sup> Finally, there are multiple **FinFluencers**<sup>294</sup> active on Twitter, YouTube, Telegram and Twitch. Characteristically for these type of information streams is the "promotion" of tokens and protocols by detailing technical/fundamental price indicators and the promotion of trading platforms.<sup>295</sup> "FinFluencing" is also practiced by world-famous celebrities as is clear from recent enforcement actions of the SEC.<sup>296</sup> Often, this is a form of client solicitation that is hard to trace to the intermediaries – hence we argue the use of referral programs, promotional web publications and sponsored links to platforms as indicators of some indirect solicitation strategy (cf. previous section).

In the same vein, US authorities are examining bankrupt crypto firm Celsius' use of social media that allegedly prompted a lack of transparency.<sup>297</sup> The information that was disclosed by Celsius was not vetted or explained and often emotional, potentially misleading users as to either exert enthusiasm in respect to some, or act in confusion and anxiety as to other crypto-assets.

On another dimension, crypto uses its **own language** and **pretends to apply conduct rules** complying with industry standards, yet these assertions (which are found on websites frequently) can hardly be proven. They further have the potential to mislead users not familiar with crypto.<sup>298</sup> As a remedy, regulations could require the use of plain language, and ban the use of unaudited facts. Yet potentially a better step is to select **skilled, fit and proper key staff** who are familiar with codes of conduct in the financial sector (through application of the fitness and properness test of licensing schemes), paired with governance requirements and business conduct rules established in the field of EU financial law. While for centralized DeFi firms this has been achieved by MiCA (cf. *infra*, at 5.1.2.), we suggest assigning entity status to decentralized protocols for the very same reasons (cf. *infra*, at 6.3.).

<sup>291</sup> Mako Mihajlović, M., 'A Guide to Crypto Twitter' (Shrimpy Academy, 11 February 2022), available at: <https://academy.shrimpy.io/post/a-guide-to-crypto-twitter>, accessed 29 March 2023.

<sup>292</sup> Cf. 'Account: @binance' (Twitter), available at <https://twitter.com/binance>, accessed 29 March 2023; 'Account: @coinbase' (Twitter), available at: <https://twitter.com/coinbase>, accessed 29 March 2023; 'Account: @AaveAave' (Twitter), available at <https://twitter.com/AaveAave>, accessed 29 March 2023;

<sup>293</sup> Cf. 'Account: @mummyftm' (Twitter), available at <https://twitter.com/mummyftm>, accessed 29 March 2023; 'Account: @SolidlyDEX' (Twitter), available at <https://twitter.com/SolidlyDEX>, accessed 29 March 2023; A listing on a CEX is seen as positive since it usually leads to an increase in token value.

<sup>294</sup> FinFluencer (Financial Influencers) are persons giving information and advice on financial topics, including crypto-assets. See, Sridharan, S., 2022, *FinFluencers: What code of conduct should we have?* (Observer Research Foundation, 8 December 2022), available at: <https://www.orfonline.org/research/finfluencers/>, accessed 29 March 2023.

<sup>295</sup> Cf. 'Account: @CryptoMichNL' (Twitter), available at <https://twitter.com/CryptoMichNL>, accessed 29 March 2023.

<sup>296</sup> U.S. Securities and Exchange Commission 'SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security' (SEC Press release, 3 October 2022), available at: <https://www.sec.gov/news/press-release/2022-183>, accessed 29 March 2023; U.S. Securities and Exchange Commission 'SEC Charges Crypto Entrepreneur Justin Sun and his Companies for Fraud and other Securities Law Violations' (SEC Press release, 22 March 2023), available at: <https://www.sec.gov/news/press-release/2023-59>, accessed 29 March 2023.

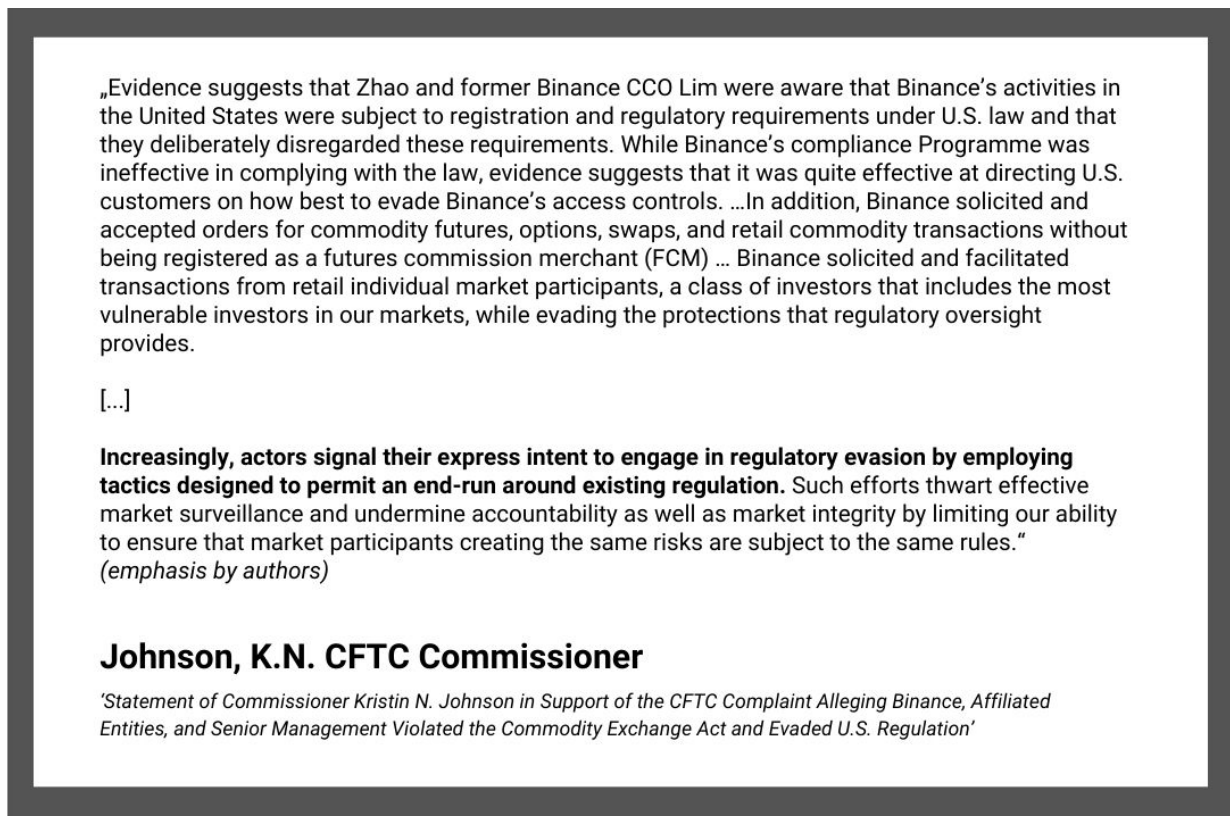
<sup>297</sup> U.S. Bankruptcy Court for the Southern District of New York 2023 'In re Celsius Network, LLC, et al. 22-10964', available at: <https://casetext.com/case/in-re-celsius-network-llc-9>, accessed 29 March 2023.

<sup>298</sup> Evidence of such claims was established by the SEC during its investigation into the Kraken Exchange. See note 257.

### 3.6.3. Outright circumvention of laws

The former suggests that some crypto-intermediaries seek ways to circumvent financial regulations.<sup>299</sup> In fact, a strategic approach to circumventing the US Commodities Exchange Act stands at the heart of the CFTC's lawsuit against the world's largest crypto exchange Binance. See Figure 10 for an extract of the CFTC Commissioner's statement on the matter.<sup>300</sup>

Figure 12: Statement by CFTC Commissioner (CFTC v Binance)<sup>301</sup>



Source: Author’s own elaboration.

### 3.6.4. Insider dealing and market manipulation

Further, the extension of market abuse rules under MAR to the crypto sector could prompt beneficial effects.

As to insider dealing and market manipulation, FTX, and Binance as its major competitor, provided reasons for concern. Some reports state that FTX’s fund Alameda traded primarily in FTX’s main crypto-asset – which is the equivalent to trading in a regulated entity’s own security. At the same time, Binance could publicly cast doubt on the financial reliability of FTX. After all, FTX had become Binance’s most serious competitor by then due to FTX’s recent growth (cf. *infra*, at 2.5.4). Such behaviour has most likely contributed to the confidence crisis in FTX and rendered any rescue effort by other parties futile

<sup>299</sup> Our findings are strengthened by the EBA’s indication of the possibility of misleading and aggressive advertising from crypto-intermediaries that may arise due to the “inadequate” advertising approaches. See ‘Report with advice for the European Commission on crypto-assets’, 2019, European Banking Authority (EBA), at para. 31, available at: <https://www.eba.europa.eu/eba-reports-on-crypto-assets>.

<sup>300</sup> Statement of Commissioner Kristin N. Johnson in Support of the CFTC Complaint Alleging Binance, Affiliated Entities, and Senior Management Violated the Commodity Exchange Act and Evaded U.S. Regulation’ (CFTC, 27 March 2023), available at: <https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement032723>, accessed 29 March 2023.

<sup>301</sup> Available at: <https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement032723>, accessed 29 March 2023.

from the beginning. Such conduct is unthinkable in the regulated finance industry where any such statement would run counter to market abuse legislation.

MiCA addresses some of the issues through a bespoke market abuse regime. Yet, the main issue of drafting market abuse legislation is achieving legal clarity and certainty as to which conduct is abusive. In this regard, the MAR and the respective implementing legislation offers an extensive catalogue of and details on conduct that may qualify as market abuse (insider dealing and/or market manipulation).<sup>302</sup> To avoid duplications of legislation, an easy solution to consider is to include all crypto-assets (as defined and regulated by MiCA) in the scope of the MAR.

The addition of crypto-assets to the MAR requires some adjustments given that **only some token issues are initiated by an issuer** (in practice, often a special purpose vehicle (SVP)). In particular, decentralized protocols claim that a token issuer is lacking; in other cases, the issuer is residing outside of the Single Market and trading has been initiated by token holders or CASPs.

We propose to adopt, for the amendment of the MAR, the solution provided in Article 80 MiCA (which is also implemented for crypto-assets other than EMT and ART in Title II MiCA): for lack of an issuer, the offeror and/or the person seeking admission to trading of the crypto-asset may assume the duties the MAR imposes on issuers. However, if our proposal to adopt entity status for DAOs is implemented many important decentralized protocols will in fact have an issuer, as the collective body of token holders is deemed to be the issuer, for regulatory purposes. See *infra*, at 6.3.

### 3.7. Non-financial regulatory challenges

Further challenges provided by DeFi not mentioned here at length include data protection and privacy. Decentralization in the datafied world means that data is accessible at many points rather than one. Equally so, due to the immutable nature of blockchains, the right to be forgotten under the General Data Protection Regulation (GDPR) will be impossible to implement in certain cases. This, together with the cross-border set-up of crypto, exacerbates data protection challenges: some servers will be subject to stricter data protection standards, others will be subject to more lenient ones.<sup>303</sup>

---

<sup>302</sup> See the list of implementing measures at 'Summaries of EU legislation (Preventing market abuse in financial markets)', available at: <https://eur-lex.europa.eu/EN/legal-content/summary/preventing-market-abuse-in-financial-markets.html> accessed 29 March 2023.

<sup>303</sup> For further details, see Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>, at 189-191.



## 4. STATUS QUO PRIOR TO MiCA AND THE REVISED TFR

### KEY FINDINGS

The status quo prior to MiCA and the revision of the TFR was characterized by **gaps** stemming from the **inconsistent application** of EU financial regulation across Member States. Ambiguity and legal uncertainty in standard terms like “financial instruments” and “e-money” were often the source of **regulatory arbitrage**. Further, in the context of Facebook’s Libra project, concerns were aired relating to **privately managed “global” stablecoins** and their impact on financial stability and national sovereignty. Finally, inconsistent and delayed application of the AMLD revisions had created gaps in the field of **AML/CTF controls**, while tracing of transactions had faced technical and practical difficulties.

### 4.1. Ambiguity and legal uncertainty

#### 4.1.1. Three categories of crypto-assets

In light of the need to provide appropriate regulatory responses to the emergence of crypto-assets and token offerings, supervisory authorities have faced difficulties finding a legal basis that enables intervention.<sup>304</sup>

Since crypto-assets can be designed in a variety of ways and entail ownership of a variety of rights, from financial interests in a company to purely non-financial rights, academic analysis tends to place crypto-assets into one of three categories, adopting a functional approach.<sup>305</sup>

**Utility tokens** grant a kind of access or right(s) to use a company’s goods or services, or are required to interact with a blockchain’s ecosystem.<sup>306</sup> These kinds of tokens often resemble the pre-payment of license fees or crowdfunding sales on websites such as Kickstarter.<sup>307</sup> A utility token falling into these schemes is not usually considered a traditional security or financial product: its aim is not to create future cash flows but rather enable functional use of a blockchain-based ecosystem.<sup>308</sup>

<sup>304</sup> Zetzsche, D. A., Annunziata, F., Arner D. W., Buckley R. P., 2021, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, Capital Markets Law Journal, 16 (2), pp. 203-225, available at: <https://academic.oup.com/cmlj/article/16/2/203/6324188?rss=1> or <https://doi.org/10.1093/cmlj/kmab005>.

<sup>305</sup> See, Barsan I., 2018, *Legal Challenges of Initial Coin Offerings*, Revue Trimestrielle de Droit Financier (RTDF), 54 (3), p. 62, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3064397](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064397) (identifying only “currency like” and “security like” tokens). Maume P., Fromberger, M., 2019, *Regulations of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws*, Chicago Journal of International Law, 19 (2), pp. 548-585, available at: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1748&context=cjil>, at p. 548, 558. Zetzsche, D. A., Buckley R. P., Arner D. W., Föhr, L., 2018, *The ICO Gold Rush: It’s a Scam, It’s a Bubble, It’s a Super Challenge for Regulators*, Harvard International Law Journal, 63 (2), available at SSRN: <https://ssrn.com/abstract=3072298> or <http://dx.doi.org/10.2139/ssrn.3072298> or <http://dx.doi.org/10.2139/ssrn.3072298> (arguing for a functional approach), at 276. See also the distinction between “app tokens” and “protocol tokens” by Rohr J., Wright A., 2019, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, Hastings Law Journal, 70, pp. 463-524, at p. 463, 469.

<sup>306</sup> Bourveau T., de George E.T., Ellahie A., Macciocchi, D., 2018, *Initial Coin Offerings: Early Evidence on the Role of Disclosure in the Unregulated Crypto Market*, 12, 18, available at: [https://www.marshall.usc.edu/sites/default/files/2019-03/thomas\\_bourveau\\_icos.pdf](https://www.marshall.usc.edu/sites/default/files/2019-03/thomas_bourveau_icos.pdf).

<sup>307</sup> Howell S. T., Niessner M., Yermack D., 2018, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sale*, ECGI Finance Working Paper 564, p. 9, available at: [https://www.ecgi.global/sites/default/files/working\\_papers/documents/finalhowellniessneryermack.pdf](https://www.ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf).

<sup>308</sup> Klöhn L., Parhofer N., Resas D., 2018, *Initial Coin Offerings (ICOs)*, Zeitschrift für Bankrecht und Bankwirtschaft, p. 89-106, pp. 89, 102. But see Boreiko D., Ferrarini G., Giudici P., 2019, *Blockchain Startups and Prospectus Regulation*, European Business Organization Law Review, 20 (4), pp. 665-694., available at: <https://link.springer.com/article/10.1007/s40804-019-00168-6>. At p. 665, 672 (arguing that almost all ICO tokens would qualify as financial instruments).

**Security/financial/investment tokens** are tied to an underlying asset and represent a fractional ownership of the overall value of the asset, albeit not of the asset itself (e.g. a firm, real estate or collectibles). They offer rights to future profits and are typically treated under financial regulatory regimes as financial products, securities, financial instruments, derivatives or collective investment schemes.

**Currency/payment tokens**, like money, serve as a means of exchange, storage of value, and unit of account.<sup>309</sup> Famously represented by Bitcoin,<sup>310</sup> currency tokens have lately grown more diverse and now include stablecoins like the aforementioned USDC. The Libra stablecoin project from Meta (formerly Facebook) has since halted.<sup>311</sup>

Despite their simplicity, these three categories create uncertainties in legal systems. This includes legal systems with narrow definitions of “security” or “financial product” such as existing EU capital markets legislation, and those with broad definitions of “security” or “financial product” such as the US under the *Howey* test<sup>312</sup> or Italy in its legal definition of “financial product” provided in addition to EU categories. This may explain why the SEC has been using enforcement actions, public statements and no-action letters to provide guidance in employing a functional, *Howey*-like approach on a case-by-case basis.<sup>313</sup>

#### 4.1.2. Divergent application

Many regulatory approaches follow these three categories.<sup>314</sup> Yet, within the scope of EU financial law, distinct national competent authorities have applied different definitions of core financial law concepts. Tokens are also often structured as hybrids with payment, securities and utility characteristics, and risks mutating over time depending on a number of internal and external factors. This renders the risk assessment relating to crypto-assets a particular challenge.<sup>315</sup>

There is significant disagreement as to the qualification of certain token types among various regulators in the EU and Member States.<sup>316</sup> For instance, stablecoins may be qualified as financial instruments, transferable securities, derivatives, collective investment schemes, units of account, e-

<sup>309</sup> Geva, B, *Cryptocurrencies and the Evolution of Banking, Money and Payments*. Brummer, C. (ed.) Cryptoassets Legal, Regulatory and Monetary Perspectives (Oxford University Press, 2019) pp.11-38, available at: <https://ssrn.com/abstract=3477513>, p. 12.

<sup>310</sup> We note that the crypto industry has a unique use of the terms “tokens” and “coins” that differs from the terminology prevailing in academia and financial regulation. See, e.g., ‘*Report with advice for the European Commission on crypto-assets*’, 2019, European Banking Authority (EBA), at Box 1, available at: <https://www.eba.europa.eu/eba-reports-on-crypto-assets>. The industry considers Bitcoin to be a “coin”, alongside so-called “altcoins” (“meaning “alternative coins”), blockchain-native assets (e.g. ETH, BNB), etc. Tokens are considered crypto-assets that are not the blockchain native’s assets but created via smart contracts on a blockchain (e.g. NEXO, LIDO, etc), see, Moreland, K. ‘*The Difference Between Coins and Tokens*’ (Ledger Academy, 23 October 2019), available at: <https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens> accessed on 17 April 2023). The EU financial regulation

<sup>311</sup> On Libra, see Zetzsche, D.A., Buckley, R.P., Arner, D.W., 2021, *Regulating Libra*, Oxford Journal of Legal Studies 41:1, pp. 80–113, available at: <https://doi.org/10.1093/ojls/gqaa036>.

<sup>312</sup> Cf. *supra*, note 224.

<sup>313</sup> See Mougayar, W., ‘*While We Wait for Laws, We Need Better Interpretations of Existing Regulation*’ (Coindesk), available at: <https://www.coindesk.com/while-we-wait-for-laws-we-need-better-interpretations-of-existing-regulation>, accessed 29 March 2023 (arguing that the results are difficult to determine).

<sup>314</sup> Blandin A., Cloots A.S., Hussain H., Rauchs M., Saleuddin R., Allen J.G., Zheng Zhang B., Cloud K., 2019, *Global Crypto-assets Regulatory Landscape Study*, University of Cambridge Faculty of Law Research Paper No. 23, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3379219](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379219).

<sup>315</sup> Zetzsche, D. A., Annunziata, F., Arner D. W., Buckley R. P., 2021, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, Capital Markets Law Journal, 16 (2), pp. 203-225, available at: <https://academic.oup.com/cmjl/article/16/2/203/6324188?rss=1> or <https://doi.org/10.1093/cmjl/kmab005>.

<sup>316</sup> See ESMA, 2019, *Advice on Initial Coin Offerings and Crypto-Assets*, ESMA50-157-1391, 4,5, 18 and annex, available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf).

money, commodities, and/or deposits, depending on the particular design of the instrument and the relevant legal and regulatory system.<sup>317</sup>

In financial regulation, the classification of instruments and transactions determines which body of law will apply, and which supervisory powers an NCA or ESA may exercise. Further, in the Single European Financial Market, uncertain classifications based on inconsistent definitions create the potential for regulatory arbitrage, where financial intermediaries seek out the most favourable regulatory environment – potentially at the cost of effective financial supervision.<sup>318</sup>

Other implications stemming from non-harmonized classifications of tokens relate to valuation for tax purposes, identification of ownership for AML purposes and the application of data protection rules (GDPR). Reducing ambiguity and enhancing legal certainty is thus a major regulatory objective in itself.<sup>319</sup>

#### 4.1.3. Under-enforcement of existing EU financial law

If the scope of financial regulation is uncertain, supervisory authorities may be disincentivized to act, and this results in under-enforcement of existing financial regulation. This is furthered by the uncertainty as to whether a given NCA has sufficient users and clients in its jurisdiction to act. For instance, the Prospectus Regulation exempts small issues of up to 150 investors.<sup>320</sup> Given the scarcity of information, many NCAs lack the means to ascertain a violation of prospectus rules. In a similar way, the widespread reliance on reverse solicitation (cf. *supra*, at 3.6.) rendered it difficult for financial supervisory authorities to enforce existing financial regulation, since a firm that relies on reverse solicitation is not in the jurisdiction of the NCA.<sup>321</sup>

## 4.2. Global stablecoins

The pre-MiCA period was characterized by the emergence of “global stablecoins” – with Facebook’s (now Meta) Libra being the most notable example.<sup>322</sup> Stablecoins have the potential to reach globally systemic dimensions from a financial stability perspective. Consistent with important voices in policy and academia, most supervisory authorities have seen a need to intervene.<sup>323</sup> For instance, with regard to global stablecoins, the FSB analysed the financial stability perspective in its October 2020 report,<sup>324</sup> IOSCO addressed certain investor protection aspects in March 2020<sup>325</sup> and the FATF provided

<sup>317</sup> See Burilov, V., 2019, *Regulation of Crypto Tokens and Initial Coin Offerings in the EU*, European Journal of Comparative Law and Governance, 6, p. 146, available at: [https://brill.com/view/journals/ejcl/6/2/article-p146\\_146.xml?language=en](https://brill.com/view/journals/ejcl/6/2/article-p146_146.xml?language=en) (arguing that EU regulators shall first ensure legal certainty by defining the scope of tokenised financial instruments).

<sup>318</sup> Zetzsche, D. A., Annunziata, F., Arner D. W., Buckley R. P., 2021, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, Capital Markets Law Journal, 16 (2), pp. 203-225, available at: <https://academic.oup.com/cmjl/article/16/2/203/6324188?rss=1> or <https://doi.org/10.1093/cmjl/kmab005>.

<sup>319</sup> Ibid.

<sup>320</sup> Art. 1(4)(b) Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1129&from=EN>.

<sup>321</sup> See Art. 42 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065>, accessed 29 March 2023.

<sup>322</sup> See D.A. Zetzsche, R.P.Buckley, D.W.Arner, *Regulating Libra*, 41:1 *Oxford Journal of Legal Studies*, 80-113 (2021), available at: <https://doi.org/10.1093/ojls/gqaa036>.

<sup>323</sup> Zetzsche, D. A., Annunziata, F., Arner D. W., Buckley R. P., 2021, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, Capital Markets Law Journal, 16 (2), pp. 203-225, available at: <https://academic.oup.com/cmjl/article/16/2/203/6324188?rss=1> or <https://doi.org/10.1093/cmjl/kmab005>.

<sup>324</sup> *Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations*, 2020, Financial Stability Board (FSB), available at: <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>.

<sup>325</sup> *Global Stablecoin Initiatives: Public Report*, 2020, The Board of the International Organization of Securities Commissions (IOSCO), available at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>.

recommendations on how to deal with “so-called stablecoins” in July 2020.<sup>326</sup> These initiatives have been complemented more recently by the ECB<sup>327</sup> and the IMF.<sup>328</sup>

### 4.3. AML/CTF concerns

In the past (and often holding true today), users of various crypto platforms, particularly as lenders or borrowers, could remain fully anonymous. There was no KYC requirement for users of crypto platforms located in the EU until recently. The US had subjected crypto intermediaries earlier to AML/CTF regulation. This proved effective since it allowed the NCAs to impose sanctions for AML/CTF violations. For instance, the crypto intermediary Kraken was sanctioned for continuing to serve Iranian customers despite an US embargo that prohibited delivering financial services to customers from Iran.<sup>329</sup>

**AMLD5** came into force in January 2020<sup>330</sup> and implemented new rules related to providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers; these two types of CASPs are now regulated under MiCA. Most notably, AMLD5 imposed KYC procedures for providers of exchange services involving fiat currencies and custodian wallet providers (cf Art. 47(1) AMLD5).

However, AMLD5 leaves some gaps:

- users can transact in some cases without custodian wallet providers and exchange services, for instance, if they function as nodes or make use of a non-custodial wallet<sup>331</sup> (vf. Recital 9 AMLD5);
- a large number of DeFi protocols do not offer custodial wallets nor fiat to cryptocurrency exchange services, although these are present in mainstream platforms for many non-expert users (in particular, centralized platforms); “non-custodial” examples include DEXs and DeFi lending protocols, and
- EU citizens can receive funds from non-EU sources on a non-custodial wallet and anonymously interact with any crypto intermediary mentioned under the previous point or send funds to another unidentified non-custodial wallet, bypassing AMLD5’s KYC checkpoints.

<sup>326</sup> FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stable-coins, 2020, Financial Action Task Force (FATF), available at: [Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf](https://www.fatf-gafi.org/publications/fatfpublications/documents/2020-07-20-stable-coins-report.pdf).

<sup>327</sup> De Guindos L., 2021, *Financial Stability Review*, European Central Bank (ECB), available at: <https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202111~8b0aebc817.en.html> p. 54 - 57.

<sup>328</sup> Bains, P., Ismail, A., Melo, F., Sugimoto N., 2022, *Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements*, available at: <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Stablecoins-and-Arrangements-523724>. Bains, P., Ismail, A., Melo, F., Sugimoto, N., 2022, *Crypto Ecosystem: The Case of Unbacked Crypto Assets*, International Monetary Fund, available at: <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715>.

<sup>329</sup> ‘Bellany, D., Mac, R. ‘U.S. Crypto Exchange Kraken Settles with Treasury Department’ (New York Times, 28 November 2022), available at: <https://www.nytimes.com/2022/11/28/technology/kraken-crypto-sanctions.html>, accessed 29 March 2023.

<sup>330</sup> Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843>.

<sup>331</sup> A non-custodial wallet is a crypto wallet that does not rely on a third-party for the custody of the private keys. The private keys are stored in the wallet itself, allowing the user full control over the crypto-assets without the need of an intermediary.

## 5. IMPACT OF MiCA AND TFR

### KEY FINDINGS

MiCA and TFR have addressed the main challenges presented by the **centralized provision of crypto services**. As such, MiCA and TFR together provide a robust framework and a good basis for the proper ordering of crypto services providers if it is developed further by virtue of bespoke implementing legislation.

#### Some challenges remain:

- (1) the delineation between MiCA's **scope** and the established terms of EU financial regulation (such as "financial instruments", "transferable securities" and "e-money") as well as the boundaries to "**fully decentralized services**" and to "**financial NFTs**";
- (2) **periodic disclosure** and **accounting** of entities subject to MiCA;
- (3) **restructuring and resolution legislation**;
- (4) **cross-border harmonization** and coordination of enforcement in light of limited information and resources of NCAs;
- (5) **the exclusion of "fully decentralized services"** (laid down in the recitals of MiCA) imposes risks on crypto clients, enhances systemic risks, and renders the enforcement of EU financial regulation difficult.

### 5.1. Beneficial impact of MiCA

MiCA and TFR address many pain points regarding crypto. The most important are discussed briefly in this section.

#### 5.1.1. Gap-filling regarding the scope of EU financial law

First and foremost, MiCA is positioned between all existing EU financial regulation. It applies if none of EU securities regulation (e.g. MiFID), EU payments regulation (e.g. PSD2, EMD), or insurance regulation (e.g. Solvency II) apply (cf. Article 2 (4) MiCA), filling a gap identified by the ESAs in 2019.<sup>332</sup>

In theory, no crypto-asset or related service as defined by MiCA would be outside the scope of EU financial law. While this ambition is laudable, it comes with practical challenges (cf. *infra*, at 5.3.1.).

#### 5.1.2. Licensing, conduct of business, prudential regulation and supervision of crypto intermediaries

Title V MiCA foresees an authorization of CASPs, that is, the provision of crypto-asset services is prohibited unless properly licensed. This way, MiCA addresses a core demand regarding the regulatory treatment of crypto intermediaries.

Under Title V MiCA, a number of legal requirements attach to licensing: the definition and delineation of the services provided, proper organization and adequate and sufficient human and IT resources, fit

<sup>332</sup> The EBA established that a "significant portion" of crypto-assets and consequential activities related to these crypto-assets were outside the scope of EU financial law, giving rise to various issues e.g. customer protection due to inadequate disclosure. See 'Report with advice for the European Commission on crypto-assets', 2019, European Banking Authority (EBA), at para. 28, available at: <https://www.eba.europa.eu/eba-reports-on-crypto-assets>.

and proper management, adequate conduct of business, and prudential regulatory rules (i.e. the maintenance of adequate capital and liquidity).<sup>333</sup> With such licensing comes clear regulatory treatment and differentiation of services provided. For instance, the title “exchange” should be reserved for entities that bring together third parties’ supply and demand in crypto-assets in an appropriately designed and managed environment, while investment firms acting as brokers, market makers or asset managers and credit institutions should be subject to tailored requirements.

MiCA foresees broad language on Level 1, with equally broad implementing powers granted to the ESAs. While much will depend on how the ESAs make use of these powers, MiCA Level 1 provides a good basis for proper ordering of the crypto industry. In particular, implementing legislation must declare as impermissible services that would result in conflicts of interests if pursued by multi-activity groups. We believe guidance should be taken from the PSD or MiFID framework. For instance, the function of an operator of a trading platform, a broker-dealer, a proprietary trader, and custodian, are, in principle, incompatible in the absence of conflict mitigation measures.

### 5.1.3. Disclosure and transparency

Information is central to financial market functioning. This is the core of the efficient markets hypothesis and of financial regulation. With crypto, mandatory disclosure has received, and to some extent receives, insufficient attention from both market participants and regulators.<sup>334</sup> First, we see a need to provide financial information analogous to what securities regulation entails. We would require from issuers some **initial documentation** (such as a prospectus), and **ongoing information** through semi-annual and annual reports and material adverse change releases. This requires appropriate and consistent information and disclosure. While MiCA provides for bespoke-white paper rules and Article 88 MiCA imposes the obligation to disclose inside information in a timely manner, we lack rules on periodic disclosures in semi-annual or annual reports, similar to what the EU Transparency Directive requires from listed issuers.<sup>335</sup>

Second, certain intermediaries need to provide information to make sure their services function adequately. MiCA satisfies these needs for centralized crypto intermediaries. In particular, licensed crypto exchanges will have to provide pre- and post-trade information and comply with best execution duties, while crypto custodians need to disclose their custody policy. Furthermore, CASPs will need to provide information about group structure and activities so that counterparties are able to evaluate and understand risks.

Beyond these disclosure rules that form part of the standard repertoire of regulators, we suggest issuers and crypto intermediaries should have to disclose the operational structure of the service and IT environment in which the crypto-asset is issued and traded. This would include disclosing which functions are centralized or decentralized. A **Programme of Operations** should disclose the unique features and architecture of many crypto-assets. It could also outline how essential decentralized

---

<sup>333</sup> This is what licensing entails. See Omarova S. T., 2020, *Dealing with Disruption: Emerging Approaches to Fintech Regulation*, Washington Journal of Law & Policy, 61 p. 25, available at: <https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2798&context=facpub>. For a contrary view, see Nabilou, H., 2020, *The dark side of licensing cryptocurrency exchanges as payment institutions*, Law and Financial Markets Review, 14 (1), pp. 39-47.

<sup>334</sup> See, e.g., Heng Chou, J., Agrawal, P., Birt J., 2022, *Accounting for crypto-assets: stakeholders’ perceptions*, Studies in Economics and Finance, Emerald Group Publishing Limited, 39 (3) pp. 471-489, available at: <https://doi.org/10.1108/SEF-10-2021-0469>.

<sup>335</sup> For instance, Coinbase, as a listed company, provides a useful counterpoint in this regard to other crypto-firms, and showcases what type of disclosures are feasible, given the right set of rules: Coinbase provides for a reasonably sophisticated “Investor Relations” website - see *Investor Relations* (COINBASE), available at: <https://investor.coinbase.com/home/default.aspx>, accessed 29 March 2023. Further information is available from the NASDAQ stock exchange - see *Coinbase Global* (NASDAQ), available at: <https://www.nasdaq.com/market-activity/stocks/coin>, accessed 29 March 2023.

functions would be maintained in times of insolvency. Such an obligation to submit a Programme of Operations to explain the systems architecture and ensure systems resilience has already been introduced as part of the DLT Pilot Regulation.<sup>336</sup> It is also required by Article 17(1)(b)(i) and 18(2)(d), 44, and 62(2)(d) MiCA for ART and EMT issuers as well as CASPs. Further details will be provided in MiCA implementing legislation. While we lack the same requirements so far under CRD IV and MiFID for crypto-friendly investment firms and credit institutions, we believe that there is sufficient ground in the broad wording of these legislative acts to require the same from these financial institutions.

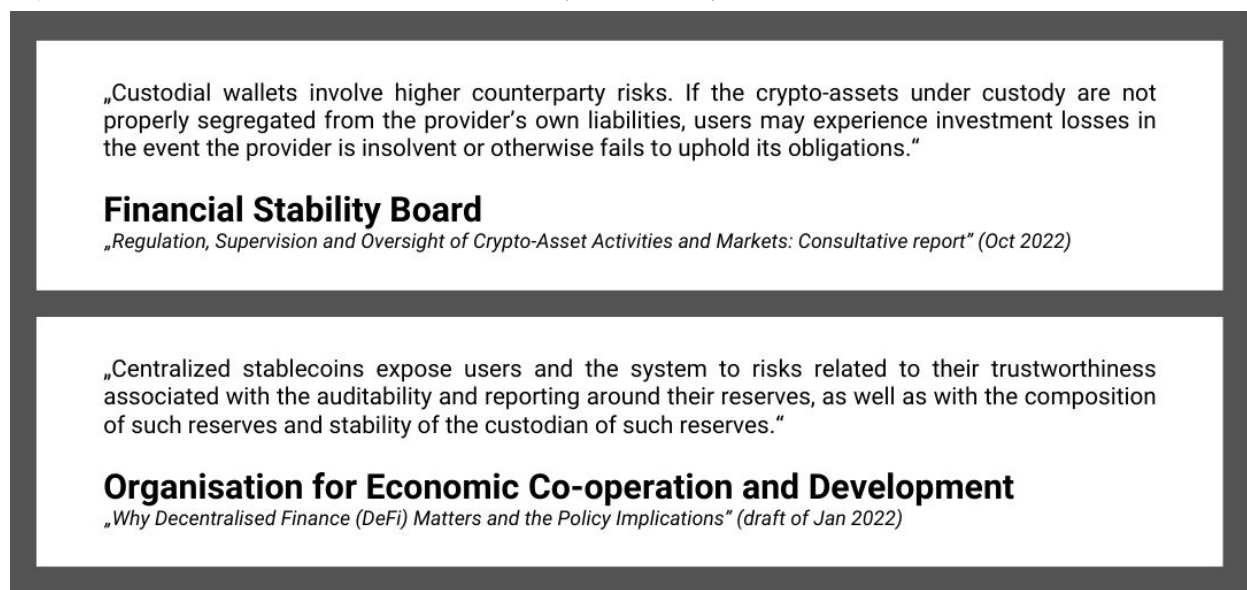
To ensure that EU clients of third-country firms are also similarly protected, we recommend that IOSCO develop a uniform standard format for these operational details, to facilitate comparison of the information disclosed.

Some additions would be desirable as to periodic disclosure (cf. 5.2.2.).

#### 5.1.4. Segregation and custody

As further shown in Figure 11, key matters relating to crypto-assets include asset segregation and custody.

Figure 13: International standard setters on crypto custody



Source: Author’s own elaboration.

To ensure safekeeping of assets, considering the industry practice,<sup>337</sup> it is of utmost importance to ensure the separation of custody (in “wallets”) from other intermediary activities (such as exchange, brokerage, market making and proprietary trading, i.e. trading on one’s own account).

If a token qualifies as a financial instrument, this is ensured given that the MiFID framework provides clear requirements for custodian services. In addition, if the crypto-asset qualifies as an Alternative Investment Fund (AIF), the Alternative Investment Fund Managers Directive (AIFMD) framework

<sup>336</sup> See Zetzsche D. A, Anker-Sørensen L., Passador M. L., and Wehrli A., 2021, *DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective*, Law and Financial Markets Review, 15 (1-2), pp. 70-115, available at: <https://doi.org/10.1080/17521440.2022.2065809>; Zetzsche D. A., and Woxholth J., 2022, *The DLT sandbox under the Pilot-Regulation*, Capital Law Markets Journal, 17 (2), pp. 212-236, available at: <https://doi.org/10.1093/cmlj/kmac003> (citing the EU DLT Pilot Regulation).

<sup>337</sup> For example, Kraken Exchange notes in its support section that they are an exchange and not a wallet service and that funds are held in the Kraken’s “corporate wallet” (cf. ‘*Differences between a crypto exchange and a crypto wallet service*’ (Kraken Support), available at: <https://support.kraken.com/hc/en-us/articles/115006441267-Differences-between-a-crypto-exchange-and-a-crypto-wallet-service/> assessed on 23 March 2023).

provides detailed rules for depositaries. These frameworks should extend to the custody of crypto-assets as a general matter. Article 70 MiCA and Article 75, Title V MiCA in fact impose such requirements. In particular, CASPs need to:

- safeguard crypto-assets to ensure ownership rights of clients, especially in the case of insolvency, and to prevent the use of clients' crypto-assets for a CASP's own account (Article 70 MiCA); and
- establish a full custodial relationship, if the CASP provides custody and administration of crypto-assets on behalf of clients (Article 75 MiCA).

Whether these rules are effective will largely depend on the implementation of MiCA. There are two types of concerns: one relating to the scope, and another to the substance of these rules. As part of the EU's custody rules, we would suggest clarity around the fiduciary duties of crypto custodians<sup>338</sup> and who falls within the scope of the definition thereof.

#### a. Scope of custody rules

To assess the effectiveness of MiCA, a definition of what "providing custody and administration of crypto-assets on behalf of clients" entails is crucial. From an industry perspective, the **retention and administration of a private key seems to be at the heart of the definition of custody**:<sup>339</sup> the private key asserts control of the assets. In line with this, Article 3(1)(17) MiCA defines as custody:

"the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys;"

This definition lacks detail and is somewhat ambiguous, but according to Recital 83 MiCA<sup>340</sup> it seems to exclude so-called "non-custodial wallets" where the private key is *not* held by a third-party entity that, as part of the contract, administers the key.

We note, however, a conflict between Article 3(1)(17) MiCA and Recital 83 MiCA. This conflict stems from the fact that in non-custodial wallets today the private key is held by the holders of the assets themselves **almost exclusively through the code of the wallet application**. In contrast to the early days of Bitcoin in which private keys were often written on a piece of paper ("paper wallet"), the private keys of today are created by code and stored somewhere in the code of the wallet application, most often never seen by the owner of the wallet.

It will be up to MiCA's implementing legislation to specify whether the software in which the private key is embedded and by which it is controlled (such as wallet software of "non-custodial wallets"), or even hardware on which the key is stored, meets the definition of "controlling, on behalf of clients". If it does not, in line with Recital 83 MiCA, users of these wallet types are unprotected by its provisions. This has the unwanted effect that ESMA is prevented from drafting implementing rules for "non-

<sup>338</sup> See, e.g., Cone, G., Bjorklund, N.S., Dyekman, G.C., 2021, *Digital assets and property rights in insolvency*, Trusts & TRUSTEES, 27(5), p. 406. See also Solinas, M., 2021, *Trustless' distributed ledgers and custodial services* in ROUTLEDGE HANDBOOK OF FINANCIAL TECHNOLOGY AND LAW, edited by Chiu I., Deipenbrock G., Routledge; Haentjens M., De Graaf T., Kokorin I., 2020, *The Failed Hopes of Disintermediation: Crypto Custodian Insolvency, Legal Risks and How to Avoid Them*, Singapore Journal of Legal Studies, p. 526.

<sup>339</sup> Cf. Sandor, K., *What Is Crypto Custody?* (CoinDesk, 18 February 2022), available at: <https://www.coindesk.com/learn/what-is-crypto-custody/> accessed on 18 April 2023 (stating that "When it comes to crypto custody, it works a little bit differently. Digital asset custodians do not technically store any of the assets because all data and transactions exist on a public ledger called the blockchain. Instead, what they guard are users' private keys – the important part of a crypto wallet that grants access to the funds held in it."). In contrast to e.g. physical coins that can be held in hand, crypto-assets only exist as data on a blockchain and thus can never be "taken off" the blockchain they are designed on. That leaves, in the authors' opinion, control over the crypto assets by way of access to the private key as the sole defining element of custody of crypto assets. Yet, the degree of control varies, and regulators should define whether embedding the private key in code, while holders never see it, rests control in the holders – or someone else.

<sup>340</sup> Recital 83 MiCA holds "Hardware or software providers of non-custodial wallets should not fall within the scope of this Regulation."



custodial wallets". This is particularly unfortunate in light of this wallet type gaining importance as a side-effect of CASPs seeking to avoid EU regulations.

A further difficulty stems from the **mix of centralized and decentralized forms of services on a single platform**. For instance, let us assume that a custody service is "fully decentralized", while an exchange service is run on the same platform by a central intermediary. Here, one can apply a granular or more general view. If one considers each part of the services (that is, exchange and custody) separately to determine the scope of MiCA, more services will be out of scope due to their "full decentralization", even though they might be offered by the same platform or CASP and are accessible to all customers of that platform or CASP. Yet, including an out-of-scope service simply because it is offered by a platform or CASP that equally provides an in-scope service will make little sense in the absence of expanding the scope to *all* decentralized services: an industry seeking to arbitrage regulations will set up centralized and decentralized services separately, to ensure regulators have only a minuscule part of the business under supervision.

#### b. Substance of custody rules

On the implementation level, the custodian's fiduciary duties must be clarified. Financial regulation must ensure that assets, without the owner's consent, may neither be lent, traded nor used as security in transactions on the intermediary's own account. Any crypto-asset transfer for the benefit of investors (i.e. crypto lending) should be properly documented, earmarked, traced across the blockchain, and monitored by the crypto custodian, while counterparty risks during the transactions should be properly managed by way of required margins and the like.

So far, Article 70 MiCA only prohibits the use of crypto-assets on the CASP's *own* account. While this was in fact the case in some high profile cases (including Babel, Celsius and most likely FTX/Alameda), there are many more use cases, which raise concerns. In particular, there is no reuse by a CASP in two variants of crypto lending where the holders themselves become: (1) connected to other lenders that collectively form the pool of lenders from which borrowers may receive credit, or (2) the counterparty of a borrower in case of peer-to-peer lending.

Further, ESMA should consider the additional technical complexity and exposure in multiple DeFi stacks in which crypto-assets are referenced or otherwise tied to other crypto-assets (discussed herein as crypto stacking). This justifies additional requirements around technical and cyber resilience. In particular, we would propose additional description of custody practices in the programme of operations under Article 60(7) MiCA or the "custody policy" mentioned in Article 75 MiCA, and rules that reduce, as far as possible, "hot wallet" storage and that mandate storage of disaggregated amounts of assets (the equivalent to omnibus accounts) in "cold wallets".

The crypto industry has already taken the initiative since the collapse of FTX to initiate Proof-of-Stake (PoR) protocols.<sup>341</sup> In this regard, the general idea is that a crypto exchange or other crypto project or intermediary subjects its reserves to audits at regular intervals. We suggest licensed crypto exchanges and projects make their PoR public (and in real time).<sup>342</sup> The regulators (and public) can then access and potentially audit the PoR statement as needed. Notwithstanding the difficulty for most of the general public to perform the blockchain analytics required to actually audit the PoR, the fact that some users

<sup>341</sup> See Maurer M., 2022, *More Crypto Exchanges Verify Reserves, But Questions About Assets Remain*, WALL STREET JOURNAL, available at: <https://www.wsj.com/articles/more-crypto-exchanges-verify-reserves-but-questions-about-assets-remain-11670153687>.

<sup>342</sup> Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, *The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*, University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

(and especially regulators) can do this (if they want to) should go a significant way to ensuring that the client funds held by a crypto exchange or project are stored safely and segregated properly.<sup>343</sup>

As to how to exercise the implementing powers envisaged in MiCA, a default rule bringing crypto-assets within the scope of the MiFID framework may well simplify matters. While the wording of MiCA is strict on custody, it does not entail explicit implementing powers that would entitle the ESAs to determine details under Article 75 MICA. While ESMA may formulate guidelines under its general mandate, it remains to be seen whether the lack of bespoke implementing powers for custody, as one of MiCA's most crucial matters, may undermine the beneficial impact of MiCA.

#### 5.1.5. Fraud and market abuse

To ensure market fairness and investor protection, regulators must implement and enforce effective rules against market abuse.<sup>344</sup>

MiCA provides for some anti-market abuse rules in Title VI, which were significantly expanded throughout the legislative process and now explicitly regulate insider dealing, among others. Yet, the rules on market abuse are quite short when compared to the legislative framework that was developed under the MAR, dealing with abuse in the context of financial instruments. ESMA and the Commission have released, over the time span of six years, an extensive set of implementing legislation and guidelines to provide legal certainty on the many facets of market abuse. Notably, core to market abuse regulations is the definition of what constitutes market abuse, and in some Member States, constitutional law prevents criminal and administrative sanctions in the absence of sufficiently detailed legislation.

In turn, to allow for effective enforcement, the enormous implementing activity on market abuse must be repeated under MiCA. This will take significant resources from the ESAs and NCAs involved in the process – resources that cannot be used for enforcement where it matters most for EU consumers. A broad regulatory treatment of crypto-assets under the MAR could close the gap we envisage. In turn, crypto-assets should be added explicitly to the scope provisions of the MAR. For details, see *supra* at 3.6.

If possible, these rules will need to be **coordinated globally** through cooperation mechanisms such as the IOSCO MMOU.<sup>345</sup> So far, the MMOU deals with securities and financial derivatives, thus crypto-assets other than EMTs and ARTs that fall in the scope of MiCA are beyond the scope of the MMOU. In turn, we encourage taking steps that result in the extension of the MMOU to cover explicitly crypto-assets other than EMTs/ARTs. In the same vein, it must be ensured that EMTs/ARTs are included in the work and the respective cooperation frameworks of the BIS, FSB, Basel Committee on Banking Supervision as the other core global financial standard-setters.

---

<sup>343</sup> See also the letter from Adrienne A. Harris, Superintendent of Financial Services to Entities Licensed Under 23 NYCRR Part 200 or Chartered as Limited Purpose Trust Companies Under the New York Banking Law That Custody Virtual Currency Assets, *RE: Guidance on Custodial Structures for Customer Protection in the Event of Insolvency*, (Jan. 23, 2023), available at: [https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/il20230123\\_guidance\\_custodial\\_structures](https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures).

<sup>344</sup> See Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>345</sup> International Organization of Securities Commissions (IOSCO), Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), IOSCO (2020).

## 5.2. Remaining challenges under MiCA

### 5.2.1. Delineating scope

As mentioned under 5.1.1., MiCA aims to fill the regulatory space outside of the scope of existing EU financial regulation (cf. Article 2(4) MiCA and Recital 16). MiCA anticipates that the borderline between the different types of financial services is clear-cut – but they are not. The delineating scope will remain a constant challenge under these conditions. Given that MiCA is not identical to EU financial laws, this will allow for arbitrage opportunities and undermine the level playing field.

**MiCA is not blind to the definitions issue.** It addresses classification in a number of different ways:

- (1) It provides for **guideline powers to ESMA** on the criteria and conditions for the qualification of crypto-assets as financial instruments, thus addressing the MiCA/MiFID interface (cf. Article 2(5) and Recital 14).
- (2) When notifying the crypto-asset white paper to the NCA, offerors of a crypto-asset, persons seeking admission to trading, or operators of trading platforms, as the case may be, shall add an **explanation** of why the crypto-asset to be sold in the Single Market is not excluded from the scope of MiCA, and also neither an EMT nor an ART. In the same vein, the issuers of ART need to deliver a **legal opinion** supporting the classification of the crypto-asset as ART. At the request of the NCA, **ESMA and EBA shall comment** on these explanations; thus, the NCAs may ask for the ESAs' opinion on each case (cf. Article 17(1), 18(2), 20(5) and 97(1)).
- (3) To ensure consistency of said explanations and legal opinions, the **ESAs shall jointly develop guidelines** to specify the content and form of the explanation. The guidelines shall include a template for the explanation, opinion and a **standardized test for the classification of crypto-assets** (Article 97(1)). This standard test for the classification of crypto-assets will address the MiCA/PSD/EMD interface as well as the delineation between EMT, ART and other crypto-assets within MiCA's scope.
- (4) NCAs may request **an opinion on the classification of crypto-assets** from one of the ESAs, including NFTs formally exempted pursuant to Article 2(3), which needs to be provided within 15 working days of receipt of the request from the competent authorities (Article 97(3)). Again, we expect the NCAs to ask for the ESAs' opinion on cases at hand.
- (5) NCAs have to **register crypto-asset white papers**. This registration will be based on a set of ESMA regulatory technical standards ensuring data that is necessary for the classification of crypto-asset white papers is delivered as part of the registration (Article 109(8)).
- (6) The ESAs shall jointly draw up **an annual report**. This report will identify, based on issues reported by NCAs, difficulties in the classification of crypto-assets and divergences in the approaches of the competent authorities, and consider the information stored in the crypto-asset (service provider) register (Article 97(4)).
- (7) The EU Commission **may adopt delegated acts specifying technical aspects of the definitions** in Art. 3(2) MiCA. This will concern, primarily, the definition of crypto-assets as well as particular terms used in MiCA, such as EMT, ART, utility tokens and other crypto-assets.
- (8) Finally, the classification matter will be **closely monitored**. The EU Commission will draw up a report within 24 and 48 months after the coming into force of MiCA; this report will also discuss classification of crypto-assets including possible divergences in approaches by competent authorities (Article 140(2)(b)).

All in all, through various measures, MiCA establishes a **centralized approach**. For developing guidelines we expect the ESAs to build on the significant work that has been done so far in the field of crypto-assets.<sup>346</sup> For the practice of this centralized approach, however, the capacity and expertise of the NCAs, as well as the ESAs, play a crucial role.<sup>347</sup> In light of the different market size and population of Member States, not all NCAs will be able to develop and focus resources on crypto-assets and their technical specificities. This is particularly true as long as the crypto industry forms, in total, a **niche sector of the economy**. In times where, for instance, a banking, economic or political crisis is on the horizon, few NCAs will pursue investing significant resources into the analysis of crypto-assets. Under these circumstances, **the more sophisticated and work-intensive a regulatory approach** the less we expect NCAs to be able to deliver on their obligations to enforce EU financial regulation. Any EU approach should thus be tailored towards easy oversight and efficient, pragmatic application of the law. Technical sophistication is a secondary concern.

A centralized, guideline-based approach may work where regulators have **years to determine their approach and incrementally fine-tune it**, similar to the development of case law. However, we see the difficulty that, at least initially, less cases of crypto-assets will come to the NCAs and the ESAs due to the prevalence of (apparent) reverse solicitation in crypto, and the importance of third-country platforms. With that industry practice prevailing, the NCAs and the ESAs must first invest immense regulatory capital to inquire into thousands of platforms, only to learn that, under the current (and uncertain) scope, the platform does not have a sufficient number of clients in that very country, or insists it is “fully decentralized” and hence out of scope.

We thus propose the implementation of a bold default rule in 6.2., which shifts the initiative to the crypto platforms and entitles ESMA to gather information on all EU clients.

### 5.2.2. Periodic disclosures and accounting

Title II MiCA establishes the duty to issue a white paper for certain crypto-assets, but **few rules on periodic disclosure after the initial launch** of the crypto-asset. It is uncertain how users receive information on platform stability, accounting data and many other details of relevance. Further, MiCA does not stipulate that the offeror subject to Title II MiCA must have **proper bookkeeping and accounts**, which may be crucial for winding up the platform in case of malfunctions or insolvency of any offeror or operator. This has proven particularly important in the Crypto Winter, with several crypto asset platforms halting operations temporarily or permanently. While MiCA requires governance arrangements for issuers of ART, including accounting rules (cf. Article 34 MiCA), and the same follows from the application of rules for e-money providers on EMT issuers, we lack the same prerequisite for issuers of other crypto-assets than ARTs and EMTs.

The two aspects differ in terms of perspective. One perspective is outward-oriented (users), and the other inward-oriented to ensure that an external administrator finds what it needs to wind up the platform.

<sup>346</sup> Cf. 'Final Report on response to the non-bank lending request from the Cfa on digital finance', 2022, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-provides-its-advice-eu-commission-non-bank-lending>; 'Advice on the review of the macroprudential framework', 2022, European Banking Authority (EBA), available at <https://www.eba.europa.eu/eba-proposes-simplify-and-improve-macroprudential-framework>. : 'Report with advice for the European Commission on crypto-assets', 2019, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-reports-on-crypto-assets>; 'Crypto-assets and their risks for financial stability', 2022, European Securities and Market Authority (ESMA), available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251\\_crypto\\_assets\\_and\\_financial\\_stability.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf); 'Advice – Initial Coin Offerings and Crypto-Assets', 2019, European Securities and Market Authority (ESMA), available at: [https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf).

<sup>347</sup> See, for instance, E. Noble, Opening Remarks to the European Economic and Social Committee (EESC) public hearing on crypto-assets: opportunities and challenges, available at: <https://www.eesc.europa.eu/en/news-media/presentations/crypto-assets-challenges-and-opportunities>, at 3-4 (stressing the need for technical capacity building and building monitoring capabilities on the side of supervisors).

While one may argue that assets of financial relevance are subject to Titles III and IV MiCA or as financial instruments subject to MiFID, we do not think that **proper accounting is dispensable by any organization of a given size** (including issuers of crypto-assets under Title II MiCA). We believe this may be addressed in three ways: (a) subjecting offerors to rules as CASPs, (b) assigning entity status to DAOs, and (c) bespoke winding up, insolvency and restructuring legislation. We provide more detail in chapter 6, but address the last matter in the next section.

### 5.2.3. Restructuring and resolution legislation

Chapter 3 of MiCA obligates issuers of ARTs to implement various measures related to asset reserves, with a view to safeguarding and ring-fencing customer funds. However, based on the experience of the Crypto Winter, the risk of insolvency (amongst other risks) is also present with other types of crypto intermediaries. At the height of the Crypto Winter, private market participants often shunned measures to preserve assets and did not engage in private litigation. One of the most likely reasons for this was legal uncertainty relating to very basic questions, for instance, whether proprietary rights are assigned to crypto-asset holders in insolvency and if so which ones and under which circumstances.<sup>348</sup> The former is true **for both centralized and decentralized DeFi services**, only that in the case of losses in the context of decentralized services the losses are spread across many DeFi asset holders and as such do not show on a single balance sheet of a centralized provider.

Financial regulation alone is incapable of solving all the legal issues surrounding crypto-assets. **Resolution legislation** would facilitate a clear line between an insolvent intermediary's (or "fully decentralized protocol's") assets subject to bankruptcy, and those that remain out of scope. Such a clear perimeter for assets subject to bankruptcy proceedings will be particularly crucial to a crypto insolvency or resolution, where code protocols in the DeFi stack are often proprietary and non-standardized, and depend on the interaction of many different actors. If the dissolution of the crypto-system seems likely, these actors will become distinctly uninterested in the maintenance and defence against cyberattacks of the DeFi stack. This in turn will quickly erode any ability to restructure the crypto environment in times of stress. Resolution legislation is crucial to provide system continuity and incentivize the many (decentralized) support functions that characterize crypto-ecosystems.

If incentives to continue operations in the event of a crisis are implemented, there should (theoretically and practically) be little need for a Lender of Last Resort (LoLR) in *fully decentralized settings*. Furthermore, when a SICI has a dominant position within an ecosystem, as is typically the case, we do not recommend the establishment of a crypto LoLR due to the conflicts and moral hazards inherent in a LoLR in these markets.<sup>349</sup> Where necessary and warranted for the financial system or one of its segments, central banks will likely have the means to inject liquidity by regulated stablecoins, synthetic central bank digital currencies (CBDCs), wholesale CBDCs or otherwise.

---

<sup>348</sup> See Woxholt J., Zetsche D., Buckley, R. P., Arner, D. W., *Competing Claims to Cryptoassets*, 2022, available at: <https://ssrn.com/abstract=4394952>; see also Lehmann, M., *Who owns Bitcoin?*, 21 Minn. J.L. Sci. & Tech. 93 (2019).

<sup>349</sup> While crypto intermediaries may play important roles in future restructuring (as JP Morgan did when Bear Stearns experienced difficulties), the FTX-Binance example (cf. *supra*, at 2.5.4.) has shown that crypto intermediaries pursue, for the most part, their own interests.

#### 5.2.4. Cross-border harmonization and coordinated enforcement

Due to the use of non-formal information and communication (cf. 3.6.), crypto raises entirely new challenges for market monitoring by regulators.<sup>350</sup> In light of these challenges, it is unfortunate that **MICA does not harmonize marketing rules** on crypto-assets. Some divergence will remain. We will address this issue separately *infra* (cf. 6.2.), by proposing a cross-border harmonization of EU third country marketing rules.

We have further shown *supra* (3.2.5.) that the decentralization of functions across borders disincentivizes compliance.<sup>351</sup> To address this, regulators need to engage in close cross-border cooperation and coordination. This principally requires the inclusion of crypto-assets in existing Memorandums of Understanding (MoUs), in particular the IOSCO MMoU (cf. *supra*, at 5.1.5.). We recommend expanding existing MoUs, including the IOSCO MMoU, to address the partial decentralization of functions that we have laid out as characteristic of crypto. Asset segregation, safekeeping, crypto staking and stacking, and particularly cross-border restructuring and administration in bankruptcy with related asset recoveries as well as NCA-sponsored collective redress, may all require the joint action of several regulators in various jurisdictions.

Industry associations may facilitate information flows in certain instances,<sup>352</sup> but where externalities are concerned, regulators are best equipped to pursue the public interest and act to provide requirements relating to public goods and externalities.<sup>353</sup>

Crypto provides a particularly suitable case for a global oversight coordination body. Yet the organizational complexity of a global regulator, deciding where the body will be located, financed and equipped, how it will be able to enforce decisions, and to what extent it can override local decisions, make the establishment of any global oversight body a significant challenge. We encourage the regulatory coordinators of traditional finance, such as the FSB, BIS and IOSCO, to expand their expertise in, and reach out to embrace the field of crypto.<sup>354</sup> As we have shown throughout this study, crypto regulation will benefit greatly from insights drawn from the regulation of traditional finance.

### 5.3. Impact of TFR

#### 5.3.1. In-scope transactions

With the implementation of the revised Transfer of Funds Regulation (TFR), the TFR's scope will include CASPs as defined by MiCA,<sup>355</sup> thus widening the scope beyond custodian wallet providers for crypto-assets and the providers of fiat to crypto-assets – and vice versa – exchange services.

Under the current and revised version, a CASP is required to collect information (name and account number) of the originator and the beneficiary of any crypto-asset transaction and more detailed information (address, ID-number, etc.) on transactions of EUR 1,000 or more performed by the CASP

<sup>350</sup> Cf. E. Noble, Opening Remarks to the European Economic and Social Committee (EESC) public hearing on crypto-assets: opportunities and challenges, <https://www.eesc.europa.eu/en/news-media/presentations/crypto-assets-challenges-and-opportunities> at p. 3-4 (arguing that regulators need to build new monitoring capabilities).

<sup>351</sup> Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>.

<sup>352</sup> Such as the Crypto Market Integrity Coalition, see CMIC, available at: <https://www.cmic.global>, accessed 29 March 2023.

<sup>353</sup> See, Arner, D.W., Zetzsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516).

<sup>354</sup> *Ibid.*

<sup>355</sup> See Art. 3(15) TFR.

(the so-called “travel rule”).<sup>356</sup> The TFR sets special requirements for transfers that are **not** made to and from accounts,<sup>357</sup> in particular to and from non-custodial wallets. CASPs must assign a unique identifier to these transactions and ensure that “the transfer of crypto-assets can be individually identified” and record the originator and beneficiary address on the distributed ledger.”<sup>358</sup>

### 5.3.2. Gap analysis

#### a. TFR’s scope limited by MiCA’s scope

Considering the definition of CASPs together with the obligation to ensure the information on non-account transfers, a gap exists that stems from the TFR’s **scope that is limited to CASPs as defined by MiCA**.<sup>359</sup> DeFi protocols that do not fit the definition of a CASP will not be subject to the TFR. For instance, the decentralized liquid staking protocol Stader argues in their terms and conditions that they (“Stader Labs”) are “not party to anything”. In their words, they merely provide information on the Stader liquid staking service and the protocol (the liquid staking service) is comprised of a non-custodial smart contract that executes peer-to-peer transactions.<sup>360</sup> In laymen’s terms the argumentation goes: Stader Labs does not store the private keys granting control over any crypto-assets flowing through or locked into the protocol and therefore does not have control of any crypto-asset going through or locked into the platform (which would meet the definition in Article 3 (17) MiCA of custody). Hence, Stader Labs believes it is not a CASP, nor an intermediary of any kind, but a mere technology operator i.e. information provider, and thus entirely outside of the scope of the TFR (and MiCA as well).

While other platforms are less explicit, the same logic is applied by other decentralized platforms. These include, for instance, decentralized crypto lending platforms such as the aforementioned Aave,<sup>361</sup> decentralized exchanges (DEXs), such as Curve with a daily trading volume of USD 132 million;<sup>362</sup> liquid staking protocols such as Lido with over 280 000 customers, USD 9.5 billion in staked tokens and USD 416 million in distributed rewards;<sup>363</sup> crypto bridge protocols such as Multichain with a cumulative lifetime volume of USD 98.5 billion; and NFT marketplaces,<sup>364</sup> such as Blur with a daily trading volume of USD 54 million<sup>365</sup> and over 146 000 users.<sup>366</sup> If the argumentation of these platforms is followed and they are classed as “fully decentralized” they will all be outside of the scope of the TFR with the result that they are not obligated to implement the travel rule. Hence, to identify the persons involved in any transactions after the use of each of these protocols, each subsequent transaction must be traced back to a transaction that took place on a regulated CASP.

<sup>356</sup> Art. 14 & 16 TFR.

<sup>357</sup> Art. 14 (3) TFR.

<sup>358</sup> Art. 14 (5) & Art. 16 (2) TFR.

<sup>359</sup> The revised Transfer of Funds Regulation (EP position available at [https://www.europarl.europa.eu/doceo/document/TA-9-2023-0118\\_EN.html#title2](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0118_EN.html#title2)) does not extend the scope of AML/CTF rules to fully decentralized platforms as Article 3(15) of the proposal refers to the MiCA definition of crypto-asset service providers as further explained in Recital 22 MiCA.

<sup>360</sup> ‘Terms of Service, Staderlabs’ (Staderlabs), available at: <https://www.staderlabs.com/terms-of-service/>, accessed 29 March 2023.

<sup>361</sup> See ‘Terms of use’ (Aave), available at: <https://aave.com/term-of-use/>, accessed 29 March 2023, at par. 2.

<sup>362</sup> Daily volume taken on 02/03/2023 (see. ‘Swap Curve’ (Curve), available at: <https://curve.fi/#/ethereum/swap>, accessed 23 March 2023).

<sup>363</sup> ‘Liquidity for Staked Tokens’ (Lido), available at: <https://lido.fi>, accessed 29 March 2023.

<sup>364</sup> ‘Cross-Chain Router Protocol’ (Multichain), available at: <https://multichain.org>, accessed 29 March 2023.

<sup>365</sup> ‘Blur’ (Dappradar), available at: <https://dappradar.com/ethereum/marketplaces/blur>, accessed 29 March 2023.

<sup>366</sup> ‘Blur’ (Blur), available at: <https://blur.io>, accessed 29 March 2023.

## b. Breaking the link

**CASPs that are in the TFR's scope** record the information to or from the initial originator or beneficiary. Due to the nature of permissionless blockchains and their transparency,<sup>367</sup> it is possible to trace each subsequent transaction from the initial wallet address unless “the link is broken”, seemingly mitigating the risks stemming from “out of scope” fully decentralized protocols. Yet the link *may* be broken **whenever some crypto intermediary further along the chain is not subject to TFR.**

Out of the TFR's scope are transactions where: (1) the nature of the asset does not qualify for the TFR, as in the case of NFTs, (2) the set-up of the intermediary does not qualify as CASP under the TFR (i.e. MiCA), as in the case of fully decentralized platforms, and (3) the geographical location of a crypto intermediary is beyond the TFR's geographical scope, and no cooperation with third-country entities is ensured. **Each of these cases constitutes a gap**, from the perspective of efficient enforcement of AML/CTF rules, as we demonstrate below with two examples.

## c. Use of NFTs

As a first example, envisage a nefarious actor like a terrorist organization creating an NFT collection anonymously and issuing this collection on one of the NFT marketplaces with the intent to raise funds.<sup>368</sup> The creation of the collection requires a minimum investment only. Depending on the blockchain, it can cost as little as USD 30 to “mint” an NFT collection of 10 000 NFTs.<sup>369</sup>

Such a small amount can be obtained rather easily and anonymously via a decentralized platform facilitating peer-to-peer transactions<sup>370</sup> or an exchange in a non-cooperative country on AML/CTF requirements. Once the collection is minted, the terrorist organization can anonymously communicate with sympathizers via an end-to-end encrypted messaging service to instruct them in which NFT collection to purchase.<sup>371</sup> Assuming that sympathizers acquire cryptocurrencies via an EU-CASP using credit card or bank details, the CASP processing these transactions will know their identity.

However, it is still not possible to identify these persons as sympathizers. Even if they directly purchase an NFT with the newly acquired funds, due to the lack of control of NFT platforms, it is practically impossible to ascertain that the collection is indeed used for terrorist financing. To prevent these transactions, intelligence services will need to scrutinize each NFT class in terms of AML/CTF risk without the NFT marketplace providing any KYC-data, and ask CASPs to monitor or blacklist any user that is linked to an address that purchased or traded an NFT identified as suspicious. Considering the number and nature of NFTs, this is practically impossible.<sup>372</sup>

<sup>367</sup> Transactions and wallet addresses on permissionless (public) blockchains are readily accessible. See ‘The Ethereum Blockchain Explorer’ (Etherscan), available at: <https://etherscan.io>, accessed 29 March 2023, ‘BNB Smart Chain Explorer’ (BscScan), available at: <https://bscscan.com>, accessed 29 March 2023, ‘Bitcoin Explorer’ (Bitcoin Explorer), available at: <https://bitcoinexplorer.org>, accessed 29 March 2023.

<sup>368</sup> An NFT marketplace does not fit the definition of CASP as long as it does not 1) provide custodian wallet services or 2) exchange fiat currency for crypto-assets (or vice versa) under the current regime and may also be out of scope under MiCA when it can claim full decentralization.

<sup>369</sup> ‘How Much Does It Cost To Create an NFT Collection?’ (Okuha, 4 January 2023), available at: <https://okuha.com/how-much-does-it-cost-to-create-an-nft-collection/>, accessed 29 March 2023..

<sup>370</sup> Depending on the level of involvement, the crypto intermediary might be able to claim that they do not provide any of the services detailed in Art. 3(16) MiCA and merely provide information i.e. an interface that the users themselves use to transact peer-to-peer (cf. *infra* 5.3.2. at the beginning).

<sup>371</sup> End-to-end encrypted services are available in almost all platforms, see Koops, B-J., Kosta E., 2018, Looking for Some Light Through the Lens of ‘Cryptotwar’ History: Policy Options for Law Enforcement Authorities Against ‘Going Dark’, Computer Law & Security Review, 34, pp. 890-900, available at: <https://ssrn.com/abstract=3249238>.

<sup>372</sup> For instance, in 2022 an NFT collection of an Indonesian student selling NFTs of personal selfies raised more than US \$1 million. Heather Chen, ‘This guy is living your wildest NFT dreams, making \$1 Million in Selfie Sales’ (Vice, 17 January, 2022), available at:



Regulatory capacity may also be wasted: unsuspecting users, unaware of any illicit fundraising activities, may buy NFTs from the terrorist organization's NFT collection alongside the sympathizers for investment purposes or simply to collect.<sup>373</sup> By subjecting the NFT marketplace to the TFR and preferably AMLD, the terrorist organization would have to identify itself prior to minting the NFT collection. In turn, it will make it substantially more difficult to execute its nefarious funding activities.

#### d. Use of other protocols that do not qualify as CASP

As a second example: any platform that does not meet the CASP definition is beyond the scope of both AMLD5 and TFR. Beyond non-custodial wallets, for instance, a **mixing service**<sup>374</sup> is not a CASP when it can claim full decentralization; this is the case if it pursues peer-to-peer transactions.<sup>375</sup> Yet due to the service of "mixing crypto-assets", tracing the transaction chain of a token class becomes impossible.<sup>376</sup>

After mixing, we do not know the parties to a transaction anymore. In turn, we will not know to whom the funds are forwarded after the use of the mixing protocol. From the recipient's perspective, we do not know where the funds come from other than from a mixing service. Regulations may respond by classifying any funds traceable to mixing services as high risk<sup>377</sup> and require CASPs to block the user's account. However, that only solves one problem and creates a new one since this user could equally "break the link" between the mixing service and the non-custodial wallet by trading NFTs or use another DeFi protocol, such as a crypto bridge,<sup>378</sup> prior to, or instead of, transacting with the CASP.

#### e. Remedies

At the core of the problem lies the TFR's limited scope, which does not include NFT marketplaces, decentralized platforms and services, as well as non-custodial wallets and platforms in non-cooperating third countries. These limits open opportunities for unidentified transactions.

Technically, an easy way to address the deficiency is to **include all DeFi protocols, including protocols solely offering non-custodial services, into the travel rule** under TFR and give up the limitation of scope depending on crypto-assets excluding NFTs and the CASP definition.<sup>379</sup> In fact, we propose something similar, yet subject to exemptions, with a default rule that classifies all crypto-assets as securities (including the ones issued by decentralized platforms) unless exempted by NCAs (cf. *infra*,

---

<https://www.vice.com/en/article/4awn3m/indonesia-nft-crypto-bitcoin-ghozali>, accessed 29 March 2023. Any terrorist can pose on selfies. How shall regulators monitor fund flows in this case?

<sup>373</sup> The FATF indicates that so-called "red flags" must be considered in context and not on a stand-alone basis. A single "nefarious NFT" can thus only be viewed as an indicator of potential risk. See Financial Action Task Force (FATF), 2020, *Virtual Asset Red Flag Indicators or Money Laundering and Terrorist Financing* (2020), available at: <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html>, at par. 18.

<sup>374</sup> A crypto mixer or a crypto bridge may be set up in such a way that it is either: 1) fully decentralized or 2) does not provide any of the services listed in Art. 3 (16) MiCA. For more information about crypto mixers, see. Stevens, R. 'Bitcoin Mixers: How Bitcoin Mixers Work and Why People Use Bitcoin Mixers' (Coindesk, 22 August 2022), available at: <https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/>, accessed 29 March 2023.

<sup>375</sup> If the logic of the protocols is followed, claiming to not be a party to any transaction, a mixing service will not qualify as a 'crypto-asset service': providing transfer services for crypto-assets on behalf of clients under MiCA Art. 3 (16)(j).

<sup>376</sup> 'Why you can't trace funds through services using blockchain analysis (and why you don't need to anyway)' (Chainalysis, 9 October 2020), available at: <https://blog.chainalysis.com/reports/blockchain-analysis-trace-through-service-exchange/> accessed 29 March 2023.

<sup>377</sup> The FATF indicates the use of a mixing service as a "red flag". See, Financial Action Task Force (FATF), 2020, *Virtual Asset Red Flag Indicators or Money Laundering and Terrorist Financing* (2020), available at: <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html>, at par. 13.

<sup>378</sup> Stevens R. 'What are blockchain bridges and how do they work?' (CoinDesk, 7 March 2022), available at: <https://www.coindesk.com/learn/what-are-blockchain-bridges-and-how-do-they-work/>, accessed 29 March 2023..

<sup>379</sup> See also, 'Why you can't trace funds through services using blockchain analysis (and why you don't need to anyway)' (Chainalysis blog, 9 October 2020), available at: <https://blog.chainalysis.com/reports/blockchain-analysis-trace-through-service-exchange/>, accessed 29 March 2023.

at 6.2.2.) and to assign entity status to DAOs for regulatory purposes (cf. *infra*, at 6.3.1.). Further, the Euro Wallet proposed *infra*, at 6.2.1 c) will ring-fence the compliant sector.

## 5.4. In depth: financial NFTs

The use of NFTs is not limited to art, gaming, and collectibles. Concerning financial services, NFTs play an important role, worthy of regulatory attention.

### 5.4.1. Functions and structure of financial NFTs

Financial NFTs are tokenized financial products. An insurance contract can be tokenized for instance, but also any other cash-flow-yielding contract like a lending agreement. Yet, the definitional boundaries of financial NFTs are not entirely clear.

#### a. Uniqueness in a technical sense

An NFT is coding that references a "minted asset" and can be enriched with certain features. According to its original meaning, a "**Non-Fungible Token**" is a cryptographic token that cannot be interchanged in a like-for-like manner.<sup>380</sup> "Like-for-like" in this case means that one token cannot be substituted for another token of the same type: in a world where one ETH token is as good as another one, the fact that a token is not akin to another is an exception. Given that the tokenization process necessarily comes with standardization in technical ways, we argue that the "**non-fungible**" aspect of NFTs is somewhat of a misnomer.

In a transferred meaning, NFTs are a type of digitally securitized real-world asset (including copyrights, pieces of music, land and others) that only exists in one copy, and hence are "unique". That uniqueness can refer to only a single token representing the same underlying asset. Further, in the case of tokenized music, the underlying asset can be represented multiple times, but *use* can be restricted to one user at a time; then the uniqueness stems from the personalization of users' rights.

NFTs in general are **unique in a technical sense**, which is achieved through the respective token standard that is used.<sup>381</sup> In particular, while fungible token standards require that each token has the same values as another token created by the same protocol (i.e. "smart contract"), the NFT standard ERC-721<sup>382</sup> allows the processing of several tokens that each have different values compared to other tokens that are created by the same protocol. Each ERC-721 NFT has a token identification code property that must be globally unique.<sup>383</sup> An analogy would be a postage stamp series where each stamp bears an individual number.

This technical uniqueness does not imply any rareness or scarcity of the underlying asset on its own. As in the stamp example, the financial underlying is not scarce, but its representation is. However, an ERC-721 NFT can be enriched with properties that **attribute rareness to the NFT within its collection**. Attributes can be unique within the collection, but do not have to be. Often, the combination of different attributes of one NFT is unique, but not the individual attributes. The rareness is often

<sup>380</sup> 'What Is an NFT?' (Binance Academy, 26 February 2020), available at: <https://academy.binance.com/en/articles/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts>, accessed 29 March 2023.

<sup>381</sup> Gabers-von Boehm, K., Haag, H., Gruber, K., 2022, *Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art*, at p. 13, available at: <http://www.europarl.europa.eu/supporting-analyses>.

<sup>382</sup> The ERC standard is unique to the Ethereum blockchain. Other blockchains use different token standards that may have different characteristics.

<sup>383</sup> 'ERC-721 Non-Fungible Token Standard' (Ethereum), available at: <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>, accessed 29 March 2023.

specified by indicating the percentage of other NFTs within the collection that have the same attributes.<sup>384</sup>

Beyond collectibles and digital art where scarcity impacts value, ERC-721 NFTs are also a common standard in financial NFTs that can function as **governance tokens** allowing holders to vote on, for example, allocation of rewards to liquidity providers during the next epoch.<sup>385</sup> Often they also function as **proof of claim** against a protocol, for example, when supplying tokens to liquidity pools of a DEX.<sup>386</sup>

#### b. Other NFT standards

ERC-721 is, however, not the only token standard that can be used to create NFTs. Several other standards allow for some type of financial use.

- ERC-998<sup>387</sup> is described as an extension of ERC-721. An ERC-998 NFT can “hold” other NFTs and fungible cryptocurrencies,<sup>388</sup> resulting in a so-called “**composable NFT**”.<sup>389</sup> To use an analogy, the ERC-998 NFT functions like a **digital basket for several unique stamps or non-unique fungible crypto-assets at once**. Examples of potential uses are legal contracts, supply chain tracking<sup>390</sup> and blockchain-based gaming.<sup>391</sup> A potentially unintended use made possible by way of the ERC-998 token standard might be the creation of **digital investment products** consisting of pooled NFTs and/or fungible tokens together. As a caveat, however, we did not find examples for such type of products, nor that the ERC-998 standard has any practical meaning at all.
- ERC-1155<sup>392</sup> is dubbed a “**multi token standard**”.<sup>393</sup> The ERC-1155 standard allows a smart contract to create fungible or non-fungible tokens or a combination of the two.<sup>394</sup> To use another analogy, the ERC-721 standard is a stamp with a unique number, while the ERC-1155 standard can be used to create limited editions of, for instance, 1,000 reproductions of an asset. These assets may well be financial in nature; a large-volume bond series for institutional investors (like 1000 x 100 TEUR) can be created this way.
- The ERC-3525<sup>395</sup> standard is referred to as a “**semi-fungible token standard**”. It allows for a combination of the unique identity features of the ERC-721 standard with a “value” property.

<sup>384</sup> An example of such an NFT is: ‘Bored Ape Yacht Club, Ape #7350’ (Opensea), available at: <https://opensea.io/assets/ethereum/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/7350> accessed 29 March 2023.

<sup>385</sup> ‘Gauge Voting & Bribes’ (Equalizer Exchange Docs), available at: <https://equalizer0x.gitbook.io/equalizer-exchange-docs/guides/gauge-voting-and-bribes>, accessed 29 March 2023 & ‘veTHE’ (THENA), available at: <https://thena.gitbook.io/thena/the-tokenomics/vethe>, accessed 29 March 2023.

<sup>386</sup> See LP Tokens (cf. *supra*, at 3.4.1.b.).

<sup>387</sup> Lockyer, M. et al ‘ERC-998: Composable Non-Fungible Token’ (Ethereum, 7 July 2018), available at: <https://eips.ethereum.org/EIPS/eip-998>, accessed 29 March 2023.

<sup>388</sup> ‘ERC-20 Token Standard’ (Ethereum), available at: <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/> accessed 29 March 2023.

<sup>389</sup> Lockyer, M. et al ‘ERC-998: Composable Non-Fungible Token’ (Ethereum, 7 July 2018), available at: <https://eips.ethereum.org/EIPS/eip-998>, accessed 29 March 2023.

<sup>390</sup> Lockyer ‘M. ‘Crypto Composables – Building Blocks and Applications’ (Medium, 1 May 2018), available at: <https://medium.com/coinmonks/crypto-composables-building-blocks-and-applications-65902709298c>, accessed 29 March 2023.

<sup>391</sup> Burns ‘B., ERC-998 and the Future of Blockchain Game Assets’ (Medium, 5 September 2018), available at: <https://medium.com/giglabs/erc-998-and-the-future-of-blockchain-game-assets-9fd1063126cf>, accessed 29 March 2023.

<sup>392</sup> Radomski, W. et al. ‘ERC-1155: Multi Token Standard’ (Ethereum, 17 June 2018), available at: <https://eips.ethereum.org/EIPS/eip-3525>, accessed 29 March 2023.

<sup>393</sup> Ibid.

<sup>394</sup> Ibid.

<sup>395</sup> Wang, W. et al. ‘ERC-3525: Semi-Fungible Token’ (Ethereum, 1 December 2020), available at: <https://eips.ethereum.org/EIPS/eip-3525>, accessed 29 March 2023.

These tokens can be disseminated in large quantities and circulate freely, but are identifiable by their unique number. **The ERC-3525 standard was designed to be used as a financial NFT** to reduce transaction costs stemming from the fact that any transaction must be tokenized or executed by way of smart contract. They allow for the issuance of a token with a unique owner, but varying notional amounts, rendering netting of transaction superfluous.

DeFi applications that rely on users to supply liquidity, such as DEXs and lending pools, issue tokens to liquidity providers (so-called “LP tokens<sup>396</sup>”). LP tokens function like **some type of promissory note representing the user’s claim against, or debt to, the liquidity pool in whatever size it is** (for instance, as part of a pooled lending program). The use of LP tokens allows liquidity providers to adjust their liquidity position (by depositing or withdrawing funds) without the need to create a new token.<sup>397</sup> This is crucial as creating new tokens is computationally intense. The LP token reduces transaction costs.

#### 5.4.2. Facts and figures

Tokenization of real-world assets is typically **pursued by centralized crypto intermediaries**. By contrast, the creation of purely digital NFTs, including certain types of financial NFTs, is mostly pursued by decentralized platforms. Further, decentralized platforms tend to organize the trading and transfer of NFTs of all categories. In turn, even if NFTs were in scope of MiCA, most platforms would be out of MiCA due to decentralization.

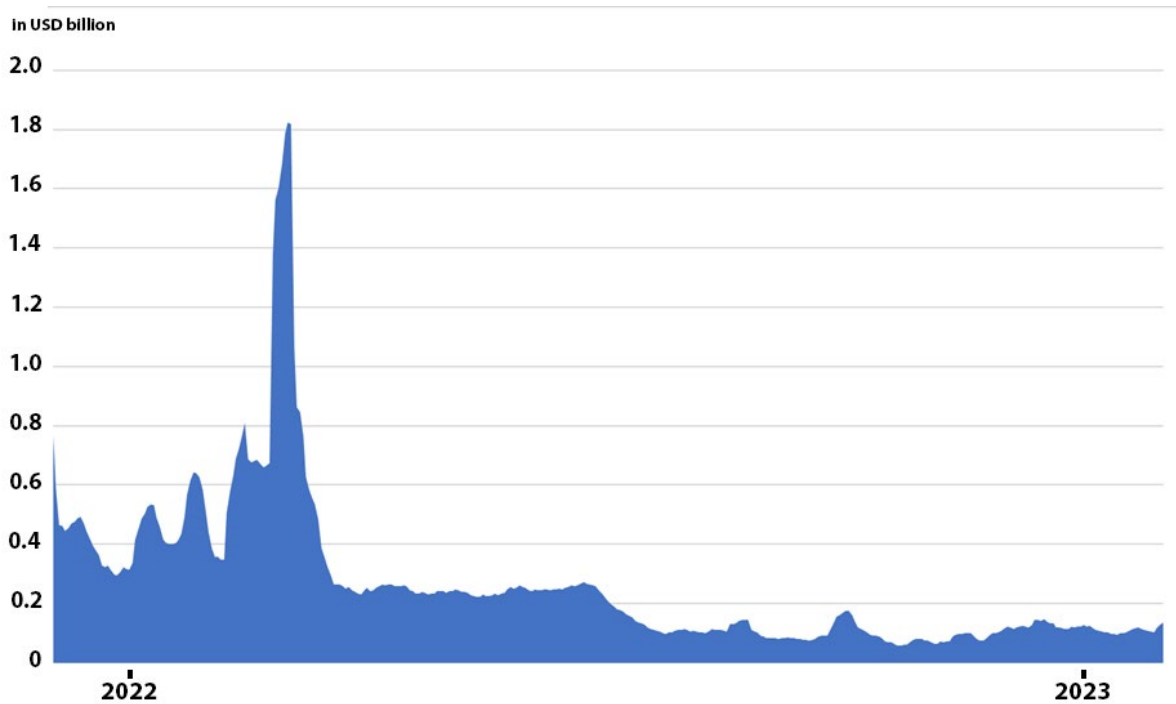
The cumulative trading volume of NFTs during the last year was close to USD 100 billion, yet trading volume differs strongly day-by-day (cf. Figure 12) and dropped together with trust in crypto being undermined, by virtue of the Terra/Luna malfunction in May 2022 (cf. *supra*, at 2.5.2.).

---

<sup>396</sup> See LP Tokens (cf. *supra*, at 3.4.1.b.)

<sup>397</sup> Wang 'W.', 'How ERC-3525 can improve position management in Uniswap V3' (Medium, 29 March 2021), available at: <https://medium.com/solv-blog/how-vnft-can-improve-position-management-in-uniswap-v3-221ab49a8cb2>, accessed 29 March 2023.

Figure 14: NFT trading volume (2022-23)



Source: 'Market Tracker' (NonFungible).<sup>398</sup>

Similar to crypto-asset trading, NFT trading is arranged by specialist crypto intermediaries, yet their trading volume differs enormously: USD 1000 to USD 63 million per 24 hours (see Figure 13).

Figure 15: NFT trading volume per 24 Hours (01-03-2023)

PLATFORM	CATEGORY	USERS	VOLUME	ENTITY	COUNTRY
Blur	Marketplace	11930	\$ 62,830,000.00	n/a	n/a
OpenSea	Marketplace	27090	\$ 10,000,000.00	Ozone Networks, Inc.	United States
X2Y2	Marketplace	562	\$ 6,530,000.00	n/a	n/a
Vulcan Market	Marketplace	382	\$ 329,000.00	Vulcan Forged	Singapore
Foundation	Marketplace	727	\$ 313,000.00	Foundation Labs, Inc.	United States
JPG Store	Marketplace	3140	\$ 249,000.00	n/a	n/a
Manifold	Marketplace	4480	\$ 234,000.00	Manifold Technologies Ltd.	Canada
Element Market	Marketplace	969	\$ 69,000.00	n/a	United States
objkt.com	Marketplace	2470	\$ 64,000.00	Objkt Ltd	Switzerland
AtomicHub	Marketplace	8820	\$ 59,000.00	pink.gg Solutions GmbH	Germany
fxhash	Marketplace	758	\$ 46,000.00	Fxhash Foundation	France
Joepegs	Marketplace	383	\$ 39,000.00	SOJ Trading Ltd	South Africa
tofuNFT	Marketplace	823	\$ 24,000.00	n/a	n/a
BitKeep NFT Market	Marketplace	770	\$ 23,000.00	BitKeep Global Inc.	Cayman Islands
Ebisu's Bay	Marketplace	495	\$ 21,000.00	Anumatech LLC	United States
Quix	Marketplace	400	\$ 10,000.00	Quix Analytics Limited	United Kingdom
Minted Network	Marketplace	369	\$ 10,000.00	Particle Research Ltd	Hong Kong
Rarible	Marketplace	3790	\$ 4,000.00	Rarible Inc	United States

Source: Authors' own presentation based on data from 'NFT Marketplaces' (DappRadar).<sup>399</sup>

<sup>398</sup> Available at: <https://nonfungible.com/market-tracker#>, accessed 29 March 2023.

<sup>399</sup> Available at: <https://dappradar.com/nft/marketplaces>, accessed 29 March 2023.

To our knowledge, detailed data on financial NFTs only is not available. The reason for this is that “financial NFT” is not a clearly defined term, but a term used in the DeFi world rather ambiguously for purposes involving NFTs and some kind of financial aspect. Yet, on several websites, financial tokens are referred to as “the next big thing”.<sup>400</sup>

### 5.4.3. Work of international standard setters on NFTs

In reports and papers of global standard-setting bodies, **NFTs** are rarely mentioned nor discussed at length. For example, the recent IMF policy paper names NFTs only once to indicate that they are classified as “other assets”.<sup>401</sup> By contrast, the FATF in its report that led to the extension of the travel rule to include CASPs names the risks associated with NFTs.<sup>402</sup>

Of interest in the context of this study, the FATF also provides a definition of NTFs in a separate guidance.<sup>403</sup> However, this definition of NFTs can be considered rather narrow and follows the definition that is often used by the industry itself.<sup>404</sup> That said, the FATF does point out that NFTs can be categorized as virtual assets (VAs), that is, they are subject to AML/CTF legislation, in case **they are not used as mere collectibles but as means of payment or investment** (i.e. a financial NFT in the sense used herein). Equally so, NFTs that *represent* financial assets are also covered by the FATF Standards under a different definition<sup>405</sup> (equivalent to the EU’s definition of financial instrument).

### 5.4.4. NFTs vs scope of MiCA

The practical difficulty under the MiCA will be drawing the line between regulated financial products and non-regulated products. Given the broad wording of MiCA and the experience with the crypto industry so far, we expect crypto intermediaries to stretch the limits of the exemption provided under MiCA. Hence, context as to the extent to which MiCA regulates financial NFTs and which NFTs are out of scope is important.

#### a. Exemption in Article 2 MiCA

Article 2(3) MiCA exempts certain tokens from MiCA’s scope: “This Regulation does not apply to crypto-assets that are unique and not fungible with other crypto-assets”.

To clarify the meaning of that exemption, regardless of Article 2 MiCA, where NFTs qualify as financial instruments under MiFID (including transferable securities and financial derivatives) they will be subject to MiFID and other EU securities regulation; the same is true if they qualify as e-money or payment services under the EMD or PSD2 (cf Recital 11 MiCA). MiCA exempts certain tokens from MiCA itself, but this does not have implications for other EU financial regulation.

<sup>400</sup> ‘Financial NFTs Could Be the Ultimate Path to DeFi Mass Adoption’ (Nasdaq), available at: <https://www.nasdaq.com/articles/financial-nfts-could-be-the-ultimate-path-to-defi-mass-adoption>, accessed 29 March 2023.

<sup>401</sup> International Monetary Fund (IMF), 2023, ‘Elements of Effective Policies for Crypto-assets, 2023, available at: <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-assets-530092>.

<sup>402</sup> Financial Action Task Force (FATF), 2022, ‘Targeted Update on Implementation of FATF’s Standards on VAs and VASPs’, available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>.

<sup>403</sup> Financial Action Task Force (FATF), 2021, ‘Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’, available at <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>, accessed 29 March 2023 at par. 53.

<sup>404</sup> The definition is “Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a non-fungible tokens (NFT) or crypto collectibles.”

<sup>405</sup> Financial Action Task Force, ‘Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’ (Publication, 28 October 2021), available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> accessed 29 March 2023 at par. 53 jo. 50.

### b. Substance over form

The exemption in Article 2 MiCA is clarified by Recitals 10 and 11 MiCA. They emphasize the concept of “**substance over form**”, hence naming a token an NFT does not assure that it is out of MiCA’s scope.

But what is the applicable substance? Firstly, it can be derived from these recitals that digital art and collectibles and crypto-assets representing services or physical assets that are unique and non-fungible, such as product guarantees or real estate, remain out of scope, while the “fractional parts of a unique and non-fungible crypto-asset should not be considered unique and non-fungible.” The latter follows from the fact that if you divide a digital token that in itself is unique by a number greater than 1, the outcome will be several fractions that have the same characteristics and by definition cannot be unique. In turn, if a piece of real estate is tokenized in a way that 1,000 tokens collectively represent the real estate, the 1,000 tokens are not exempted from MiCA.

Secondly, MiCA acknowledges that exempted NFTs may still be traded on the marketplace and be accumulated speculatively. This makes sense, as a single piece of art may well be traded at unbelievable prices.

### c. Valuation test

To assess the potential of financial NFTs to facilitate regulatory arbitrage, the legal question that matters is: where is the difference between crypto-assets in scope of MiCA or EU financial regulation, at large, and the tokens that are “unique” and “not fungible with other crypto-assets”?

We hold that the most important criteria that the recitals establish is what we call herein the “**valuation test**”. The recitals state that:

- “the value of such unique and non-fungible crypto-assets is attributable to each crypto-asset’s unique characteristics and the utility it gives to the token holder.” [while]
- [these assets] “are not readily interchangeable and the relative value of one such crypto-asset in relation to another, each being unique, cannot be ascertained by means of comparison to an existing market or equivalent asset.”

It is explicitly stated that “[s]uch features limit the extent to which those crypto-assets can have a financial use, thus limiting risks to holders and the financial system, and justifying their exclusion from the scope of this Regulation.” Where valuation *does* derive from a comparison of crypto-assets with the same features, rendering it fungible, the crypto-asset is not exempted.

The recitals emphasize that the issuance of **a series or collection of NFTs** indicates fungibility, while the mere attribution of a unique identifier to a crypto-asset is not sufficient to classify it as unique and non-fungible. Again, this is easy to fathom, given that if all economic and technical features are the same, adding an ID does not assign a different value, similar to a collection of stamps that is numbered: each has, in principle, the same value.

We hold that “indicates” should be explained as is, meaning that NFTs issued as series or collection could **potentially be fungible**. When issuing a collection or series becomes synonymous with fungibility it will result in, for example, NFT art collections being included in the scope of MiCA. As a comparison, works of Rothko or Warhol are, in principle, not fungible; even if they are part of a print series of 100 copies since one copy can be in a different state than another one. Yet, under MiCA, if they are issued as part of a series (such as NFTs where the only difference is the identification number) they will be subjected to MiCA. The rationale of that regulatory treatment is that tokens do not deteriorate

in state when they are traded or used; they neither get damaged nor harmed by water or sun. Thinking this further, an at-face-value NFT art collection series may well turn out to be a financial instrument.<sup>406</sup>

To remain in that analogy, what determines the characterization as “unique” and justifies the exemption from MiCA are features that lead to **a unique value**, and interfere with the comparison of one token with another. This stands at the heart of the valuation test.

#### d. Industry view vs MiCA

The features that render a token “unique” under MiCA are of utmost practical importance, especially considering financial NFTs. The industry (as described above) tends to rely **merely on the token standard** to determine non-fungibility. The **industry jargon** seems to hold that wherever a token type is used that ensures *technical uniqueness* (for instance, using the ERC-721 standard) the token is non-fungible and therefore out of scope.

*Example:* A series of ERC-721 tokens (with unique identifiers) may each reflect a promissory note in which A promises to B to pay 500 on the 1<sup>st</sup> of March. The mere fact to establish uniqueness by way of the token standard would result in these promissory notes being considered unique since each has a unique ID number. Tokenization by using the ERC-721 standard thus leads to the classification as (financial) NFT. This would be the case even where the:

- underlying obligation of A to B is standardized, like in terms of a bond, and
- the personal relationship between A and B created by the promissory note is disintegrated; that is, where tokenization would entitle *any bearer* to ask A to pay 500 on the 1<sup>st</sup> of March.

From that perspective, financial NFTs can not only be traded and exchanged as any bond, since they have become, due to tokenization, some type of bearer instrument (albeit with a number), but also one of these tokens will influence the value of the other. If A defaults on one token, the default will impair the value of all other tokens, regardless of the individual number. This may even be the case if the name of the rights holder is inscribed in the token. Notwithstanding the former, applying the industry view, MiCA would not apply.

Under the MiCA valuation test, however, tokens that are economically linked to each other, so that the value of one token derives from a comparison with the value of another token, are in scope. This leads to a much narrower exemption from MiCA:

- (1) Where the debt is turned into a bearer instrument, it is most likely a transferable security under MiFID and MiFID applies.
- (2) MiCA can only apply to crypto-assets that are less standardized, hence more unique than bonds, but not entirely unique.
- (3) This leaves for the exemption de facto only tokens where **the underlying legal relationship is unique even in the state of tokenization**.

*Example:* If the underlying is A’s claim against B, only a token in which this personal relationship is maintained 1:1, and where only A can demand from B the amount tokenized, is a token exempted from both MiFID and MiCA. That is, the token securitizes that B owes 500 to A, and nothing more. Depending on legal classification and a country’s law, creditors of A may now cease the claim against B indirectly

<sup>406</sup> For instance, the US SEC has classified certain NFTs as securities. Cf. Sander Lutz, ‘SEC vs BAYC? Here’s What Legal Experts Say It Means for NFTs’ (Decrypt, 18 October 2022), available at: <https://decrypt.co/112190/sec-bayc-legal-experts-nfts-yuga-bored-apes>, accessed 29 March 2023. See also Stempel, J., *U.S. judge permits lawsuit claiming NBA Top Shot NFTs are securities*, (Reuters, 22 February 2023), available at: <https://www.reuters.com/legal/us-judge-permits-lawsuit-claiming-nba-top-shot-nfts-are-securities-2023-02-22/>.



by ceasing the token, and then enforce A's right against B. However, beyond this special situation, the claim against B may only be enforced by A.

By contrast, if the personal right to claim 500 from A is widened to any bearer, or if A consents that B may cede the claim to any third party while that cession takes place by transferring the token, **the token could qualify either as a bearer security (subject to MiFID) or a crypto-asset under MiCA.**

The question remains how large the series must be to prevent the use of the exemption. This again derives from the **valuation test**: as soon as an asset type is sufficiently traded or valued by users, it carries a comparison. We hold that under the right circumstances of commercialization, and **with financial rights embedded** (such as in a claim against a given person with interests and/or profit participation) already a five to a dozen assets of the same type can prevent the use of the exemption. In the absence of cash flow participation (as in art, collectibles) the number is higher.

Financial law rationales support our view. In particular, adopting the industry view based on technical uniqueness would open the door to circumvent MiCA and EU financial law, undermine the efforts to establish a level playing field, and fail to ensure user protection.

It is presently uncertain whether the implementing legislation will be so clear as to foreclose circumvention of EU financial law stated herein. If that is ensured, **the need to regulate in the field of (financial) NFTs is much smaller** as most remaining matters are dealt with in EU consumer law, such as through a right to withdrawal in the case of distance selling.<sup>407</sup> Experience is, however, that the scope of EU financial law will not always be applied consistently. In this case, some prevention measures may be advisable as safeguards for consumers. We describe which risks could be addressed in the next section.

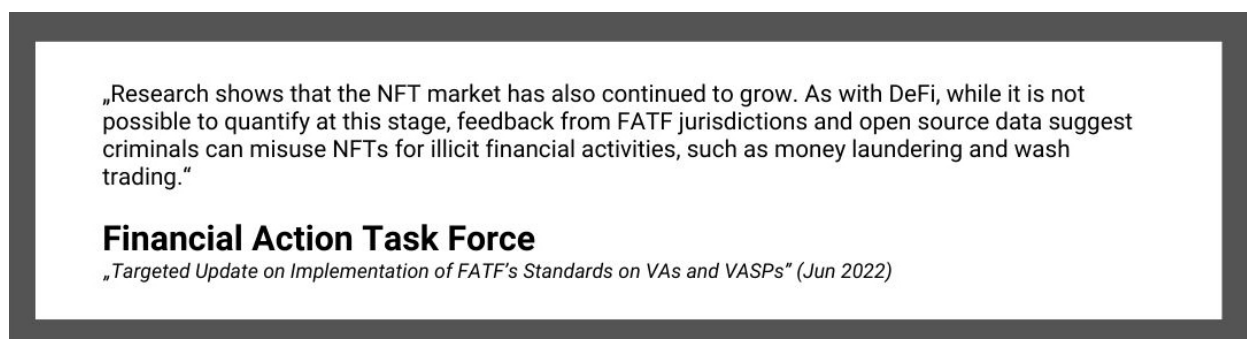
#### 5.4.5. Remaining risks

Ensuring that EU financial law is enforced, as laid out above, is crucial to avoid the risks linked to NFTs being imposed on consumers and financial institutions alike. Yet, a nuanced view is essential.

##### a. AML/CTF

According to regulators, NFTs are used for money laundering, terrorist financing, and the circumvention of state sanctions (see Figure 14).

Figure 16: International standard setters on NFTs



Source: Author's own elaboration.

<sup>407</sup> Note that in our view, the fact that the asset is exempt from MiCA ensures that the consumer's right to withdraw may be effectively used, as the use of the exemption implies illiquidity. This forecloses the argument that the value of NFTs is fluctuating on financial markets, under Art. 16(b) Directive 2011/83/EU on consumer rights and Art. 6(2) Directive 2002/65/EC concerning the distance marketing of consumer financial services. While crypto-assets within MiCA's scope are financial services under Directive 2002/65/EC concerning the distance marketing of consumer financial services (Recital 79 MiCA).

We have laid out *supra* (cf. 5.2. and 5.3.) that NFTs may be used for money laundering and terrorist financing as long as MiCA and the FTR exempt NFTs and non-CASP services. This includes fully decentralized protocols run by a non-incorporated DAO and potentially non-custodial wallets under certain circumstances. Assigning entity status to DAOs (cf. *infra*, at 6.3.) will address the main concerns.

#### b. Counterparty and financial risk

The risk inherent in the embedded claim is usually equivalent to the underlying legal relationship, such as in credit contracts. In the EU, consumer protection laws govern many of these relationships, where consumers are concerned. For example, this includes mortgage or lending relationships if the providers of finance act on a commercial basis and/or cross-border and/or by distance selling. While enforcement of existing laws may face the same difficulties as everywhere else in DeFi due to uncertainty surrounding: (1) who markets the service on a commercial basis to the consumer, (2) which laws apply, and (3) who the counterparty is (cf. *supra*, at 3.), NFTs do not pose a *special* risk from a private law perspective as to counterparty and financial risks. This is also MiCA's perspective.<sup>408</sup>

Since we propose to address these general concerns by tailor-made policy tools (cf. *infra*, at 6.2. and 6.3.), we do not see a reason to take further steps from the perspective of counterparty and financial risk.

#### c. Valuation risk

Risks for users stem from the valuation, as there is no second item with the same economic and legal features. This is different if uniqueness is determined merely by token type, as the industry view suggests. Then, any fair valuation would require initial and ongoing disclosure of audited, material information. Further, regulation would need to ensure fair market practice and prevent insider dealing. That said, by all definitions unique NFTs have been fluctuating heavily in valuation and are often sold for large amounts.<sup>409</sup>

#### d. Operational risk

As compared to traditional one-on-one contracts, NFTs pose additional operational risk as the tokenization comes with the possibility of a tokenization platform's malfunctioning. The additional risk stems from the additional technical layer on top of the always-existing legal layer (in our example, the promissory note). This risk is most notable with regard to LP tokens. If LP tokens are lost or accidentally traded, the original holder will be unable to redeem the underlying assets.<sup>410</sup> Equally, if a DEX goes out of business and thus the interface to interact with the protocol and redeem the underlying assets is out of operations, the redemption of assets is highly unlikely, even if the assets are retained in the asset pool.<sup>411</sup> This justifies the bespoke rules to address operational risk we propose *infra*, at 6.4.

---

<sup>408</sup> See Recital 29 MiCA ("Even though some offers of crypto-assets other than asset-referenced tokens or e money tokens are exempt from various obligations of this Regulation, Union legislative acts that ensure consumer protection, such as Directive 2005/29/EC of the European Parliament and of the Council or Council Directive 93/13/EEC, including any information obligations contained therein, remain applicable to offers to the public of crypto-assets where they concern business-to-consumer relationships.").

<sup>409</sup> 'The 20 Top-Selling NFT Artists to Collect Right Now' (Gotham Magazine, 9 March 2023), available at: <https://gothammag.com/top-selling-nft-artists>, accessed 29 March 2023.

<sup>410</sup> 'How to use Liquidity Pool (LP) tokens' (Metamask), available at: <https://support.metamask.io/hc/en-us/articles/4409347883675-How-to-use-Liquidity-Pool-LP-tokens>, accessed 29 March 2023.

<sup>411</sup> 'How to Add/Remove Liquidity' (PancakeSwap), available at: <https://docs.pancakeswap.finance/products/pancakeswap-exchange/liquidity-guide>, accessed 29 March 2023.

## 6. POLICY CONSIDERATIONS

### KEY FINDINGS

The main challenges remaining after MiCA and the revision of the TFR may be addressed by:

- (1) a centralization of competences to inquire into cases of apparent **reverse solicitation** in the hands of the ESAs,
- (2) a broad **default rule** that shifts the onus to prove that a conduct is exempted from, or in, the scope of EU regulation, respectively, from the NCAs to crypto,
- (3) enhanced cross-border cooperation of regulators beyond EU borders,
- (4) assigning regulatory entity status to “Decentralized Autonomous Organizations” involved in financial services, and
- (5) a separate section to be added to MiCA addressing the additional operational and financial risks concerning NFTs.

**Bespoke bankruptcy and resolution legislation**, the harmonization of **private law** on crypto, and enhancing legal certainty in the field of **court jurisdiction and choice of law** should address (partial) decentralization.

To further effective enforcement, the new **EU AML Authority should be mandated to share data with NCAs** on custodial and non-custodial wallets, crypto intermediaries and their clients with NCAs. Finally, EU institutions should develop, by way of expanding the eIDAS Regulation and the creation of foundational infrastructure, a “**Euro Wallet**” with embedded compliance features that limits contracting with, and transfer to and from, regulated and supervised intermediaries residing in cooperating countries, thereby using **RegTech** to counter regulatory arbitrage.

### 6.1. Work of global standard setters (IOSCO, BIS, IMF, FATF, FSB)

Each of the global standard setters have and are dedicating considerable resources to crypto.

**IOSCO** currently has two work streams that focus on, firstly, crypto and digital assets in general and, secondly, decentralized finance. Both are part of their Crypto-asset Roadmap.<sup>412</sup>

The **BIS** has published several papers on different aspects of the crypto industry. Examples include: “Cryptocurrencies: looking beyond the hype”, a report that analyses the current and potential value of distributed ledger technology in relation to banking,<sup>413</sup> “Regulating cryptocurrencies: assessing market reactions”, a paper that assesses how the value of cryptocurrencies reacts to news about regulations<sup>414</sup> and “Prudential treatment of cryptoasset exposures”<sup>415</sup>, a paper addressing the risk of exposure to

<sup>412</sup> IOSCO, *Crypto-Asset Roadmap for 2022-2023* (7 July 2022), available at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD705.pdf>, accessed 29 March 2023.

<sup>413</sup> BIS, *Cryptocurrencies: looking beyond the hype* (BIS Annual Economic Report, 17 June 2018), available at: <https://www.bis.org/publ/arpdf/ar2018e5.htm>, accessed 29 March 2023.

<sup>414</sup> Raphael Auer R., and Stijn Claessens ‘S., 2018, *Regulating cryptocurrencies: assessing market reactions*’ (BIS Quarterly Review, September 2018), available at: [https://www.bis.org/publ/qtrpdf/r\\_qt1809f.htm](https://www.bis.org/publ/qtrpdf/r_qt1809f.htm), accessed 29 March 2023.

<sup>415</sup> BIS, *Prudential treatment of cryptoasset exposures*, 2022, available at: <https://www.bis.org/bcbs/publ/d545.pdf>.

crypto-assets for commercial banks. Additionally, closely linked to their stakeholders which constitute central banks, the BIS has over ten project groups dedicated to different aspects of CBDCs.<sup>416</sup>

The **IMF** has published and continues to publish policy papers on topics related to crypto. The February 2023 policy paper “Elements of Effective Policies for Crypto-assets” presents a policy framework for crypto-assets that aims to achieve key policy objectives such as macroeconomic stability, financial stability, consumer protection, and market and financial integrity.<sup>417</sup> The IMF refers to the FTX case, an insolvency of centralized intermediary, as a “debacle” and a clear indication of the need to strengthen “the case for consistent and comprehensive regulation”.<sup>418</sup>

The **FATF** has not only been instrumental by advising measures such as the extension of the travel rule to cryptocurrencies,<sup>419</sup> but was ahead of its time compared to other standard-setting bodies by publishing a report on key definitions and the potential AML/CFT risks of virtual currencies as early as 2014.<sup>420</sup>

The **FSB** has issued over 20 publications related to crypto-assets,<sup>421</sup> dating back to 2018. In spring 2023, they published a comprehensive report on the financial stability risk of DeFi, addressing a broad range of topics and providing useful comparisons where the DeFi risks are similar to those found in traditional finance.<sup>422</sup>

With regard to certain aspects, these publications reflect the permissive approach that also characterized the European Commission’s draft of MiCA, as seen in the draft MiCA’s intent to regulate but equally allow for innovation and development, seeing the potential benefits of crypto and DLT at large.<sup>423</sup> With regard to other aspects, however, the standard setting bodies are **less lenient towards the industry**. In particular, MiCA’s exclusion of fully decentralized platforms from the scope of regulation does not find recognition in (draft) policy documents that analyse the events of the Crypto

<sup>416</sup> BIS, ‘Innovation Hub projects’, available at:

[https://www.bis.org/about/bisih/projects.htm?bisih\\_projects=ZnJvbT0mdGlsbD0mdG9waWNzPTIxNiZvYmppZD1iaXNpaF9wcm9qZWV0cyZwYWdlPSZwYWdpbmdfbGVuZ3RoPTI1JnNvcnRfbGlzdD1kYXRlX2Rlc2MmdGhlbWU9c2ltcGxlZGF0ZV90b3BpYyZtbD1mYWxzZSZtbHVybD0mZW1wdHlsaXN0dGV4dD0mdmldz1zaG93X3RvcGljcyUzRHRydWU%253D](https://www.bis.org/about/bisih/projects.htm?bisih_projects=ZnJvbT0mdGlsbD0mdG9waWNzPTIxNiZvYmppZD1iaXNpaF9wcm9qZWV0cyZwYWdlPSZwYWdpbmdfbGVuZ3RoPTI1JnNvcnRfbGlzdD1kYXRlX2Rlc2MmdGhlbWU9c2ltcGxlZGF0ZV90b3BpYyZtbD1mYWxzZSZtbHVybD0mZW1wdHlsaXN0dGV4dD0mdmldz1zaG93X3RvcGljcyUzRHRydWU%253D), accessed 29 March 2023.

<sup>417</sup> IMF, ‘Elements of Effective Policies for Crypto Assets’ (Policy Paper, 23 February 2023), available at:

<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092?cid=pr-com-PPEA2023004>, accessed 29 March 2023.

<sup>418</sup> Ibid, at ANNEX III.

<sup>419</sup> FATF, ‘Targeted Update on Implementation of FATF’s Standards on VAs and VASPs’ (Publication, 30 June 2022), available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>, accessed 29 March 2023.

<sup>420</sup> FATF, ‘Virtual Currencies, Key Definitions and Potentials AML/CFT Risks’ (Report, June 2014), available at: <https://www.fatf-gafi.org/en/publications/Methodsand Trends/Virtual-currency-definitions-aml-cft-risk.html>, accessed 30 March 2023.

<sup>421</sup> For details please see the website of the FSB, section publications, policy area: Crypto Assets, available at: [https://www.fsb.org/publications/?policy\\_area%5B%5D=5587&mt\\_orderby=0](https://www.fsb.org/publications/?policy_area%5B%5D=5587&mt_orderby=0) accessed on 18 April 2023.

<sup>422</sup> ‘The Financial Stability Risks of Decentralised Finance’, 2023, Financial Stability Board (FSB), available at: <https://www.fsb.org/wp-content/uploads/P160223.pdf>.

<sup>423</sup> For instance, the considerable efforts of BIS with regard to CBDCs (e.g. BIS, 2018, ‘Annual Economic Report, Chapter V., Cryptocurrencies: looking beyond the hype’, available at: <https://www.bis.org/publ/arpdf/ar2018e5.pdf>) and the OECDs recent publications on the impact of DeFi (see, OECD, 2022, ‘Why Decentralised Finance (DeFi) Matters and the Policy Implications’, available at: <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf>).

Winter.<sup>424</sup> The SEC made clear it would treat “fully decentralized exchanges” (DEX) as in scope of US securities regulation.<sup>425</sup>

## 6.2. Capturing cross-border crypto

The main regulatory issue is to bring crypto services into scope of financial regulation and into the jurisdiction of EU regulators when they serve clients residing in the Single Market. So far, centralized crypto intermediaries and decentralized platforms, CeFi and DeFi alike, often refer to reverse solicitation.

They can do so for **four reasons**:

- (1) the crypto intermediary masks **how many EU users** at which volume reside **in which country**, i.e. whether any single NCA has a case to intervene;
- (2) there is legal uncertainty as to the **boundaries of reverse solicitation** under EU financial regulation;
- (3) even with MiCA in force, there is uncertainty on the **scope of EU financial regulation** and in turn, for example, whether a “financial NFT” is subject to the exemption will be construed broadly by crypto providers; and
- (4) decentralized platforms argue that there is **no legal entity involved** that could apply for licensing or could be regulated, as the economic function provided is the result of non-custodial, peer-to-peer protocols (‘smart contracts’) downloaded and applied by users themselves functioning, in contrast to a service from an entity to a client.

We propose to disintegrate this four-step argument with **four distinct policy measures in this and the next section**.

### 6.2.1. Solicitation cloaked as reverse solicitation

The first set of policy measures concerns solicitation of crypto clients.

While MiCA provides language on solicitation and stresses the need to scrutinize the conduct cloaked as reverse solicitation (cf. Article 61 MiCA), the yet unspecified matter is what conduct, in detail, provides for solicitation or reverse solicitation respectively. Crypto stresses this legal uncertainty when relying on:

- **referral programmes** (where users acquire new users for a reward in crypto, similar to a “kick-back”);
- **partnership or loyalty programmes** (where new users receive rewards for signing up, thus are being compensated for the work they undertake to find the programme and contract with it);

<sup>424</sup> For instance, the FSB applies a strict approach in its report ‘Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report’, where it states with regard to decentralized protocols “Regulators and supervisors need to look past the labels and marketing around a product or service, and consider the facts and circumstances of each case to establish ways to identify who exercises effective control on the protocol or provides access to the protocol, and to make them accountable under existing or future regulation.” See Financial Stability Board (FSB), 2022, ‘Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report’, available at: <https://www.fsb.org/wp-content/uploads/P111022-3.pdf>.

<sup>425</sup> The SEC proposes an amendment to the Securities Exchange Act that would bring “more Alternative Trading Systems (ATS) that trade Treasuries and other government securities under the regulatory umbrella”. SEC proposes to assess the services purely on the effects and risks that it has for its users to eliminate the ambiguous line/overlap between CeFi and Defi. Cf. ‘SEC Reopens Comment Period for Proposed Amendments to Exchange Act Rule 3b-16 and Provides Supplemental Information’ (SEC, 14 April 2023), available at: <https://www.sec.gov/news/press-release/2023-77>, accessed on 18 April 2023.

- **creation of interest inside the EU through newsletters and messaging boards operated by third-party websites**, which discuss services and products (often cloaked as discussion of technology) operated and/or offered by third-country firms;
- **indirect incentives** through rewards for pooling with users outside of the Single Market; and
- in some cases, **advice to clients** on how to locate services outside of the regulatory perimeter.

Further, we lack rules dealing with reverse solicitation in a clear-cut manner for **other EU financial law than MiCA**. We find, for instance, some language on reverse solicitation in Article 42 MiFID, yet that language is little more than confirmation of the permissibility of reverse solicitation. Note that where assets qualify as financial instruments or e-money, the MiCA rules on reverse solicitation will not apply, while the rules of MiFID/MiFIR or the EMD, respectively, have not yet been amended to cover **digitally advanced methods of solicitation**.

The matter surrounding reverse solicitation **is not unique to crypto**. Similar issues have been discussed across Europe, for instance, regarding collective investment schemes (where it led to the adoption of the Directive (EU) 2019/1160 on cross-border distribution of collective investment undertakings), lending and insurance services. If reverse solicitation is addressed by bespoke crypto regulation only, crypto promoters will cloak their services so that it is subject to a different piece of EU regulation that does not provide these details, while continuing to use the same methods to attract EU users.

We propose to address the issue in three steps.

a. [Cross-border solicitation of financial services regulation](#)

We suggest implementing **a cross-sectoral regulation** (a Cross-Border Solicitation of Financial Services Regulation) that governs the **delineation of solicitation and reverse solicitation in all EU financial services**. This regulation may set the broad principles, combined with empowerments to the ESAs/the Commission to adopt detailed L2 legislation and to issue cross-sectoral guidelines.

b. [Inquiry right of the ESAs regarding third-country crypto firms](#)

As part of the new regulation, we suggest **granting powers to the ESAs** to inquire into the conduct and business model of **third-country intermediaries and platforms on behalf of all NCAs**. While MiCA entitles the EBA to do so in Article 122 MiCA, this power is limited to inquiring into the circumstances of significant ARTs and significant EMTs; further, the ESAs may function as supervisory authority and for sanctioning purposes, once a platform is blacklisted for previous violations of EU financial law in the register pursuant to Article 94 MiCA. As a general matter beyond the infringement case, and as part of a cross-sectoral regulation, we propose to expand these powers and include all crypto-assets and all other types of financial services.

These powers would entitle the ESAs (collectively, as Joint Committee) to collect data on the user base of any third country crypto platform or intermediary in the Single Market that is not licensed in the EU, country-by-country, and the type of services and products applied, as well as the methods of user acquisition. The information thus generated would be forwarded to all NCAs in the Single Market.

If third-country intermediaries do not cooperate with the ESAs' request, the ESAs may impose sanctions, order the geo-blocking of the respective websites<sup>426</sup> and blacklist and issue warning releases

<sup>426</sup> While geo-blocking may be circumvented via the use of a virtual private network (VPN), geo-blocking at least ensures that the intermediary's website is less accessible for large-scale retail use and shows the general public that the intermediary is acting in breach of EU law.

that a given website is non-cooperative on EU financial regulation (including client solicitation and money laundering rules). These disclosures and warnings will prompt regulated intermediaries to interrupt business contact, rendering, for instance, the transfer of fiat currencies or the linking of wallets between duly licensed EU intermediaries and non-cooperating intermediaries difficult.

The concentration of powers to inquire on behalf of all NCAs in the Single Market will **save costs** on the side of NCAs and **effectuate EU financial regulation**. To find acceptance among the EU Member States, however, it is crucial that this power of the ESAs is **limited to information gathering and forwarding this information to the NCAs**. Given that government funds and supervisory fees can be spent only once, any further intervention into the supervisory relationship between NCAs and the licensed firms is counterproductive, as it will deprive the NCAs of resources crucial for an effective enforcement of EU financial law within their jurisdiction.

### c. RegTech: the “Euro Wallet”

Part of the problem stems from the anonymity features of token technology. While there are good reasons for anonymity in finance<sup>427</sup>, the best way to balance justified reasons for anonymity with the need to enforce EU financial regulation properly, is the use of foundational IT infrastructure with embedded compliance features, thereby using **RegTech** to counter regulatory arbitrage.

In particular, EU institutions should develop, by way of **expanding the eIDAS Regulation**<sup>428</sup> and the related EU identity infrastructure already created by way of the eIDASR, a **“Euro Wallet”** that allows contracting with, and transfer to and from, regulated and supervised intermediaries residing in cooperating countries only. If technology is well designed, these Euro Wallets, while ensuring compliance by technical means, would be linked to the users’ identity through the process embedded through eIDASR, yet anonymous vis-à-vis third parties. Since they are provided by public infrastructure and supervised by technical means, these wallets would benefit from a cost advantage compared to private wallet offerings. Over time, these Euro Wallets would crowd out other wallet types that are less supervised.

**Crucial regulatory requirements and functions may be implemented into the Euro Wallet by way of technology.** For instance, the Euro Wallet could:

- (1) forward data on its energy consumption with regard to token types to an algorithm, which assembles the data of all wallets in which these tokens are held, to allow for **reporting on sustainability impacts**;
- (2) provide technical routines that allow the collective **representation of token holders** by an administrator in insolvency, or in a regulatory-sponsored **collective redress scheme** on behalf of token-holders. Examples can be taken from the national regulations on valuation errors in the context of collective investment schemes.<sup>429</sup> In these cases, the damage of each fund investor is too small to prompt meaningful legal action, but the collective damage of all

<sup>427</sup> In particular, the disclosure of wealth may put the family members at risk of abduction. Fraudsters and thieves frequently seek out wealthy victims. Data protection is vested in the belief that individuals shall enjoy freedom and personal achievements, and pursue their life happily and unharmed by jealousy.

<sup>428</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

<sup>429</sup> See, for instance, CSSF Circular 02/77 on NAV calculation error and investment breaches. UCITS Management Companies must put in place robust policies, processes and procedures on NAV calculation errors and investment breaches that ensure investors are compensated, with the board of directors of the UCITS management company and, if applicable, the board of directors of the UCITS corporate vehicle being finally accountable for the execution. The CSSF monitors the execution of said policy, and undertakes enforcement actions where necessary, to ensure that investors are reimbursed for any damage they suffered.

investors together is significant. For that reason, financial regulation seeks to overcome collective action problems of dispersed investors. In these cases, the fund manager must draw up a reimbursement plan, and the NCA monitors the execution of that plan. We propose to implement similar schemes designed to overcome collective action problems in the financial regulation on crypto-assets;

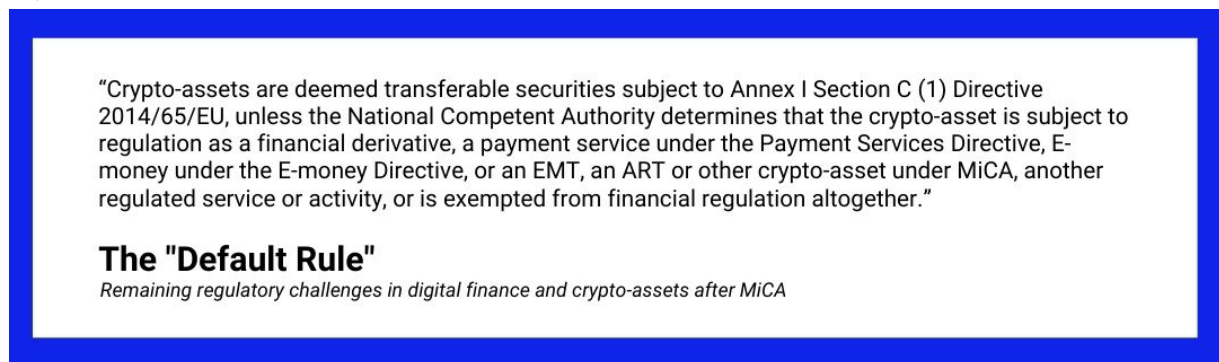
(3) pave the way for a future **Digital Euro** issued by the ECB to be booked into the Euro Wallet.

We are aware that the development of a Euro Wallet will require careful planning and execution. Yet, in the EU, the example of the gradually expanded eIDAS<sup>430</sup> and examples from countries outside the EU that are advanced in RegTech<sup>431</sup> demonstrate that the building of foundational infrastructure and RegTech is the best way going forward to balance rightful interests in privacy with utterly necessary enforcement of financial regulation.

### 6.2.2. Broad default rule for scope and definitions

As a remedy for the scope and definitions issue, we suggest implementing **a broad default rule that could be formulated as follows:**

Figure 17: The “default rule”<sup>432</sup>



Source: Author’s own elaboration.

Under such a rule (which is at its core purely procedural) crypto-assets are, **by default, considered as transferable securities (i.e. financial instruments), unless exempted** (or requalified) by NCAs. In turn, crypto intermediaries that seek regulatory lenience (for instance, that argue that MiFID and the Prospectus Regulation do not apply), would first need to contact an NCA and apply for an exemption.

#### a. Rationale

Due to the proposed Cross-Border Solicitation of Financial Services Regulation (cf. *supra*, 6.2.1), NCAs will know about users in their jurisdiction, the volume, type of services and methods to attract EU users. Yet, they may nevertheless hesitate to act if they first have to inquire into the facts as a precondition for enforcing EU financial regulation. Prior to any enforcement action regulators will have to decipher the details of crypto-asset related services and activities. Based on the authors’ experience visiting dozens of crypto websites and reading the respective product descriptions, we predict that any NCA

<sup>430</sup> See Arner, D.W., Zetsche, D.A., Buckley, R.P., Barberis, J., “The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities”, 20 EBOR (2019), 55–80.

<sup>431</sup> In particular, an “India Wallet” is discussed as an extension of the India Stack. See Policy 4.0, 2021, *An Innovative Crypto Regulation Approach – the India Wallet*, available at: <https://policyfourpointo.com/publications/>.

<sup>432</sup> As an alternative, the EU financial regulation could adopt a very broad definition of transferable securities, as is the case with the US *Howey* test (*supra* note 224). The SEC has determined in more than 100 cases that crypto-assets are securities under that test. However, we are not supportive of implementing the *Howey* test in EU law as it raises essentially the same questions in a different framework that need to be answered for the proper application of EU financial regulation.



interested in enforcing EU financial law will then face **a broad collection of technical “gibberish” used to cloak the economic function at stake.**

If the onus is on the NCAs to reveal what is behind this “gibberish” in terms of economic function, entities and risks, any NCA must, besides becoming a crypto expert, invest a lot of regulatory capital. An NCA will do so only if: (1) it can be sure that many users residing in a jurisdiction are concerned so that the threshold for the application of MiCA is clearly exceeded, *or* (2) if prominent users have lost large amounts of money, *or* (3) some link to that country may be clearly established, for instance, if key staff of the service provider reside in that country. **In most cases, enforcement will then come too late** to prevent losses from operational or financial risks as materialized during the Crypto Winter.

At the same time, given crypto is a niche market crypto resources at NCAs will be reduced as soon as some crisis in the core financial / banking market or the economy requires a redirecting of resources.

#### b. Ex ante rulemaking time consuming and regulatory intense

Legal certainty is paramount to ensure proper enforcement.<sup>433</sup> We have laid out in 5.2.1. MiCA’s tools that should ensure a harmonized, even centralized approach to the classification of crypto-assets. The regulatory tools are sufficiently developed and the development of this centralized approach will lead to legal certainty, albeit **over a long period.**

We are facing an environment currently characterized by:

- high innovative capacity in the DeFi space;
- a “hide-and-seek” situation where regulators chase new legal interpretations of protocols and structures tailor-made for regulatory arbitrage;
- the existence of 10,000 different types of crypto-assets all of which are, in some way, unique;
- many crypto-assets meeting the definition of various legal concepts at the same time;<sup>434</sup> and
- an inconsistent, and in parts entirely different application of core concepts of EU financial law across NCAs.

Under such conditions, **we doubt that a comprehensive regulatory approach to definitions can be drafted and implemented** on an EU level at all **within any reasonable time and at costs proportionate to the cause.** In turn, **legal uncertainty will prevail** and some crypto intermediaries may either remain, or seek to stay, outside of the scope of regulation. That uncertainty as to whether certain crypto conduct is within the regulatory perimeter will result in under-enforcement, as all enforcement bodies are resource-constrained.

#### c. Procedural approach: default rule

Even if successful, specifying definitions more clearly, in delegated acts, guidelines or case by case, when implementing MiCA will **only partially address the problem.** To make all the MiCA classification tools described in 5.2.1 work, we propose **to add additional legislation on Level 1 that reverses the onus of arguing that a given crypto-asset is outside of the scope of EU financial regulation.** If MiCA is implemented, NCAs will remain in the unfortunate position of needing to gather facts to justify the

<sup>433</sup> See generally Lee J., L’heureux F., 2020, A Regulatory Framework for Cryptocurrency, *European Business Law Review*, 31 (3), pp. 423-446. See also Van der Linden T., Shirazi T., 2023, Markets in Crypto-assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-assets, *Financial Innovation*, 9 (22), available at: <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00432-8#citeas>.

<sup>434</sup> See, e.g., Goforth C., 2019, U.S. Law: Crypto Is Money, Property, A Commodity, And A Security, All At The Same Time, *Journal of Financial Transformation*, Capco Institute, 49, pp. 102-109.

application of EU law. For that, they will need to be experts in the classification criteria set up by various MiCA tools (cf. 5.2.1.).

Even if these criteria are crystal clear (which we do not expect anytime soon), under MiCA **the cooperative market participants will bear the costs of compliance** (when they issue explanations and legal opinions subject to Article 8(4), 17, 18 MiCA), while **non-cooperative market participants will benefit from regulatory arbitrage** as they will, quite reasonably, rely on the assumption that NCAs are limited in their enforcement capacity.

To reverse this incentive structure we propose to shift the burden and costs from the NCAs (seeking to enforce EU laws) to the **offerors of crypto-assets, the persons seeking admittance of the crypto-asset to the market**, and, as a fall back, to the market operators that admit the crypto-asset to trading.

This regulatory tool of choice is a **very clear procedural approach that subjects all crypto-assets to scrutiny by NCAs**. Based on this procedural rule, the various MiCA tools aimed at achieving convergence in the EU may function according to their purpose. A straightforward solution in this regard is the implementation of a **default rule**. Under that default rule, all crypto-assets may be deemed, at first hand, a “transferable security”.<sup>435</sup> This means, that they, or the respective service providers, are subject to, as a fall-back solution, the scope of MiFID/MiFIR, the Prospectus Regulation, MAR and Transparency Directive, among others, *unless the crypto-asset is exempted by an NCA*. Under this default rule, **any placement-as-a-service of, and any trading of crypto-assets on a trading platform, is subject to licensing**, while in the absence of exemptions the **MiFID rules for custodians will apply**. Further, if crypto-assets are by default transferable securities, NCAs are entitled to order *all* CASPs and issuers to provide information to them. Given that existing AML/CTF rules apply to all transactions involving transferable securities, the default rule proposed herein also ensures full compliance with such rules irrespective of the degree of decentralization. This secures a **high level of protection**, subject to an exemption.

The **exemption** may either be the result of the **NCA’s own assessment** (based on MiCA’s various convergence tools) or, most likely, the **exemption will be granted upon an application from the respective crypto intermediary or platform**. For instance, the application may seek to establish regulatory treatment as a *payments token* (subjecting them to PSD2, the EMD or the regulation for EMTs or ARTs under Title III and IV MiCA, as appropriate) or a *utility token* (for which Title II MiCA foresees bespoke legislation). Given that the respective rules are more adequate for payments and utility tokens, the initiators of the crypto-asset (offeror or person seeking admission to trading) have a personal interest to seek the exemption.

The proposed default rule shifts the **burden of information gathering from the NCAs** (where it currently rests) **to the crypto intermediaries as “cheapest cost avoiders”**: the intermediaries are the entities best equipped to provide the information (“cheapest cost avoider”), and stand to most benefit from the issuance of, and additional services in relation to, crypto-assets. Hence, if there are grounds to apply for exemptive relief these entities will disclose voluntarily all facts important for this relief – without the NCAs having to undertake major efforts.

---

<sup>435</sup> We propose to use the framework for “transferable securities” as a default rule, as the MiFID definition of “financial instrument” leaves some room, as to which rules in detail will apply. For instance, a financial instrument may be a share or a financial derivative. Both come with entirely different duties for the intermediaries and risks for investors. We are not aware that tokens, which come with a holder’s personal obligations beyond the holders’ initial investment are widespread; these would require an assessment of a holder’s risk of default. The personalization that this requires is at odds with the crypto approach. In turn, rules on financial derivatives are inappropriate. At the same time, the EU rules on transferable securities are robust, and also cover so-called “structured securities” with derivative features embedded (i.e. high risk of losses). This allows for the adequate treatment of leverage inside crypto-assets.

The outcome of such a default rule may, however, be proportional: while the crypto intermediaries must register and ensure proper disclosure to regulators of the categorization of their offering as a precondition for distributing crypto-assets and related services, regulation may be designed so as to ensure that the issue itself is not automatically subject to licensing. For instance, Title II MiCA does not provide for licensing of the issuer in the case of an ICO of a mere utility token. However, **the issuer**, in line with what Article 8(4), 17, 18 MiCA foresees, **must make the case for this privilege**.

#### d. Cost-benefit analysis

We acknowledge that our solution is rather simplistic. Deeming a crypto-asset a transferable security will not magically transport the crypto-asset into a regime “ready built to provide proper or even efficient oversight or clarity”, but instead may create “both a lack of clarity and inefficiency in compliance” – since securities regulation generally fails to account for critical aspects of the crypto-asset ecosystem and may impose obligations with little to no relevance for crypto-assets.<sup>436</sup> Nevertheless, we suggest that **this situation is preferable to the current converse situation where most crypto conglomerate businesses and decentralized platforms remain unregulated** and engage in a type of “hide and seek” with regulators. Furthermore, such acknowledged inefficiencies may be rectified through exemptive powers granted to the NCAs in their dealings with crypto.

Our default rule has many advantages as it introduces rules for crucial fields, such as (1) disclosure, (2) custody, (3) AML/CTF, (4) market abuse, (5) conflicts of interests, (6) sanctioning and whistleblowing, and many other aspects. It could fill these gaps and avoid duplication of many provisions existing somewhere else in EU financial regulation that, in the absence of a default rule, will need to be adopted as part of MiCA’s implementing legislation. Further, to ensure the development of a consistent approach to crypto-assets throughout the Single Market, exemptions granted by the NCAs could be stored in a public register provided by the NCAs. At a later date, these exemptive cases may then become the factual basis for an abstract exemptive release by way of ESAs Guidelines.

#### e. Harmonizing thresholds

Openness to innovation may be provided by setting proportionate **thresholds**, such as a number of minimum users per country or the EU as a whole: if the threshold is not bypassed, the exemption may be granted.

EU financial regulation already foresees these **thresholds**. There are different thresholds for prospectus-style rules and authorization requirements. As to the former, under Title II MiCA and Article 1(3) and (4) of the Prospectus Regulation, disclosures in a white paper and prospectus are subject to the condition that the issue attracts 150 or more non-qualified users and a consideration exceeding EUR 1 million in twelve months.

As to **licensing**, ART issuers and their white papers do not need an authorisation where the offer is below EUR 5 million, yet they still have to issue a white paper under the conditions of Title II MiCA (cf. Article 16 MiCA). At the same time, **no exemptions for low-volume investment services is provided in Article 2 and 3 MiFID**. In turn, if a crypto-asset qualifies as financial instrument even very small CASPs will be subject to MiFID.

We propose concurrently establishing a **uniform exemption threshold applicable across all EU financial laws and for any type of financial disclosure and licensing of relevance to crypto-assets**,

<sup>436</sup> Written Testimony, Brummer, C., Written testimony before the US House of Representatives, Agricultural Committee, Subcommittee on Commodity Exchanges, Energy, and Credit The Future of Digital Asset Regulation at 2 (Jun. 23, 2022), available at: [https://agriculture.house.gov/uploadedfiles/brummer\\_congressional\\_testimonythe\\_future\\_of\\_digital\\_asset\\_regulation.pdf](https://agriculture.house.gov/uploadedfiles/brummer_congressional_testimonythe_future_of_digital_asset_regulation.pdf).

at EUR 5 million in value and 150 users per Member State, **and a total EU threshold of EUR 20 million and 500 users**, subject to the procedural requirement that service providers must **apply for an exemption** with the NCAs prior to relying on the low volume-exemption. This uniform threshold will help implement the principle of “tech neutrality”, which is also a cornerstone of the EU’s digital finance action plan and EU financial regulation, in general. It also ensures that the ESAs and the NCAs will have the information for the various reports MiCA requires the NCAs, the ESAs and the EU Commission to write.

To ensure low administration costs on the side of regulators, the exemption may be automated based on the template to be drafted under Article 97(1) MiCA, with additional information on the volume of the issue.

### 6.2.3. Cross-border cooperation among regulators

We further argue in favour of expanding cross-border cooperation in the field of crypto by expanding existing supervisory networks to crypto-assets. Cooperation shall be enhanced inside the EU, and with third countries.

#### a. Cooperation of AML/CTF authorities with ESAs and NCAs

While the code of token protocols does not reveal the client names, some information may be gathered by crypto intermediaries, wallet providers and decentralized protocols on users of the protocols. Given that the AML/CTF KYC rules require the collection of client data, these data, if forwarded to the ESAs and NCAs, may support the effective enforcement of EU financial regulation. For instance, EU licensed entities may forward the data of intermediaries to which or from whom crypto-assets were transferred. They will do so in response to inquiries by their respective NCA.

At the same time, AML/CTF authorities may gather some insights on clients and improper conduct. As the CFTC’s inquiry into Binance demonstrates<sup>437</sup> violations of AML/CTF rules often go hand-in-hand with violations of financial regulation. In turn, we propose to mandate that AML/CTF authorities exchange data on client locations and use of intermediaries with the ESAs and NCAs, to assist the later in identifying conduct and DeFi applications that potentially circumvent EU financial regulation.

#### b. International supervisory networks, in particular IOSCO

As to third countries, the IOSCO framework and MMoU extend to securities and derivatives.<sup>438</sup> It is yet uncertain whether crypto-assets fall under that term, hence whether NCAs can demand information exchange and on-site visits from third-country competent authorities under that framework.

We propose to add crypto-assets (broadly defined) to the IOSCO cooperation frameworks, in line with the default set out above, so that cooperating authorities provide information that assists in enforcing EU securities regulation. This would facilitate the **exchange of crucial information**, for instance on the technical interlinkages and the user/client base, which is crucial to assess the risks for the EU financial sector (traditional or crypto), and also assist in effectively addressing market abuse and insider dealing, a bankruptcy or operational malfunction. The latter has been shown to be of paramount importance in the Crypto Winter.

<sup>437</sup> ‘CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange’ (CFTC, 27 March 2023), available at: <https://www.cftc.gov/PressRoom/PressReleases/8680-23>, accessed 29 March 2023.

<sup>438</sup> International Organization of Securities Commissions, 2002 ‘Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information,’ available at: <https://www.iosco.org/about/?subsection=mmou>, accessed 29 March 2023.

Expanding supervisory networks would also complement the work of **supervisory colleges for significant ARTs and EMTs**. First, the network expansion would help identify NCAs interested in participating in the college. Second, Recital 59-60 MiCA stresses the importance of assessing “the true size and impact” of ARTs and EMTs to ascertain the impact on “financial stability, monetary policy transmission or monetary sovereignty”.<sup>439</sup> Even when NCAs will not participate in a college, they may be more forthcoming in a cooperation framework to share data on the base, market capitalization, operational risks, number of transactions, and other parameters important for enforcing EU financial law.

### 6.3. Addressing (partial) decentralization

While the measures presented *supra* (6.2.) concern centralized and decentralized crypto, the policy proposals that we present in this section focus on (partial) decentralization.

#### 6.3.1. Decentralized platforms and entity status for DAOs

##### a. Decentralization as foundation of regulatory arbitrage

Crypto intermediaries, and in particular decentralized platforms, often argue that there is **no legal entity involved** that could apply for licensing or could be regulated, as the economic function provided is the result of non-custodial protocols (‘smart contracts’) that are interacted with by users on their own accord in a peer-to-peer manner. MiCA acknowledges this argument and exempts “fully decentralized” providers of crypto-asset services, while “partially decentralized” providers are in scope. We have highlighted the related difficulties of distinguishing between centralized and decentralized set-ups *supra* (2.3.4.).

Further, we have identified throughout this study that **decentralization has often become the main argument for the non-application of many financial regulations**, ranging from AML/CTF to disclosure, licensing and fit and proper rules and the sustainability-oriented disclosures under SFDR and the Taxonomy Regulation (to name only two). The same discussion implicitly concerns the non-application of certain rules in case of “non-custodial wallets”, “mixing services” and many other innovations crypto has come forward with that fall out of scope due to their (apparent) decentralization.

##### b. Rationale for exempting decentralized protocols inconclusive

In short, **we do not share the view that decentralization justifies exemptions from all financial laws**. As we argued in 2018, the understanding that multiple nodes may cooperate virtually on their own with no humans involved is a rather simplistic description of reality.<sup>440</sup> In actuality, humans prompt their servers to function as nodes, and humans write or upload the protocol, respectively, on their computers, which then later provide the (decentralized) operations. Similarly, many decentralized platforms provide customer services via Telegram and Discord: these serve humans, not computers. At the heart of fully decentralized platforms thus lies **human cooperation**, exercised through the steering of computers and servers. Human cooperation already results in the entity status of a “cooperation” under the private laws of some EU countries,<sup>441</sup> and in most jurisdictions potentially results in joint

<sup>439</sup> Direct quote from Recital 59 MiCA.

<sup>440</sup> Zetsche D. A., Buckley, R. P., and Arner, D. W., 2018, *The Distributed Liability of Distributed Ledgers: The Legal Risks of Blockchain*, University of Illinois Law Review, pp. 1361-1407.

<sup>441</sup> In particular, we have argued *ibid* that under German, Austrian and Dutch law, cooperation among humans may be treated as “Gesellschaft bürgerlichen Rechts” which has been granted entity status in third-party relations, while all of its members are subject to personal unlimited liability for the entity’s obligations. We note that recently this position was shared by an US judge, who held that the

liability of all contributors of that cooperation.<sup>442</sup> In particular, the mere cooperation of a team of developers or community members that either founded the project or volunteered to keep it afloat suffices in some jurisdictions for entity status.

Given that the smart contracts that underlie the functioning of DeFi protocols are coded, put into operation and modified by humans, and humans decide to let them operate on their information technology, the argument that the mere use of smart contracts results in a product that is something different from the result of human cooperation, is inconclusive. If all parts of something involve human cooperation, then the sum of the parts cannot be something else.

### c. Regulatory entity status for DAOs

We propose to acknowledge the legal qualification assigned to human cooperation in EU financial regulation. As part of EU financial regulation, we suggest the establishment of **EU cross-sectoral legislation**<sup>443</sup> that **(DAOs) are treated as entities for licensing purposes under EU financial regulation**. The former shall be irrespective of:

- whether the DAO is incorporated, formally or informally established, capitalized or not;
- where the DAO is established;
- whether it is merely set up by way of protocols that apply in a decentralized manner, or by other means; and
- where and in which way the multiple token holders take collective decisions.

Rather than being open to the argument that there are no issuers or CASPs (that could be subject to financial regulation and AML/CTF rules), by way of regulation, the DAO as a whole is deemed the issuer or CASP, as the case may be, and must meet the regulatory prerequisites if the other conditions for licensing apply.

Note that this does not automatically mean that all DAOs are subject to licensing. For that, a DAO collectively must:

- (1) provide a service that comes with licensing (which is not the case if it merely issues utility tokens, for instance, and has received the exemption from the default rule proposed herein);
- (2) serve users;
- (3) who reside in the Single Market;
- (4) the exemption for reverse solicitation does not apply; and
- (5) proportionate size thresholds are exceeded.

**If, however, the DAO is acknowledged as an entity for regulatory purposes and if it is a CASP it will have to:**

- lay out the details of its operations, risk management, compliance functions and so on, in a programme of operations (cf. Article 62(2) MiCA);

---

cooperating developers and nodes could form an unregistered General Partnership, and developers and nodes could be held liable, in turn. See Gilbert, A., *Governance Tokens Might Come With Legal Liability, US Judge Says - bZx DAO and Founders Were Sued After \$55M Hack*, 30 March 2023, available at: <https://thedefiant.io/gov-tokens-legal-risk>.

<sup>442</sup> Zetzsche D. A., Buckley, R. P., Arner, D. W., 2018, *The Distributed Liability of Distributed Ledgers: The Legal Risks of Blockchain*, University of Illinois Law Review, pp. 1361-1407.

<sup>443</sup> A cross-sectoral legislation is necessary given that decentralized services can be performed in all sectors of EU financial services.

- provide a business continuity policy that allows for the proper winding-up of the DAO's operations in the case of insolvency (cf. Article 34(9) MiCA); and
- meet all other requirements set for CASPs under MiCA and the respective other EU financial regulation.

In addition, in line with our proposal to extend sustainable finance regulation to DeFi (cf. *supra*, at 3.5.), regulators could mandate a DAO to provide sustainability-related disclosures under the SFDR and the Taxonomy Regulation, where the platform provides services or activities that are in scope of these regulations (for instance, where the service qualifies as (collective) portfolio management under SFDR, or the issuer of transferable securities under the Taxonomy Regulation).

#### d. Service to members only?

Another path to evade EU financial legislation is the argument that **DAOs do not serve clients (that is, externals)**, but only serve their members. The argument is similar to the case where investment clubs are exempted from the AIFMD and all members collectively participate in the investment decision at all times: these investment clubs are exempted from the AIFMD for lack of “external management.”<sup>444</sup> However, for good reasons, in the context of alternative investment funds ESMA applies the “self-management exemption” quite strictly<sup>445</sup> as it facilitates circumvention of EU financial regulation.

We propose to clarify that **only where all or an overwhelming (90%) majority of token holders are personally involved in all financial decisions at all times**, the argument is accepted that there are no external clients, but members only, running the financial service. For instance, if a single lending or borrowing decision is taken by way of the smart contract only, rather than by the exercise of the DAO-specific consensus mechanism, case-by-case, with active participation of 90 percent of the members, we would find that the DAO provides services to clients rather than “its members only.”

While crypto enthusiasts would deny this, in terms of risk we find that the situation in smart contract-based crypto services operated and maintained by some developer group, is not very different from a large ETF for which the management company operates subscription, portfolio management and execution entirely through information technology. The “same risks, same rules” rationale therefore supports a narrow construction of (potential) exemptions.

#### e. Ensuring representation

Some **additional rules** may assist the effective implementation of our proposal.

These rules mimic existing rules for CASPs. In particular, any DAO shall name a **legal representative** in the EU for regulatory purposes. In particular, the legal entity engaged in product development and distribution of services of a fully decentralized platform shall register itself as operator for purposes of complying with EU financial regulation, including sustainability disclosure obligations on behalf of the platform.<sup>446</sup> In case the developing firm does not register itself a representative, we propose to implement the rule from Title II and Article 88 MiCA, mandating, in that sequel, offerors and persons

<sup>444</sup> See Zetzsche, D. A., Preiner, C. D., 2020, Scope of the AIFMD in Zetzsche, D. A., *The Alternative Investment Fund Managers Directive*, 3rd ed., at pp. 29-32, Kluwer Law International.

<sup>445</sup> Cf. ESMA Final report, Guidelines on key concepts of the AIFMD (ESMA/2013/600), pp. 31 and 15; see on this exemption D.A. Zetzsche, in Assmann/Wallach/Zetzsche, KAGB (German Collective Investment Schemes Act), 2nd ed. 2022, Otto-Schmidt-Verlag, at § 1 ¶ 32-38 (arguing that up to 10% of the collective assets regulatory leniency may be justified).

<sup>446</sup> While Art. 122(4) MiCA entitles the EBA to address the legal representative in the case of significant EMTs and ARTs, a developer firm creating a fully decentralized platform will argue that it is not the legal representative of the platform. For that reason, legislation must specify who the representative is, if the developer firm does not register itself as a representative.

seeking admission to trading, and as a fall-back solution, the trading platform to register on behalf of the DAO.

f. **Bespoke bankruptcy legislation.**

We have emphasized *supra* (at 5.2.3.) the need for **bespoke crypto bankruptcy and restructuring legislation for both centralized and decentralized protocols**. This could form part of Directive 2014/59/EU ('BRRD') or a new section of MiCA. That legislation would ensure **business continuity** with incentives in cases of malfunctions, crises and bankruptcy, and ensure that the multiple parties that are crucial for any aspect of the crypto ecosystem continue to operate until the assets are properly liquidated.

That need still exists with MiCA into force: while MiCA requires a business continuity policy for CASPs and issuers of ARTs, among others,<sup>447</sup> these policies cannot determine and invalidate any third parties' rights in the platform's bankruptcy. Such an invalidation may be a precondition, however, for the restructuring of the platform. Hence, we suggest to adopt bespoke bankruptcy and restructuring legislation for centralized and (apparently fully) decentralized crypto services.

The bespoke bankruptcy and restructuring legislation is particularly important to address the negative impacts of decentralization: from the platform's perspective, token holders may or may not be third parties; their representation in bankruptcy and regulatory-sponsored collective redress will be crucial to avoid that beneficiaries of illicit conduct may retain their proceeds for good. Rectifying any harm done to token holders is not only crucial from the perspective of client protection, but also sets a disincentive for illicit acts in the first place and, thus furthers financial stability at large.

### 6.3.2. Private law

It is critical to further the **harmonizing of private law**, and particularly with the recognition of property rights, negotiability, and the need to establish clear rules on court jurisdiction and applicable law. This may happen through EU legislation, but harmonizing private law is notoriously difficult. Instead, we suggest the endorsement of Unidroit approaches or working on a new Hague Convention.

Further, EU law could provide for **a variant of a limited partnership on the EU level** as *optional* semi-corporate form for DAOs.

### 6.3.3. Court jurisdiction, choice of law

On court jurisdiction and choice of law, we propose **ensuring legal certainty** by adding crypto-assets to Rome I and Brussels Regulation. For instance if crypto-assets of the same series are seen as case of lit d) of Art 6 IV Rome I Regulation, the law applicable at the place of the main service provider would govern all rights and obligations relating to crypto-assets of the same series.

## 6.4. NFTs

We have held *supra*, at 5.4.4., that the (potential) exemption of financial NFTs from MiCA pose AML/CTF risks, counterparty and financial risk, valuation and other operational risks. Most of these risks vanish if "financial NFTs" are in scope. To ensure that, we suggest clarifying, as part of implementing legislation, that "financial NFTs" are treated as financial instruments or crypto-assets under MiCA, as the case may be, whenever the token takes the characteristic of a bearer instrument. This means: it is traded freely, at least five to a dozen tokens exist, and any holder of the token is entitled to exercise the tokenized

<sup>447</sup> Cf. Art. 17, 18, 34, 60 and 62 MiCA.



rights. In addition to ensuring client protection, systemic risk prevention and proper measures to address market abuse, this would enable the application of anti-money laundering laws.

Further, following examples of securitization laws in some Member States, regulators may **require licensing of tokenization intermediaries involved in tokenization of (all types of) NFTs**. So far, under MiCA pure NFT tokenization intermediaries are exempted (unless they deal with crypto-assets under MiCA or provide any other regulated financial service). Given that general consumer protection law deals with the main consumer risk already, this licensing requirement would focus on the **additional operational and financial risk** only created by the tokenization in itself. For that purpose, **a separate section on “NFT-CASPs” can be added to MiCA**. The section would only refer to MiCA rules for CASPs that deal with the additional operational and financial risk of tokenization and DLT-based asset transfer. The reason is that NFTs raise essentially the same operational risk, from a technical and legal perspective, as crypto-assets, only that the number of users potentially harmed may be smaller. At the same time, matters relating to mis-marketing, valuation and terms of use would be largely subject to EU consumer law already in place, at least when the narrow interpretation of NFTs as proposed in this study is exercised.

## 7. CONCLUSIONS

### KEY FINDINGS

Crypto poses significant challenges to EU financial regulation. The starting point is an understanding that the market has evolved rapidly, is showing many similar issues present in traditional finance and requires similar regulatory attention in order to function appropriately. MiCA and TFR partly address these issues, as does the existing corpus of EU financial regulation. However, the intersection remains unclear, particularly in the jurisdictional context, both within and beyond the EU. We argue for a series of approaches to address these issues in order to support the appropriate development of the market going forward.

Crypto poses significant challenges to EU financial regulation. We have identified that crypto often evades regulation due to the lack of transparency and anonymity of users, uncertain scope of EU financial regulation, testing of the boundaries of exemptive concepts, reverse solicitation, and decentralization and use of smart contracts and DAOs instead of formal legal entities, as procedural and legal reference points.

MiCA and TFR partly address these matters. Where a central intermediary is involved in providing crypto services, MiCA provides a bespoke set of rules that could address the most important risks and challenges. Yet, much depends on the implementation. Core aspect in this regard is the definitional matter, which is linked to the delineation of various types of EU financial regulation and providing details on crucial concepts, such as custody, client solicitation and so on. Shortcomings need to be addressed in the field of bespoke bankruptcy legislation, NFTs, private law, and particularly with the recognition of property rights, negotiability, and the need to establish clear rules on court jurisdiction and applicable law.

Yet MiCA and TFR struggle with platforms that claim to be fully decentralized but in most cases are not, that we find often in crypto today. We have made bespoke proposals to address these matters by assigning, for licensing purposes, entity status to DAOs and restrict the backdoor to argue that a DAO would only serve its members.

Principally, we recommend addressing the cross-border issue with a cross-sectoral EU regulation on cross-border solicitation in financial services, a centralized authority of the ESAs to inquire into the EU user base and make this information available to the NCAs, as well as RegTech, by virtue of a Euro Wallet.

## REFERENCES

### Literature List

- *About restricted financial products certification* (Google), available at: <https://support.google.com/adspolicy/answer/7645254>.
- Adams A., and Ibert M., 2022, *Runs on Algorithm Stablecoins: Evidence from Iron, Titan and Steel*, Board of Governors of the Federal Reserve System, FEDS Notes, available at: <https://www.federalreserve.gov/econres/notes/feds-notes/runs-on-algorithmic-stablecoins-evidence-from-iron-titan-and-steel-20220602.html>.
- Adejumo O., 2022, 'Aave developers to get \$16.8 in retroactive funding', Cryptoslate, available at: <https://cryptoslate.com/aave-developers-to-get-16-8m-in-retroactive-funding/>.
- *Advice on the review of the macroprudential framework*, 2022, European Banking Authority (EBA), available at <https://www.eba.europa.eu/eba-proposes-simplify-and-improve-macroprudential-framework>.
- Aliaj O., Fontanella-Khan J., Oliver J., Chipolinain S., and Palma S., 2022, *Binance Ditches Deal to Rescue Rival Crypto Exchange FTX*, Financial Times, available at: <https://www.ft.com/content/ad440b22-00e2-44e9-b95d-449bb89fd504>.
- Allen A. G., and Mcweeney Jr S. G., 2021, *15 Faqs on the Digital Assets and Registered Exchanges ('DARE') Act, 2020*, GrahamThomson News & Insights, 3 (1), available at: <https://grahamthompson.com/wp-content/uploads/2021/01/GT-News-Insights-Vol-3-Issue-1-DARE.pdf>.
- Allen F., and Gu X., 2018, *The Interplay between Regulations and Financial Stability*, Journal of Financial Services Research 53 Journal of Financial Services Research 53, 233, available at: <https://link.springer.com/article/10.1007/s10693-018-0296-7#citeas>.
- Allison I., 2022, *Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet*, Coindesk, available at: <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>.
- Anker-Sørensen, L., and Zetsche D. A., 2021, *From Centralized to Decentralized Finance: The Issue of 'Fake-DeFi*, available at SSRN: <https://ssrn.com/abstract=3978815> or <http://dx.doi.org/10.2139/ssrn.3978815>.
- Anoop V. S., and Goldston J., 2022, *Decentralized finance to hybrid finance through blockchain: a case-study of acala and current*, Journal of Banking and Financial Technology 6, 109, available at: <https://link.springer.com/article/10.1007/s42786-022-00041-0>.
- Antolin M., 2022, *What Are Liquidity Pools?*, Coindesk, available at: <https://www.coindesk.com/learn/what-are-liquidity-pools/>.
- Aquilina M., Frost J., and Scrimpf A., 2023, *Addressing the risks in crypto: laying out the options*, Bank of International Settlement (BIS), available at: <https://www.bis.org/publ/bisbull66.htm>.
- Arner D.W., Barberis, J and Buckley R.P., 2017, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, Northwest Journal of International Law and Business, 37.

- Arner, D.W., Zetsche, D.A., Buckley, Sergeev, A., 2022, *Digital Finance, Financial Inclusion, and Sustainable Development: Building Better Financial Systems* in Beirne J., Villafuerte J., and Zhang B., *Fintech and COVID-19 Impacts Challenges and Policy Priorities for Asia*, Asian Development Bank Institute.
- Arner, D.W., Zetsche, D.A., Buckley, R.P., Kirkwood, J.M., 2023, 'The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023', University of Hong Kong Faculty of Law Research Paper No. 2023/19, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4372516](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4372516)
- Asgari A., 2022, *FTX allowed trading affiliate Alameda to borrow unlimited funds*, Financial Times, available at: <https://www.ft.com/content/9f07539f-497d-495c-a1e3-3315b8c6f9c9>.
- Auer R., and Claessens S., 2018, *Regulating cryptocurrencies: assessing market reactions*, BIS Quarterly Review, available at: [https://www.bis.org/publ/qtrpdf/r\\_qt1809f.pdf](https://www.bis.org/publ/qtrpdf/r_qt1809f.pdf).
- Bains P., Ismail A., Melo F., and Sugimoto N., 2022, *Crypto Ecosystem: The Case of Unbacked Crypto Assets*, International Monetary Fund, available at: <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715>.
- Bains P., Ismail A., Melo F., and Sugimoto N., 2022, *Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements*, available at: <https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Stablecoins-and-Arrangements-523724>.
- Baker N., 2023, *USDC Stablecoin Depeds, Crypto Market Goes Haywire After Silicon Valley Bank Collapses*, Coindesk, available at: <https://www.coindesk.com/markets/2023/03/11/usdc-stablecoin-and-crypto-market-go-haywire-after-silicon-valley-bank-collapses/>.
- Barsan I., 2018, *Legal Challenges of Initial Coin Offerings*, Revue Trimestrielle de Droit Financier (RTDF), 54 (3), p. 62, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3064397](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064397).
- Bavosa A., 2020, *Supplying Assets to the Compound Protocol – Quick Start Guide*, Compound Finance, available at: <https://medium.com/compound-finance/supplying-assets-to-the-compound-protocol-ec2cf5df5aa>.
- Behrens A., 2020, *Aave Officially Hands Over Governance Keys to DeFi Community*, Decrypt, available at: <https://decrypt.co/46544/aave-officially-hands-over-governance-keys-to-defi-community/>.
- Belyakov A., 2020, *First Credit Default Swap on Aave Credit Delegation Launched*, Medium.com, available at: <https://medium.com/opium-network/first-credit-default-swap-on-aave-credit-delegation-launched-5e3efc961317#:~:text=About%20Aave%20Credit%20Delegation%20Aave%20Credit%20Delegati on%20is,contract%20that%20executes%20predefined%20functions%2C%20removing%20that%20trust>.
- Berwick A., and Wilson T., 2022, *Exclusive: Behind FTX's fall, battling billionaires and a failed bid to save crypto*, Reuters, available at: <https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/>.
- *Binance: End of Year Report, 2022*, Bnbstatic. Available at: <https://public.bnbstatic.com/static/content/End-of-Year-Report-2022.pdf>.

- Birdthistle, W. A., 2010, *Breaking Bucks in Money Market Funds*, Wisconsin Law Review, 5, pp. 1155-1201, available at: <https://ssrn.com/abstract=1728929>.
- Blandin A., Cloots A.S., Hussain H., Rauchs M., Saleuddin R., Allen J.G., Zheng Zhang B., and Cloud K., 2019, *Global Crypto-assets Regulatory Landscape Study*, University of Cambridge Faculty of Law Research Paper No. 23, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3379219](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379219).
- Boreiko D., Ferrarini G., and Giudici P., 2019, *Blockchain Startups and Prospectus Regulation*, European Business Organization Law Review, 20 (4), pp. 665-694., available at: <https://link.springer.com/article/10.1007/s40804-019-00168-6>.
- Bourveau T., de George E.T., Ellahie A., and Macciocchi D., 2018, *Initial Coin Offerings: Early Evidence on the Role of Disclosure in the Unregulated Crypto Market*, 12, 18, available at: <http://dx.doi.org/10.2139/ssrn.3193392>
- Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. K., 2020, *Techrisk*. Singapore Journal of Legal Studies, 35-62, available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3478640](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640).
- Burns B., 2018, *ERC-998 and the Future of Blockchain Game Assets*, GigLans, available at: <https://medium.com/giglabs/erc-998-and-the-future-of-blockchain-game-assets-9fd1063126cf>.
- Burilov V., 2019, *Regulation of Crypto Tokens and Initial Coin Offerings in the EU*, European Journal of Comparative Law and Governance, 6, p. 146, available at: [https://brill.com/view/journals/ejcl/6/2/article-p146\\_146.xml?language=en](https://brill.com/view/journals/ejcl/6/2/article-p146_146.xml?language=en).
- *Busting Crypto Myths: "Bitcoin is Destroying the Environment"*, 2022, Kraken, available at: <https://blog.kraken.com/post/16645/crypto-myths-bitcoin-destroying-environment/>.
- Carapella F., Dumas E., Gerszten J., Swem N., and Wall L., 2022, *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, Finance and Economics Discussion Series 2022-057, Washington: Board of Governors of the Federal Reserve Board, available at: <https://www.federalreserve.gov/econres/feds/files/2022057pap.pdf>.
- Chen, H., 2022, *This Guy is Living Your Wildest NFT Dreams, Making %1 Million in Selfie Sales*, Vice World News, available at: <https://www.vice.com/en/article/4awn3m/indonesia-nft-crypto-bitcoin-ghozali>.
- Chidinma Okoye M.m and Clark J., 2019, *Toward Cryptocurrency Lending* in Zohar A. et al., *Financial Cryptography and Data Security*, Springer, pp. 367–380.
- Coffee J.C., and Sale H.A. 2012, *Securities Regulation - Cases and Materials*, Foundation Press, 12th ed., pp. 247-269.
- Cone G., Bjorklund N.S., and Dyekman G.C., 2021, *Digital assets and property rights in insolvency*, *Trusts & Trustees*, 27(5), p. 406.
- *Cryptocurrencies: looking beyond the hype*, 2018, BIS Annual Economic Report 2018, available at: <https://www.bis.org/publ/arpdf/ar2018e5.pdf>.
- *Crypto winter end in sight as Ethereum looks to shake the chills-analysts*, 2022, Reuters, available at: <https://www.reuters.com/markets/currencies/crypto-winter-end-sight-ethereum-looks-shake-chills-analysts-2022-12-12/>.

- *Decentralized Finance Market Size, Share & Trends Analysis Report*, 2022, Grand View Research, available at: <https://www.grandviewresearch.com/industry-analysis/decentralized-finance-market-report>.
- De Guindos L., 2021, *Financial Stability Review*, European Central Bank (ECB), available at: <https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202111~8b0aebc817.en.html>.
- De N., and Allison I., 2023, *Policy: Silvergate Closes SEN Platform Institutions Used to Move Money to Crypto Exchanges*, CoinDesk, available at: <https://www.coindesk.com/policy/2023/03/03/silvergate-suspends-sen-exchange-network/>.
- Elder B., 2022, *Untangling the knotty empire of Bankman-Fried and FTX*, Financial Times, available at: <https://www.ft.com/content/c28e0570-d4c4-433c-b0a0-c99fba613822>.
- *Elements of Effective Policies for Crypto-assets*, 2023, International Monetary Fund (IMF), available at: <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-assets-530092>.
- *ELI Principle on the Use of Digital Assets as Security*, 2021, Report of the European Law Institute, available at: [https://www.europeanlawinstitute.eu/fileadmin/user\\_upload/p\\_eli/Publications/ELI\\_Principles\\_on\\_the\\_Use\\_of\\_Digital\\_Assets\\_as\\_Security.pdf](https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf).
- Encila J., 2022, *Tron Uses Nearly 100% Less Energy Than Bitcoin and Ethereum, Study Shows*, Binance, available at: <https://www.binance.com/en/news/top/7184556>.
- Enriques L., and Zetsche D. A., 2020, *Corporate Technologies and the Tech Nirvana Fallacy*, Hastings Law Journal, 72, pp. 55-98, available at: <https://ssrn.com/abstract=3392321> or <http://dx.doi.org/10.2139/ssrn.3392321>.
- Essaghoolian N., 2019, *Initial Coin Offerings: Emerging Technology's Fundraising Innovation*, University of California Los Angeles Law Review 66 (1), p. 294.
- *Ethereum Proof-Of-Stake Attack and Defense*, 2022, Ethereum.org, available at: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attack-and-defense/>.
- Evans D., 2022, *Permissioned DeFi Goes Live with Aave Arc + Fireblocks*, Fireblocks, available at: <https://www.fireblocks.com/blog/permissioned-defi-goes-live-with-aave-arc-fireblocks/>.
- Fama E. F., 1970, *Efficient Capital Markets: A Review of Theory and Empirical Work*, Journal of Finance, 25(2), p. 383.
- Faife C., 2022, *Beanstalk founders dismissed concerns about governance attacks before losing \$182 million*, available at: <https://www.theverge.com/2022/4/22/23037325/beanstalk-dismissed-governance-attacks-lost-182-million>.
- *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stable-coins*, 2020, Financial Action Task Force (FATF), available at: [Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf](https://www.fatf-gafi.org/media/42087255-92ad-45b7-b5ad-3b8457e0c1f8).
- *Final Report on response to the non-bank lending request from the CfA on digital finance*, 2022, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-provides-its-advice-eu-commission-non-bank-lending>.
- Foley S., 2022, *FTX US auditor Armanino defends work for failed crypto exchange*, Financial Times, available at: <https://www.ft.com/content/42087255-92ad-45b7-b5ad-3b8457e0c1f8>.

- Gabers-von Boehm, K., Haag, H., Gruber, K., 2022, *Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art*, available at: <http://www.europarl.europa.eu/supporting-analyses>.
- Geva B., 2020, *Cryptocurrencies and the Evolution of Banking, Money, and Payments* in Brummer C., *Crypto-assets: Legal, Regulatory, and Monetary Perspectives*, Oxford Academic, p. 12.
- Goldberg, M., and Schär, F., 2023, *Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations*, *Journal of Business Research* 160 (2023) 113764.
- Goforth C., 2019, *U.S. Law: Crypto Is Money, Property, A Commodity, And A Security, All At The Same Time*, *Journal of Financial Transformation*, Capco Institute, 49, pp. 102-109.
- Goodhart C., et al., 1988, *The rationale for regulation in Financial Regulation: Why, How and Where Now?*, Routledge, 1998, 1.
- Goodwin, D., 'What Is SEO – Search Engine Optimization?' (Search Engine Land), available at: <https://searchengineland.com/guide/what-is-seo>.
- Gonzalez N. E., 2022, *Does Cryptocurrency Staking Fall under SEC Jurisdiction?*, *Fordham Journal of Corporate and Financial Law* 27 (2), pp. 521-561.
- Goswami R., and Sigalos M., 2022, *In defensive interview, Sam Bankman-Fried claims he's broke and committed no fraud*, CNBC, available at: <https://www.cnbc.com/2022/11/30/former-ftx-ceo-sam-bankman-fried-says-i-didnt-ever-try-to-commit-fraud.html>.
- Haber S., and Stornetta, W.S., 1991, *How to time-stamp a digital document*, *Journal of Cryptology*, 3, pp. 99–111, available at: <https://doi.org/10.1007/BF00196791>.
- Hacioglu U., 2019, *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age*, Springer Cham, available at: <https://link.springer.com/book/10.1007/978-3-030-25275-5>.
- Haentjens M., De Graaf T., and Kokorin I., 2020, *The Failed Hopes of Disintermediation: Crypto Custodian Insolvency, Legal Risks and How to Avoid Them*, *Singapore Journal of Legal Studies*, p. 526.
- Hern A., and Milmo D., 2022, *What do we know so far about collapse of crypto exchange FTX?*, *The Guardian*, available at: <https://www.theguardian.com/technology/2022/nov/18/how-did-crypto-firm-ftx-collapse>.
- Heng Chou J., Agrawal P., and Birt J., 2022, *Accounting for crypto-assets: stakeholders' perceptions*, *Studies in Economics and Finance*, Emerald Group Publishing Limited, 39 (3) pp. 471-489.
- Herlin-Karnell E., and Ryder N., 2019, *Market Manipulation and Insider Trading: Regulatory Challenges in the United States of America, the European Union and the United Kingdom*, Hart Publishing.
- *How Much Does It Cost To Create An NFT Collection?* 2023, Okuha, available at: <https://okuha.com/how-much-does-it-cost-to-create-an-nft-collection/#:~:text=Creating%20an%20NFT%20collection%20costs%20anything%20between%200%2430,to%20the%20costs%20of%20creating%20an%20NFT%20collection>.

- Howell S. T., Niessner M., and Yermack D., 2018, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sale*, ECGI Finance Working Paper 564, p. 9, available at: [https://www.ecgi.global/sites/default/files/working\\_papers/documents/finalhowellniessneryermack.pdf](https://www.ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf).
- Hristovand G., Ullmanand S., and Nusca A., 2023, *Best Crypto Lending Rates 2023*, Milkroa, available at: <https://milkroad.com/lend>.
- Huang V.G., Osipovich A., and Kowsmann P., 2022, *FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall*, The Wall Street Journal, available at: <https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732?mod=e2tw>.
- Huang V.G., Miao H., and Ostroff C., 2023, *Circle's USDC Stablecoin Breaks Peg With \$3.3 Billion Stuck at Silicon Valley Bank*, The Wall Street Journal, available at: <https://www.wsj.com/articles/crypto-investors-cash-out-2-billion-in-usd-coin-after-bank-collapse-1338a80f>.
- Iacurci G., 2022, *As BlockFi files for bankruptcy, what to know about crypto investor protections*, CNBC, available at: <https://www.cnbc.com/2022/11/28/what-to-know-about-crypto-investor-protections-as-blockfi-files-for-bankruptcy.html>.
- *Important Client Update*, 2022, BlockFi, available at: <https://blockfi.com/November28-ClientUpdate>.
- *IOSCO Crypto-Asset Roadmap for 2022-2023*, 2022, International Organization of Securities Commissions, available at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD705.pdf>.
- Irresberger F., Kose J., Mueller P., and Saleh F., 2021, *The Public Blockchain Ecosystem: An Empirical Analysis*, NYU Stern School of Business, p. 5.
- Katz M. L., and Shapiro C., 1985, *Network Externalities, Competition, and Compatibility*, American Economic Review, 75(3) p. 424.
- Kharif O., 2022, *Binance To Sell \$529 Million of Bankman-Fried's FTT Token*, Bloomberg, available at: <https://www.bloomberg.com/news/articles/2022-11-06/binance-to-sell-529-million-of-ftt-token-amids-revelations#xj4y7vzkg>.
- Klöhn L., Parhofer N., and Resas D., 2018, *Initial coin offerings (ICOs)*, Zeitschrift für Bankrecht und Bankwirtschaft, p. 89-106.
- Knight O., 2022, *How crypto Lender Celsius Overheated*, Coindesk, available at: <https://www.coindesk.com/business/2022/06/16/how-crypto-lender-celsius-overheated/>.
- Koops, B-J., Kosta E., 2018, *Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against 'Going Dark'*, Computer Law & Security Review, 34, pp. 890-900, available at: <https://ssrn.com/abstract=3249238>.
- Korsmo C. R. 2017, *The Audience for Corporate Disclosure*, Iowa Law Review, 102(4) p. 1581, available at: <https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/ILR-102-4-Korsmo.pdf>.
- Kregel J. A., 2010, *Is this the Minsky Moment for Reform of Financial Regulation?*, Levy Economics Institute Working Paper No. 586, available at: <https://ssrn.com/abstract=1559382> or <http://dx.doi.org/10.2139/ssrn.1559382>.
- Lang H., Howcroft E., and Wilson T., 2022, *Analysis: Clients of crypto lender Celsius face long wait over fate of their funds*, Reuters, available at: <https://www.reuters.com/technology/clients-crypto-lender-celsius-face-long-wait-over-fate-their-funds-2022-07-15/>.



- Lang H. and Chakroborti A., 2023, *Crypto focused bank Silvergate plans to wind down following blow from FTX*, Reuters, available at: <https://www.investing.com/news/stock-market-news/cryptofocused-bank-silvergate-plans-to-wind-down-operations-3025518>.
- Land H., and Prentice C., 2023, *U.S. securities regulator charges Genesis, Gemeni with unregistered offerings*, Reuters, available at: <https://www.reuters.com/markets/us/us-securities-regulator-charges-genesis-gemini-with-unregistered-offerings-2023-01-12/>.
- Lau H., and Tse S., 2021, *Decentralized Basic Income: Creating Wealth with On-Chain Staking and Fixed-Rate Protocols*, Cornell University, available at: <https://arxiv.org/pdf/2107.14312.pdf>.
- Lee J. and L'heureux F., 2020, *A Regulatory Framework for Cryptocurrency*, European Business Law Review, 31 (3), pp. 423-446.
- Lehmann, M., and Krysa, F., Prévost, E., Schinerl, F., Vogelauer, R., *Staking Your Crypto: What are the Stakes?* (Jan 27, 2023). Available at: <https://ssrn.com/abstract=4339687> or <http://dx.doi.org/10.2139/ssrn.4339687>.
- Lehmann, M., *Who owns Bitcoin?*, 21 Minn. J.L. Sci. & Tech. 93 (2019).
- Levitin A. J. 2022, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, Texas Law Review (forthcoming), 101, available at: <https://ssrn.com/abstract=4107019> or <http://dx.doi.org/10.2139/ssrn.4107019>.
- Lielacher A., 2023, *CEX.IO is a well-regulated exchange with a lot to offer*, Investopedia, available at: <https://www.investopedia.com/cex-io-review-5215239>.
- Lielacher A., 2023, *Best Crypto Exchanges: Our top picks for the best cryptocurrency exchanges of 2023*, Investopedia, available at: <https://www.investopedia.com/best-crypto-exchanges-5071855>.
- Liu B., 2022, *Feature or Flaw? Aave Left With \$1.7M in Bad Debt*, Blockworks, available at: <https://blockworks.co/news/aave-curve-bad-debt>.
- Locke T., 2022, *Did a 'concerted attack' cause Terra's UST to crash below \$1? An exec behind the largest stablecoin and experts agree it is suspicious*, Fortune, available at: <https://fortune.com/2022/05/13/terra-ust-stablecoin-crash-suspicious-potential-attack-george-soros/>.
- Lockyer M., 2018, *Crypto Composables-Building Blocks and Applications*, Coinmonks, available at: <https://medium.com/coinmonks/crypto-composables-building-blocks-and-applications-65902709298c>.
- Lopatto E., 2022, *How the Anchor protocol helped sink Terra*, The Verge, available at: <https://www.theverge.com/2022/5/20/23131647/terra-luna-do-kwon-stablecoin-anchor>.
- Lutz S. and Beganski A., 2023, *Silicon Valley Bank Contagion: Crypto Companies Affected Include BlockFi, Circle, Avalanche, Ripple*. Decrypt, available at: <https://decrypt.co/123199/silicon-valley-bank-crypto-companies-contagion>.
- Mangano, 2019, *The insolvency of cryptocurrency exchanges: Lessons from the BitGrail case - reification of coins, pari passu ranking, and nominalism*, Banking & Finance Law Review, 35(1), pp. 197-204, available at: <https://pure.unipa.it/en/publications/the-insolvency-of-cryptocurrency-exchanges-lessons-from-the-bitgr>.

- Maurer M., 2022, *More Crypto Exchanges Verify Reserves, But Questions About Assets Remain*, Wall Street Journal, available at: <https://www.wsj.com/articles/more-crypto-exchanges-verify-reserves-but-questions-about-assets-remain-11670153687>.
- Maume P., and Fromberger M., 2019, *Regulations of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws*, Chicago Journal of International Law, 19 (2), pp. 548-585, available at: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1748&context=cjil>.
- Mihajlović M., 2022, *AAVE Tokenomics Explained*, Shrimpy, available at: <https://academy.shrimpy.io/post/aave-tokenomics-explained>.
- Mihajlović M., 2022, *A Guide to Crypto Twitter*, Shrimpy Academy, available at: <https://academy.shrimpy.io/post/a-guide-to-crypto-twitter>.
- Moesman N., and Munro A., *De 11 beste crypto exchanges in Nederland (in English: The 11 best crypto exchanges in the Netherlands)*, Finder, available at: <https://www.finder.com/nl/cryptomunten/beurzen>.
- Mollman S., 2022, *A lot of people have compared this to Lehman. I would compare it to Enron: Larry Summers has some choice words for Sam Bankman-Fried and FTX*, Fortune, available at: <https://fortune.com/2022/11/11/larry-summers-ftx-crypto-collapse-more-like-enron-than-lehman/>.
- Mougayar W., 2020, *While We Wait for Laws, We Need Better Interpretations of Existing Regulation*, Coindesk, available at: <https://www.coindesk.com/while-we-wait-for-laws-we-need-better-interpretations-of-existing-regulation>.
- Moy C., and Carlson J., 2021, *Cryptocurrencies can enable financial inclusion. Will you participate?*, Weforum, available at: <https://www.weforum.org/agenda/2021/06/cryptocurrencies-financial-inclusion-help-shape-it/>.
- Nabilou H., 2020, *The dark side of licensing cryptocurrency exchanges as payment institutions*, Law and Financial Markets Review, 14 (1), pp. 39-47.
- Neuder M., Moroz D., Rao R., Parkes D., 2021, *Low-cost attacks on Ethereum 2.0 by sub-1/3 stakeholders*, School of Engineering and Applied Sciences, Harvard University, p. 5, available at: <https://arxiv.org/pdf/2102.02247.pdf>.
- Nexo's Guiding Principles for Always Keeping Your Assets Safe, 2022, Nexo, available at: <https://nexo.com/blog/nexo-guiding-principles-for-always-keeping-your-assets-safe>.
- Ngetich D., 2023, *USDC Is In Trouble, But It Won't Go To Zero Like UST Did-Here's Why*, Newsbtc, available at: <https://www.newsbtc.com/stablecoin/usdc-is-in-trouble-but-it-wont-go-to-zero-like-ust-did-heres-why/>.
- Oi R., 2022, *Top 10 Biggest Crypto Failures of 2022*, Fintechnews.sg, available at: <https://fintechnews.sg/67859/crypto/top-10-biggest-crypto-failures-of-2022/>.
- Omarova S. T., 2020, *Dealing with Disruption: Emerging Approaches to Fintech Regulation*, Washington Journal of Law & Policy, 61 p. 25, available at: <https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2798&context=facpub>.
- Ponnann J.P., 2023, *ERC-721 Non-Fungible Token Standard*, Ethereum, available at: <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>.

- *Prudential treatment of cryptoasset exposures*, 2022, Bank of International Settlements (BIS), available at: <https://www.bis.org/bcbs/publ/d545.pdf>.
- Race M., and Miller M. 2022, *FTX boss Sam Bankman-Fried arrives in US to face charges*, BBC News, available at: <https://www.bbc.com/news/business-64036615>.
- *Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations*, 2020, Financial Stability Board (FSB), available at: <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>.
- *‘Report with advice for the European Commission on crypto-assets’*, 2019, European Banking Authority (EBA), available at: <https://www.eba.europa.eu/eba-reports-on-crypto-assets>.
- Reyes M., Shen M., and Pan D., 2023, *Signature Bank’s Real-Time Crypto Payments Network Still Online, For Now*, Bloomberg, available at: <https://www.bloomberg.com/news/articles/2023-03-13/signature-bank-s-signet-real-time-crypto-payments-network-still-online-for-now#xj4y7vzkg>.
- Rodriguez G., 2023, *6 Best Crypto Exchanges of March 2023*, Money.com, available at: <https://money.com/best-crypto-exchanges/>.
- Rohr J., and Wright A., 2019, *Blockchain- Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, Hastings Law Journal, 70, pp. 463-524.
- *‘Right to be Forgotten Overview’* (Google), available at: <https://support.google.com/legal/answer/10769224?hl=en>.
- Sander Lutz, *‘SEC vs BAYC? Here’s What Legal Experts Say It Means for NFTs’* (Decrypt, 18 October 2022), available at: <https://decrypt.com/112190/sec-bayc-legal-experts-nfts-yuga-bored-apes>
- Sandor, K., *‘What Is Crypto Custody?’* (CoinDesk, 18 February 2022), available at: <https://www.coindesk.com/learn/what-is-crypto-custody/>.
- Sarra S., Gullifer QC (Hon) L., 2019, *Crypto claimants and bitcoin bankruptcy: Challenges for recognition and realization*, International Insolvency Review, 28 (2) pp. 233– 272, available at: <https://doi.org/10.1002/iir.1346>.
- Schär F., 2021, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, Economic Research Federal Reserve Bank of St. Louis Review, Second Quarter 2021, 103 (2), pp. 153-174, available at: <https://doi.org/10.20955/r.103.153-74>.
- Schär F., 2020, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, SSRN, available at: <https://ssrn.com/abstract=3571335> or <http://dx.doi.org/10.2139/ssrn.3571335>.
- Sears J., and Ng J., 2022, *Bit by Bit - the Future Direction of English Insolvency Law and Cryptocurrency, Corporate Rescue and Insolvency*, 15 (2), pp. 53–55, available at: <https://www.dentons.com/en/insights/articles/2022/april/19/bit-by-bit-the-future-direction-of-english-insolvency-law-and-cryptocurrency>.
- *SEC Reopens Comment Period for Proposed Amendments to Exchange Act Rule 3b-16 and Provides Supplemental Information*, (SEC, 14 April 2023), available at: <https://www.sec.gov/news/press-release/2023-77>.
- Sedlmeir J., et al., 2020, *The Energy Consumption of Blockchain Technology: Beyond Myth*, Business and Information Systems Engineering Journal, 62 (6), p. 599.

- Shubba K., Oliver J., and Indap S., 2022, *New FTX chief says crypto group's lack of control worse than Enron*, Financial Times, available at: <https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7>.
- Shumba C., 2022, *US Justice Department Wants FTX Fraud Allegations to Be Investigated*, CoinDesk, available at: <https://www.coindesk.com/policy/2022/12/02/us-justice-department-wants-ftx-fraud-allegations-to-be-investigated/>.
- Solinas M., 2021, *Trustless' distributed ledgers and custodial services in Routledge Handbook of Financial Technology and Law*, edited by Chiu I., and Deipenbrock G., Routledge.
- Sridharan S., 2022, *FinFluencers: What code of conduct should we have?*, Observer Research Foundation (ORF), available at: <https://www.orfonline.org/research/finfluencers/>.
- Stempel, J., 'U.S. judge permits lawsuit claiming NBA Top Shot NFTs are securities' (Reuters, 22 February 2023), available at: <https://www.reuters.com/legal/us-judge-permits-lawsuit-claiming-nba-top-shot-nfts-are-securities-2023-02-22/>
- Stevens R., 2022, *BlockFi's Rise and Fall: A Timeline*, Coindesk, available at: <https://www.coindesk.com/learn/blockfis-rise-and-fall-a-timeline/>.
- Stevens R., 2022, *Bitcoin Mixers: How Do They Work and Why Are They Used?*, Coindesk, available at: <https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/>.
- Stevens R., 2022, *What Are Blockchain Bridges and How Do They Work?*, Coindesk, available at: <https://www.coindesk.com/learn/what-are-blockchain-bridges-and-how-do-they-work/>.
- Surujnath R., 2017, *Off The Chain! A Guide to Blockchain Derivatives Markets and the Implications on Systemic Risk*, Fordham Journal of Corporate and Financial Law, 22 (2), pp. 256–304, available at: <https://ir.lawnet.fordham.edu/jcfl/vol22/iss2/3>.
- Swan E. J., and Virgo J, 2019, *Market Abuse Regulation*, OUP Oxford.
- Szalay E., 2022, *EU should ban energy-intensive mode of crypto mining, regulator say*, Financial Times, available at: <https://www.ft.com/content/8a29b412-348d-4f73-8af4-1f38e69f28cf>.
- *Targeted Update on Implementation of Standards on VAs and VASPs*, 2022, Financial Action Task Force (FATF), available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>.
- *The Financial Stability Risks of Decentralized Finance*, 2023, Financial Stability Board (FSB), available at: <https://www.fsb.org/wp-content/uploads/P160223.pdf>.
- *Tokenization: Opening Illiquid Assets to Investors*, 2019, BNY Mellon, available at: <https://www.bnymellon.com/us/en/insights/all-insights/tokenization-opening-illiquid-assets-to-investors.html>.
- Valery, *Which are the Available Markets?*, Crypto.com, available at: <https://help.crypto.com/en/articles/1341655-which-are-the-available-markets>.
- Van der Linden T. and Shirazi T., 2023, *Markets in Crypto-assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-assets*, Financial Innovation, 9 (22), available at: <https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00432-8#citeas>.
- *Venus: The Money Market & Synthetic Stablecoin Protocol*, 2020, Venus, available at: <https://venus.io/Whitepaper.pdf>

- *Virtual Currencies, Key Definitions and Potentials AML/CFT Risks*, 2014, Financial Action Task Force (FATF) Report, available at: [Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf](#).
- Volcon I., 2023, *About YouHodler*, YouHolder, available at: <https://www.youhodler.com/company>.
- Wang W., 2021, *How ERC-3525 can improve position management in Uniswap V3*, Solv Protocol, available at: <https://medium.com/solv-blog/how-vnft-can-improve-position-management-in-uniswap-v3-221ab49a8cb2>.
- *Web3 and Blockchain*, 2023, Bain & Company, available at: <https://www.bain.com/insights/management-tools-web3-and-blockchain>.
- *What Are Liquidity Pool (LP) Tokens?*, 2022, Academy.Binance.com, available at: <https://academy.binance.com/en/articles/what-are-liquidity-pool-lp-tokens>.
- *What Is an NFT?*, 2020, Academy Binance, available at: <https://academy.binance.com/en/articles/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts>.
- *Why You Can't Trace Funds Through Services Using Blockchain Analysis (And Why You Don't Need to Anyway)*, 2020, Chainalysis, available at: <https://blog.chainalysis.com/reports/blockchain-analysis-trace-through-service-exchange/>.
- Wolff M., 2018, *Introducing Marble: A Smart Contract Bank*, Medium.com, available at: <https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890>.
- Wollinsky J., 2022, *How Hedge Fund Three Arrows Capital Was Crypto's Long-Term Capital Management*, Forbes, available at: <https://www.forbes.com/sites/jacobwolinsky/2022/08/24/how-hedge-fund-three-arrows-capital-was-cryptos-long-term-capital-management/?sh=25ccac2c633e>.
- Woxholt J., Zetsche D., Buckley, R. P., and Arner, D. W., *Competing Claims to Crypto-assets*, 2022, SSRN, available at: <https://ssrn.com/abstract=4394952>.
- Yaffe-Bellany D., Rashbaum W. K., and Goldstein M., 2022, *FTX's Sam Bankman-Fried Is Arrested in the Bahamas*, New York Times, available at: <https://www.nytimes.com/2022/12/12/business/ftx-sam-bankman-fried-bahamas.html?ref=upstrack.com>.
- Yaffe-Bellany D., Rashbaum W. K., and Goldstein M., 2022, *Sam-Bankman-Fried Pleads Not Guilty to Fraud and Other Charges*, New York Times, available at: <https://www.nytimes.com/2023/01/03/technology/sam-bankman-fried-pleads-not-guilty.html>.
- Yaffe-Bellany D., and Mac R., 2022, *U.S. crypto exchange Kraken settles with Treasury Department*, New York Times, available at: <https://www.nytimes.com/2022/11/28/technology/kraken-crypto-sanctions.html>.
- Zamani E., Ying He, and Phillips M., 2020, *On the Security Risks of the Blockchain*, Journal of Computer Information Systems, 60 (6), p. 495.
- Zetsche D. A., Buckley, R. P., and Arner, D. W., 2018, *The Distributed Liability of Distributed Ledgers: The Legal Risks of Blockchain*, University of Illinois Law Review, pp. 1361-1407.
- Zetsche D. A., Preiner C. D., 2020, *Scope of the AIFMD* in Zetsche D. A., *The Alternative Investment Fund Managers Directive*, 3rd ed., Ch. 2., Kluwer Law International.
- Zetsche D. A., and Woxholth J.P., 2022, *The DLT sandbox under the Pilot-Regulation*, Capital Markets law Journal, 17 (2), pp. 212-236, available at: <https://doi.org/10.1093/cmlj/kmac003>.

- Zetzsche, D.A., Anker-Sørensen L.C., Passador M. L., and Wehrli A., 2021, *DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective*, Law and Financial Markets Review, 15 (1-2), pp. 70-115, available at: <https://doi.org/10.1080/17521440.2022.2065809>.
- Zetzsche, D. A., Anker-Sørensen, L., 2022, *Regulating Sustainable Finance in the Dark*, European Business Organization Law Review, 23, pp. 47–85, available at: <https://doi.org/10.1007/s40804-021-00237-9>.
- Zetzsche, D. A., Bodellini M., and Consiglio R., 2022, *The EU Sustainable Finance Framework in Light of International Standards*, Journal of International Economic Law, 25 (4), pp. 659–679, available at: <https://doi.org/10.1093/jiel/jgac043>.
- Zetzsche, D. A., and Buckley R. P., Arner D. W., and Föhr, L., 2018, *The ICO Gold Rush: it is a Scam, it is a Bubble, it is a Super Challenge for Regulators*, Harvard International Law Journal, 63 (2), available at SSRN: <https://ssrn.com/abstract=3072298> or <http://dx.doi.org/10.2139/ssrn.3072298>.
- Zetzsche, D. A., Arner D. W., Buckley R. P., 2020, *Decentralized Finance*, Journal of Financial Regulation, 6 (2), pp. 172–203, available at: <https://ssrn.com/abstract=3539194> or <https://doi.org/10.1093/jfr/fjaa010>.
- *3rd Annual Global Crypto Hedge Fund Report 2021*, 2021, PricewaterhouseCoopers, available at: [https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto\\_hedge-fund-report-\(may-2021\).pdf](https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto_hedge-fund-report-(may-2021).pdf).

#### Regulatory releases and cases cited

- Commodity Futures Trading Commission (CFTC) v. Changpeng Zhao, Binance Holdings Limited, Binance Holdings (IE) Limited, Binance (Services) Holdings Limited, and Samuel Lim. *Case: 1:23-cv-01887*. Available at: <https://www.cftc.gov/media/8351/%20enfbinancecomplaint032723/download>
- European Commission 2018 ‘*Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions Action Plan: Financing Sustainable Growth*’ COM/2018/097 final available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0097>.
- European Commission 2021 ‘*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Strategy for Financing the Transition to a Sustainable Economy*’ COM/2021/390 final available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0390>.
- European Parliament and the Council 2019 ‘*Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)*’ available at: <https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf>.
- European Parliament and the Council 2021 ‘*Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast)*’ available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422>.
- International Organization of Securities Commissions, 2002 ‘*Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information*’ available at: <https://www.iosco.org/about/?subsection=mmou>.

- International Organization of Securities Commissions, 2020, *Global Stablecoin Initiatives: Public Report*, The Board of the International Organization of Securities Commissions (IOSCO), available at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>.
- Securities and Exchange Commission 2022 '*BlockFi Lending LLC, 3-20758*' available at: <https://www.sec.gov/litigation/admin/2022/33-11029.pdf>
- U.S. Bankruptcy Court for the Southern District of New York 2023 '*In re Celsius Network, LLC, et al. 22-10964*' available at: <https://www.iosco.org/about/?subsection=mmou>.
- U.S. District Court Northern District of California San Francisco Division 2023 '*SEC v Payward Ventures, Inc. and Payward Trading, Ltd. (Kraken) 23-cv-588*' available at: <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-25.pdf>.
- U.S. Supreme Court 1943 '*SEC v C.M. Joiner Leasing Corp. 320 U.S. 344*' available at: <https://supreme.justia.com/cases/federal/us/320/344/>.
- U.S. Supreme Court 1946 '*SEC v Howey Co. 328 U.S. 293, 301*' available at: <https://supreme.justia.com/cases/federal/us/328/293/>.
- U.S. Supreme Court 1967 '*Tcherepnin v Knight 389 U.S. 332*' available at: <https://supreme.justia.com/cases/federal/us/389/332/>.
- U.S. Supreme Court 1975 '*United Housing Foundation, Inc v Forman 421 U.S. 837*' available at: <https://supreme.justia.com/cases/federal/us/421/837/>.
- U.S. Supreme Court 2004 '*SEC v Edwards 540 U.S. 389*' available at: <https://supreme.justia.com/cases/federal/us/540/389/>.
- U.S. Bankruptcy Court NJ 2023 '*BlockFi Inc., 22-19361 (MBK)*' available at: <https://www.njb.uscourts.gov/BlockFi>.

---

This study analyses the need to adopt further EU financial regulation on decentralized finance after the implementation of the Markets in Crypto Asset Regulation and the revision of the Transfer of Funds Regulation, with a special view on crypto lending, crypto staking, crypto custody, the use of non-formal information, NFTs and sustainability.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the Committee on Economic and Monetary Affairs (ECON).

---

---

PE 740.083  
IP/A/ECON/2022-51

Print ISBN 978-92-848-0563-1 | doi:10.2861/3783 | QA-03-23-159-EN-C  
PDF ISBN 978-92-848-0564-8 | doi:10.2861/10909 | QA-03-23-159-EN-N